Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

X.1372

(03/2020)

SÉRIE X: RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

Applications et services sécurisés (2) – Sécurité des systèmes de transport intelligents

Lignes directrices relatives à la sécurité des communications de véhicule à tout autre élément (V2X)

Recommandation UIT-T X.1372

Union internationale des télécommunications

RECOMMANDATIONS UIT-T DE LA SÉRIE X

RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

RÉSEAUX PUBLICS DE DONNÉES	X.1–X.199
INTERCONNEXION DES SYSTÈMES OUVERTS	X.200–X.299
INTERFONCTIONNEMENT DES RÉSEAUX	X.300–X.399
SYSTÈMES DE MESSAGERIE	X.400–X.499
ANNUAIRE	X.500–X.599
RÉSEAUTAGE OSI ET ASPECTS SYSTÈMES	X.600–X.699
GESTION OSI	X.700–X.799
SÉCURITÉ	X.800–X.849
APPLICATIONS OSI	X.850–X.899
TRAITEMENT RÉPARTI OUVERT	X.900–X.999
SÉCURITÉ DE L'INFORMATION ET DES RÉSEAUX	
Aspects généraux de la sécurité	X.1000–X.1029
Sécurité des réseaux	X.1030–X.1049
Gestion de la sécurité	X.1050–X.1069
Télébiométrie	X.1080–X.1099
APPLICATIONS ET SERVICES SÉCURISÉS (1)	
Sécurité en multidiffusion	X.1100–X.1109
Sécurité des réseaux domestiques	X.1110–X.1119
Sécurité des télécommunications mobiles	X.1120–X.1139
Sécurité de la toile	X.1140–X.1149
Protocoles de sécurité (1)	X.1150–X.1159
Sécurité d'homologue à homologue	X.1160–X.1169
Sécurité des identificateurs en réseau	X.1170–X.1179
Sécurité de la télévision par réseau IP	X.1180–X.1199
SÉCURITÉ DU CYBERESPACE	
Cybersécurité	X.1200–X.1229
Lutte contre le spam	X.1230–X.1249
Gestion des identités	X.1250–X.1279
APPLICATIONS ET SERVICES SÉCURISÉS (2)	
Communications d'urgence	X.1300–X.1309
Sécurité des réseaux de capteurs ubiquitaires	X.1310–X.1319
Sécurité des réseaux électriques intelligents	X.1330–X.1339
Courrier certifié	X.1340–X.1349
Sécurité de l'Internet des objets (IoT)	X.1360–X.1369
Sécurité des systèmes de transport intelligents	**X.1370–X.1389**
Sécurité de la technologie des registres distribués	X.1400–X.1429
Sécurité de la technologie des registres distribués	X.1430–X.1449
Protocoles de sécurité (2)	X.1450–X.1459
ECHANGE D'INFORMATIONS SUR LA CYBERSÉCURITÉ	
Aperçu général de la cybersécurité	X.1500–X.1519
Echange concernant les vulnérabilités/les états	X.1520–X.1539
Echange concernant les événements/les incidents/l'heuristique	X.1540–X.1549
Echange de politiques	X.1550–X.1559
Heuristique et demande d'informations	X.1560–X.1569
Identification et découverte	X.1570–X.1579
Echange garanti	X.1580–X.1589
SÉCURITÉ DE L'INFORMATIQUE EN NUAGE	
Aperçu de la sécurité de l'informatique en nuage	X.1600–X.1601
Conception de la sécurité de l'informatique en nuage	X.1602–X.1639
Bonnes pratiques et lignes directrices concernant la sécurité de l'informatique en nuage	X.1640–X.1659
Mise en oeuvre de la sécurité de l'informatique en nuage	X.1660–X.1679
Sécurité de l'informatique en nuage (autres)	X.1680–X.1699
COMMUNICATIONS QUANTIQUES	
Terminologie	X.1700–X.1701
Générateur quantique de nombres aléatoires	X.1702–X.1709
Cadre de sécurité pour les réseaux QKDN	X.1710–X.1711
Conception de la sécurité pour les réseaux QKDN	X.1712–X.1719
Techniques de sécurité pour les réseaux QKDN	X.1720–X.1729
SÉCURITÉ DES DONNÉES	
Sécurité des mégadonnées	X.1750–X.1759
SÉCURITÉ DE LA 5G	X.1800–X.1819

Pour plus de détails, voir la Liste des Recommandations de l'UIT-T.

Recommandation UIT-T X.1372

Lignes directrices relatives à la sécurité des communications de véhicule à tout autre élément (V2X)

Résumé

La Recommandation UIT-T X.1372 donne des lignes directrices relatives à la sécurité des communications de véhicule à tout autre élément (V2X). L'expression V2X est un terme générique désignant les modes de communication de véhicule à véhicule (V2V), de véhicule à infrastructure (V2I), de véhicule à dispositif nomade (V2D) et de véhicule à piéton (V2P) examinés dans la présente Recommandation.

Des progrès importants ont été faits ces dernières années dans le domaine des communications de véhicule dans l'environnement des systèmes de transport intelligents (ITS). Les communications V2X permettent d'améliorer considérablement la sécurité sur les routes, de réduire les embouteillages et d'améliorer le confort. En revanche, elles rendent les entités intervenant dans l'environnement ITS vulnérables à différentes formes de cyberattaques.

Pour résoudre ce problème de sécurité, la présente Recommandation recense les menaces existant dans l'environnement des communications V2X et définit des exigences de sécurité pour ce type de communications afin de réduire ces menaces. Elle donne en outre une description d'une mise en œuvre possible de communications V2X sécurisées.

Historique

Edition	Recommandation	Approbation	Commission d'études	ID unique*
1.0	ITU-T X.1372	2020-03-26	17	11.1002/1000/14091

Mots clés

Analyse des risques, analyse des menaces, exigences de sécurité, sécurité des systèmes ITS, V2I, V2V, V2D, V2P, V2X.

* Pour accéder à la Recommandation, reporter cet URL http://handle.itu.int/ dans votre navigateur Web, suivi de l'identifiant unique, par exemple http://handle.itu.int/11.1002/1000/11830-en.

AVANT-PROPOS

L'Union internationale des télécommunications (UIT) est une institution spécialisée des Nations Unies dans le domaine des télécommunications et des technologies de l'information et de la communication (ICT). Le Secteur de la normalisation des télécommunications (UIT-T) est un organe permanent de l'UIT. Il est chargé de l'étude des questions techniques, d'exploitation et de tarification, et émet à ce sujet des Recommandations en vue de la normalisation des télécommunications à l'échelle mondiale.

L'Assemblée mondiale de normalisation des télécommunications (AMNT), qui se réunit tous les quatre ans, détermine les thèmes d'étude à traiter par les Commissions d'études de l'UIT-T, lesquelles élaborent en retour des Recommandations sur ces thèmes.

L'approbation des Recommandations par les Membres de l'UIT-T s'effectue selon la procédure définie dans la Résolution 1 de l'AMNT.

Dans certains secteurs des technologies de l'information qui correspondent à la sphère de compétence de l'UIT-T, les normes nécessaires se préparent en collaboration avec l'ISO et la CEI.

NOTE

Dans la présente Recommandation, l'expression "Administration" est utilisée pour désigner de façon abrégée aussi bien une administration de télécommunications qu'une exploitation reconnue.

Le respect de cette Recommandation se fait à titre volontaire. Cependant, il se peut que la Recommandation contienne certaines dispositions obligatoires (pour assurer, par exemple, l'interopérabilité et l'applicabilité) et on considère que la Recommandation est respectée lorsque toutes ces dispositions sont observées. Le futur d'obligation et les autres moyens d'expression de l'obligation comme le verbe "devoir" ainsi que leurs formes négatives servent à énoncer des prescriptions. L'utilisation de ces formes ne signifie pas qu'il est obligatoire de respecter la Recommandation.

DROITS DE PROPRIÉTÉ INTELLECTUELLE

L'UIT attire l'attention sur la possibilité que l'application ou la mise en œuvre de la présente Recommandation puisse donner lieu à l'utilisation d'un droit de propriété intellectuelle. L'UIT ne prend pas position en ce qui concerne l'existence, la validité ou l'applicabilité des droits de propriété intellectuelle, qu'ils soient revendiqués par un membre de l'UIT ou par une tierce partie étrangère à la procédure d'élaboration des Recommandations.

A la date d'approbation de la présente Recommandation, l'UIT avait été avisée de l'existence d'une propriété intellectuelle protégée par des brevets à acquérir pour mettre en œuvre la présente Recommandation. Toutefois, comme il ne s'agit peut-être pas de renseignements les plus récents, il est vivement recommandé aux développeurs de consulter la base de données des brevets du TSB sous http://www.itu.int/ITU-T/ipr/.

© UIT 2020

Tous droits réservés. Aucune partie de cette publication ne peut être reproduite, par quelque procédé que ce soit, sans l'accord écrit préalable de l'UIT.

TABLE DES MATIÈRES

Page

Recommandation UIT-T X.1372

Lignes directrices relatives à la sécurité des communications de véhicule à tout autre élément (V2X)

1 Domaine d'application

La présente Recommandation donne des lignes directrices relatives à la sécurité des communications de véhicule à tout autre élément (V2X). L'expression V2X est un terme générique désignant les modes de communication de véhicule à véhicule (V2V), de véhicule à infrastructure (V2I), de véhicule à dispositif nomade (V2D) et de véhicule à piéton (V2P) examinés dans le cadre de la présente Recommandation. Elle identifie les menaces existant dans l'environnement des communications V2X, définit des exigences de sécurité pour ce type de communications et donne une description d'une mise en œuvre possible de communications V2X sécurisées.

Les contrôles de sécurité pour les communications V2X ne relèvent pas du domaine d'application de la présente Recommandation.

2 Références

Les Recommandations UIT-T et autres références suivantes contiennent des dispositions qui, par suite de la référence qui y est faite, constituent des dispositions de la présente Recommandation. Au moment de la publication, les éditions indiquées étaient en vigueur. Les Recommandations et autres références étant sujettes à révision, les utilisateurs de la présente Recommandation sont invités à rechercher la possibilité d'appliquer les éditions les plus récentes des Recommandations et autres références énumérées ci-dessous. Une liste des Recommandations UIT-T en vigueur est publiée périodiquement. La référence à un document figurant dans la présente Recommandation ne donne pas à ce document en tant que tel le statut de Recommandation.

Aucune.

3 Définitions

3.1 Termes définis ailleurs

La présente Recommandation emploie les termes suivants définis ailleurs:

3.1.1 imputabilité [b-UIT-T X.800]: Propriété qui garantit que les actions d'une entité ne peuvent être imputées qu'à cette entité.

3.1.2 authenticité [b-UIT-T X.641]: Protection par authentification mutuelle et authentification de l'origine des données.

3.1.3 authentification [b-UIT-T X.1252]: Processus utilisé pour obtenir une confiance suffisante dans le lien entre l'entité et l'identité présentée.

NOTE – Dans un contexte de gestion d'identité (IdM), le terme authentification désigne l'authentification d'entité.

3.1.4 autorisation [b-UIT-T X.800]: Attribution de droits, comprenant la permission d'accès sur la base de droits d'accès.

3.1.5 disponibilité [b-UIT-T X.800]: Propriété d'être accessible et utilisable sur demande par une entité autorisée

3.1.6 autorité de certification (CA, *certification authority*) [b-UIT-T X.509]: Autorité jouissant de la confiance d'un ou de plusieurs utilisateurs pour la création et la signature numérique de certificats de clé publique. L'autorité de certification peut, de manière optionnelle, créer les clés des utilisateurs.

3.1.7 confidentialité [b-UIT-T X.800]: Propriété d'une information qui n'est ni disponible, ni divulguée aux personnes, entités ou processus non autorisés.

3.1.8 intégrité [b-UIT-T X.800]: Propriété assurant que des données n'ont pas été modifiées ou détruites de façon non autorisée.

3.1.9 code d'authentification de message (MAC, *message authentication code*) [b-UIT-T X.813]: Valeur de contrôle cryptographique utilisée pour assurer l'intégrité des données et l'authentification de leur origine.

3.1.10 dispositif nomade [b-UIT-T F.749.1]: Tous les types de dispositifs d'information et de communication, ainsi que tous les types de dispositifs de divertissement qui peuvent être amenés dans le véhicule par le conducteur ou les passagers et utilisés lorsque le véhicule roule, par exemple les téléphones mobiles, les ordinateurs portables, les tablettes, les dispositifs de navigation mobiles, des lecteurs média portables et des téléphones intelligents multifonctions.

3.1.11 non-répudiation avec preuve de l'origine [b-UIT-T X.800]: Le destinataire des données reçoit la preuve de l'origine des données. Cela le protégera de toute tentative de l'expéditeur de nier le fait qu'il a envoyé les données ou leur contenu.

3.1.12 pseudonyme [b-UIT-T X.1252]: Identificateur dont le lien avec une entité est inconnu ou n'est connu que dans une certaine mesure, dans le contexte dans lequel il est utilisé.

