الاتحـــــــــــاد الدولـــــــــــي للاتصـــــــــــالات

ITU-T

قطاع تقييس الاتصالات
في الاتحاد الدولي للاتصالات

H.551

(2022/01)

السلسلة H: الأنظمة السمعية المرئية والأنظمة متعددة الوسائط

البوابات المحمولة على مركبات وأنظمة النقل الذكية (ITS) – معمارية البوابات المحمولة على مركبات

معمارية أنظمة الوسائط المتعددة في المركبات

التوصية ITU-T H.551

توصيات السلسلة H الصادرة عن قطاع تقييس الاتصالات

الأنظمة السمعية المرئية والأنظمة متعددة الوسائط

خصائص أنظمة الهاتف المرئي	H.199–H.100
البنية التحتية للخدمات السمعية المرئية	
اعتبارات عامة	H.219–H.200
تعدد الإرسال والتزامن في الإرسال	H.229–H.220
جوانب الأنظمة	H.239–H.230
إجراءات الاتصالات	H.259–H.240
تشفير الصور المتحركة الفيديوية	H.279–H.260
جوانب تتعلق بالأنظمة	H.299–H.280
الأنظمة والتجهيزات المطرافية للخدمات السمعية المرئية	H.349–H.300
معمارية خدمات الأدلة للخدمات السمعية المرئية والخدمات متعددة الوسائط	H.359–H.350
معمارية جودة الخدمات السمعية المرئية والخدمات متعددة الوسائط	H.369–H.360
الحضور عن بعد، البيئات الغامرة، والواقع الافتراضي والواقع الموسع	H.439–H.420
خدمات إضافية في تعدد الوسائط	H.499–H.450
إجراءات التنقلية والتعاون	
لمحة عامة عن التنقلية والتعاون، تعاريف وبروتوكولات وإجراءات	H.509–H.500
التنقلية لأغراض الأنظمة والخدمات متعددة الوسائط في السلسلة H	H.519–H.510
تطبيقات وخدمات التعاون للوسائط المتعددة المتنقلة	H.529–H.520
الأمن في الأنظمة والخدمات المتنقلة متعددة الوسائط	H.539–H.530
الأمن في تطبيقات وخدمات التعاون للوسائط المتعددة المتنقلة	H.549–H.540
البوابات المحمولة على مركبات وأنظمة النقل الذكية (ITS)	
معمارية البوابات المحمولة على مركبات	**H.559–H.550**
واجهات البوابات المحمولة على مركبات	H.569–H.560
خدمات النطاق العريض وتعدد الوسائط ثلاثي الخدمات	
خدمات متعددة الوسائط بالنطاق العريض على خط المشترك الرقمي فائق السرعة (VDSL)	H.619–H.610
تطبيقات وخدمات الوسائط المتعددة المتقدمة	H.629–H.620
تطبيقات إيصال المحتوى وشبكة الاستشعار الشمولية	H.649–H.640
خدمات وتطبيقات تلفزيون بروتوكول الإنترنت متعددة الوسائط من أجل تلفزيون بروتوكول الإنترنت	
جوانب عامة	H.719–H.700
تلفزيون بروتوكول الإنترنت – الأجهزة المطرافية	H.729–H.720
تلفزيون بروتوكول الإنترنت – البرمجيات الوسيطة	H.739–H.730
تلفزيون بروتوكول الإنترنت – مناولة أحداث تطبيقات	H.749–H.740
تلفزيون بروتوكول الإنترنت – البيانات الشرحية	H.759–H.750
تلفزيون بروتوكول الإنترنت – أطر التطبيقات متعددة الوسائط	H.769–H.760
تلفزيون بروتوكول الإنترنت – اكتشاف الخدمة حتى الاستهلاك	H.779–H.770
اللافتات الرقمية	H.789–H.780
أنظمة وخدمات وتطبيقات الصحة الإلكترونية متعددة الوسائط	
الأنظمة الصحية الشخصية	H.819–H.810
اختبار الامتثال لقابلية التشغيل البيني لأنظمة الصحة الشخصية (HRN وPAN وLAN وWAN)	H.859–H.820
خدمات تبادل البيانات المتعلقة بالصحة الإلكترونية باستخدام الوسائط المتعددة	H.869–H.860
الاستماع الآمن	H.879–H.870

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

التوصية ITU-T H.551

معمارية أنظمة الوسائط المتعددة في المركبات

ملخص

تعرف التوصية ITU-T H.551 تشكيلة أنظمة الوسائط المتعددة في المركبات (VMS)، والنموذج المرجعي لمعمارية أنظمة الوسائط المتعددة في المركبات، والحل المرجعي لتطبيقات الوسائط المتعددة لأنظمة الوسائط المتعددة في المركبات.

التسلسل التاريخي

الطبعة	التوصية	تاريخ الموافقة	لجنة الدراسات	معرف الهوية الفريد*
1.0	ITU-T H.551	2022-01-28	16	11.1002/1000/14811

مصطلحات أساسية

معمارية، أنظمة الوسائط المتعددة في المركبات.

* 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/حقوق تأليف ونشر البرمجيات 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 المناسبة لدى قطاع تقييس الاتصالات المتاحة من خلال الموقع الإلكتروني لقطاع تقييس الاتصالات عبر الرابط: http://www.itu.int/ITU-T/ipr/.

جدول المحتويات

الصفحة

الصفحة

معمارية أنظمة الوسائط المتعددة في المركبات

1 مجال التطبيق

تحدد هذه التوصية سمات وتشكيلات أنظمة الوسائط المتعددة في المركبات (VMS) والنموذج المرجعي لمعمارية أنظمة الوسائط المتعددة في المركبات. ويتم أيضاً تحديد النموذج المرجعي لمنصة خدمة الوسائط المتعددة في المركبات، وكدسة البروتوكولات المرجعية لتقارب الإرسال، ونموذج المستقبل المرجعي للأجهزة داخل السيارة لتطبيقات الوسائط المتعددة لأنظمة الوسائط المتعددة في المركبات. كما يرد شرح لقضايا أمن أنظمة الوسائط المتعددة في المركبات وحماية المعلومات المحددة لهوية الأشخاص ومسائل الخصوصية.

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 للمراجَعة، يُشجع جميع مستعملي هذه التوصية على بحث إمكانية 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 F.749.3] التوصية ITU-T F.749.3 (2020)، *حالات استعمال ومتطلبات من أجل شبكات الوسائط المتعددة في المركبات*.

3 التعاريف

1.3 المصطلحات المعرَّفة في وثائق أخرى

تستخدم هذه التوصية المصطلحات التالية المعرَّفة في وثائق أخرى:

1.1.3 شبكات الوسائط المتعددة في المركبات (VMN) (vehicular multimedia networks) [ITU-T F.749.3]: تتألف شبكات الوسائط المتعددة في المركبات من منصة خدمات الوسائط المتعددة في المركبات (VMSP)، وشبكات الإذاعة والاتصالات، ونظام الوسائط المتعددة في المركبات (VMS) داخل المركبة.

2.1.3 منصة خدمات الوسائط المتعددة في المركبات (VMSP) (vehicular multimedia service platform) [ITU-T F.749.3]: منصة في السحابة تمكن خدمات الوسائط المتعددة للمستعملين النهائيين في المركبة.

3.1.3 نظام الوسائط المتعددة في المركبات (VMS) (vehicle multimedia system) [ITU-T F.749.3]: يشمل مدخلات نظام الوسائط المتعددة في المركبات (VM I/P)، ووحدة الوسائط المتعددة في المركبة (VMU) ومخرجات نظام الوسائط المتعددة في المركبات (VM O/P).

2.3 المصطلحات المعرَّفة في هذه التوصية

تعرِّف هذه التوصية المصطلح التالي:

1.2.3 الوظيفة الأساسية لنظام الوسائط المتعددة في المركبات (VMS core function): هي وظيفة تتعامل مع البيانات المادية والوظيفية والمنطقية للنظام VMS.

2.2.3 الوظيفة المرتبطة لنظام الوسائط المتعددة في المركبات (VMS associated function): هي وظيفة تستقبل وتعرض فقط البيانات الوظيفية والمنطقية من الأنظمة أو الأنظمة الفرعية الأخرى.

3.2.3 الوظيفة المشتركة لنظام الوسائط المتعددة في المركبات (VMS shared function): هي وظيفة تستخدمها الأنظمة أو الأنظمة الفرعية الأخرى لتبادل البيانات المادية والوظيفية والمنطقية ومعلومات التحكم.

4 المختصرات والأسماء المختصرة

تستعمل هذه التوصية الاختصارات والأسماء المختصرة التالية:

ADAS نظام متقدم لمساعدة السائق *(Advanced Driver Assistance System)*

AM التشكيل بالاتساع *(Amplitude modulation)*

ANC الإزالة النشطة للضوضاء *(Active noise cancellation)*

APP تطبيق *(Application)*

AR الواقع المزيد *(Augmented reality)*

AVM مراقبة الرؤية المحيطة *(Around view monitoring)*

bCall نداء في حالة حدوث عطل *(Breakdown call)*

BGS مسح الخلفية *(Background scan)*

CA النفاذ المشروط *(Conditional access)*

CDN شبكات توزيع المحتوى (*Content Distribution Network*)

CDR النظام الراديوي الرقمي المتقارب *(Convergent digital radio)*

DAB إذاعة صوتية رقمية *(Digital audio broadcasting)*

DASH البث الدينامي التكيفي عبر البروتوكول HTTP *(Dynamic Adaptive Streaming over HTTP)*

DMS نظام مراقبة السائق *(Driver monitoring system)*

DNT عدم التتبع *(Do not track)*

DRM إدارة الحقوق الرقمية *(Digital rights management)*

DTTB الإذاعة التلفزيونية الرقمية للأرض *(Digital Terrestrial Television Broadcasting)*

eCall نداء طوارئ *(Emergency call)*

ECM رسالة التحكم في الاستحقاق *(Entitlement control message)*

ECU وحدة التحكم الإلكتروني *(Electronic control unit)*

EMM رسالة إدارة الاستحقاق *(Entitlement management message)*

FM التشكيل بالتردد *(Frequency modulation)*

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

HEO مدار أرضي مرتفع *(High earth orbit)*

HLS بث حي بالبروتوكول HTTP *(HTTP live streaming)*

HMI السطح البيني بين الإنسان والآلة *(Human machine interface)*

HTTP بروتوكول نقل النصوص الترابطية *(Hypertext Transfer Protocol)*

HVAC التدفئة والتهوية وتكييف الهواء *(Heating, ventilation and air conditioning)*

IAM إدارة الهوية والنفاذ *(Identity and Access Management)*

IBOC في نفس النطاق ونفس القناة *(In-band on-channel)*

iCall نداء معلومات *(Information call)*

IP بروتوكول الإنترنت *(Internet Protocol)*

LCD شاشة عرض بالبلورات السائلة *(Liquid crystal display)*

LED ثنائي المساري بانبعاث ضوئي *(Light emitting diode)*

LEO مدار أرضي منخفض *(Low earth orbit)*

MR الواقع المختلط *(Mixed reality)*

NAT ترجمة عنوان الشبكة *(Network Address Translation)*

OBD التشخيص على متن المركبة *(On-board diagnostics)*

OEM المصنّع الأصلي للمعدات *(Original equipment manufacturer)*

OLED ثنائي المساري العضوي بانبعاث ضوئي *(Organic light emitting diode)*

OS نظام التشغيل *(Operating system)*

OTA عبر الأثير *(Over the air)*

PD تنوع الطور *(Phase diversity)*

PII المعلومات المحدِّدة لهوية الأشخاص *(Personally identifiable information)*

PUF وظيفة فيزيائية غير قابلة للنسخ *(Physical unclonable function)*

RDS نظام بيانات راديوي *(Radio data system)*

RF التردد الراديوي *(Radio frequency)*

RVC كاميرا الرؤية الخلفية *(Rear view camera)*

TCP بروتوكول التحكم في النقل *(Transfer Control Protocol)*

TMC قناة رسائل حركة المرور *(Traffic message channel)*

UDP بروتوكول وحدة بيانات المستعمل *(User Datagram Protocol)*

V2I التوصيل من المركبة إلى البنية التحتية *(Vehicle-to-infrastructure)*

V2P التوصيل من المركبة إلى الأشخاص *(Vehicle-to-person)*

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

V2X التوصيل من المركبة إلى كل شيء *(Vehicle-to-everything)*

VM الوسائط المتعددة للمركبات *(Vehicular Multimedia)*

VM I/P مدخلات نظام الوسائط المتعددة في المركبات *(Vehicle multimedia system inputs)*

VM O/P مخرجات نظام الوسائط المتعددة في المركبات *(Vehicle multimedia system outputs)*

VMN شبكة الوسائط المتعددة للمركبات *(Vehicular multimedia network)*

VMSP منصة خدمات الوسائط المتعددة في المركبات *(Vehicular multimedia service platform)*

VMS نظام الوسائط المتعددة في المركبات *(Vehicle multimedia system)*

VMU وحدة الوسائط المتعددة للمركبة *(Vehicle multimedia unit)*

VR الواقع الافتراضي *(Virtual reality)*

5 الاصطلاحات

فيما يلي الكلمات الأساسية الواردة في هذه التوصية:

- كلمة "يُشترط" تعني متطلباً يجب التقيد به تماماً ولا يسمح بأي انحراف عنه في حال ادعاء المطابقة مع هذه التوصية.
- كلمة "يحظر" تعني متطلباً يجب التقيد به تماماً ولا يسمح بأي انحراف عنه في حال ادعاء المطابقة مع هذه التوصية.
- كلمة "يوصى" تعني متطلباً يوصى به دون أن يكون شرطاً ملزماً. ولذلك لا يتعين وجود هذا المتطلب في ادعاء المطابقة.
- العبارة "لا يُوصى" تعني متطلباً لا يوصى به لكن ليس ممنوعاً قطعاً. لذا يمكن ادعاء المطابقة مع هذه المواصفات حتى بوجود هذا المتطلب.