NOTE – Un pseudonyme peut permettre d'éviter ou de réduire les risques en matière de confidentialité associés à l'utilisation de liens d'identification susceptibles de divulguer l'identité de l'entité.

3.1.13 certificat de clé publique (PKC, *public key certificate*) [b-UIT-T X.509]: Clé publique d'une entité, associée à certaines autres informations qui sont rendues non falsifiables par signature numérique en utilisant la clé privée de l'autorité de certification émettrice.

3.2 Termes définis dans la présente Recommandation

La présente Recommandation définit le terme suivant:

3.2.1 comportement anormal: Comportement ayant pour effet qu'un dispositif envoie des informations erronées à cause desquelles d'autres dispositifs pourraient prendre des mesures erronées, ou qu'un dispositif prenne la mauvaise mesure bien qu'il ait reçu la bonne information.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

AES norme de chiffrement perfectionné (*advanced encryption standard*)

AVN audio, vidéo et navigation

CA autorité de certification (*certification authority*)

CAMP Crash Avoidance Metrics Partnership

CCM mode compteur avec code d'authentification de message à enchaînement de blocs de chiffrement (*counter mode with cipher block chaining message authentication code*)

CCU unité centrale de communication (*central communication unit*)

DDoS déni de service réparti (*distributed denial of service*)

EEBL feu électronique de freinage d'urgence (*electronic emergency brake light*)

ECDSA algorithme de signature numérique à courbe elliptique (*elliptic curve digital signature algorithm*)

ECIES système de chiffrement intégré à courbe elliptique (*elliptic curve integrated encryption scheme*)

ECU unité de commande électronique (*electronic control unit*)

GPS système mondial de localisation (*global positioning system*)

HDMI interface multimédia haute définition (*high-definition multimedia interface*)

ID identifiant

ITS système de transport intelligent (*intelligent transportation system*)

IVN réseau embarqué (*in-vehicle network*)

KDF fonction de calcul de clé (*key derivation function*)

LDM carte locale dynamique (*local dynamic map*)

LOS dans le champ de vision (*line of sight*)

LTE évolution à long terme (*long term evolution*)

MAC code d'authentification de message (*message authentication code*)

MHL liaison mobile à haute définition (*mobile high-definition link*)

NFC communication en champ proche (*near field communication*)

NGN réseaux de prochaine génération (*next generation networks*)

NLOS en dehors du champ de vision (*non-line of sight*)

OBD diagnostic embarqué (*on-board diagnostics*)

OBU unité embarquée (*on-board unit*)

PII informations d'identification personnelle (*personally identifiable information*)

PKI infrastructure de clé publique (*public key infrastructure*)

QoS qualité de service (*quality of service*)

RSU unité de bord de route (*road-side unit*)

SCMS système de gestion des justificatifs de sécurité (*security credential management system*)

SHA algorithme de hachage sécurisé (*secure hash algorithm*)

USB bus série universel (*universal serial bus*)

V2I de véhicule à infrastructure (*vehicle-to-infrastructure*)

V2D de véhicule à dispositif nomade (*vehicle to nomadic device)*

V2P de véhicule à piéton (*vehicle to pedestrian*)

V2V de véhicule à véhicule (*vehicle-to-vehicle*)

V2X de véhicule à tout autre élément (*vehicle to everything*)

VGP plate-forme de passerelle de véhicule (*vehicle gateway platform*)

VRU usager de la route vulnérable (*vulnerable road user*)

WAVE accès hertzien dans l'environnement des véhicules (*wireless access in vehicular environments*)

WiFi fidélité sans fil (*wireless fidelity*)

5 Conventions

Aucune.

6 Communications V2X

6.1 Aperçu

Un système de transport intelligent (ITS) comprend un large éventail de technologies de l'information et de la communication conçues afin d'améliorer la sécurité et l'efficacité du système de transport. Des progrès importants ont été accomplis ces dernières années, en particulier en ce qui concerne les systèmes de communication de véhicule.

Les systèmes de communication pour véhicule prennent en charge les échanges de données entre véhicules, entre les véhicules et l'infrastructure, ainsi qu'entre les véhicules et des dispositifs nomades. Les types de données échangées incluent des éléments tels que la position actuelle, la vitesse du véhicule et les avertissements provenant des capteurs embarqués. En outre, les unités de bord de route (RSU) peuvent offrir des liaisons de communication vers des systèmes de surveillance du trafic qui recueillent les alertes concernant des situations dangereuses et les transmettent aux véhicules à proximité. Toutefois, si la sécurité n'est pas assurée, un système ITS peut devenir un danger pour la sécurité routière ainsi que pour la vie humaine. Par conséquent, des études sont menées au sujet de la sécurité des systèmes ITS afin de permettre leur bon déploiement en toute sécurité.

La Figure 1 montre un aperçu des communications de véhicule. Ces communications peuvent être classées en deux catégories, selon qu'elles sont externes ou internes à un véhicule. Le réseau interne d'un véhicule, appelé réseau embarqué (IVN), rassemble les composants du véhicule tels que les capteurs et les unités de commandes électroniques (ECU). Les communications externes peuvent être classées en communication V2V, V2I, V2D et V2P. Les unités embarquées (OBU) sont les unités de communication sans fil embarquées dans les véhicules, tandis que les unités RSU sont les unités d'accès hertzien situées le long de la route. L'infrastructure comprend des unités RSU et des installations dorsales, comme les systèmes de gestion du trafic, les systèmes de surveillance, l'autorité de certification (CA). Les unités RSU peuvent être connectées aux installations dorsales via des réseaux filaires ou hertziens.

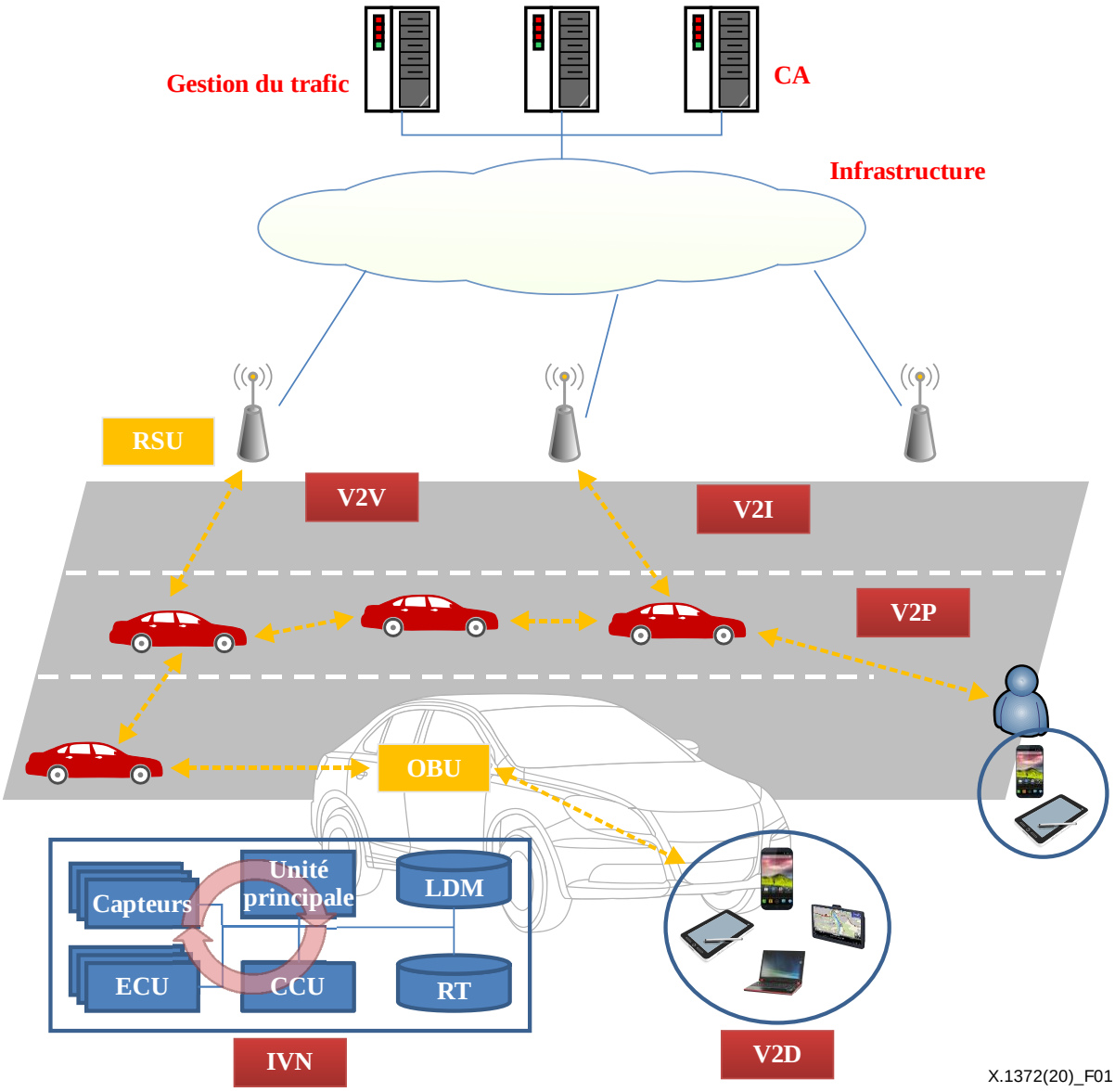


Figure 1 – Aperçu des communications de véhicule

6.2 Communications V2V

Les communications V2V comprennent la transmission sans fil de données entre véhicules. L'objectif de ces communications est d'empêcher les accidents grâce au partage et à l'envoi d'informations entre véhicules. En fonction du type de mise en œuvre de la technologie V2V, le véhicule pourra recevoir une alerte lui indiquant un possible risque d'accident. Le véhicule pourra alors prendre des mesures préventives, par exemple freiner pour ralentir. L'utilisation des communications V2V pour les pelotons routiers pourrait rendre possible la circulation en groupe grâce à l'échange de données concernant la vitesse et les conditions de circulation. En outre, un mode balise pourrait être utilisé pour l'échange d'informations entre véhicules afin de prendre en charge une conduite facile et sûre. Grâce aux communications V2V, un véhicule peut recueillir des informations comprenant la connaissance de son environnement à 360°.

Les scénarios de communication V2V ci-après peuvent être identifiés:

– Transmission d'avertissements V2V:

Dans un scénario de transmission d'avertissements V2V, un message d'avertissement est transmis d'un véhicule à l'autre. Par exemple, en cas d'accident de la circulation, un message d'alerte devrait être transmis à tous les véhicules arrivant en amont de l'accident, pour les informer qu'une collision a eu lieu plus loin sur la route. Par ailleurs, à l'approche d'un véhicule d'urgence, par exemple une voiture de police, un message d'avertissement devrait être transmis à tous les véhicules se trouvant à proximité et devant le véhicule d'urgence afin que celui-ci puisse passer en toute sécurité sans avoir à ralentir. La Figure 2 illustre une situation dans laquelle un message est transmis aux véhicules arrivant en amont pour les avertir qu'un accident a eu lieu plus loin sur la route, tandis que la Figure 3 illustre une situation dans laquelle un véhicule d'urgence arrive par l'arrière et le message d'avertissement est transmis aux véhicules qui le précèdent.

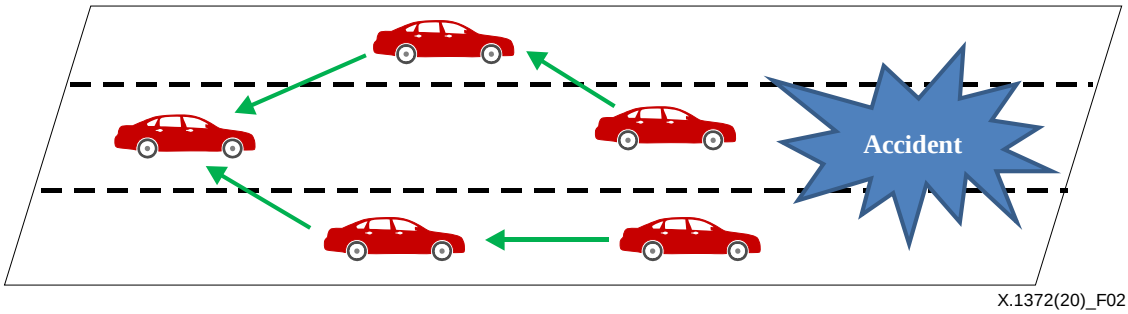


Figure 2 – Diffusion d'avertissements V2V – Diffusion vers les véhicules arrivant en amont

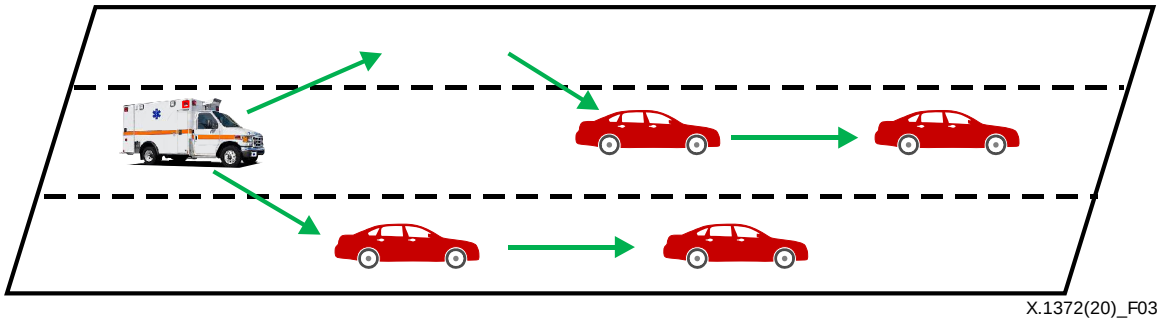


Figure 3 – Diffusion d'avertissements V2V – Diffusion vers les véhicules arrivant en aval

– Communications V2V en mode peloton:

Dans un scénario de communications V2V en mode peloton, plusieurs véhicules constituent un groupe et peuvent communiquer entre eux à l'intérieur de ce groupe. Par exemple, des véhicules suivant le même itinéraire, au moins pendant un certain temps, peuvent former un peloton. Des informations sur l'état des véhicules peuvent être communiquées dans ce groupe afin de renforcer la sécurité au volant. La Figure 4 montre les communications V2V en mode peloton.

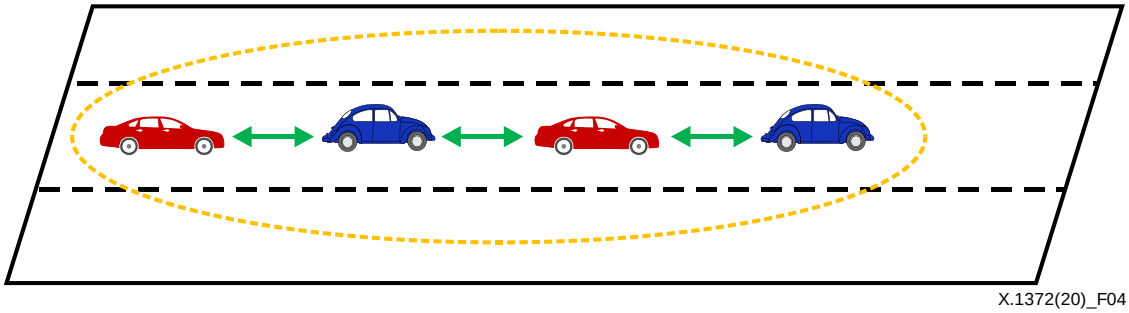


Figure 4 – Communications V2V en mode peloton

– Communications V2V en mode balise:

Dans un scénario de communications V2V en mode peloton, chaque véhicule envoie régulièrement aux véhicules à proximité les informations sur son état, telles que sa vitesse actuelle, sa direction et sa position. La Figure 5 montre les communications V2V en mode balise.

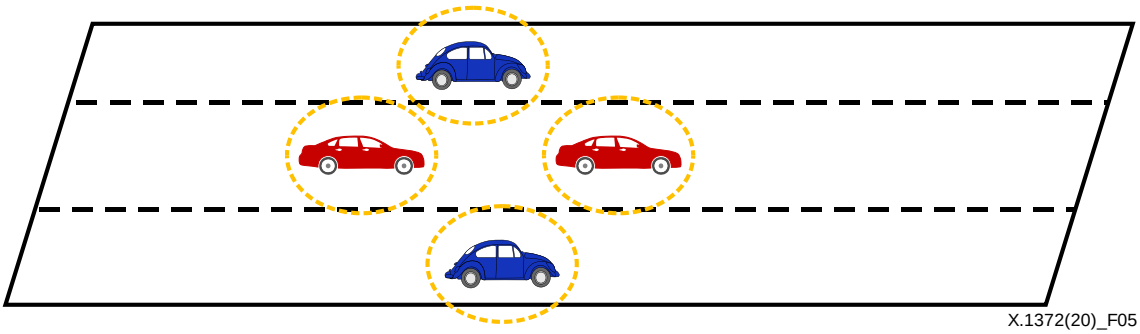


Figure 5 – Communications V2V en mode balise

6.3 Communications V2I

On entend par communications de véhicule à infrastructure (V2I) la transmission sans fil de données entre un véhicule et l'infrastructure, par exemple une unité de bord de route (RSU).

Les scénarios de communications V2I ci-après peuvent être identifiés:

– Avertissements V2I:

Le scénario d'avertissements V2I permet à un véhicule et à l'infrastructure, par exemple des unités RSU, de communiquer. Par exemple, lorsqu'un accident se produit à une intersection, une unité RSU pourrait envoyer un message d'avertissement aux véhicules qui approchent de l'intersection. Les alertes indiquant la présence d'un véhicule à proximité lorsqu'un conducteur souhaite bifurquer à droite ou à gauche à une intersection ou lors d'un rétrécissement de voie sont d'autres cas d'utilisation des communications V2I. La Figure 6 donne un exemple de scénario d'avertissement V2I.

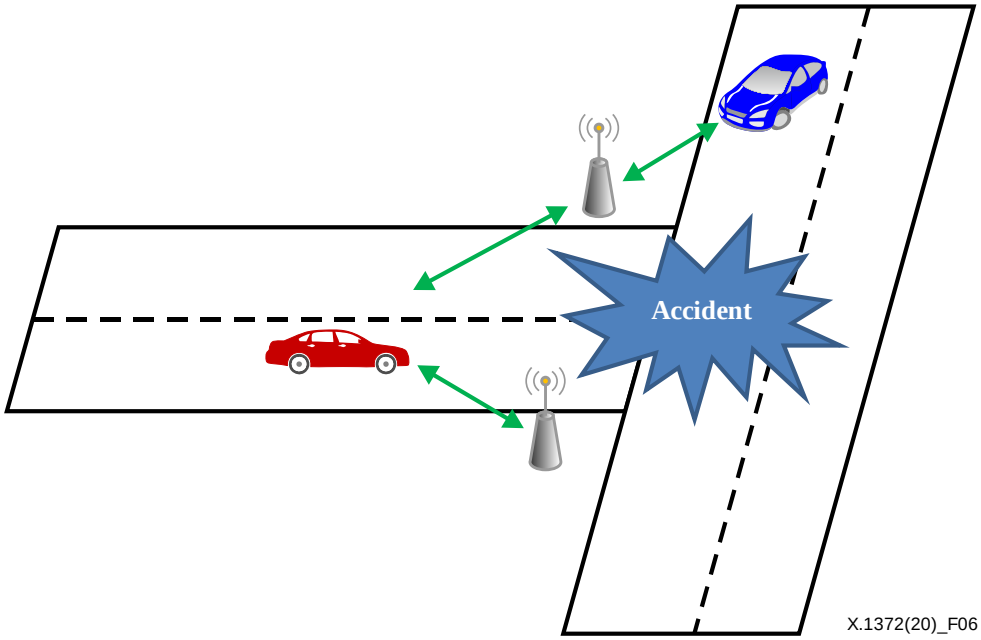


Figure 6 – Avertissement V2I

– Échange d'informations V2I (y compris V2V):

L'échange d'informations V2I peut concerner des informations comme l'affichage/les informations embarqués, des informations sur la phase des signaux et la durée des feux de circulation, des données relatives au véhicule fournies par des capteurs, des informations comptables (par exemple, péage), des informations sur les conditions d'adhérence/météorologiques/de visibilité et sur les zones de chantier rencontrées. Les cas d'utilisation sont par exemple les suivants:

- Téléchargement de données simples sur le transport:

  Dans un système ITS, un certain nombre de messages V2I peuvent contenir des messages d'avertissement. Pour traiter ces messages, un véhicule a souvent besoin d'une carte de son emplacement actuel ou de son lieu de destination ou il pourra avoir besoin d'informations en temps réel sur son environnement. Ces informations sont souvent téléchargées depuis l'infrastructure, par exemple les unités RSU.

- Données pour appuyer l'efficacité des transports:

  Dans un système ITS, un véhicule peut communiquer ponctuellement avec l'infrastructure afin d'obtenir des informations sur les conditions de circulation, par exemple sur les mesures de restriction temporaire de circulation, etc. Ainsi, un véhicule peut connaître l'emplacement des embouteillages pour pouvoir optimiser son itinéraire avec l'aide de l'infrastructure, par exemple en actualisant son itinéraire grâce à un navigateur permettant de se connecter au réseau mobile. Par conséquent, l'utilisation des communications V2I peut améliorer l'efficacité des véhicules. Autre exemple, l'infrastructure peut elle aussi actualiser les informations sur le trafic sur la base du message fourni par le véhicule grâce aux communications V2I. La Figure 7 montre l'échange d'informations V2I.

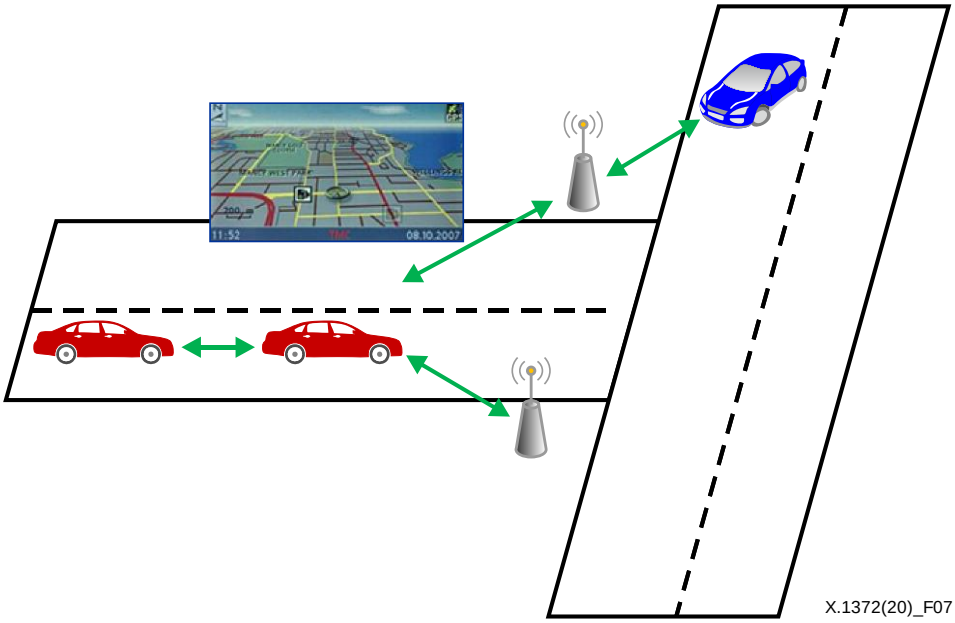


Figure 7 – Échange d'informations V2I

6.4 Communications V2D

Avec la technologie de communications V2D, un véhicule est connecté à des dispositifs mobiles tels que les téléphones intelligents, les ordinateurs portables et les systèmes de navigation qui se trouvent à l'intérieur du véhicule, par l'intermédiaire d'une architecture ouverte comprenant une interface normalisée avec le bus du gestionnaire de réseau de communication (CAN, *controller area network*) du véhicule ou moyennant la mise en œuvre d'une passerelle qui transmet les demandes/réponses du dispositif nomade au système exploité sur le véhicule. Il est possible d'utiliser un téléphone intelligent ou un téléphone mobile pour fournir des fonctions à distance afin d'identifier et de gérer les informations sur l'état du véhicule, par exemple sur les pièces d'entretien. En outre, d'autres services pratiques devraient être mis au point.

Par exemple, pour organiser un déplacement, lorsqu'un conducteur choisit une destination sur un dispositif nomade, le dispositif nomade peut ensuite planifier l'itinéraire en recoupant différentes informations provenant de différentes sources, par exemple les horaires des transports publics (train, métro, bus, etc.) ainsi que les informations sur le trafic en temps réel. Le véhicule suit l'itinéraire planifié et fait des détours en cas de modification à court terme des conditions de circulation. Non seulement le dispositif nomade prend des décisions concernant les manœuvres et les exécute, mais il réagit également en fonction des conditions de circulation au niveau local, par exemple en suivant d'autres véhicules, en évitant des obstacles, en changeant de files ou encore en s'arrêtant aux feux rouges. Ce dispositif nomade peut être connecté aux réseaux embarqués. Par conséquent, l'auteur d'une attaque pourrait avoir la possibilité d'accéder aux systèmes internes d'un véhicule. En cas de menaces pour la sécurité utilisant le Bluetooth, un code malveillant peut être exécuté via des applications installées sur un téléphone intelligent connecté au véhicule. Les systèmes audio, vidéo et de navigation (AVN) embarqués sont vulnérables aux attaques par microprogramme via les mémoires de stockage multimédia et peuvent être facilement piratés via le système mondial de localisation (GPS) ou les canaux de communication par satellite. Il convient de lutter contre les attaques menées via des dispositifs nomades afin d'éviter de mettre en danger la sécurité du véhicule.