6 خلفية

تُعرف في هذه التوصية سمات وتشكيلات أنظمة الوسائط المتعددة في المركبات (VMS) والنموذج المرجعي لمعمارية النظام VMS طبقاً للمتطلبات الواردة في [ITU-T F.749.3]. ويتم أيضاً تحديد النموذج المرجعي لمنصة خدمة الوسائط المتعددة في المركبات (VMSP)، وكدسة البروتوكولات المرجعية لتقارب الإرسال، ونموذج المستقبل المرجعي للأجهزة الموجودة داخل المركبة لتطبيقات الوسائط المتعددة لأنظمة الوسائط المتعددة في المركبات. كما يرد شرح لقضايا أمن أنظمة الوسائط المتعددة في المركبات وحماية المعلومات المحددة لهوية الأشخاص (PII) ومسائل الخصوصية.

والتوصية منظمة على النحو التالي:

تعرف الفقرة 7 سمات وتشكيلات أنظمة الوسائط المتعددة في المركبات. وتعرف الفقرة 8 النموذج المرجعي لمعمارية النظام VMS. وتعرف الفقرة 9 النموذج المرجعي لمنصة خدمة الوسائط المتعددة في المركبات، وكدسة البروتوكولات المرجعية لتقارب الإرسال لمحتويات الوسائط المتعددة عبر شبكات غير متجانسة، ونموذج المستقبل المرجعي للأجهزة الموجودة داخل المركبة. وتتناول الفقرة 10 قضايا أمن أنظمة الوسائط المتعددة في المركبات. وتتناول الفقرة 11 حماية المعلومات المحددة لهوية الأشخاص ومسائل الخصوصية.

7 سمات وتشكيلات أنظمة الوسائط المتعددة في المركبات

1.7 سمات أنظمة الوسائط المتعددة في المركبات

تُحدد سمات أنظمة الوسائط المتعددة في المركبات طبقاً للمبادئ التالية:

- تجربة المستعمل وسمات الترفيه والمعلومات والتطبيقات الخاصة بالسائق والركاب.
- متطلبات السوق، والمتطلبات الإقليمية والقطرية.
- المتطلبات القانونية والإلزامية.

بيد أن سمات أنظمة الوسائط المتعددة في المركبات لا تصف المعمارية العامة للشبكة في المركبات أو دمج ميادين متعددة في المركبات.

2.7 تشكيلات أنظمة الوسائط المتعددة في المركبات

تستند تشكيلات أنظمة الوسائط المتعددة في المركبات إلى المبادئ التالية:

- تعرف تشكيلات أنظمة الوسائط المتعددة في المركبات المتطلبات المستقلة للترفيه وعرض المعلومات للسائق والركاب.
- يوصى بتعريف تشكيلات أنظمة الوسائط المتعددة في المركبات على مستوى السمات والوظائف.
- يوصى بأن تتضمن تشكيلات أنظمة الوسائط المتعددة في المركبات مكونات الأجهزة داخل النظام VMS.
- إمكانية وجود تشكيلات متعددة لأنظمة الوسائط المتعددة في المركبات.
- يوصى بأن تكون تشكيلات أنظمة الوسائط المتعددة في المركبات شديدة التغير. يوصى بمراعاة كل من منتجات الأنظمة VMS الخاصة بالمصنّع الأصلي للمعدات أو المنتجات التي تُثبت بعد الطرح في الأسواق.

بيد أن تشكيلات أنظمة الوسائط المتعددة في المركبات لا تصف المعمارية العامة للشبكة في المركبات أو دمج ميادين متعددة في المركبات.

1.2.7 عوامل اتخاذ القرار

تُحدد تشكيلات أنظمة الوسائط المتعددة في المركبات استناداً إلى عوامل اتخاذ القرار التالية:

- متطلبات الاستعمال.
- المتطلبات المتعلقة بالسمات والمتطلبات الوظيفية.
- المتطلبات المتعلقة بالسطوح البينية.
- المتطلبات المتعلقة بالتكلفة.
- المتطلبات المتعلقة بالمقارنة المرجعية.

3.7 قائمة بسمات أنظمة الوسائط المتعددة في المركبات

تُلخص في الجدول 1 السمات المرجعية لأنظمة الوسائط المتعددة في المركبات.

الجدول 1 – السمات المرجعية لأنظمة الوسائط المتعددة في المركبات

السمات	السمات الفرعية	قابلة للتشكيل
السطح البيني بين الإنسان والآلة (HMI)	تكنولوجيا شاشة العرض	ثنائي المساري بانبعاث ضوئي (LED)/شاشة عرض بالبلورات السائلة (LCD)/ثنائي المساري العضوي بانبعاث ضوئي (OLED) وما إلى ذلك
	عدد شاشات العرض	متعددة (أمامية، في الوسط، في الخلف، وما إلى ذلك).
	التحكم	وسائل تحكم تقليدية: أزرار/مقابض/أدوات تحكم باللمس، وما إلى ذلك.
		وسائل تحكم ذكية: تحكم صوتي، تمييز الوجه، بيومترات صوتية، الإيماءات، التحكم بالسمات الشخصية، التحكم بحركة العين، اللمس المرن للتغذية الراجعة، وما إلى ذلك.
	التفاعل بين الشاشات المتعددة	بث المعلومات لشاشات مختلفة
		عرض ملفات الفيديو بشكل متزامن أو غير متزامن
		شاشة تصفح مزدوجة
		مطابقة حرة للسطح البيني لشاشة العرض
	لغة النظام	السطح البيني للمستعمل: متطلبات لغات مختلفة كما هو منصوص عليه في اللوائح
	شاشة عرض للكاميرا	كاميرا الرؤية الخلفية (RVC)/ مراقبة الرؤية المحيطة (AVM)
	التحكم وشاشة العرض	شاشة العرض الخاصة بالتدفئة والتهوية وتكييف الهواء (HVAC) ووسائل التحكم فيها
		التحكم في مساعدات السائق وشاشات العرض الخاصة بها

الجدول 1 – السمات المرجعية لأنظمة الوسائط المتعددة في المركبات

السمات	السمات الفرعية	قابلة للتشكيل
الإذاعة	للأرض	التماثلية: إذاعة بتشكيل الاتساع (AM)، إذاعة بتشكيل التردد (FM)، إذاعة بتشكيل التردد (FM) مع مولف مزدوج وتنوع الطور (PD)، إذاعة FM مع مسح الخلفية (BGS)، نظام بيانات راديوي (RDS)، إلخ.
		الرقمية: الإذاعة الصوتية الرقمية (DAB)، الإذاعة التلفزيونية الرقمية للأرض (DTTB)، تكنولوجيات البث في نفس النطاق ونفس القناة (IBOC)، النظام الراديوي الرقمي المتقارب (CDR)، إلخ.
	الساتلية	الخدمات الصوتية/الفيديوية الساتلية (مثل خدمات البث الصوتي/الفيديوي الساتلية)
توصيلية الشبكة الخارجية	الشبكات الخلوية	5G/4G/3G
	السواتل ثنائية الاتجاه	شبكات الاتصالات الساتلية ثنائية الاتجاه ذات المدار الأرضي المنخفض (LEO)
		شبكات الاتصالات الساتلية ثنائية الاتجاه ذات المدار الأرضي المرتفع (HEO)
	التوصيل من المركبة إلى كل شيء (V2X)	التوصيل من مركبة إلى مركبة (V2V)، التوصيل من المركبة إلى البنية التحتية (V2I)، التوصيل من المركبة إلى الأشخاص (V2P)
	الشبكات المحلية اللاسلكية	بؤر توصيل المعيار IEEE 802.11
التوصيلية المتنقلة داخل المركبة		مكالمات بدون استخدام اليدين وتشغيل الموسيقى باستخدام الشبكات الشخصية
		تصفح الويب باستخدام الشبكات المحلية IEEE 802.11
		مشاركة الشاشة باستخدام شبكات الاتصالات قصيرة المسافة
		تطبيقات السطوح البينية للمركبات لأطراف ثالثة
التشكيلات التليماتية	عن بعد	المراقبة والتحكم ونقل بيانات المركبة عن بعد
	النداءات	نداء الطوارئ (eCall)، النداء في حالة حدوث عطل (bCall)، نداء المعلومات (iCall)
مستودعات/مجموعات التطبيقات على الإنترنت	مستودعات التطبيقات	تنزيل سمات جديدة
	سوق الأشياء المظهرية والوظائف الحاسوبية للتطبيقات	استبدال المظهر الحاسوبي للأشياء والوظائف الحاسوبية
التحديث عبر الأثير (OTA)		برمجيات عبر الأثير
الوسائط	صوت	دقة عادية وعالية
	صورة	بأنساق مختلفة
	فيديو	فيديو عادي باستبانات مختلفة، الواقع المزيد (AR)، الواقع الافتراضي (VR)، الواقع المختلط (MR)
التصفح	التصفح المحلي	
	التصفح السحابي	البيانات من مودم صندوق البيانات التليماتية (5G/4G/3G)/بيانات المستعمل المتنقلة
	حركة المرور في الوقت الفعلي	قناة رسائل حركة المرور (TMC)، فريق خبراء بروتوكول النقل (TPEG)، مركز حركة المرور في الوقت الفعلي، إلخ.
	خدمات	خدمات الملاحة، خدمات التنبؤ بالطقس في الوقت الفعلي، إلخ.
	السمات المتقدمة	تطبيقات السفر الذكية مثل الرزنامة وأدوات التخطيط وما إلى ذلك.
التعرف على الصوت (VR) وتركيبه	التعرف على الصوت محلياً، والتعرف على الصوت وتركيبه سحابياً	فهم اللغة الطبيعية
		التعرف التلقائي على الكلام
		تحويل النص إلى كلام
الصوت	جودة الصوت	وظيفة ضبط الصوت حسب السرعة
		خوارزميات الصوت

الجدول 1 – السمات المرجعية لأنظمة الوسائط المتعددة في المركبات

السمات	السمات الفرعية	قابلة للتشكيل
		الإزالة النشطة للضوضاء (ANC)
		إعدادات الشخصنة (أنماط الصوت والتعرف على الوجه)
		ضبط أفضل وضع للاستماع
		تكنولوجيا تقليل جودة الصوت
	تشكيلات المكبرات	مكبرات مدمجة متعددة القنوات
		مضخمات مع مكبرات الصوت
	تشكيل الصوت	تشكيلات متعددة لمكبرات الصوت مكبر الصوت tweeter (مكبر الصوت عالي الطبقة)/مكبر الصوت woofer (مكبر الصوت منخفض الطبقة)/مكبرات الصوت ذات النطاق الكامل
الأمن		إدارة الهوية والنفاذ (IAM)، والاستيقان والتخويل ومراجعة العمليات
		أمن الشبكة
		الأمن التشغيلي
		أمن التطبيقات
		أمن البرمجيات عبر الأثير
		أمن العتاد
		أمن التجفير
الخصوصية		اعتبارات حماية البيانات العامة
		حماية المعلومات الشخصية
		حماية رؤية البيانات
		السرية والسلامة والتيسر
السمات الذكية	نظام مراقبة السائق (DMS)	التعب والتعبير والتعرف على المشاعر
	الصحة	جهاز مراقبة ضربات القلب، جهاز مراقبة ضغط الدم
	البيئة المكتبية	البريد الإلكتروني، مكالمات المؤتمرات الفيديوية، العرض المجسم، التعرف على الإيماءات، التحكم بحركة العين، المذكرة المكتوبة بخط اليد
	الألعاب	ألعاب مسابقات تفاعلية قائمة على الصوت، ألعاب تفاعلية مجسمة، ألعاب مغامرات
	التواصل الاجتماعي	تطبيقات التواصل الاجتماعي في المركبة

ملاحظة – تُعتبر سمات الأمن والخصوصيات أساسية لأنظمة الوسائط المتعددة في المركبات ذات التشكيلات من M1 إلى M5، ولكنها قابلة للتشكيل لأنظمة الوسائط المتعددة في المركبات ذات التشكيل M0. وترد في التذييل الأول للتوصية [ITU-T F.749.3] أمثلة على أنظمة الوسائط المتعددة في المركبات ذات التشكيلات من M0 إلى M5.

8 معمارية نظام الوسائط المتعددة في المركبات

تعرف هذه الفقرة تصنيف وظائف النظام VMS وعوامل اتخاذ القرار والنموذج المرجعي لمعمارية النظام VMS.

1.8 وظائف نظام الوسائط المتعددة في المركبات

بشكل عام، يمكن تصنيف وظائف النظام VMS إلى ثلاث فئات، وهي الوظائف الأساسية للنظام VMS والوظائف المرتبطة للنظام VMS والوظائف المشتركة للنظام VMS.

والوظائف الأساسية للنظام VMS هي وظائف النظام VMS التي تتعامل مع البيانات المادية والوظيفية والمنطقية للنظام VMS. وتتضمن أمثلة الوظائف الأساسية للنظام VMS وظائف المؤلف ومعالجة الوسائط وشاشة العرض وما إلى ذلك.

والوظائف المرتبطة للنظام VMS هي وظائف النظام VMS التي تستقبل فقط وتعرض البيانات الوظيفية والمنطقية من أنظمة أو أنظمة فرعية أخرى. وتتضمن أمثلة الوظائف المرتبطة للنظام VMS تغذية الكاميرا من الكاميرا الخلفية للمركبة، وشاشة معلومات النداء eCall الذي ينطلق بسبب حادث، وما إلى ذلك.