Deux types différents de communications V2D sont décrits ci-après:

– Communications V2D par liaison indirecte:

  Les véhicules et les dispositifs nomades peuvent communiquer par des liaisons indirectes, ce qui signifie qu'un équipement tiers tel qu'un point d'accès ou un routeur assure les communications entre les nœuds d'extrémité. Les téléphones cellulaires et les téléphones intelligents utilisent une technologie large bande mobile sans fil comme la technologie évolution à long terme (LTE) ou fidélité sans fil (WiFi). L'utilisation de la technologie WiFi dans les téléphones intelligents pour communiquer avec des véhicules est de plus en plus fréquente. Les technologies 5G sont elles aussi un canal de communication privilégié pour ces liaisons indirectes.

– Communications V2D par liaison directe:

  Les véhicules et les dispositifs nomades peuvent communiquer par des liaisons directes sans intermédiaire ou via des technologies de communication sans fil comme les technologies Bluetooth, ZigBee et communication en champ proche (NFC).

  Les véhicules et les dispositifs nomades peuvent également communiquer par des liaisons filaires. Par exemple, il est possible de connecter physiquement un dispositif nomade à un véhicule en utilisant un bus série universel (USB), une liaison mobile haute définition (MHL) ou une interface multimédia haute définition (HDMI). La norme OBD II (diagnostics embarqués II) spécifie les interfaces de diagnostic et donne en outre une liste des paramètres du véhicule et des procédures possibles pour la transmission des données.

  Les communications V2P pourraient être considérées comme un cas particulier des communications V2D lorsque le véhicule communique avec un dispositif nomade associé à un piéton.

  Les communications V2P ont des applications pour un large éventail d'usagers de la route vulnérables, dont les usagers non motorisés comme les piétons et les cyclistes, ainsi que pour les motocyclistes et les personnes handicapées ou à mobilité réduite.

  En raison du nombre élevé d'accidents de la circulation impliquant des usagers vulnérables, les systèmes ITS proposent des solutions pour améliorer la sécurité routière grâce à la collecte de données fournies par des capteurs ainsi qu'à des concepts tels que la collecte d'information et la prise en charge d'échanges d'informations entre les véhicules et les piétons. Point encore plus important, les communications V2P permettront non seulement d'avertir le conducteur d'un véhicule qu'un piéton approche, afin qu'il arrête son véhicule, mais elles permettront également d'envoyer une alerte sur le téléphone mobile du piéton pour indiquer qu'un véhicule approche.

  Un système ITS peut détecter les usagers de la route vulnérables et contribuer à éviter les collisions entre un véhicule et un usager vulnérable. La Figure 8 illustrant le cas d'un piéton situé dans le champ de vision d'un automobiliste et la Figure 9 celui d'un piéton en dehors du champ de vision d'un automobiliste montrent comment un système ITS peut améliorer la sécurité des usagers vulnérables.

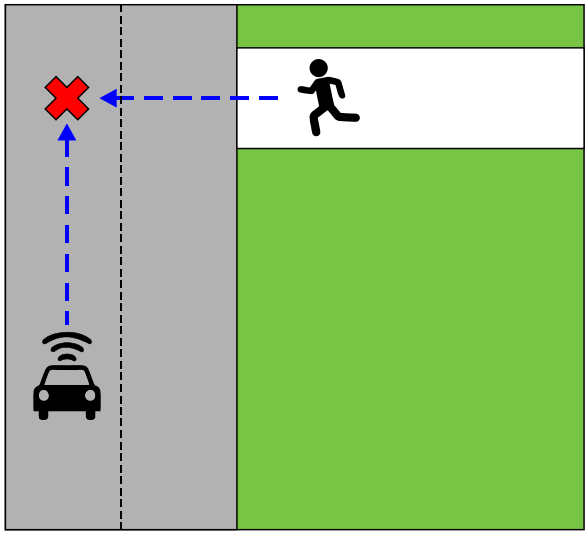


Figure 8 – Piéton dans le champ de vision

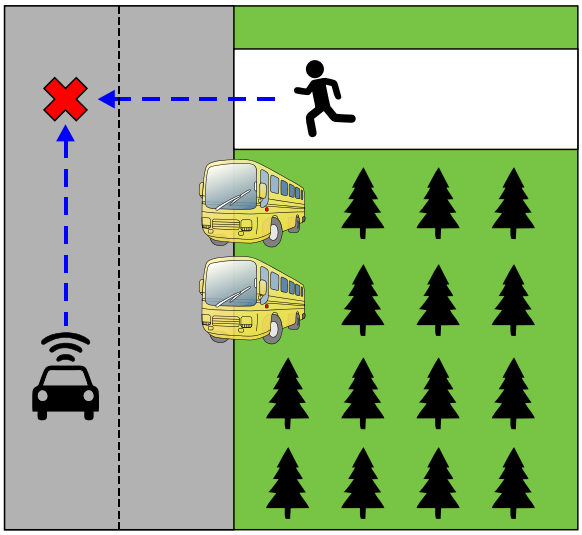


Figure 9 – Piéton en dehors du champ de vision

– Piéton dans le champ de vision du conducteur:

  Comme on le voit sur la Figure 8, des capteurs actifs, comme des radars, des capteurs ultrason, des télémètres lasers et des caméras vidéo adoptent des méthodes fondées sur la vision par ordinateur applicables à la détection des piétons lorsque ceux-ci sont visibles depuis le véhicule. Lorsqu'un piéton approche, le véhicule en déplacement le détecte et peut alors prendre la décision qui s'impose. Parallèlement, le véhicule peut envoyer une alerte sur le téléphone cellulaire du piéton pour prévenir celui-ci du danger potentiel.

– Piéton en dehors du champ de vision du conducteur:

  La capacité de détection des piétons est limitée par le champ de vision des capteurs. Dans la Figure 9, le piéton est caché par des obstacles, par exemple des arbres ou des bus en stationnement. Les communications de véhicule permettent toutefois d'annoncer et de diffuser des informations concernant des éléments qui ne sont pas dans le champ de vision des capteurs. Dès que le véhicule reçoit la notification d'une alerte, il met à jour sa carte locale dynamique (LDM) et évalue le caractère critique de la situation pour prendre une décision. Parallèlement, le piéton reçoit une notification d'alerte sur son téléphone cellulaire.

7 Menaces identifiées

7.1 Menaces pour la confidentialité

Les menaces pour la confidentialité décrites dans le présent paragraphe sont illustrées dans la Figure 10.

– Interception:

  L'auteur d'une attaque peut "renifler" (c'est-à-dire lire et/ou enregistrer) les messages V2V des véhicules situés à proximité et les messages V2I des unités RSU, puis analyser les informations sur le trafic en traitant les messages reniflés.

  L'auteur d'une attaque peut renifler des messages V2D échangés entre une unité centrale de communication et un dispositif nomade et ensuite analyser les informations dynamiques concernant le véhicule, comme son emplacement et sa vitesse.

  L'auteur d'une attaque peut renifler des messages V2P et provoquer une situation dangereuse pour le piéton.

– Fuite des informations d'identification personnelle:

L'auteur d'une attaque peut analyser des informations afin de savoir qui est le propriétaire d'un véhicule en collectant les messages V2X du véhicule et en suivant sa localisation sur le trajet pour une personne donnée.

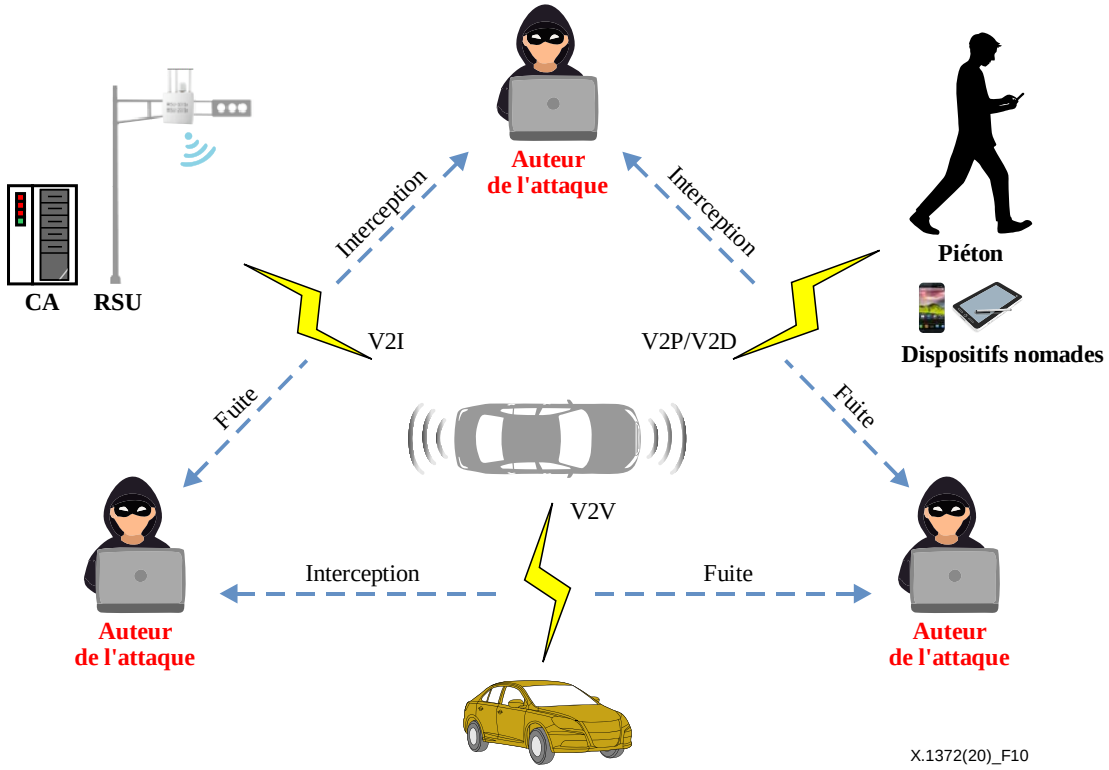


Figure 10 – Menaces pour la confidentialité

7.2 Menaces pour l'intégrité

Les menaces pour l'intégrité décrites dans le présent paragraphe sont illustrées dans la Figure 11.

– Manipulation des messages de routage:

Un nœud intermédiaire malveillant modifie le message de routage; les véhicules recevront alors des informations fausses.

– Manipulation des informations relatives aux justificatifs:

La manipulation des justificatifs signifie que la clé privé ou l'identité du véhicule (identifiant) est modifiée, de telle sorte que l'auteur d'une attaque peut utiliser les informations relatives aux justificatifs d'un autre véhicule sans autorisation.

– Manipulation des informations fournies par les capteurs:

L'auteur d'une attaque peut modifier l'adresse physique d'un module de communication ou manipuler les informations fournies par l'ECU, comme celles provenant du capteur de vitesse. En outre, de nombreux autres capteurs sont installés sur un véhicule, comme le radar et la caméra, pour aider à la conduite. Des données de capteur fausses comme la latitude, la longitude, l'altitude, la vitesse, la direction, l'angle de braquage des roues et l'accélération, pourraient être fournies à d'autres unités embarquées ou unités RSU. Ces données manipulées pourraient entraîner des perturbations du trafic. Par exemple, une valeur d'accélération fausse pourrait amener les véhicules à proximité à déclencher leurs feux électroniques de freinage

d'urgence (EEBL) pour réduire les risques de collision impliquant plusieurs véhicules, même si les conditions réelles de circulation sont bonnes.

– Manipulation d'une application sur un dispositif nomade:

Une application manipulée peut nuire au bon fonctionnement d'un véhicule via l'interface de communication V2V. Par exemple, cette application peut forcer le dispositif nomade à envoyer un grand nombre de messages inoffensifs à un véhicule, pratique appelée inondation de messages. Par ailleurs, l'application peut injecter un code malveillant dans une unité embarquée et envoyer un message nécessitant d'importantes ressources de calcul. L'application manipulée peut également envoyer un grand nombre de messages d'une taille bien plus grande que la capacité de stockage disponible sur l'unité embarquée.

– Attaque par rejeu:

L'auteur d'une attaque peut intercepter des messages V2V provenant de véhicules à proximité et des messages V2I provenant des unités RSU. Il peut ensuite repasser ces messages ou informations à des fins malveillantes.

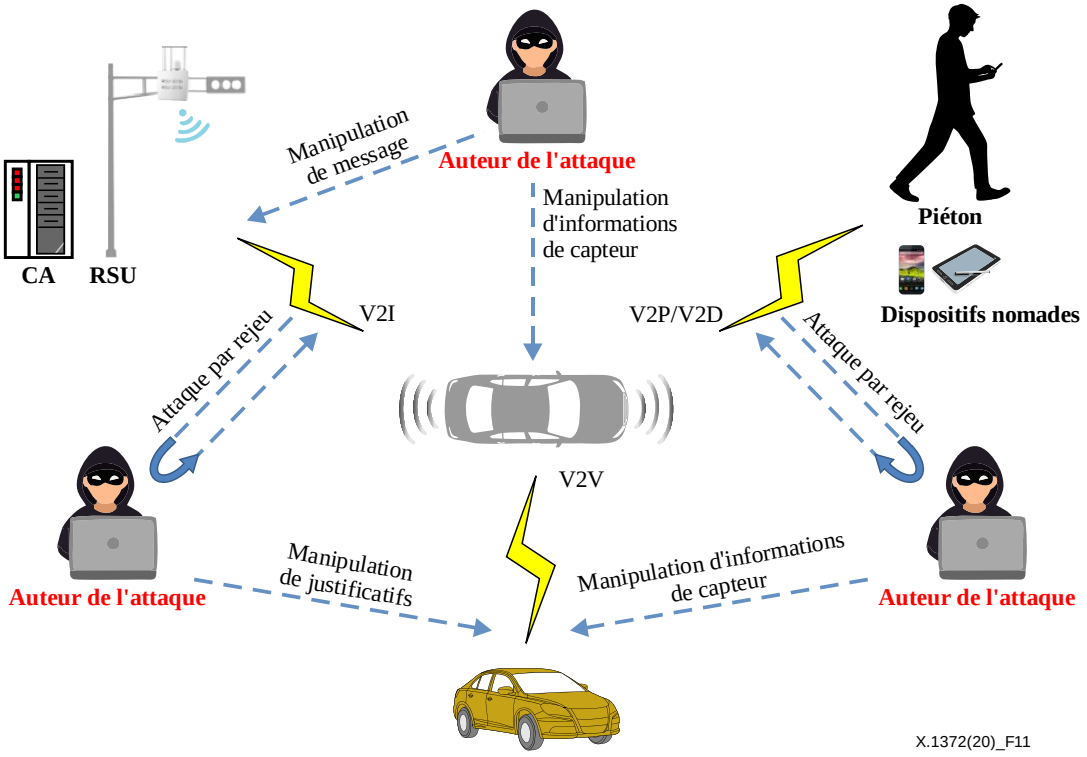


Figure 11 – Menaces pour l'intégrité

7.3 Menaces pour la disponibilité

Les menaces pour la disponibilité décrites dans le présent paragraphe sont illustrées dans la Figure 12.

– Brouillage intentionnel et attaque par déni de service réparti (DDoS) sur le canal de communication V2X:

L'auteur d'une attaque peut envoyer un grand nombre de messages inutiles. Cette pratique est appelée inondation de messages. La réexpédition d'un message particulier uniquement par un nœud de routage peut être considérée comme une attaque de ce type.

– Attaque DDoS visant l'unité embarquée:

L'auteur d'une attaque peut injecter des codes malveillants dans une unité embarquée et envoyer des messages nécessitant d'importantes ressources de calcul. Il peut également

envoyer des messages qui, pris tous ensemble, ont une taille plus importante que la capacité de stockage de l'unité embarquée. En particulier, des mises à jour logicielles fréquentes sans autorisation constituent un exemple d'attaque grave de ce type.

– Attaque temporelle:

Une attaque temporelle consiste, par exemple, à retarder la fourniture d'un message de sécurité aux autres véhicules. Elle peut par conséquent empêcher le bon fonctionnement de services de communication V2X utiles, comme la diffusion de messages d'avertissement.

– Piratage de capteurs:

Les capteurs peuvent faire l'objet d'attaques et provoquer des défaillances, l'objectif étant de fournir de mauvaises valeurs. En général, deux types de défaillances peuvent se produire dans le capteur: les défaillances transitoires ou les défaillances permanentes. Une défaillance transitoire peut se produire alors que le système fonctionne normalement et disparaître rapidement. Dans la pratique, la plupart des capteurs appliquent un modèle en cas de défaillance transitoire qui limite la durée pendant laquelle ils fournissent des mesures erronées. Par exemple, il n'est pas rare qu'un GPS perde la connexion avec les satellites (ou reçoivent des signaux brouillés), en particulier dans les villes où les bâtiments sont hauts. De même, un capteur transmettant des données sur un réseau surchargé (par exemple, en utilisant le protocole TCP/IP avec des retransmissions) risque de ne pas pouvoir fournir les mesures qu'il a effectuées dans les délais, d'où des informations incorrectes lorsque les messages arrivent. Toutefois, parce qu'elles sont très brèves, les défaillances transitoires ne devraient pas être considérées comme une menace pour la sécurité du système.

À l'inverse, les défaillances permanentes sont des défauts de capteur qui durent plus longtemps et peuvent nuire considérablement au bon fonctionnement du système. Par exemple, un capteur peut être endommagé, entraînant un biais permanent des mesures effectuées. Dans ce scénario, à moins que la défaillance puisse être corrigée par le logiciel, il serait préférable que le système ne tienne pas du tout compte du capteur endommagé.

En fonction de l'objectif de l'auteur de l'attaque, les attaques visant les mesures effectuées par les capteurs peuvent entraîner des défaillances transitoires ou permanentes. Ces défaillances ont chacune leurs avantages et inconvénients pour l'auteur de l'attaque. Faire en sorte que le capteur se comporte comme s'il y avait une défaillance transitoire peut permettre à l'auteur d'une attaque de passer inaperçu mais limite aussi ses capacités, tandis qu'une attaque plus longue imitant une défaillance permanente sera plus grave, mais pourrait être repérée plus rapidement.

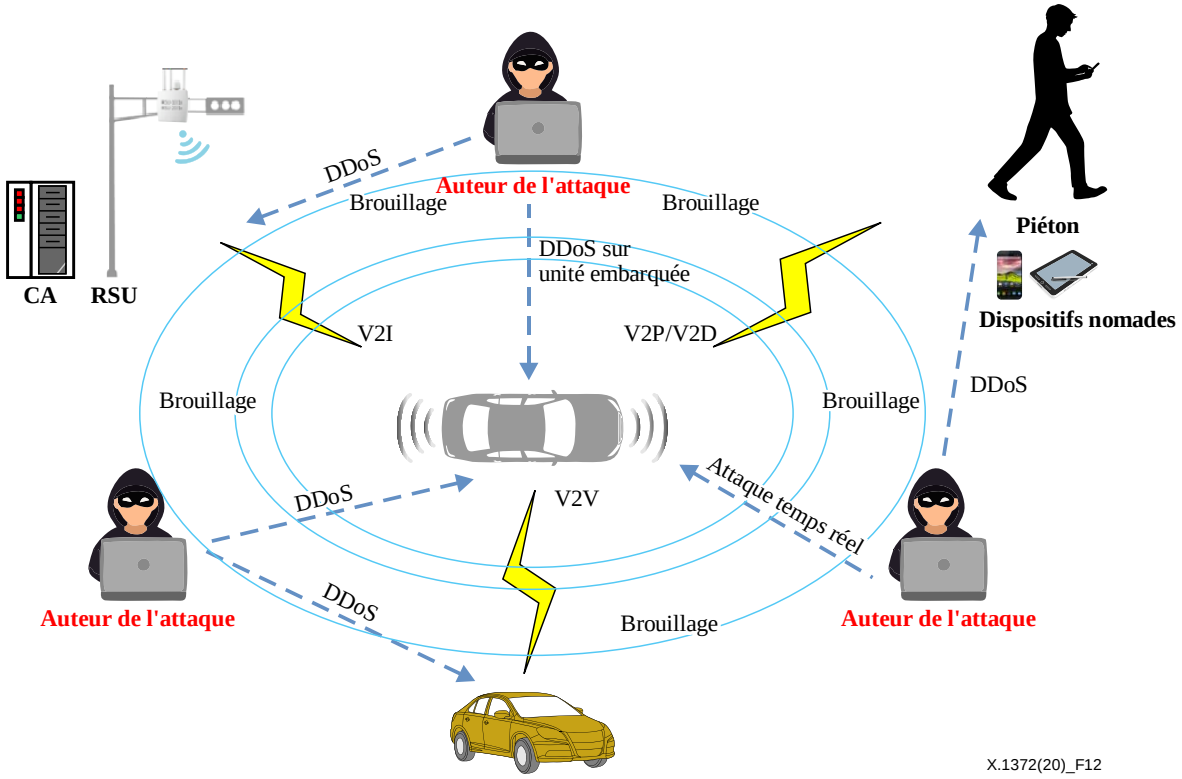


Figure 12 – Menaces pour la disponibilité

7.4 Menaces pour la non-répudiation

Les menaces pour la non-répudiation décrites dans le présent paragraphe sont illustrées dans la Figure 13.

– Manipulation de la base de données de certification:

  L'auteur d'une attaque peut manipuler la base de données de pseudonymes dans l'autorité de certification, puis modifier la relation entre un certificat à long terme et un certificat de pseudonyme à court terme.

– Accès non autorisé aux justificatifs:

  L'auteur d'une attaque peut avoir accès à une clé privée et à un certificat sans autorisation. Si la clé privée est exposée, alors la non-répudiation du véhicule, de l'unité RSU et du dispositif nomade ne peut pas être assurée.

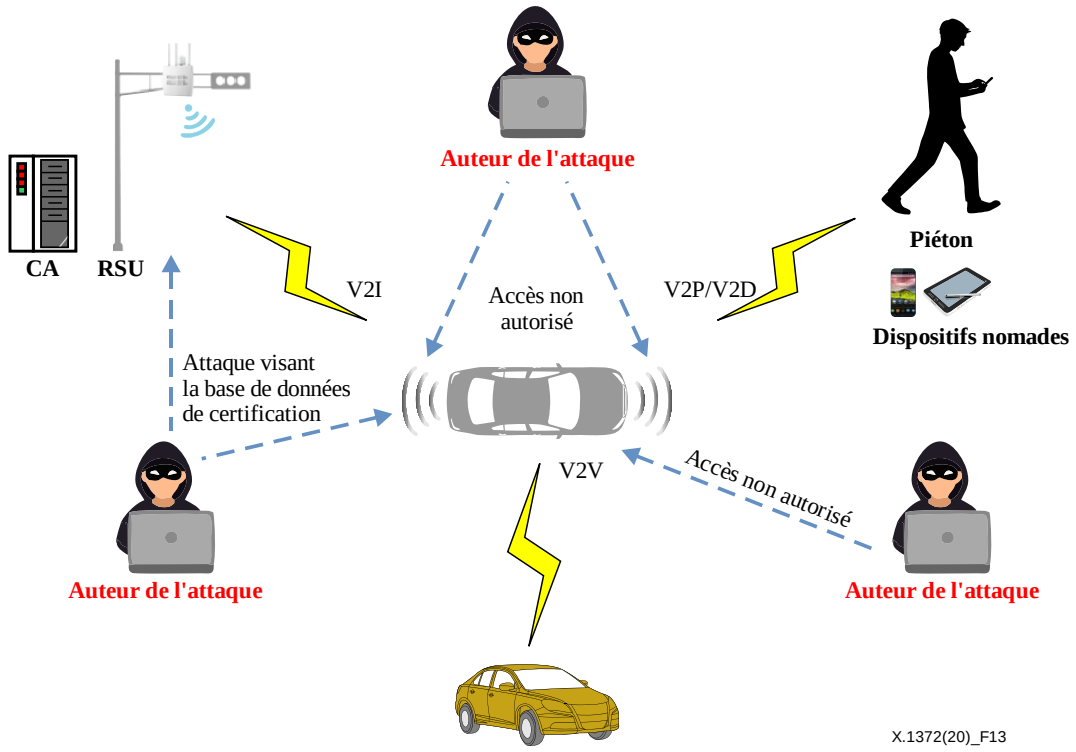


Figure 13 – Menaces pour la non-répudiation

7.5 Menaces pour l'authenticité

Les menaces pour l'authenticité décrites dans le présent paragraphe sont illustrées dans la Figure 14.

– Attaque par modification de la table de routage et de la carte locale dynamique (LDM):

  L'auteur d'une attaque peut imiter les informations GPS d'un véhicule et modifier les informations géospatiales originales.

– Attaque par usurpation d'identité:

  L'auteur d'une attaque peut se faire passer pour une autre entité en dérobant les informations d'identité de cette autre entité. Il peut ensuite recevoir les messages qui sont normalement destinés à l'autre entité et également envoyer des messages comme s'ils étaient générés normalement par l'autre entité. Par exemple, si l'autre entité est un véhicule d'urgence, l'auteur d'une attaque peut envoyer un message aux véhicules à proximité de type "Je suis un véhicule d'urgence, merci de vous ranger pour me laisser passer".

  L'auteur d'une attaque peut également envoyer un faux signal de dysfonctionnement au nom d'un véhicule qui n'a pas de problème, lequel pourrait être ensuite révoqué par l'autorité de certification.