والوظائف المشتركة للنظام VMS هي وظائف النظام VMS التي تستخدمها أنظمة أو أنظمة فرعية أخرى لتبادل البيانات المادية والوظيفية والمنطقية ومعلومات التحكم. وتتضمن أمثلة الوظائف المشتركة للنظام VMS أدوات التحكم في التدفئة والتهوية وتكييف الهواء من خلال وحدة الوسائط المتعددة في المركبة (VMU)، إلخ.

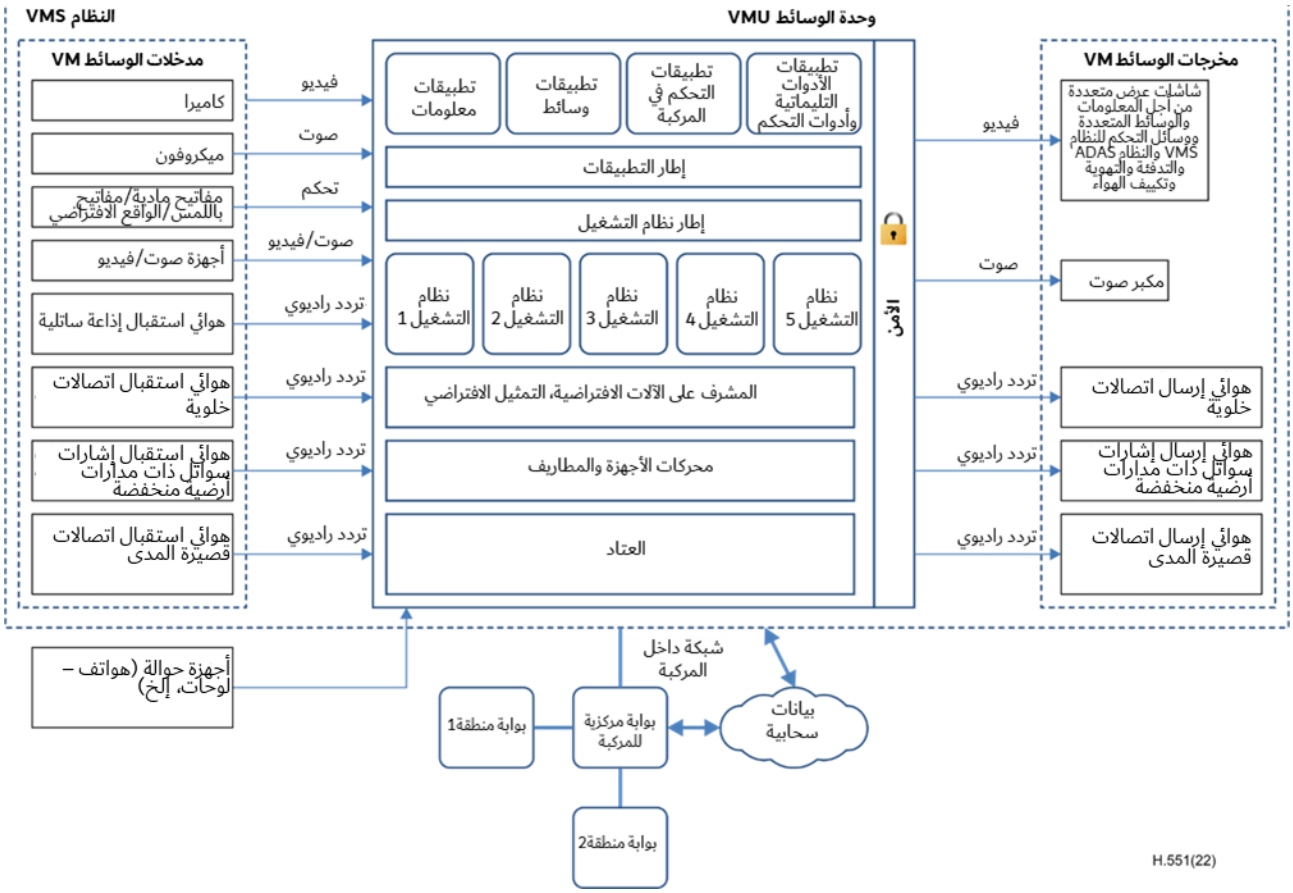
2.8 عوامل اتخاذ القرار في معمارية نظام الوسائط المتعددة في المركبات

العوامل التالية هي عوامل اتخاذ القرار في معمارية نظام الوسائط المتعددة في المركبات:

- المتطلبات التقنية
- متطلبات نظام التشغيل والذاكرة والعتاد
- السمات والأنظمة الوظيفية والفرعية والمتطلبات المنطقية والفيزيائية
- متطلبات السطوح البينية
- المتطلبات المتعلقة بالتكلفة
- متطلبات الاستعمال
- المتطلبات المتعلقة بالمقارنة المرجعية
- متطلبات الامتثال للمعايير

3.8 النموذج المرجعي لمعمارية نظام الوسائط المتعددة في المركبات

تُعرف معمارية نظام الوسائط المتعددة في المركبات على مستوى السطوح البينية والأنظمة الفرعية والأنظمة. ويرد في الشكل 1 نموذج مرجعي لمعمارية نظام الوسائط المتعددة في المركبات.



الشكل 1 – النموذج المرجعي لمعمارية نظام الوسائط المتعددة في المركبات

1.3.8 التطبيقات

تشمل تطبيقات النظام VMS:

- تطبيقات المعلومات، على سبيل المثال، مجموعة الأدوات، وشاشات العرض الأمامية، والملاحة والطقس.
- تطبيقات الوسائط المتعددة، مثل وسائل الإعلام والملاحة والواقع الافتراضي والسطح البيني بين الإنسان والآلة.
- تطبيقات التحكم في السيارة، مثل التدفئة والتهوية وتكييف الهواء والسيارات الموصولة.
- التطبيقات التليماتية، مثل جهاز التحكم والتشخيص والنفاذ إلى البيانات عن بعد.
- تطبيقات شاشات العرض، على سبيل المثال، تطبيقات شاشات العرض الأمامية والخلفية.

2.3.8 إطار التطبيقات

يتم النفاذ إلى سمات ووظائف النظام VMS عبر أدوات السطوح البينية للمستعمل المصممة طبقاً لإطار تطبيق ما.

3.3.8 إطار نظام التشغيل (OS)

يتعامل إطار نظام التشغيل مع خدمات النظام. وقد يكون إطار قائم على الملكية للمصنِّعين الأصلين للمعدات ومطوري الأنظمة VMS.

4.3.8 نظام التشغيل

يتم استخدام العديد من أنظمة التشغيل (OS) وبرامج التشغيل اعتمادًا على متطلبات حمل المعالجة والسرعة والدقة.

5.3.8 المشرف على الآلات الافتراضية والتمثيل الافتراضي

تُستخدم تقنيات المشرف على الآلات الافتراضية والتمثيل الافتراضي لدعم أنظمة تشغيل متعددة ومهام المعالجة بواسطة معالج واحد عالي الطاقة من خلال التشارك في الموارد الحاسوبية.

6.3.8 محركات الأجهزة والمطاريف

تشمل محركات الأجهزة محرك السطح البيني لشبكة المركبة ومحركات الصوت والفيديو ومحركات شاشات العرض ومحركات بروتوكول المعالجات البينية ومحركات بروتوكول المعالجة الداخلية.

7.3.8 العتاد

يشمل العتاد المعالجات والذاكرة والمكونات الأخرى.

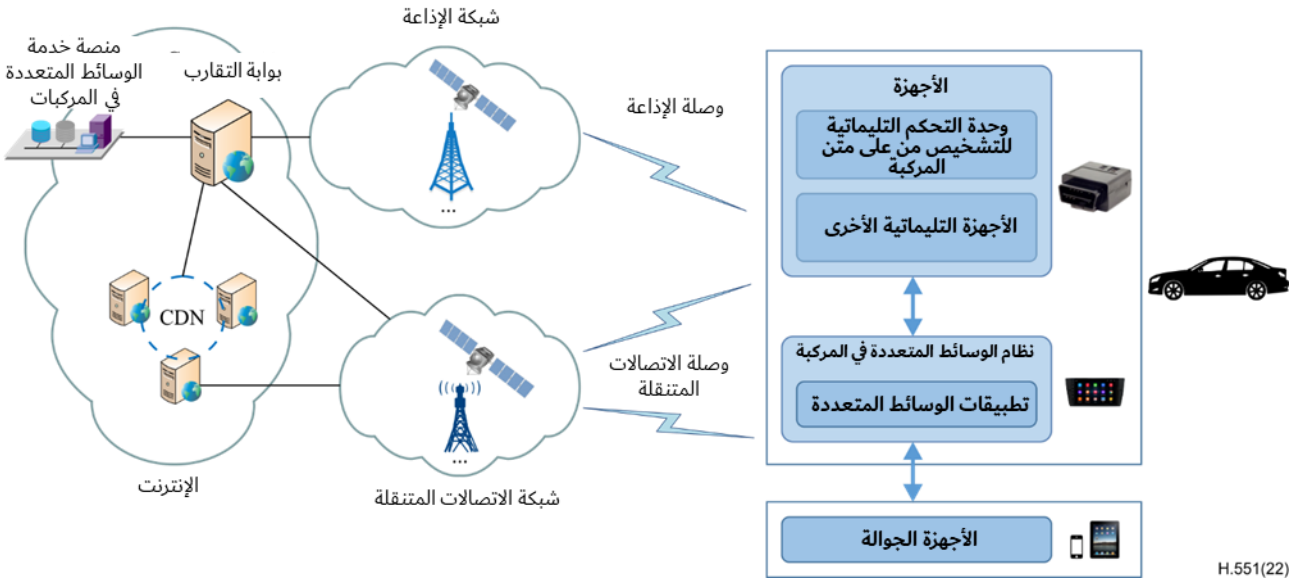
8.3.8 البيانات السحابية

تشمل البيانات السحابية:

- بيانات من أجل خدمات الوسائط المتعددة
- بيانات من أجل الخدمات التليماتية، أي خدمات التشخيص عن بعد، خدمات تحديث البرمجيات عبر الأثير، وخدمات النداءات iCall/bCall وخدمات الملاحة.

9 تطبيقات الوسائط المتعددة للنظام VMS

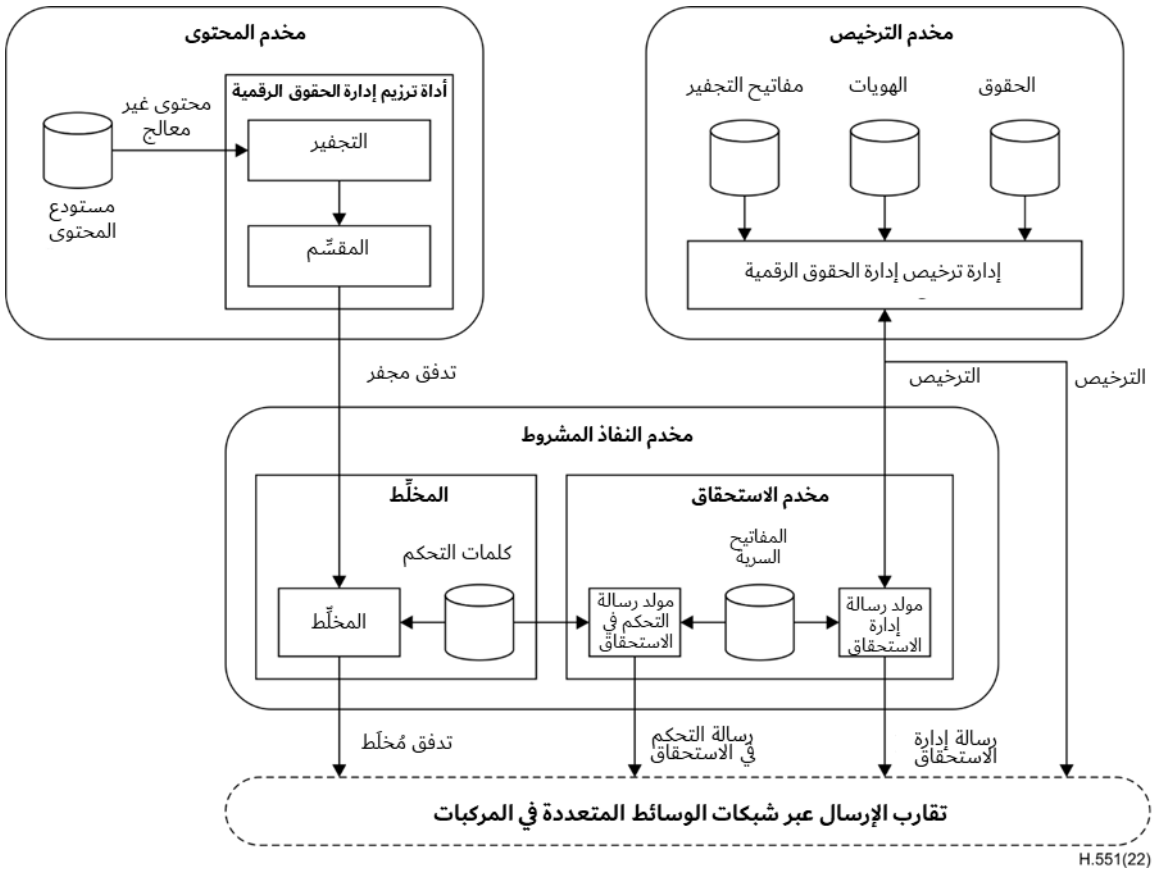
يصور الشكل 2 نظاماً لتطبيقات الوسائط المتعددة للنظام VMS، والذي يتكون من منصة خدمة الوسائط المتعددة في المركبات (VMSP) في السحابة والشبكات غير المتجانسة والأجهزة داخل المركبة. ويستخدم مخطط تقارب الإرسال لتحسين كفاءة إرسال محتويات الوسائط المتعددة عبر الشبكات غير المتجانسة، أي شبكات الإذاعة الساتلية وشبكات الاتصالات المتنقلة. وتصف هذه الفقرة النموذج المرجعي للمنصة VMSP (الفقرة الفرعية 1.9)، وكدسة البروتوكول المرجعي لتقارب إرسال محتويات الوسائط المتعددة عبر الشبكات غير المتجانسة (الفقرة الفرعية 2.9)، ونموذج المستقبل المرجعي للأجهزة داخل المركبة (الفقرة الفرعية 3.9).