– Attaque Sybil:

  On parle d'attaque Sybil, par exemple, lorsqu'un véhicule unique simule de multiples véhicules en utilisant des multiples identifiants de véhicules.

– Attaque par analyse des pseudonymes:

  L'auteur d'une attaque peut analyser la relation entre les identifiants des véhicules et les pseudonymes pour trouver les multiples pseudonymes utilisés pour le même véhicule.

– Manipulation de la base de données de certification:

  L'auteur d'une attaque peut manipuler la base de données de pseudonymes dans l'autorité de certification. Il peut ensuite modifier la relation entre un certificat à long terme et un certificat de pseudonyme à court terme.

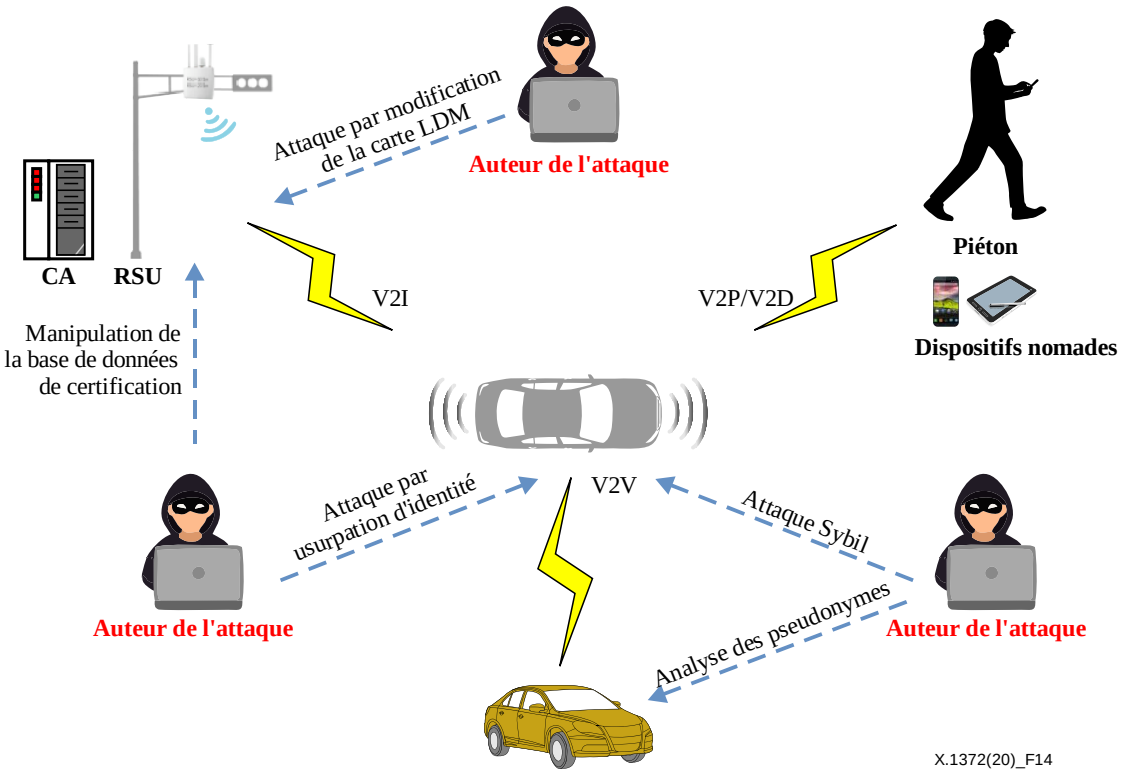


Figure 14 – Menaces pour l'authenticité

7.6 Menaces pour l'imputabilité

Les menaces pour l'imputabilité décrites dans le présent paragraphe sont illustrées dans la Figure 15.

– Duplication non autorisée d'un dispositif nomade:

  Pour certains services particuliers, par exemple les diagnostics embarqués, il est nécessaire qu'un dispositif nomade autorisé puisse accéder à l'unité centrale de communication d'un véhicule. Or, si l'autorisation de ce dispositif est copiée par des dispositifs malveillants, ce qui peut survenir par exemple en cas d'utilisation du compte du dispositif autorisé par un autre dispositif malveillant, le dispositif malveillant en question peut accéder à l'unité centrale de communication d'un véhicule, laquelle pourrait alors être manipulée par un dispositif nomade non autorisé.

– Duplication non autorisée d'un véhicule et d'une unité RSU:

  Lorsque l'auteur d'une attaque s'empare de l'identité d'un véhicule et d'une unité RSU (qu'il la duplique), le véritable véhicule et la véritable unité RSU perdent leur imputabilité.

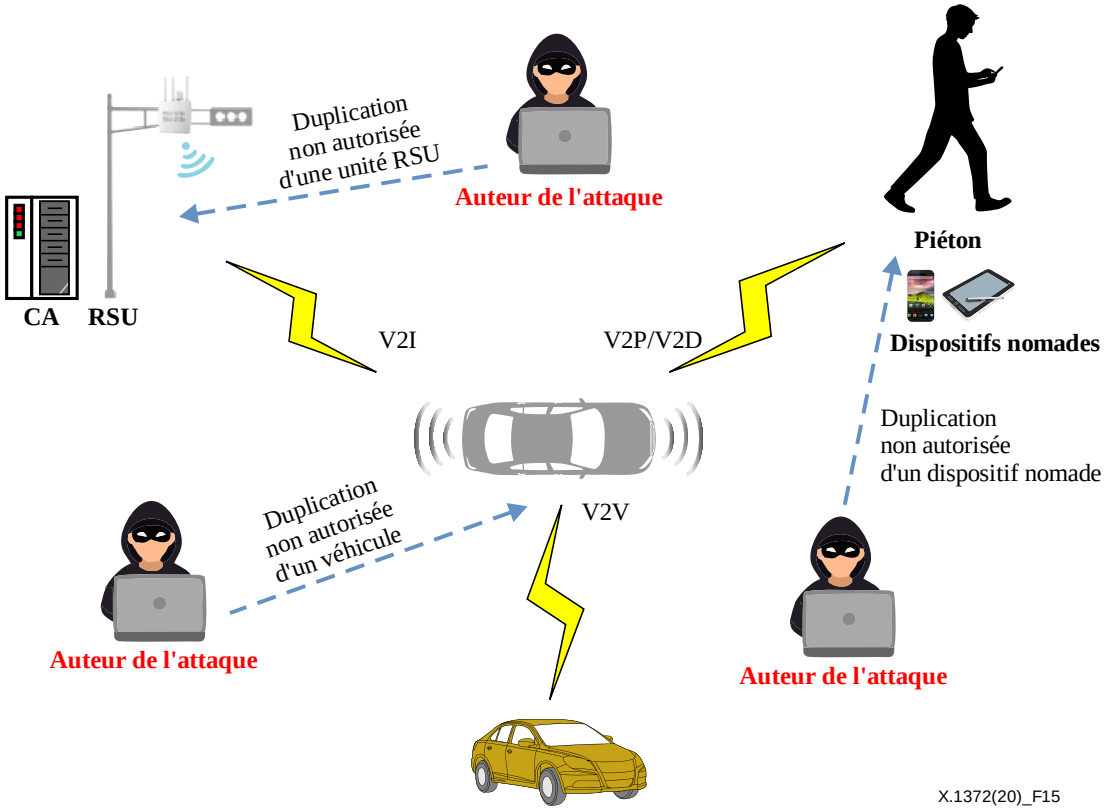


Figure 15 – Menaces pour l'imputabilité

7.7 Menaces pour l'autorisation

Les menaces pour l'autorisation décrites dans le présent paragraphe sont illustrées dans la Figure 16.

– Accès non autorisé à des informations essentielles pour la sécurité d'un véhicule:

  En l'absence de contrôle d'autorisation, une application ou un utilisateur malveillant peut commander un véhicule sans autorisation. Par exemple, l'application destinée à mettre de la musique dans un véhicule ne devrait pas être autorisée à accéder à des informations essentielles pour la sécurité, comme la vitesse du véhicule et l'état des freins.

  L'auteur d'une attaque qui agit sans autorisation peut également manipuler, effacer ou remplacer des données essentielles pour la sécurité du véhicule, y compris des paramètres tels que le seuil de déclenchement du système de freinage ou de l'airbag en cas d'urgence, ainsi que le journal du système.

  Dans le cas d'un véhicule électrique, l'auteur d'une attaque qui agit sans autorisation peut manipuler les paramètres de configuration des fonctions de recharge du véhicule.

– Utilisation de dispositifs nomades pour accéder sans autorisation à certaines fonctions dans un véhicule:

  Il est essentiel de définir des fonctions de contrôle d'accès pour les dispositifs nomades qui se connectent à un véhicule. Ces dispositifs sont généralement utilisés comme outils audio, vidéo et de navigation dans le véhicule et leurs contenus peuvent en outre s'afficher sur l'unité multimédia principale. Des fonctionnalités non autorisées, comme l'utilisation d'un dispositif nomade pour communiquer avec une passerelle centrale dans le véhicule, peut nuire gravement à la sécurité.

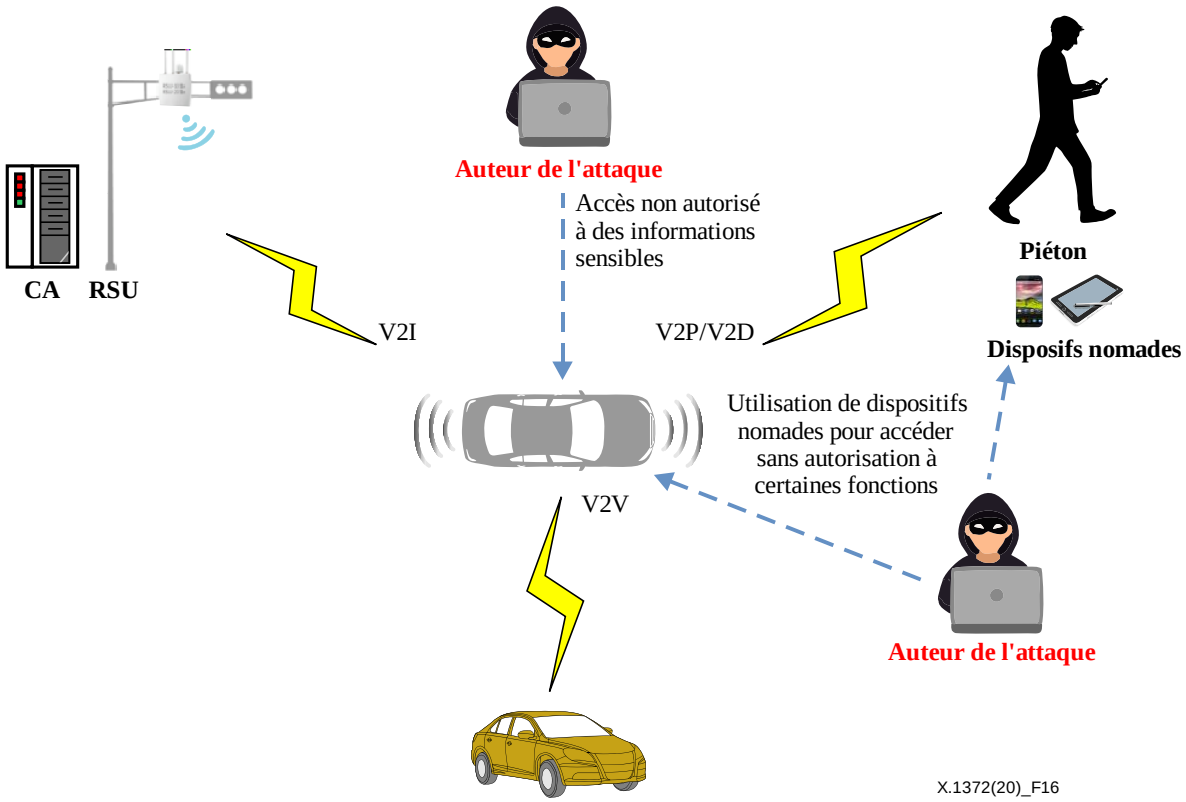


Figure 16 – Menaces pour l'autorisation

8 Exigences de sécurité

Les paragraphes ci-après décrivent les exigences de sécurité pour les communications V2X. Les paragraphes 8.1 à 8.7 décrivent les exigences de sécurité relatives aux communications V2X et le paragraphe 8.8 contient des précisions complémentaires concernant ces exigences.

8.1 Confidentialité

Une entité non autorisée ne devrait pas pouvoir révéler les messages échangés entre véhicules, entre les véhicules et l'infrastructure, entre les véhicules et les dispositifs nomades et entre les véhicules et les piétons.

Une entité non autorisée ne devrait pas pouvoir analyser l'identification d'une personne grâce aux informations d'identité personnelle (PII) contenues dans les messages, comme l'emplacement ou l'itinéraire suivi par une personne donnée.

8.2 Intégrité

Les messages envoyés ou reçus par un véhicule, une unité RSU ou un dispositif nomade devraient être protégés contre les modifications et les suppressions non autorisées.

8.3 Disponibilité

Une entité devrait pouvoir envoyer et recevoir des messages avec un temps de latence appropriée. Par exemple, un message signalant une collision plus loin sur le trajet devrait être transmis à un véhicule avant que celui-ci arrive à l'endroit où s'est produit l'accident. Si ce message d'avertissement ne peut être délivré au véhicule à cause d'une attaque par brouillage intentionnel, l'application de sécurité V2V/V2I pourrait être inutile.

Une entité devrait pouvoir traiter une information échangée en temps réel, d'où la nécessité de mettre en œuvre des algorithmes de chiffrement pour environnements contraints et à faible surdébit.

8.4 Non-répudiation

Une entité ne devrait pas pouvoir nier avoir déjà envoyé un message. Il est possible de mettre en œuvre cette exigence en utilisant des signatures numériques dans les systèmes de communication V2X.

8.5 Authenticité

Les entités telles que les unités embarquées et les unités RSU dans un environnement de communications V2V/V2I devraient être capables de fournir la preuve qu'elles sont bien le titulaire autorisé d'une identité légitime. Cette exigence est appelée authentification de l'entité. Elle est également requise entre un véhicule et un dispositif nomade.

Dans le cas d'une communication au sein d'un groupe, il n'est pas nécessaire qu'un véhicule prouve son identité. Le véhicule devrait prouver qu'il est un membre authentique du groupe. Cette exigence est appelée authentification d'attribut.

8.6 Imputabilité

Une entité devrait pouvoir repérer et/ou empêcher les comportements anormaux des unités embarquées ou des capteurs de véhicule en vérifiant leurs données.

Par exemple, une unité embarquée pour vérifier certaines informations dans un message reçu afin d'établir la validité cinématique par rapport au message précédent. Si les données concernant la position contenues dans le message montrent des changements impossibles dans le comportement dynamique du véhicule, il peut s'agir d'un comportement anormal de l'autre entité. Par conséquent, l'information peut être filtrée ou ignorée.

8.7 Autorisation

Il est essentiel de définir des contrôles d'accès et des autorisations pour les différentes entités. Des règles particulières devraient être mises en œuvre pour autoriser ou interdire à telle ou telle entité d'accéder à certaines fonctions ou données et/ou de les utiliser.

8.8 Applicabilité des exigences de sécurité V2X

Le Tableau 1 répertorie les exigences de sécurité décrites dans les paragraphes 8.1 à 8.7 ainsi que leur applicabilité aux différents types de communications V2X.

Tableau 1 – Exigence de sécurité pour les communications V2X

	Propagation d'avertissements V2V	**Communications V2V en mode peloton**	**Communications V2V en mode balise**	**Avertissements V2I**	**Échange d'informations V2V/V2I**	**Communications V2D**	**Communications V2P**
Confidentialité (général)	–	O	–	–	O	O	O
Confidentialité (informations PII)	O	O	O	▲	O	O	O
Intégrité	O	O	O	O	O	O	O
Disponibilité	O	O	O	O	O	▲	O
Non-répudiation	O	O	O	O	O	O	O
Authenticité	O	▲	O	O	O	O	O
Imputabilité	O	O	O	O	O	O	O
Autorisation	–	O	–	–	O	O	–

O: Requise, –: Non requise, ▲: en partie requise

Dans le cas d'une propagation d'avertissements V2V, la confidentialité ne doit pas être obligatoirement assurée étant donné que les messages échangés entre deux véhicules contiennent des informations déjà publiques, telles qu'un accident de la circulation sur le trajet ou l'arrivée des véhicules d'urgence. En l'espèce, les messages diffusés ne comportent pas d'informations liées à l'autorisation.

Dans un scénario de communications V2V en mode peloton, l'authentification du véhicule est en partie requise, ce qui signifie que chaque véhicule ne doit pas nécessairement authentifier chaque véhicule du groupe. L'authentification d'entité désigne le processus par lequel une entité est assurée de l'identité de l'autre entité participant à la communication. Or, dans un scénario de communications V2V en mode peloton, le véhicule n'a pas besoin de l'authentification exacte de chaque entité du groupe. Dans ce cas, il suffit de prouver que chaque véhicule est membre du groupe. En d'autres termes, il n'y a pas d'assurance concernant l'identité d'un véhicule, mais uniquement concernant le fait que le véhicule est membre du groupe. Ce type d'authentification peut être appelé authentification d'attribut. Dans ce cas de figure, les messages contiennent également des informations sur l'autorisation, telles que le véhicule de tête du peloton ou les membres du peloton.

Dans un scénario de communications V2V en mode balise, les informations concernant la diffusion devraient être protégées contre toute modification ou suppression sans autorisation. Toutefois, s'il ne contient pas les informations d'identification du véhicule, le message ne doit pas obligatoirement être crypté. De plus, l'autorisation n'est pas requise pour le scénario de communications V2V en mode balise, étant donné que l'information diffusée ne sera pas utilisée dans un but de commande.

Dans un scénario d'avertissement V2I, les informations échangées entre un véhicule et un élément de l'infrastructure, par exemple une unité RSU, sont généralement des informations sur le trafic dont la diffusion est publique. La confidentialité dans un environnement d'avertissement V2I n'est donc pas requise. L'indication selon laquelle la protection des informations PII dans un cas d'avertissement V2I est en partie requise signifie que cette protection est nécessaire pour un véhicule, mais pas pour une unité RSU. L'emplacement actuel et l'historique des déplacements d'un véhicule devraient être protégés si le conducteur est lié aux véhicules. Toutefois, une unité RSU n'a pas d'informations PII étant donné qu'elle n'a aucun lien avec des personnes.

Dans un scénario de communications V2D, le dispositif nomade est utilisé dans le véhicule. Lorsqu'il communique avec celui-ci, la disponibilité n'a pas les mêmes incidences que dans le cas d'un scénario de communications V2V car, dans la pratique, le nombre de dispositifs dans le véhicule est inférieur au nombre de véhicules sur la route dans les environnements réels.

Dans un scénario de communications V2P, le dispositif nomade d'un piéton ou d'un usager de la route vulnérable ne peut pas avoir de fonction nécessitant l'autorisation du véhicule.

9 Mise en œuvre de communications V2X sécurisées

Les paragraphes ci-après présentent de possibles mises en œuvre de communications V2X afin de répondre aux exigences de sécurité telles que la confidentialité, l'intégrité, la disponibilité, etc., qui sont décrites au paragraphe 8. Les grands algorithmes de chiffrement adaptés aux environnements des communications de véhicule sont présentés brièvement, ainsi que la manière de les utiliser dans des scénarios de communications V2X, tels que les avertissements en cas d'urgence et les communications mode peloton.

9.1 Chiffrement pour assurer l'authentification des entités et la confidentialité des messages

La fonction d'authentification d'une entité V2X peut être assurée grâce à des algorithmes de signature numérique. La fonction de confidentialité des messages peut être mise en œuvre grâce à des algorithmes de chiffrement symétriques et à clé publique. La présente Recommandation donne des exemples qui mettent en œuvre ces fonctions. L'adaptation et le choix des mécanismes et des

paramètres, qui sont liés aux fonctions d'authentification des entités et de confidentialité des messages, dépendent de la politique de déploiement.

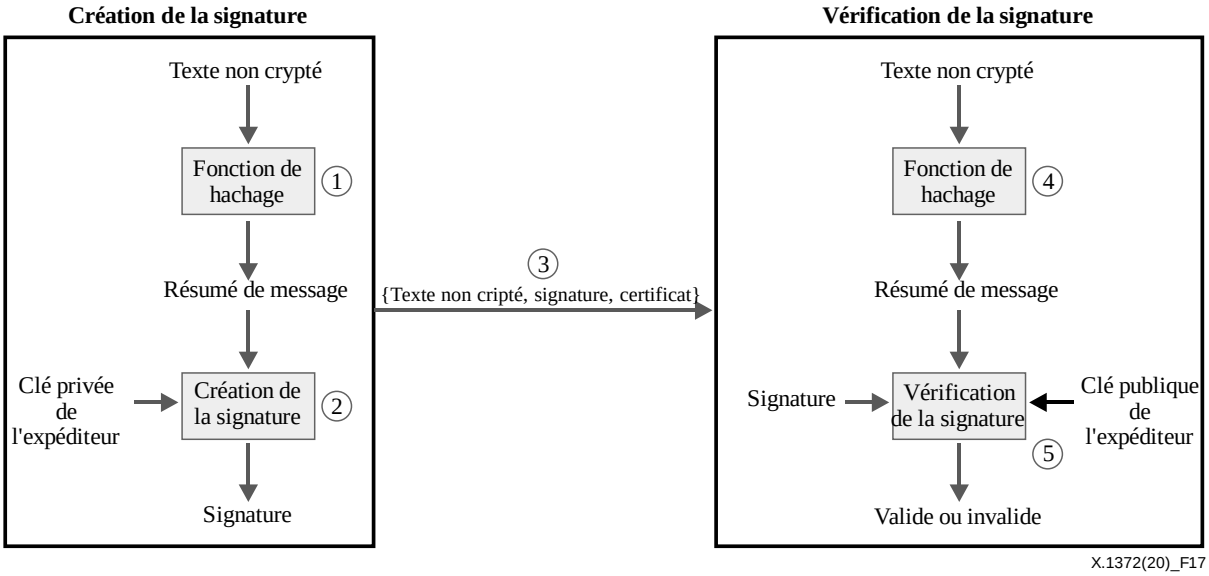


Figure 17 – Création et vérification de la signature

Un algorithme de signature numérique comprend un processus de création de la signature et un processus de vérification de la signature comme indiqué dans la Figure 17. Un signataire utilise le processus de création afin d'appliquer une signature numérique sur les données. Un vérificateur utilise le processus de vérification pour vérifier l'authenticité de la signature. Chaque signataire a une clé publique et une clé privée. Comme on le voit dans la Figure 17, la clé privée est utilisée dans le processus de création de la signature, tandis que la clé publique du signataire est utilisée dans le processus de vérification.

La procédure globale de création et de vérification de la signature est la suivante:

– Étape 1: une fonction de hachage (par exemple l'algorithme de hachage sécurisé avec clés codées sur 256 bits (SHA-256)) est utilisée pour calculer un résumé de message à partir d'un message non crypté. Par exemple, le résumé est calculé à partir de la version du protocole, de l'en-tête, de la charge utile et de la longueur de la queue.

– Étape 2: une signature du résumé du message est créée avec la clé privée de l'expéditeur.

– Étape 3: le message non crypté, la signature et le certificat de l'expéditeur sont transmis un destinataire.

– Étape 4: le destinataire calcule le résumé du message en utilisant le message non crypté envoyé par l'expéditeur.

– Étape 5: le destinataire calcule une valeur de vérification en utilisant le résumé de message obtenu à l'étape 4, la signature reçue et la clé publique de l'expéditeur. Si la valeur de vérification est identique à la valeur figurant dans la signature, alors la signature reçue est valide. Si la valeur de vérification est différente de la valeur figurant dans la signature reçue, la signature n'est pas valide.

L'algorithme de signature numérique à courbe elliptique (ECDSA) peut être utilisé comme algorithmes de signature numérique pour les communications V2X.

Les algorithmes de chiffrement sont utilisés pour prendre en charge la confidentialité des messages V2X. Un algorithme de chiffrement asymétrique, par exemple le système de chiffrement intégré à courbe elliptique (ECIES), est utilisé pour le transport d'une clé pour un algorithme de clé symétrique telle que la norme de chiffrement perfectionné (AES). La procédure de chiffrement

associée au système ECIES est décrite dans la Figure 18. Dans cette Figure, le système ECIES utilise les fonctions suivantes:

– Concordance de clés (KA): fonction utilisée pour créer un secret partagé par deux entités.

– Fonction de calcul de clé (KDF): mécanisme qui produit un ensemble de clés à partir d'éléments de calcul de clé et de plusieurs paramètres optionnels.

– Chiffrement: algorithme de chiffrement de clé symétrique.

– Code d'authentification de message (MAC): algorithme de création de code MAC.

Dans la Figure 18, les notations suivantes sont utilisées:

– ***u***: clé privée de l'expéditeur;

– **U**: clé publique de l'expéditeur;

– **v**: clé privée du destinataire;

– **V**: clé publique du destinataire.