الشكل 2 – مخطط نظام لتطبيقات الوسائط المتعددة لنظام الوسائط المتعددة في المركبات

1.9 النموذج المرجعي لمنصة خدمة الوسائط المتعددة في المركبات

تتكون منصة خدمة الوسائط المتعددة في المركبات من مخدم المحتوى ومخدم الترخيص (اختياري) ومخدم النفاذ المشروط (CA) (اختياري). ويُوضح نموذجها المرجعي في الشكل 3.



الشكل 3 – النموذج المرجعي لمنصة خدمة الوسائط المتعددة في المركبات

يتكون مخدم المحتوى من مستودع المحتوى وأداة ترزيم إدارة الحقوق الرقمية (DRM). ويُستخدم مستودع المحتوى لتخزين المحتويات غير المعالجة التي يريد مورد المحتوى (CP) توزيعها. ويُلاحظ أن مستودع المحتوى غالباً ما يتم تضمينه في حل إدارة الحقوق الرقمية أو يتم دمجه أحياناً في نظام إدارة المحتوى الذي يُوصل بينياً بمخدم إدارة الحقوق الرقمية. وتقوم أداة ترزيم إدارة الحقوق الرقمية بتجفير وتغليف محتويات الوسائط المتعددة لبثها عبر الشبكات VMN. ويُستخدم مخدم الترخيص لإدارة إصدار وتعديل وإلغاء تراخيص إدارة الحقوق الرقمية. ويحتوي الترخيص DRM على الهويات ومواصفات الحقوق ومفاتيح التجفير. يمكن عادة لعملاء DRM الحصول على تراخيص DRM الخاصة بهم من مخدم الترخيص باستخدام توصيلات شبكة الاتصالات المتنقلة. وتتضمن مخططات التغليف المرشحة للبث في الشبكات VMN المعيارين MPEG-DASH [b-ISO/IEC 23009-1] وHLS [b-IETF RFC 8216].

يتكون مخدم النفاذ المشروط (CA) من المخلِّط ومخدم الاستحقاق. ويُستخدم المخلِّط لتخليط التدفقات الواردة باستخدام كلمات التحكم. ويُستخدم مخدم الاستحقاق لتوليد رسالة التحكم في الاستحقاق (ECM) ورسالة إدارة الاستحقاق (EMM). عادةً، يتم توصيل التدفقات الصادرة المخلَطة ورسائل التحكم في الاستحقاق ورسائل إدارة الاستحقاق عبر شبكات الإذاعة الساتلية. ومع ذلك، هناك الاستثناءان التاليان:

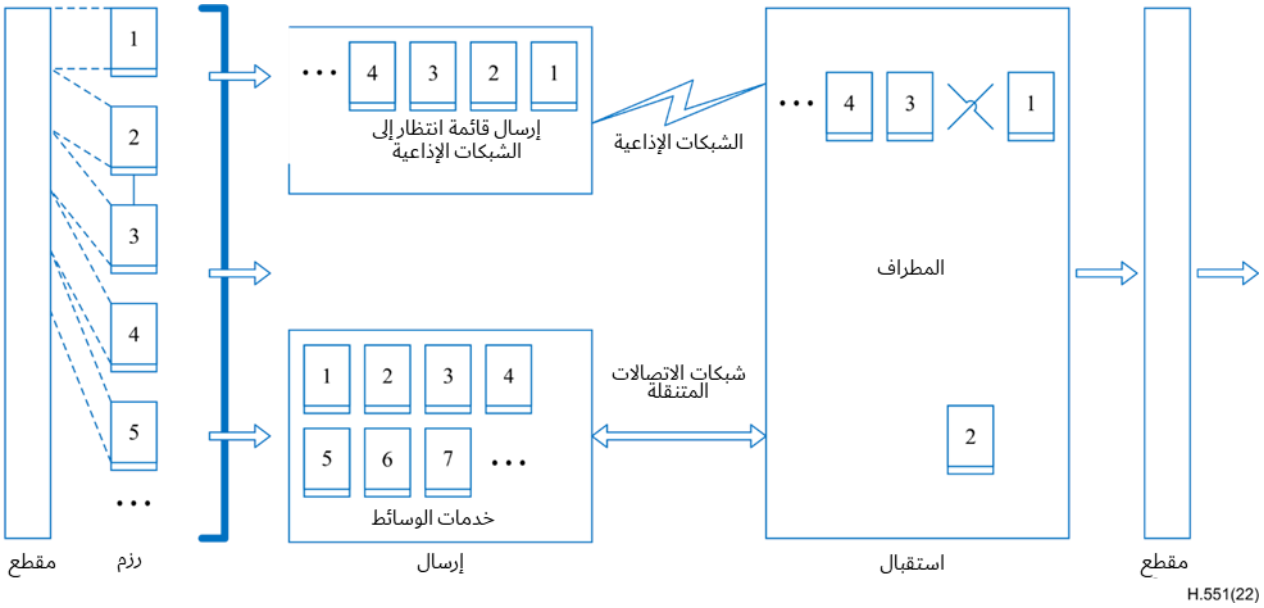
1) عندما يقود المستعمل إلى مكان لا توجد به تغطية للهاتف الخلوي، لا يمكن الحصول على تراخيص DRM من خلال أي شبكة اتصالات متنقلة. وفي هذه الحالة، يمكن دمج تراخيص DRM في الرسائل EMM وتوصيلها إلى المستعمل عبر الشبكات الساتلية. وبالتالي، يمكن تحقيق استمرارية الخدمة.

2) عندما يبدأ مشغل الخدمة عمله، قد يحاول الآلاف من العملاء الجدد تفعيل أجهزتهم في فترة زمنية قصيرة. ومع ذلك، قد لا يتوفر عرض النطاق المطلوب لتوصيل الرسائل EMM لهذه الأجهزة في شبكات الإذاعة الساتلية. وفي هذه الحالة، يمكن إلغاء تحميل الرسائل EMM مؤقتاً من شبكات الإذاعة الساتلية إلى شبكات الاتصالات المتنقلة. وبالتالي، يمكن ضمان إطلاق ناجح للأعمال.

2.9 كدسة البروتوكول المرجعي لتقارب الإرسال

تُعتبر الإذاعة بشكل عام الطريقة الأكثر فعالية من حيث التكلفة لتوصيل البرامج الخطية لعدد كبير من السكان في مناطق جغرافية شاسعة. وعلى الرغم من نجاح الإذاعة التلفزيونية الرقمية في النطاقين Ka وKu في جميع أنحاء العالم، فقد تبين أن توفير الخدمة عبر الإذاعة للمركبات يمثل تحدياً. فعلى سبيل المثال، في بيئة حضرية، تعتبر موثوقية الاتصالات الإذاعية مشكلة إلى حد ما بسبب أجهزة الاستقبال المتحركة والحجب المتكرر للإشارات بواسطة المباني العالية. وعلى الرغم من أنه يمكن معالجة قضية التغطية الحضرية للإذاعة من خلال شبكا ت المكررات الأرضية التي تملأ فجوات الانقطاع، إلا أن إنشاء البنية التحتية لملء الفجوات يعد مكلفاً ويستغرق وقتاً طويلاً. وهناك قيد آخر بالنسبة للاتصالات الإذاعية يتمثل في أنها يمكنها توفير خدمات أحادية الاتجاه فقط، وبالتالي لا تستطيع استيعاب الخدمات الشخصية أو دعم تفاعلات المستعملين.

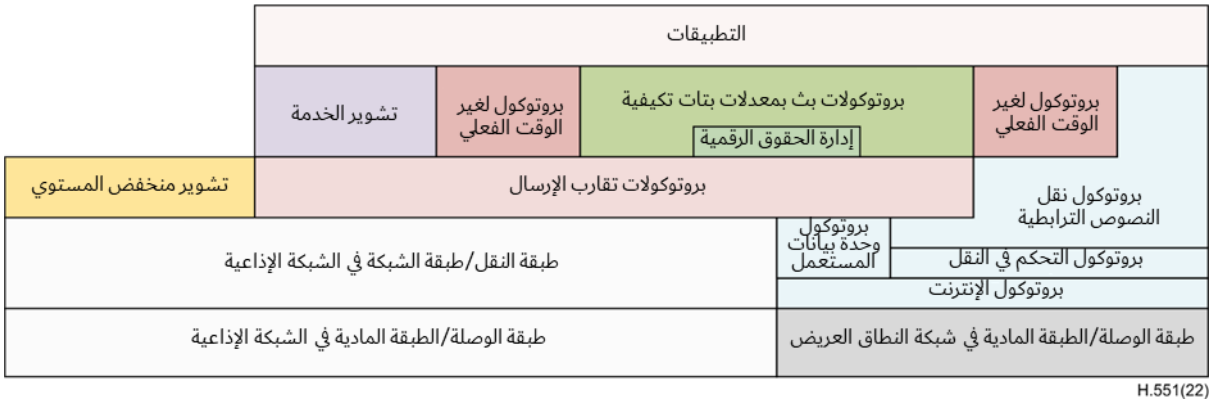
ولمواجهة هذه التحديات، يُقترح مخطط لتقارب الإرسال من أجل إرسال محتويات الوسائط المتعددة عبر الشبكات VMN، حيث تُوصل معظم محتويات الوسائط إلى عدد ضخم من المستعملين عبر الشبكات الإذاعية، وتستخدم شبكات الاتصالات المتنقلة فقط لاستعادة الرزم التي تم إسقاطها بواسطة الشبكات الإذاعية. وتُرسل التدفقات المخلطة من المنصة VMSP إلى بوابات التقارب، حيث يتم ترزيم مقاطع الوسائط في رزم متسلسلة وتُذاع على جميع المستعملين عبر الشبكة الساتلية. وعند المطراف، يمكن اكتشاف الرزم المفقودة أو الخاطئة من تدفقات البث بسهولة. وتتم استعادة الرزم التي يتم إسقاطها عن طريق إعادة الإرسال عبر شبكة الاتصالات المتنقلة. وبمجرد إعادة تجميع تدفقات الوسائط بسلاسة، لا يمكن للمطراف تشغيل تدفقات الوسائط هذه على شاشات عرض ومكبرات الصوت الخاصة بكابينة القيادة فحسب، بل يعمل أيضاً كمركز معلومات ترفيهي محلي لمشاركة تدفقات الوسائط هذه عبر تكنولوجيا Wi-Fi مع جميع الركاب الذين يستخدمون أجهزتهم الشخصية مثل الهواتف الذكية والأجهزة اللوحية. ويوضح الشكل 4 مخطط تقارب الإرسال.



الشكل 4 – معالجة تقارب الإرسال

يستفيد مخطط تقارب الإرسال بجميع مزايا نقاط القوة التكميلية للشبكات الإذاعية وشبكات الاتصالات المتنقلة. وبالتالي، تُستمثل كفاءة نظام خدمات بث الوسائط المتعددة عبر الشبكات VMN.

وترد في الشكل 5 كدسة البروتوكول المرجعي لتقارب إرسال محتويات الوسائط المتعددة عبر الشبكات VMN. ويُلاحظ أن بروتوكولات تقارب الإرسال لا تراعي معايير الطبقة المادية الأساسية وتكون شفافة بالنسبة لمعايير الطبقة العليا. وبالتالي، يمكن ضمان الحد الأدنى من التعديلات للبنى التحتية الحالية للإذاعة أو الاتصالات المتنقلة.



الشكل 5 – كدسة البروتوكول المرجعي لتقارب الإرسال

والافتراض العام هو أن بروتوكول طبقة الشبكة قد يعتمد على كلا الإصدارين من بروتوكول الإنترنت (IPv4 وIPv6). ويُنصح باختيار الإصدار IPv6 [b-IETF RFC 8200] من أجل التوصيلية المباشرة والآمنة بين النظام VMS والمنصات السحابية، للأسباب التالية:

- ينصح فريق مهام هندسة الإنترنت منظمات وضع المعايير (SDO) الأخرى بشكل واضح بتفضيل الإصدار IPv6 [b-IAB]. ونتيجة لذلك، يوصى بعمل التقييس على افتراض الإصدار IPv6.
- تم استنفاد مساحة عناوين الإصدار IPv4 رسمياً في يناير 2011، عندما قامت هيئة تخصيص أرقام الإنترنت (IANA) بتخصيص آخر مساحة لديها من عناوين المستوى الأعلى للإصدار IPv4 (أي 8/). لذلك، فإن اعتماد الإصدار IPv6 باعتباره بروتوكول الشبكة الوحيد يمثل الحل الوحيد القابل للتطبيق لضمان تطور خدمات الشبكة وتطبيقاتها.

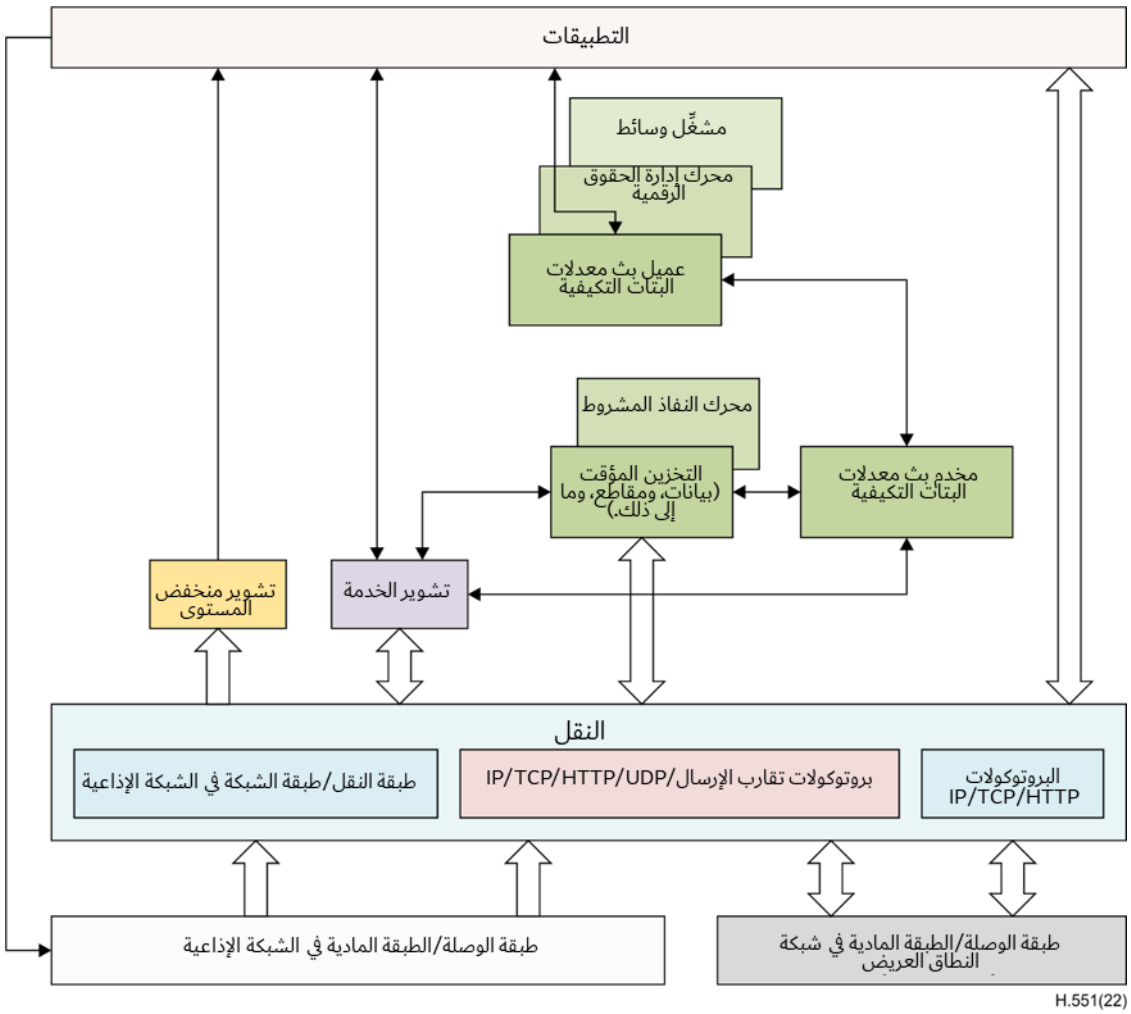
- يعتبر الانتقال إلى الإصدار IPv6 فقط مبادرة إستراتيجية من قبل العديد من الوكالات الحكومية. وهناك مثال، من بين أمثلة أخرى، يمثله المعيار [b-USG OMB]، حيث تفرض الحكومة الفيدرالية الأمريكية مواعيد نهائية وأهدافاً محددة لتحويل شبكات الوكالات الوطنية إلى الإصدار IPv6.
- قد تتطلب أجهزة المستعملين الموجودة داخل أي مركبة إمكانية الوصول من طرف إلى طرف، على سبيل المثال، لتوصيل بأي تطبيقات ومنصات. وهذه هي الحالة التي لا يمكن فيها استخدام ترجمة عنوان الشبكة (NAT) [b-IETF RFC 2663] المقترنة بعناوين الإصدار IPv4 الخاصة. وعلى العكس من ذلك، يوفر الإصدار IPv6 الدعم الكامل لمخطط العنونة العالمي حيث يمكن الوصول إلى أجهزة المستعملين دائماً.

على الرغم من أن الناس أكثر دراية بالإصدار IPv4، وأن نشر الإصدار IPv6 تكتنفه بعض التحديات الجديدة، فإن زيادة مستعملي الإصدار IPv6 وحركته أسرع بكثير من تلك الخاصة بالإصدار IPv4. وهذا يعني أنه مع مراعاة جميع الأمور، فإن الحكمة الجماعية للصناعة قد اختارت IPv6 للمستقبل [b-ETSI WP35].

3.9 نموذج المستقبل المرجعي

يرد نموذج المستقبل المرجعي للأجهزة الموجودة داخل السيارة في الشكل 6، حيث تُحدد الوظائف التالية:

- توصيلات الإذاعة وتوصيلات النطاق العريض التي توفر التوصيلية للمستقبل لاستقبال التشوير والبيانات.
- بروتوكول تقارب الإرسال/كدسة البروتوكولات UDP/HTTP/TCP/IP وكدسة البروتوكولات HTTP/TCP/IP التي توفر بروتوكولات النقل الموجهة للكائنات للمستقبل لاستقبال موارد بث معدلات البتات التكيفية (على سبيل المثال، DASH أو HLS) لخدمات بث الوسائط المتعددة.
- التشوير منخفض المستوى: التشوير عبر الشبكات الإذاعية التي تمكّن المستقبل من إنشاء قائمة خدمات أساسية والتمهيد لاكتشاف تشوير الخدمة لكل خدمة وسائط متعددة.
- تشوير الخدمة: التشوير المتعلق بالخدمة والذي يمكّن المستقبِل من اكتشاف خدمات بث الوسائط المتعددة ومكونات محتواها والنفاذ إليها.
- التخزين المؤقت: التخزين المؤقت ومعالجة البيانات ومقاطع التدميث ومقاطع الوسائط التي يتم تسهيل استقبالها عن طريق تشوير الخدمة.
- مخدم بث معدلات البتات التكيفية (أي DASH/HLS): مخدم محلي لبث معدلات البتات التكيفية يُستخدم لتجريد الطبقات الأساسية إلى عميل بث معدلات البتات التكيفية. وبالنسبة لعميل بث معدلات البتات التكيفية، يتم توفير البيانات ومقاطع التدميث ومقاطع الوسائط من خلال مخدم بث معدلات البتات التكيفية.
- عميل بث معدلات البتات التكيفية: وظيفة تستهلك البيانات والمقاطع وتتواصل مع المكونات الأخرى في المستقبل لشخصنة تجربة الوسائط بناءً على إمكانيات المنصة وتفضيلات المستعمل وتفاعله.
- التطبيق: تطبيق أصلي أو تم تنزيله يستخدم بيانات الإذاعة أو النطاق العريض لتوفير عرض ثري وتفاعلي للمستعمل النهائي.



الشكل 6 – نموذج المستقبل المرجعي للأجهزة داخل المركبة

يُعرض أدناه تسلسل دعم نمطي للمستقبل المرجعي:

- يطلب التطبيق قائمة خدمات مشكلة سلفاً في تشوير المستوى المنخفض. وتُسلم قائمة الخدمات إلى التطبيق، والذي يوفر بعد ذلك سطح بيني للمستعمل لاختيار خدمات بث الوسائط المتعددة. ويختار المستعمل خدمة بث الوسائط المتعددة لاستهلاكها.
- يستخدم التطبيق معلومات نقطة دخول تشوير الخدمة المنقولة في قائمة الخدمات للخدمة المختارة لتوفير معلومات النفاذ إلى كدسة بروتوكولات تقارب الإرسال/IP/TCP/HTTP/UDP من أجل استعادة تشوير الخدمة. ويتم تسليم تشوير الخدمة للتطبيق.
- باستخدام إشارات الخدمة، يوفر التطبيق معلومات النفاذ لكدسة بروتوكولات تقارب الإرسال/IP/TCP/HTTP/UDP لتنزيل مكونات الوسائط المنسقة للبث بمعدلات البتات التكيفية للخدمة المحددة، والتي يتم إرسالها إلى ذاكرة التخزين المؤقت ليتم تخزينها، ثم إزالة تخليطها ومن ثم إعادة تسييرها إلى مخدم البث بمعدلات البتات التكيفية.
- عند اختيار الخدمة، ينشط التطبيق عميل البث بمعدلات البتات التكيفية، مما يتسبب في قيام عميل DASH/HLS بطلب واستقبال مقاطع الوسائط من مخدم البث بمعدلات البتات التكيفية في أوقات بدء توفر مقاطع الوسائط أو بعد ذلك.
- عند استقبال مقاطع الوسائط، تقوم الوظيفة المركبة التي تشتمل على عميل البث بمعدلات البتات التكيفية ومحرك إدارة الحقوق الرقمية ومشغل الوسائط بفك تشفير مقاطع الوسائط المستقبلة، وتُعاد الوسائط التي تم فك تشفيرها إلى التطبيق لتشغيلها.

10 أمن نظام الوسائط المتعددة في المركبات

يوصى بأن تقتصر التفاعلات بين النظام VMS والمكونات الأخرى المشاركة في أمن السيارة (عادةً وحدة التحكم الإلكتروني (ECU)) على الوظائف المشتركة المذكورة في الفقرة 1.8.

وترد التفاصيل في الملحق A.

11 حماية المعلومات المحدِّدة لهوية الأشخاص (PII) والخصوصية

يوصى بأن يوفر النظام VMS الحماية من طرف إلى طرف عندما تصبح المركبات موصولة وتوفر المزيد من الخدمات التفاعلية. ويجب حماية المزيد من بيانات المستعملين والمعلومات المتعلقة بالخصوصية لضمان سرية وسلامة بيانات المستعملين المخزنة في النظام VMS، أو في المركبة وسحابة النظام VMS أو المخدمات الخلفية.

وترد التفاصيل في الملحق B.

الملحق A

أمن نظام الوسائط المتعددة في المركبات

(يشكل هذا الملحق جزءاً لا يتجزأ من هذه التوصية)

1.A نظرة عامة

يوصى بأن تقتصر التفاعلات بين النظام VMS والمكونات الأخرى المشاركة في أمن السيارة (عادةً وحدة التحكم الإلكتروني (ECU)) على الوظائف المشتركة المذكورة في الفقرة 1.8. وفي الواقع، يوصى بألا يؤثر النظام VMS بالسلب على وظائف المكونات الأخرى التي تضمن الأمن المطلوب للسيارة، لا سيما في حالة المركبات ذاتية القيادة.

وفيما يتعلق بأمن النظام VMS، تُلخص التهديدات المفترضة التي تعترض النظام VMS ونظامه الإيكولوجي في الفقرة 2.A، وتُقدم القدرات الأمنية لمواجهة هذه التهديدات كمرجع إعلامي في الفقرة 3.A.

2.A التهديدات المفترضة التي تعترض النظام VMS ونظامه الإيكولوجي

1.2.A التهديدات المتعلقة بمنصة خدمات الوسائط المتعددة في المركبات (VMSP)

في السنوات الأخيرة، زاد تنوع التوصيلية في المركبات بشكل ملحوظ، وعلى وجه الخصوص، اشتد الطلب على التوصيلية مع مختلف المخدمات الموجودة في منصة خدمات الوسائط المتعددة في المركبات. وفي سياق النظام، تُعرف المخدمات الخلفية بمنصة خدمات الوسائط المتعددة في المركبات، بما في ذلك المخدمات التي توفرها الشركة المصنّعة للمعدات الأصلية (OEM) والمخدمات التي يوفرها المورّد والمخدمات التي توفرها خدمة تكنولوجيا المعلومات والاتصالات (ICT) لدعم النظام الإيكولوجي للمركبة من الواجهة الخلفية البعيدة. ويمكن تحديد التهديدات التالية فيما يتعلق بالمنصة VMSP:

- المخدمات الموجودة في المنصة VMSP والمستخدمة كوسيلة لمهاجمة مركبة أو استخراج البيانات.
- الخدمات المقدمة من منصة VMSP تم اختراقها
- فقدان البيانات الموجودة في المخدمات أو العبث بها

2.2.A التهديدات التي تتعرض لها المركبات فيما يتعلق بقنوات الاتصالات الخاصة بها

تشمل اتصالات المركبات الاتصالات الخارجية من خلال الشبكات الخلوية والشبكات الساتلية ذات المدارات الأرضية المنخفضة والشبكات الإذاعية والشبكات قصيرة المدى. وقد تكون القنوات المستخدمة في هذه الاتصالات أهدافاً لهجمات من قبيل الانتحال أو التنصت أو التلاعب بالرسائل وما إلى ذلك. ويمكن تحديد التهديدات التالية فيما يتعلق بقنوات الاتصالات:

- التلاعب أو الحذف غير المرخص به أو أي تعديلات أخرى في الشفرة/البيانات المحمولة في المركبة
- يمكن استخدام السطوح البينية للوسائط المتعددة في المركبات للنفاذ إلى المزيد من البنى التحتية (الذكية) داخل المركبة (على سبيل المثال، وحدة التحكم الإلكتروني غير المرتبطة بالنظام VMS)
- استخدام رسائل غير موثوق بها/لا يمكن الاعتماد عليها وهجمات اختطاف/إعادة تشغيل الدورة
- يمكن تحديث تطبيقات الوسائط المتعددة في المركبات باستخدام الوسط الأثيري، كما يمكن لهذه الهجمات أن تضرب الوسائط المتعددة في المركبات أيضاً
- الكشف عن المعلومات

  انظر الفقرة 9 من التوصية [ITU-T F.749.3].
- هجمات رفض الخدمة

- قد لا تتمكن الوسائط المتعددة في المركبات نفسها من النفاذ إلى البنية التحتية الحرجة داخل المركبة، ولكن يمكن أن تكون بمثابة بوابة لتلك الهجمات.
- نفاذ امتياز لمستخدم ليس له امتياز
- نظراً لأنه يمكن ربط حسابات المستعملين الشخصية بتطبيقات الوسائط المتعددة في المركبات، فإن النفاذ غير المتميز ممكن. وقد لا يوفر النفاذ غير المتميز عبر الوسائط المتعددة في المركبات نفاذاً مباشراً إلى البنية التحتية الحرجة (على سبيل المثال، الوصول إلى الجذر؛ النفاذ إلى نظام الكبح)، ولكن يمكن أن يعمل مرة أخرى كبوابة للنفاذ إلى البنية التحتية للمركبة.
- الفيروسات المدمجة في وسائط الاتصالات
- تعتمد الوسائط المتعددة في المركبات (VM) الذكية على نقل البيانات بين النظام VMS ومنصة VMSP في سحابة. ومن خلال اختراق قناة الاتصالات هذه، قد يستخدم المهاجمون عمليات نقل الرسائل/البيانات من المنصة VMSP إلى النظام VMS لنشر البرمجيات الضارة.
- رسائل خبيثة المحتوى

تعتمد الوسائط المتعددة في المركبات (VM) الذكية على نقل البيانات بين النظام VMS ومنصة VMSP في سحابة، مثلاً. ومن خلال اختراق قناة الاتصالات هذه، يمكن للمهاجمين تعديل عمليات نقل الرسائل/البيانات من المنصة VMSP إلى النظام VMS للحصول على نفاذ إلى النظام VMS و/أو إلى وحدات التحكم الإلكتروني داخل المركبة الذكية المستهدفة.

3.2.A التهديدات التي تتعرض لها المركبات فيما يتعلق بإجراءات التحديث الخاصة بها

هناك طريقتان لتحديث أنظمة المركبات، وهما التحديث السلكي عبر منفذ التشخيص على متن المركبة (OBD) أو الأجهزة المحمولة مثل بطاقة رقمية آمنة (SD) أو محرك ناقل ذاكرة USB والتحديث اللاسلكي عبر الأثير. وقد تكون البرمجية المراد تحديثها برمجية ثابتة أو بيانات تشكيل خاصة بالمركبة. ويمكن تحديث غالبية المشكلات الإلكترونية وعيوب البرمجيات وحلها إلكترونياً دون نفاذ مادي، وذلك عن طريق اختبار OBD مثلاً. وعلاوةً على ذلك، فإن التحديثات (اللاسلكية) عبر الأثير تساعد في تقصير دورة التحديث لتقليل التعرض للهجمات بالنسبة لمواطن الضعف الأمنية المعروفة للبرمجية. ويمكن تحديد التهديدات التالية فيما يتعلق بإجراءات التحديث:

- سوء استخدام إجراءات التحديث أو العبث بها

بغض النظر عن استخدام التحديث عبر الأثير أو التحديث المحلي/المادي، قد ينطوي إجراء التحديث على تهديدات باستخدام برامج تحديث النظام المفبركة أو البرمجيات الثابتة التي تعرضت للعبث.

ويمكن التلاعب بالبرمجية قبل عملية التحديث، على الرغم من أن عملية التحديث سليمة. إذ يقوم موردو البرمجيات باستحداث/إعداد برمجياتهم للتحديث ويتم تسليم البرمجية إلى الأنظمة المستهدفة التي تتطلب التحديث. ولذلك، قد يكون هناك تهديد خطير باحتمال التلاعب بالبرمجية وإفسادها قبل استخدامها.

وفي أثناء إجراء التحديث بشكلٍ خاص، قد تتعرض للخطر مواد التجفير، مثل مفاتيح التجفير والشهادات المستخدمة في تحديث البرمجية وبالتالي قد تتسبب في تحديث برمجية غير صالحة أو ضارة.

- رفض الخدمة ورفض التحديث المشروع

قد يكون هجوم رفض الخدمة على مخدم التحديث أو الشبكة لمنع نشر تحديثات البرمجيات الحرجة و/أو الإفراج عن الميزات الخاصة بالعملاء بمثابة هجوم محتمل عند إجراء تحديث البرمجيات. ومن الممكن أيضاً رفض تحديثات مشروعة.

4.2.A التهديدات للمركبات فيما يتعلق بتوصيليتها وتوصيلاتها الخارجية

بالنسبة لطائفة متنوعة من خدمات الراحة، يمكن تجهيز المركبات بمكونات للتواصل مع المخدمات في المنصة VMSP ويمكنها التواصل مع كل شيء خاضع للتمكين من جانب مستخدمي الطرق عبر توصيل لاسلكي. وإلى جانب ميزات الراحة، هناك مزايا

السلامة مثل وظيفة نداءات الطوارئ التلقائية وتلك التي تدعمها الاتصالات من المركبة إلى كل شيء (V2X). ومع ذلك، كلما تزايد توصيل المركبات مع كيانات خارجية لتعزيز التوصيلية، تزايدت التهديدات ومواطن الضعف نظراً لتوسع أسطح الهجمات جراء السطوح البينية الإضافية. ويمكن تحديد التهديدات التالية فيما يتعلق بالتوصيلية والوصلات الخارجية:

- التلاعب في توصيلية وظائف المركبات

لا يوفر النظام VMS نفاذاً مباشراً إلى وظائف المركبة الحرجة ولكن يمكن استخدامه كبوابة للنفاذ إلى تلك المكونات الحرجة، على سبيل المثال، وحدات التحكم الإلكتروني المخصصة.

- برمجية طرف ثالث مستضافة

يمكن تضمين تطبيقات النظام VMS ضمن فئة "برمجيات الطرف الثالث المستضافة".

- الأجهزة الموصولة بالسطوح البينية الخارجية

كما هو مبين في التوصية [ITU-T F.749.3]، يمكن أن تستند التوصيلية إلى أجهزة مدمجة مثل الهواتف الذكية.

3.A القدرات الأمنية المستندة إلى التهديدات المحددة

1.3.A إدارة خدمات الهوية والنفاذ (IAM)، والاستيقان والترخيص ومراجعة العمليات

يشترك في خدمات النظام VMS العديد من المدراء والمستعملين، ويتوفر النفاذ إلى هذه الخدمات واستعمالها داخلياً وخارجياً. وتدعو الحاجة إلى إدارة الهويات ليس فقط من أجل حمايتها، بل لتسهيل عمليات إدارة النفاذ والاستيقان والترخيص ومراجعة العمليات في هذه البنية التحتية الدينامية والمفتوحة للنظام VMS.

وتحتاج إدارة خدمات الهوية والنفاذ إلى واحد أو أكثر من نماذج الثقة المشتركة من أجل استيقان الهويات، كما يحتاج إليها المطوّرون والمشرفون على الآلات الافتراضية وغيرهم من مكونات النظام من أجل استيقان مكونات النظام من قبيل وحدات البرمجيات أو التطبيقات أو مجموعات البيانات التي جرى تنزيلها.

وتساهم إدارة خدمات الهوية والنفاذ في ضمان سرية الخدمات والموارد وسلامتها وتوفرها، وتعتبر بالتالي أساسية في النظام VMS. وعلاوةً على ذلك، فقد تمكن إدارة خدمات الهوية والنفاذ من إنشاء اتحاد بهوية واحدة وتوقيع دخول واحد إلى النظام VMS باستخدام آليات استيقان مختلفة أو موزعة في ميادين أمنية مختلفة.

وتوفر مراجعة العمليات الحماية من التنصل، وتسمح بإجراء تحليل جنائي بعد حادث أمني، وتقوم بردع الهجمات (الاقتحامية أو الداخلية المصدر على السواء). ومع أن مراجعة العمليات تنطوي على أكثر من مجرد عملية تسجيل، إلا أنها تشمل أيضاً المراقبة الفاعلة بهدف التأشير على الأنشطة المريبة.

2.3.A أمن السطوح البينية

تؤمن هذه القدرة بقاء السطوح البينية مفتوحة لمطوري النظام VMS و/أو بائعي المنصات VMSP الآخرين المتعاقدين الذين يتم من خلالهم توفير الأنواع المختلفة من الأنظمة VMS، كما تؤمن الاتصالات القائمة على هذه السطوح البينية. وتشمل الآليات المتاحة لضمان أمن السطوح البينية على سبيل المثال لا الحصر: الاستيقان أحادي الجانب/المتبادل، والتحقق من السلامة بواسطة المجموع التدقيقي، والتجفير من طرف إلى طرف، والتوقيع الرقمي.

3.3.A أمن الشبكات

يتيح أمن الشبكات في بيئة النظام VMS عزل كل من الشبكات المادية والافتراضية ويؤمن الاتصالات بين جميع المشاركين. كما يتيح تجزئة الميدان الأمني للشبكات والتحكم في النفاذ على حدود الشبكات (كجدران الحماية مثلاً)، وكشف الاقتحام ومنعه، وفصل حركات الشبكات استناداً إلى سياسات الأمن، كما يحمي الشبكة من الهجمات في البيئتين المادية والافتراضية على السواء.

4.3.A الأمن التشغيلي

توفر هذه القدرة حماية أمنية لعمليات التشغيل والصيانة اليومية للنظام VMS والبنية التحتية للمنصة VMSP.

وتتضمن القدرة الأمنية التشغيلية هذه ما يلي:

- تحديد مجموعات من سياسات الأمن وأنشطة الأمن مثل إدارة التشكيلات وتحديث الرقع البرمجية وتقييم الأمن والاستجابة إلى الحوادث؛
- مراقبة التدابير الأمنية للمنصة VMSP وفعاليتها وتقديم تقارير مناسبة إلى الأنظمة VMS المتأثرة؛

وفي الحالة التي تتغير فيها التدابير الأمنية للمنصة VMSP أو فعالية هذه التدابير، يتم تنبيه جميع الأنظمة VMS في اتجاه المقصد بشأن هذه التغييرات.

وتمكن هذه التقارير والتنبيهات الأنظمة VMS المرخص لها من رؤية الحوادث المناسبة ومعلومات المراجعة وبيانات التشكيلات المتعلقة بها.

5.3.A عمليات تحديث البرمجيات والبرامج الثابتة

يجب أن تتوافق عمليات التحديث عبر الأثير الآمنة مع معايير الأمن الأساسية. ويوصى بأن تأخذ عملية التحديث في الاعتبار العوامل التشغيلية (على سبيل المثال، توقيت التحديثات وعمليات التجفير/فك التجفير). يساهم وجود العديد من المصنعين الأصليين للمعدات والبائعين من الأطراف الثالثة في سطوح بينية للأنظمة الفرعية المختلفة داخل المركبة. وعلى هذا النحو، يمكن لأي ثغرة أمنية أو مخاطر سيبرانية تستهدف هؤلاء المصنعين الأصليين للمعدات أو الموردين أن تختطف بشكل فعال تحديث مشروع لبرمجيات المصنعين الأصليين للمعدات، والذي يتم إرساله بعد ذلك كبيانات سحابية ليتم نشرها على المركبات.

ويوصى بتصميم وتنفيذ وتشغيل آلية لتحديث البرمجيات والبرامج الثابتة الخاصة بالنظام VMS (وحدات التحكم الإلكتروني والأنظمة ذات الصلة).

وعند تطوير خدمة من خدمات النظام VMS، يوصى بتصميم آلية لتحديث البرمجيات والبرامج الثابتة للنظام VMS وتنفيذها كوظيفة أساسية. ويوصى أيضاً بتنفيذ آلية سحب للبرمجيات والبرامج الثابتة عند التصميم، لاستخدامها عند فشل التحديث.

وعند استخدام ودعم خدمة للنظام VMS، تحتوي حزمة تحديث البرمجيات/البرامج الثابتة على توقيعها الرقمي وشهادات التوقيع وسلسلة شهادات التوقيع التي يتم التحقق منها بواسطة الجهاز، قبل بدء عملية التحديث.

ويوصى باستخدام مفاتيح التجفير لتحديث حماية السلامة والسرية بحيث تتم إدارتها بشكل آمن وتشغيلها بشكل مناسب. وعند إجراء التحديثات عبر الأثير (OTA)، يوصى بإجراء التحديثات عبر قنوات اتصالات مجفرة.

ويوصى بالتحديثات التي تُجرى عبر الأثير إما لكي تنجح تماماً أو تفشل بطريقة قابلة للاسترداد. وفي حالة فشل التحديث، يوصى بعودة الجهاز إلى آخر تشكيل جيد معروف، ويوصى بعدم توفير قدرة على تعطيل توصيلة الجهاز بمخدم التحديث.

6.3.A أمن التطبيقات

غالباً ما يتم استخدام هذه الإمكانات الأمنية لتحسين أمن "تطبيقات النظام VMS" عادة عن طريق البحث عن الثغرات الأمنية وإصلاحها ومنعها في النظام VMS ونظامه الإيكولوجي. وتُستخدم تقنيات مختلفة لإبراز مثل هذه الثغرات الأمنية في مراحل مختلفة من دورة حياة التطبيقات مثل التصميم والتطوير والنشر والتحديث والصيانة.

7.3.A إدارة الحوادث

تنص إدارة الحوادث على مراقبة الحوادث والتنبؤ بها والتحذير منها والاستجابة لها. والمراقبة المستمرة ضرورية (مثلاً مراقبة الأداء في الوقت الفعلي للمخدمات المستخدمة في المنصة VMSP) لمعرفة ما إذا كان النظام VMS يعمل على النحو المتوقع على كامل البنية التحتية. ومن شأن ذلك أن يمكّن الأنظمة من معرفة الوضع الأمني للخدمة، وتحديد الظروف غير الطبيعية، وتوفير إنذار مبكر

بالحمولات الزائدة للنظام الأمني والخروقات وانقطاع الخدمة وما إلى ذلك. وبعد حصول الحوادث الأمنية، يتم تحديد المشكلة والاستجابة للحادث بسرعة سواء بطريقة أوتوماتية أو بتدخل المسؤول البشري. أما الحوادث الوثيقة الصلة فيتم تسجيلها وتحليلها لمعرفة الأنماط الأساسية المحتملة للتمكن من معالجتها بشكل استباقي.

8.3.A التجفير

تضمن هذه القدرة سرية وسلامة البيانات المستخدمة والمتبادلة في النظام VMS وأنظمته الإيكولوجية. وهذه هي الطريقة الأساسية لتخزين البيانات وإرسالها في شكل معين بحيث لا يتمكن من قراءتها ومعالجتها إلا المعنيون بها. ولا تحمي هذه القدرة بيانات النظام VMS من السرقة أو التغيير فحسب، بل يمكن استخدامها أيضاً لاستيقان المستعمل، وما إلى ذلك.

وكمثال جيد لتنفيذ التجفير، ترد المبادئ التوجيهية بشأن اختيار أساسيات التجفير لأنظمة تلفزيون بروتوكول الإنترنت في [b-ITU-T X.1197 Amd1] ويمكن تطبيقها على تدفقات الوسائط المتعددة في أنظمة المركبات، بقدر ما هي متطابقة في مستوى الأهمية/الحتمية كتدفقات الوسائط المتعددة في أنظمة تلفزيون بروتوكول الإنترنت غير الخاصة بالمركبات. وبالمثل، بالنسبة للمركبات ذات توصيلية الجيل الخامس (5G)، توفر [b-ITU-T X.1811] مزيداً من الإرشادات حول كيفية تنفيذ مستويات الأمن الأساسية للتوصية [b-ITU-T X.1197 Amd1]، بما في ذلك على سبيل المثال لا الحصر تدفقات الوسائط المتعددة.

علاوة على ذلك، مع حل إدارة الحقوق الرقمية المستند إلى تجفير قوي ومستيقن منه، والذي يهدف إلى السماح باستهلاك المحتوى الشرعي المحمي بحقوق الطبع والنشر فقط بواسطة نظام المعلومات والترفيه، ستؤخذ فقط في الاعتبار تدفقات الوسائط المتعددة الخارجية على خط البصر المشروعة بواسطة نظام المعلومات والترفيه ونظام القيادة المساعدة، وبالتالي السماح للحركة بالمضي قدماً دون أي اضطراب.

9.3.A أمن العتاد

تهدف هذه القدرة إلى القضاء على مواطن التعرض ونقاط الضعف الأمنية المتأصلة في عتاد النظام VMS، وتوفر بيئة آمنة للتنفيذ على مستوى العتاد. وعلى وجه الخصوص، أصبح من الضروري تنفيذ العديد من وظائف التجفير الأساسية في العتاد، مثل إدارة مفاتيح التجفير، وتنفيذ التجفير/فك التجفير، وتوفير التوقيعات الرقمية والاستيقان القوي، والتي تُستخدم بشكل مهم لضمان الأمن في النظام VMS. ولهذا الغرض، من الضروري تحري الأمن عند التصميم والتحقق من تشغيل العتاد ذي الصلة من مرحلة تصميم العتاد، مع مراعاة التهديدات والهجمات المحتملة.

فعلى سبيل المثال، لضمان الأمن على مستوى وحدة التحكم الإلكتروني في معمارية النظام VMS، يوصى بحماية كل وحدة تحكم إلكتروني مستخدمة بواسطة الوحدات HSM والوظائف PUF، وهي مكونات نموذجية لوحدات أمن العتاد.

10.3.A القدرات الأمنية العامة

ملاحظة – القدرات الأمنية التالية اختيارية لهذه التوصية. ومع ذلك، يمكن استخدام هذه القدرات بشكل فعال لتحسين أمن النظام VMS.

- تقييم الأمن ومراجعته

تسمح هذه القدرة بإجراء تقييم أمني للنظام VMS. وهي تمكن الطرف المرخّص له بالتحقق من أن النظام يمتثل لمتطلبات الأمن المعمول بها. ويمكن إجراء التقييم الأمني أو المراجعة الأمنية بواسطة النظام VMS أو المنصة VMSP أو طرف ثالث، كما يمكن اعتماد شهادات أمنية بواسطة طرف ثالث مرخّص له.

وتنفذ معايير الأمن المناسبة بحيث توفر تفاهماً متبادلاً للمستوى الأمني بين النظام VMS والمنصة VMSP.

- نموذج الثقة

يعتبر نموذج الثقة المشترك ضرورياً لأي نظام يتعاون فيه عدد من مقدمي الخدمات لتوفير خدمة جديرة بالثقة.

ونظراً إلى الطابع متعدد أصحاب المصلحة ذي الدرجة العالية للنظام VMS، سيكون على بيئة النظام VMS إدراج نموذج شامل للثقة. ويتيح نموذج الثقة هذا إيجاد جزر و/أو اتحادات من الكيانات الموثوقة بحيث تتمكن العناصر المتفرقة للنظام

من استيقان هوية الكيانات والمكونات الأخرى والحقوق المسموحة. ويستند كلّ من جزر أو اتحادات الثقة إلى واحدة أو أكثر من السلطات الموثوقة (مثلاً سلطة إصدار شهادات البنية التحتية للمفاتيح العمومية (PKI)).

- عزل البيانات وحمايتها

أ) عزل البيانات

قد يتحقق عزل البيانات بطريقة منطقية أو مادية تبعاً لدقة العزل المطلوب والنشر المحدد لبرمجيات وعتاد النظام VMS.

ب) حماية البيانات

تضمن حماية البيانات أن تكون بيانات النظام VMS والبيانات المشتقة منه والمحتفظ بها في المنصة VMSP محمية بالشكل المناسب بحيث لا يمكن النفاذ إليها أو تغييرها إلا على النحو الذي يسمح به النظام VMS. وقد تشمل هذه الحماية توليفة من قوائم التحكم في النفاذ، وتدقيق السلامة، وتصحيح الأخطاء/استعادة البيانات، والتجفير، وغير ذلك من الآليات المناسبة.

وعندما توفر المنصة VMSP إمكانية تجفير التخزين للأنظمة VMS، فقد تكون هذه الوظيفة تجفيراً من جانب العميل (مثلاً ضمن تطبيق خاص بمورد CSP) أو تجفيراً من جانب المخدّم.

- التنسيق الأمني

بما أن الأنظمة VMS المختلفة تقتضي تنفيذ وسائل تحكم أمنية مختلفة، فإن هذه القدرة الأمنية تنسق بين آليات الأمن غير المتجانسة لتفادي أوجه التضارب في الحماية.

والأطراف التي تؤدي أدواراً مختلفة في النظام الإيكولوجي للنظام VMS تتسم بدرجات مختلفة من التحكم في الموارد والخدمات المادية أو الافتراضية، بما في ذلك التحكم في الأمن.

وتتوفر لكل طرف آليات أمنية متنوعة، بما فيها عزل المشرفين على الآلات الافتراضية، وإدارة خدمات الهوية والنفاذ.

وحماية الشبكات، وما إلى ذلك. ويعتمد التنسيق الأمني على قابلية التشغيل البيني وتناسق الآليات الأمنية المتنوعة.

- أمن سلسلة التوريد

تستعمل المنصة VMSP عدداً من الموردين لبناء خدماتها. ويكون بعض هؤلاء الموردين من المشاركين في صناعة الأنظمة VMS، بينما يكون بعضهم الآخر من الموردين التقليديين لتجهيزات وخدمات تكنولوجيا المعلومات (IT)، مثل صانعي العتاد ممن لا يمتون بصلة مباشرة إلى النظام VMS. وتتيح هذه القدرة إرساء علاقة ثقة بين المنصة VMSPوجميع المشاركين في سلسلة التوريد عبر أنشطة أمنية. وتشمل أنشطة أمن سلسلة التوريد هذه تحديد وتجميع المعلومات عن المكونات والخدمات التي حازت عليها المنصة VMSP والتي تستخدم لتوفير خدمات الحوسبة السحابية وإنفاذ سياسات أمن سلسلة التوريد.

وعلى سبيل المثال، يمكن أن تشمل أنشطة الأمن في سلسلة التوريد في منصة VMSP ما يلي:

أ) تأكيد المعلومات الأساسية عن المشاركين في سلسلة التوريد؛

ب) التحقق من صلاحية العتاد والبرمجيات والخدمات التي تستخدمها المنصة VMSP؛

ج) فحص العتاد والبرمجيات التي تقتنيها المنصة VMSP للتأكد من عدم التلاعب بها أثناء العبور؛

د) توفير آليات للتحقق من منشأ برمجيات النظام VMS، مثلاً الشفرة المقدمة من بائع البرمجيات.

وتستمر هذه القدرة بتغطية التطورات الجارية للنظام وتحديثاته.

- تأمين بيئة وإجراءات التطوير

تهدف هذه القدرة إلى تجنب انعدام الأمن في النظام VMS وأنظمته الإيكولوجية أثناء التطوير. وتشمل بيئة التطوير الأشخاص والعمليات والتكنولوجيا والمرافق المرتبطة بتطوير النظام. ويوصى مطور خدمات النظام VMS بتقييم المخاطر في جهود التطوير الفردية للنظام VMS وتهيئة بيئات تطوير آمنة مع الأخذ في الاعتبار:

أ) العاملون في البيئة؛

ب) منهجيات التطوير التطبيقي وعمليات معالجة البرمجيات والبيانات؛

ج) استخدام المنتجات والخدمات الخاصة بمصادر خارجية؛

د) البيئة المادية والشبكية؛

هـ) التعايش مع جهود التطوير والتشغيل الأخرى.

ويجب على مطور خدمات النظام VMS أيضاً تحديد بيئة التطوير والإجراءات المرتبطة بها للحد من المخاطر. ويوصى بتعميم الإجراءات على الأفراد المشاركين في جهود التطوير.

الملحق B

حماية المعلومات المحدِّدة لهوية الأشخاص (PII) والخصوصية

(يشكل هذا الملحق جزءاً لا يتجزأ من هذه التوصية)

يوصى بأن يوفر النظام VMS الحماية من طرف إلى طرف عندما تصبح المركبات موصولة وتوفر المزيد من الخدمات التفاعلية. ويجب حماية المزيد من بيانات المستعملين والمعلومات المتعلقة بالخصوصية لضمان سرية وسلامة بيانات المستعملين المخزنة في النظام VMS، أو في المركبة وسحابة النظام VMS أو المخدمات الخلفية.

وفقاً للمعهد الوطني للمعايير والتكنولوجيا (NIST) في الولايات المتحدة، فإن المعلومات المحدِّدة لهوية الأشخاص هي "أي تمثيل للمعلومات يسمح باستنتاج هوية الفرد الذي تنطبق عليه المعلومات بشكل معقول إما عن طريق وسائل مباشرة أو غير مباشرة" [b-NIST SP 800-79-2].

ولا يوجد تعريف واحد لمصطلح "الخصوصية". ويعتمد معنى الخصوصية على السياقات القانونية والسياسية والمجتمعية والثقافية والاجتماعية والتكنولوجية.

وبشكل عام، يمكن تعريف خصوصية المعلومات على النحو التالي:

1) يتمتع الفرد بخصوصية معلوماتية إذا كان محمياً ضد الاختراق أو التدخل أو النفاذ إلى بيانات الخاصة من قبل الآخرين غير المصرح لهم.

وحماية البيانات PII هي أحد جوانب ضمان الخصوصية.

وقد يقوم النظام VMS بتخزين البيانات PII أو قد يعمل كبوابة للنفاذ إلى المعلومات PII الخاصة بمالك المركبة و/أو السائق و/أو الركاب الآخرين.

1.B مصادر المعلومات

يشتمل النظام VMS على العديد من مصادر إدخال المعلومات، مثل:

- أجهزة الاستشعار (كاشفات الحركة، كاشفات الموقع، إلخ.)،
- الكاميرا (الشخصنة، التعرف على الميزات، إلخ.)
- الميكروفون – الصوت (يمكن استخدامه أيضاً للتسجيلات الصوتية والتعرف على الصوت، والقياسات البيومترية للصوت، وما إلى ذلك)
- معرّفات هوية بروتوكولات الاتصالات الشبكية مثل عنوان IP وعنوان MAC وما إلى ذلك.
- مصادر الوسائط مثل مفتاح ذاكرة USB وبطاقة ذاكرة رقمية آمنة وقرص صلب خارجي وما إلى ذلك.
- تطبيقات الأطراف الثالثة وبوابات الدفع والخدمات والأجهزة والملحقات وما إلى ذلك.

ويقوم النظام VMS بتخزين المعلومات ومشاركتها مع الأنظمة الأخرى في المركبة أو السحابة بناءً على معمارية المركبة، والمتطلبات الإقليمية والتشريعية والمتطلبات المتعلقة بالاعتماد.

2.B تنفيذ حماية المعلومات المحدِّدة لهوية الأشخاص: اعتبارات عامة

يجب حماية البيانات الشخصية (على سبيل المثال، في البيانات أو النصوص أو الصوت أو الفيديو أو الصور)، وكذلك أي محتوى يستخدمه المستعملون بخلاف العميل المقصود أو أي مستعمل نهائي (مثل السحابة البعيدة أو المخازن أو العمليات) باستخدام قد يطلبه النظام VMS.

يجب أن يكون هناك اتفاق لمشاركة البيانات الخاصة بالبيانات الشخصية المتعلقة بكل عميل والمستعملين النهائيين والأطراف الثالثة. ويجب أن يستند أي اتفاق مع العميل أو أي اتفاقات أخرى ذات صلة تحكم استخدام خدمات النظام VMS إلى المعايير التالية:

- النفاذ المشخصن بناءً على اختيار المستعمل للخدمات والاهتمامات.
- تصميم النظام VMS بحيث يسمح باستخدامه وفقاً للمتطلبات التنظيمية للخصوصية.
- يجب أن يسمح تصميم برمجيات النظام VMS والعتاد والشبكة بالنفاذ المستيقن فقط.
- يجب تصميم حماية البيانات PII والخصوصية في النظام للمركبات الخاصة لمستخدم واحد ولمركبة مشتركة مع العديد من المستخدمين.

3.B وضوح البيانات وشفافيتها

يوصى بتنفيذ معايير أمنية معروفة جيداً وخاضعة للتدقيق الشديد. ويوصى بتجنب خوارزميات التشفير المسجلة الملكية.

ويوصى باعتماد عمليات معروفة جيداً.

ويوصى بإعلام المستخدمين بالبيانات المخزنة/التي يمكن النفاذ إليها من خلال النظام VMS. وبما أن الشفافية تعزز قبول المستخدم، يوصى بإعلام المستخدمين بتضمين معلومات حول نوع البيانات والغرض من التجميع وهوية كيانات معالجة البيانات ومدة تخزين البيانات.

1.3.B الخصوصية بالتغيب

يوصى بأن يكون المستخدمون قادرين على التحكم في حد تنزيل البيانات، وكذلك الاشتراك في/إلغاء الاشتراك في تنزيل البيانات وتخزينها. وتعد استراتيجيات إلغاء الاشتراك أكثر حفاظاً على الخصوصية وتتوافق بشكل أفضل مع مبادئ الخصوصية بالتغيب. لذلك، يوصى بإستراتيجيات إلغاء الاشتراك.

ويوصى بأن يقوم النظام VMS بتحديد قائمة لحالات الاستعمال التي تفي بمتطلبات وإعدادات خصوصية البيانات.

قد تستخدم التطبيقات موارد متعددة لحالات استعمال محددة. فعلى سبيل المثال، في حالة خدمات الموقع، يمكن استخدام البلوتوث أو النظام العالمي لتحديد الموقع (GPS) أو بؤر توصيل Wi-Fi ذات المصادر الجماعية أو مواقع الأبراج الخلوية لتحديد المواقع التقريبية للمستخدم. ويوصى بأن يزود النظام VMS المستخدمين بإمكانية إيقاف إمكانيات تتبع محددة. ويمكن استخدام التحكم في الإعدادات العامة لتحقيق ذلك من خلال تحديد سياسات الخصوصية لجميع التطبيقات. وبدلاً من ذلك، يجوز تمكين الركاب من التحكم في النفاذ إلى البيانات على مستوى تطبيق واحد. يمكن استخدام ضوابط الخصوصية مثل نُهج PRICON posit، والتي تجمع بين كلا النهجين. وقد يكون هناك خيار آخر للنظام VMS هو إشارة "عدم التعقب" ("DNT") التي تستخدمها بالفعل متصفحات الويب. والإشارة DNT هي حقل رأسية للبروتوكول HTTP يشير إلى تفضيل المستخدم لتتبع أنشطة المستخدم على خدمة ما أو من خلال تتبع المستخدم عبر المواقع.

قد تطلب التطبيقات أو عناصر التحكم استقبال، على سبيل المثال، بيانات الموقع فقط أثناء استخدام التطبيق أو السماح بها في أي وقت. وقد يختار الركاب عدم السماح بهذا النفاذ ويوصى بأن يكون بوسعهم تغيير اختيارهم في أي وقت في الإعدادات. وإذا تم التطبيق على خدمة تعمل أيضاً داخل الاتحاد الأوروبي، فإن اللائحة العامة لحماية البيانات (GDPR) تطالب بتمكين المستخدم من اتخاذ قرارات خصوصية مستنيرة. ويمكن اتخاذ قرار مستنير بشأن الخصوصية إذا كان المقرر على دراية بعواقب الكشف عن البيانات (من يحصل على أي بيانات، ولأي غرض، وبأي شروط) أو الرفض (ما هي الوظائف المحددة التي يتم تقييدها).

إذا تم منح تطبيق ما حق النفاذ إلى بيانات معينة، لاستخدامها في وضع الخلفية، فيجب تذكير المستخدمين بموافقتهم والسماح لهم بتغيير نفاذ التطبيق.

ويوصى بأن تكون معمارية النظام VMS قوية لمنع التطبيقات من النفاذ إلى المعلومات التي لم يصرح المستخدم بشكل واضح بالنفاذ إليها.

4.B دقة البيانات وسلامة البيانات

يوصى بأن يحفظ النظام VMS جميع جوانب البيانات، مثل تحميل البيانات وتنزيلها والاتصال بها وحذفها بطريقة محددة.

الأمن من طرف إلى طرف – حماية لدورة الحياة بأكملها. ويوصى بإجراء مراجعة منتظمة للشفرة وإجراء اختبارات أمن صارمة. علاوة على ذلك، يوصى بتنفيذ استراتيجيات الحماية على مستوى الإذاعة ومستوى قاعدة البيانات ومستوى المستقبل.

يوصى بتوفير ضمان أمن البرمجيات من أجل منع الخسارة أو عدم الدقة أو التغيير أو عدم التيسر أو إساءة استخدام البيانات والموارد التي يتم استخدامها والتحكم فيها وحمايتها.

يوصى بالسماح للمستخدمين بالتحقق من دقة المعلومات PII وقانونية معالجتها؛

وتعني السلامة الحفاظ على اتساق البيانات ودقتها وموثوقيتها بمرور الوقت. ومن ثم، يوصى بإنشاء حماية ضد تعديل المعلومات أو إتلافها بشكل غير لائق. ويوصى باتخاذ التدابير المناسبة لضمان عدم التنصل من المعلومات واستيقانها.

في الإعدادات، يوصى بأن يتسنى للمستعملين معرفة التطبيقات التي يُسمح فيها لهم بالنفاذ إلى معلومات معينة، بالإضافة إلى منح أو إبطال أي نفاذ مستقبلي.

بالإضافة إلى ذلك، يوصى بأن يفرض نظام تشغيل النظام VMS قيوداً تمنع حركة البيانات بين التطبيقات والحسابات المثبتة بواسطة حل إدارة بيانات موثوق به وتلك المثبتة من قبل المستخدم.

يمكن للمستخدمين طلب تصحيح أو تعديل أو حذف المعلومات PII الخاصة بهم إذا كانت غير دقيقة أو إذا كانوا يعتقدون أن معالجة المعلومات PII الخاصة بهم تنتهك القانون المعمول به.

وينبغي تنفيذ الأنظمة والتطبيقات والإجراءات لتأمين المعلومات PII، لتدنية مخاطر السرقة أو التلف أو فقدان المعلومات أو النفاذ أو الاستخدام غير المصرح به للمعلومات.

ويوصى بالكشف عن أي تغييرات غير مصرح بها على المعلومات PII في النظام VMS أو السحابة وإبلاغ المستخدم بها.

5.B السرية

تتمثل السرية في الحفاظ على القيود المصرح بها على النفاذ والإفصاح، بما في ذلك وسائل حماية الخصوصية الشخصية ومعلومات الملكية.

1.5.B مستويات تأثير السرية

يوصى بتقييم المعلومات PII لتحديد مستوى تأثير السرية، بحيث يمكن تطبيق الضمانات المناسبة. ولا يوصى بمعالجة جميع البيانات PII المخزنة أو التي يتم إنشاؤها على قدم المساواة.

ويوصى بتقييم مستويات تأثير السرية على أنها منخفضة أو متوسطة أو عالية اعتماداً على قابلية التعرف على الهوية وحساسية البيانات والالتزام بالحماية وفقاً للوائح.

2.5.B حماية السرية

يوصى بتحقيق حماية السرية عبر التدابير التالية:

- تنفيذ آلية تحكم في النفاذ باستخدام كلمة مرور للنفاذ إلى البيانات من النظام VMS.
- النفاذ متعدد الطبقات إلى المعلومات PII ذات السرية عالية التأثير.
- التحكم في النفاذ متعدد المستويات من الهواتف المحمولة والحواسيب المحمولة والأجهزة الرقمية الشخصية.
- تجفير المعلومات PII قبل إرسالها. ويرد وصف التدابير التفصيلية في الفقرة 8.3.A (التجفير).

علاوة على ذلك، يوصى بإجراء تقييمات للمخاطر قبل نشر المتطلبات الجديدة. ويوصى بتنفيذ آلية مراقبة مستمرة للمخاطر لتقييم التغييرات في النظام VMS أو تحديد هوية المخاطر الجديدة المرتبطة بالنظام VMS.

6.B إخفاء هوية البيانات

إخفاء هوية البيانات هي عملية تغيير البيانات المصنفة بشكل لا رجعة فيه من أجل حماية موضوعات بيانات المعلومات PII.

ومن خلال إخفاء هوية البيانات المتداولة في بيئة النظام VMS، يمكن تحقيق قدر كبير من عمليات تحليل البيانات وتبادلها.

7.B تيسر البيانات

يتطلب التيسر ضمان النفاذ إلى المعلومات واستخدامها في الوقت المناسب وبطريقة موثوقة.

يوصى بتزويد الركاب المعتمدين بتحكم مفصل في استخدام خدمات النظام لمعلومات الموقع. ويتضمن ذلك قدرتها على إيقاف تشغيل تضمين معلومات الموقع ضمن المعلومات التي يتم جمعها بواسطة التطبيقات الداخلية، وسجل البحث الخاص بالتنقل، ومعلومات النفاذ عبر Bluetooth وWi-Fi. وإذا قام المستخدم بتسجيل الدخول إلى سحابة مصنّع OEM، فسيتم منح التطبيقات الضرورية وظيفياً النفاذ بالتغيب إلى سحابة المصنّع OEM. ويوصى بأن يتحكم المستخدمون في نفاذ كل تطبيق إلى السحابة في الإعدادات.

وإذا تم النفاذ إلى المعلومات PII عن بُعد عن طريق القياسات التليماتية، يوصى بتشغيل الخدمات الموصولة باستيقان متعدد المستويات.

وبما أن البيانات متاحة عن طريق إجراء عمليات معالجة مختلفة للبيانات (الحساب والمعالجة الإحصائية وما إلى ذلك) بنسق مجفر (على سبيل المثال، باستخدام تجفير متماثل الشكل)، يمكن إجراء معالجة بيانات مماثلة على البيانات الموجودة في النظام VMS.

بيبليوغرافيا

[b-ITU-T X.1197 Amd1] Recommendation ITU-T X.1197 Amd.1 (2019), *Guidelines on Criteria for Selecting Cryptographic Algorithms for IPTV Service and Content Protection, Amendment 1*.

[b-ITU-T X.1811] Recommendation ITU-T X.1811 (2020), *Security Guidelines for Applying Quantum-Safe Algorithms in 5G Systems*.

[b-ETSI WP35] ETSI White Paper 35 (2020), *IPv6 Best Practices, Benefits, Transition Challenges and the Way Forward*. https://www.etsi.org/images/files/ETSIWhitePapers/etsi_WP35_IPv6_Best_Practices_Benefits_Transition_Challenges_and_the_Way_Forward.pdf

[b-IEEE 802.11] IEEE 802.11-2020, *IEEE Standard for Information Technology – Telecommunications and Information Exchange between Systems – Local and Metropolitan Area Networks – Specific Requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.*

[b-IETF RFC 2663] IETF RFC 2663 (1999), *IP Network Address Translator (NAT) Terminology and Considerations*.

[b-IETF RFC 8200] IETF RFC 8200 (July 2017), *Internet Protocol, Version 6 (IPv6) Specification.*

[b-IETF RFC 8216] IETF RFC 8216 (2017), *HTTP Live Streaming*.

[b-ISO/IEC 23009-1] ISO/IEC 23009-1:2019, *Information technology – Dynamic adaptive streaming over HTTP (DASH) – Part 1: Media presentation description and segment formats*.

[b-IAB] Internet Architecture Board (IAB) statement on IPv6 address exhaustion (November 2016). https://www.iab.org/2016/11/07/iab-statement-on-ipv6/ [Online].

[b-NIST SP 800-79-2] NIST Special Publication 800-79-2 (2015), *Guidelines for the Authorization of Personal Identity Verification Card Issues (PCI) and Derived PIV Credential Issuers (DPCI)*.

[b-USG OMB] US Office of Management and Budget (November 2020), *Memorandum for heads of executive departments and agencies*. https://www.whitehouse.gov/wp-content/uploads/2020/11/M-21-07.pdf [Online].

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، 2022