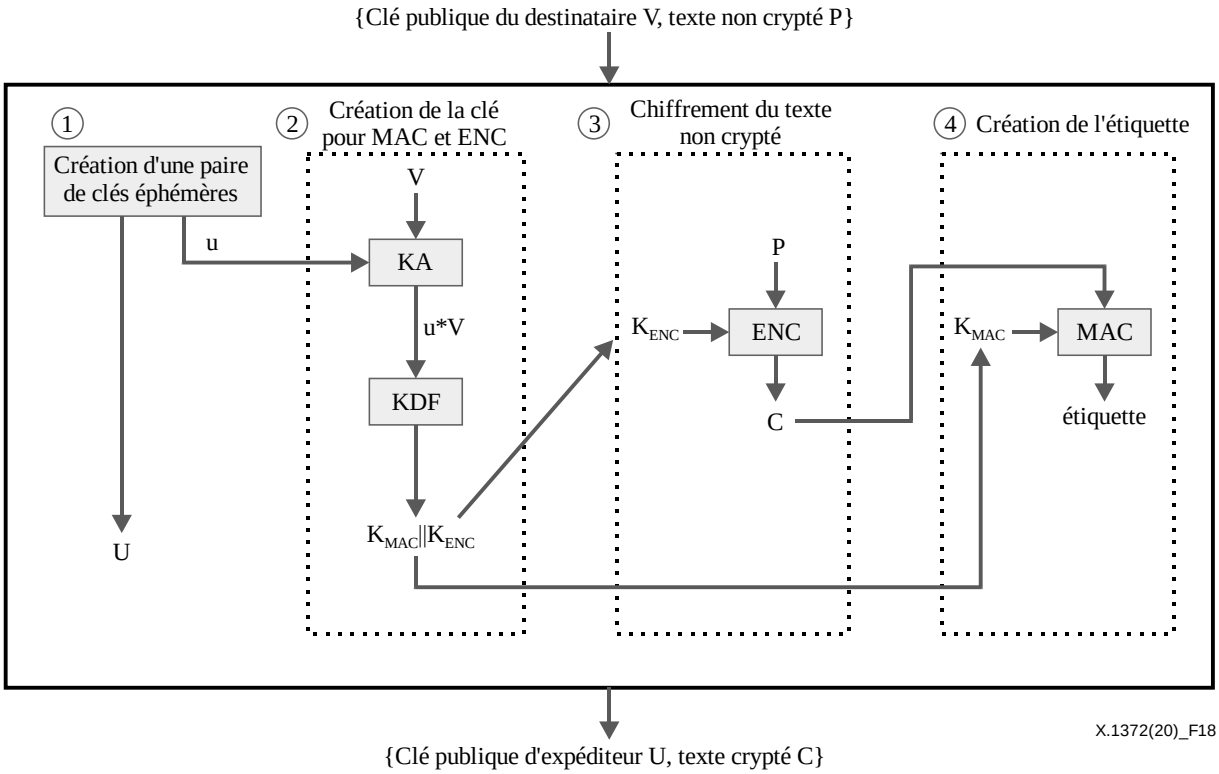


Figure 18 – Procédure de chiffrement ECIES

Comme on le voit sur la Figure 18, les données nécessaires pour mener à bien la procédure de chiffrement sont la clé publique du récepteur ***V*** et le texte non crypté ***P***. Les éléments générés avec la procédure de chiffrement sont la clé publique de l'expéditeur ***U***, l'étiquette et le texte crypté ***C***. La procédure de chiffrement de message est composée des étapes suivantes:

– Étape 1: création d'une paire de clés éphémères

L'expéditeur génère la clé privée ***u*** et la clé publique ***U.*** Il est recommandé que la clé publique ***U*** soit générée peu avant pour chaque opération de chiffrement.

– Étape 2: création de la clé pour les fonctions MAC et ENC

La fonction de concordance de clés (KA) génère un secret partagé par la clé privée éphémère de l'expéditeur ***u*** et la clé publique du destinataire ***V***. La fonction de calcul de clé (KDF)

fondée sur le hachage SHA-256 prendra ce secret partagé pour générer la concaténation de la clé de code MAC (***K**MAC*) et la clé de chiffrement (***K**ENC*).

– Étape 3: chiffrement du texte non crypté

Le texte non crypté ***P*** est chiffré avec la clé ***K**ENC* au moyen d'algorithmes de chiffrement symétriques.

Le système ECIES est utilisé pour chiffrer les clés symétriques dans le cas du chiffrement des messages V2X selon la norme de chiffrement perfectionné - mode compteur avec code d'authentification de message à enchaînement de blocs de chiffrement (AES-CCM). Par conséquent, le texte non crypté est en fait la clé de chiffrement pour la norme AES-CCM.

– Étape 4: création de l'étiquette

Une fonction MAC à hachage SHA-256 génère une étiquette du texte chiffré, qui est la clé symétrique AES-CCM, afin de prendre en charge l'intégrité du message.

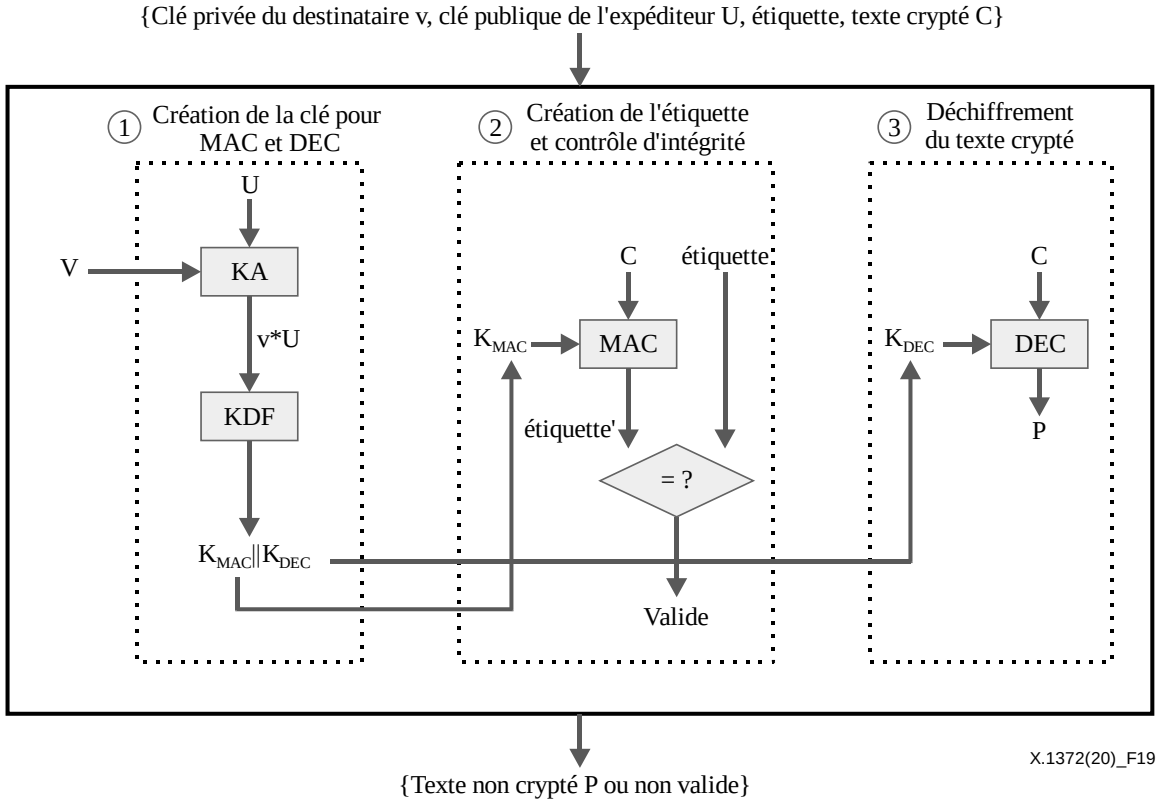


Figure 19 – Procédure de déchiffrement ECIES

La procédure de déchiffrement du système ECIES est décrite dans la Figure 19. Comme on le voit sur cette Figure, les données nécessaires pour mener à bien la procédure de déchiffrement sont la clé privée du destinataire ***v***, la clé publique de l'expéditeur ***U***, l'étiquette et le texte crypté ***C***. Les éléments générés avec la procédure de déchiffrement sont le texte non crypté ***P*** ou les résultats du test d'intégrité du message. Dans la Figure 19, DEC signifie procédure de déchiffrement de l'algorithme de clé symétrique. La procédure de déchiffrement des messages est composée des étapes suivantes:

– Étape 1: création de la clé pour les fonctions MAC et DEC

La fonction de concordance de clés (KA) génère un secret partagé par la clé publique éphémère de l'expéditeur ***U*** et la clé privée du destinataire ***v***. La fonction de calcul de clé (KDF) fondée sur le hachage SHA-256 prendra ce secret partagé pour générer la concaténation de la clé de code MAC ***K**MAC* et la clé de déchiffrement ***K**DEC*. Il est à noter que ***K**ENC* et ***K**DEC* sont des valeurs identiques dans le cas d'un algorithme de clé symétrique.

– Étape 2: création de l'étiquette et contrôle d'intégrité

  La fonction MAC génère une étiquette du texte crypté reçu $\boldsymbol{C}$ avec la clé $\boldsymbol{K_{MAC}}$. L'étiquette ainsi obtenue est comparée à l'étiquette reçue. Si les valeurs ne sont pas identiques, le message reçu est écarté, le contrôle d'intégrité du message n'étant pas concluant.

– Étape 3: déchiffrement du texte crypté

  Le texte crypté $\boldsymbol{C}$ est déchiffré avec la clé $\boldsymbol{K_{DEC}}$ au moyen d'algorithmes de chiffrement symétrique.

Le système ECIES est utilisé pour chiffrer les clés symétriques dans le cas du chiffrement des messages V2X selon la norme AES-CCM. Par conséquent, le texte non crypté est en fait la clé de chiffrement AES-CCM.

9.2 Confidentialité des messages d'avertissement de sécurité en cas d'urgence

La Figure 20 montre un cas générique d'utilisation pour les avertissements en cas d'urgence. L'unité ECU du système de freinage envoie un message à l'unité de communication V2X d'un véhicule par l'intermédiaire de son unité centrale de communication (CCU). L'application ITS correspondante dans l'unité de communication V2X reçoit le message envoyé par l'ECU du système de freinage et génère un message d'avertissement V2X. Le message généré est envoyé à la couche réseau et transport. Ce message devrait être signé ou chiffré par la couche sécurité. La couche physique envoie ensuite le message signé ou chiffré à un canal de communication sans fil, qui est utilisé pour transmettre le message au destinataire. Au niveau du destinataire, le message est vérifié ou déchiffré par la couche sécurité et enfin transmis à la couche supérieure, à savoir l'application ITS correspondante. L'application ITS correspondante peut mettre à jour la carte LDM ou alerter le conducteur via le dispositif d'interface et pourra envoyer un message de commande à l'ECU du système de freinage afin de réduire la vitesse du véhicule.

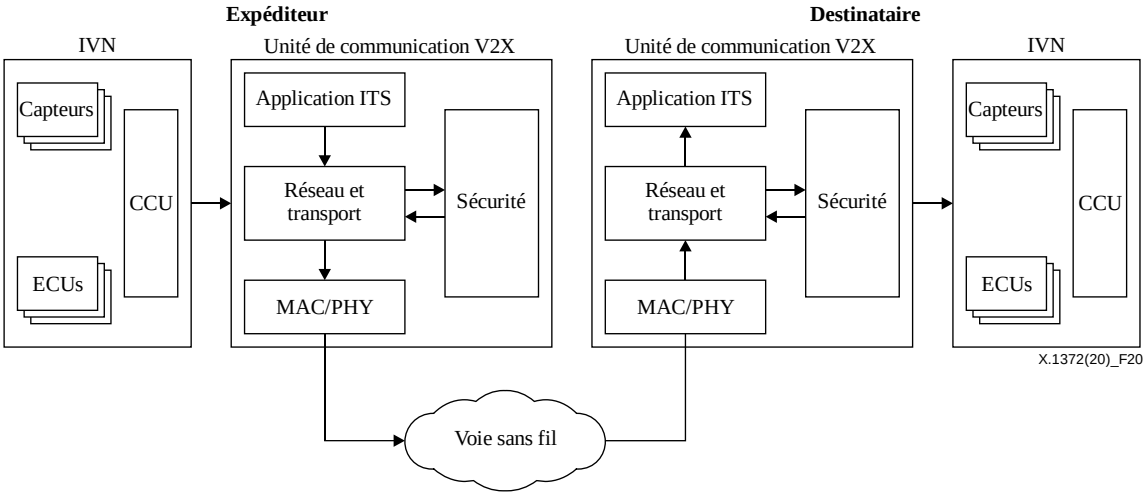


Figure 20 – Procédure d'avertissement en cas d'urgence

9.3 Authentification des entités pour la formation de pelotons routiers

La formation de pelotons routiers est une approche efficace qui consiste à passer d'un modèle de conduite individuelle à un mode collectif. En général, la conduite en peloton routier fait intervenir un groupe de véhicules ayant des intérêts communs, dans le cadre duquel les véhicules se suivent en étant séparés par une courte distance presque constante, formant ainsi un peloton routier comme on le voit sur la Figure 21. Trois opérations principales peuvent être effectuées sur les pelotons: intégration dans le peloton, coopération/maintien dans le peloton et séparation du peloton.

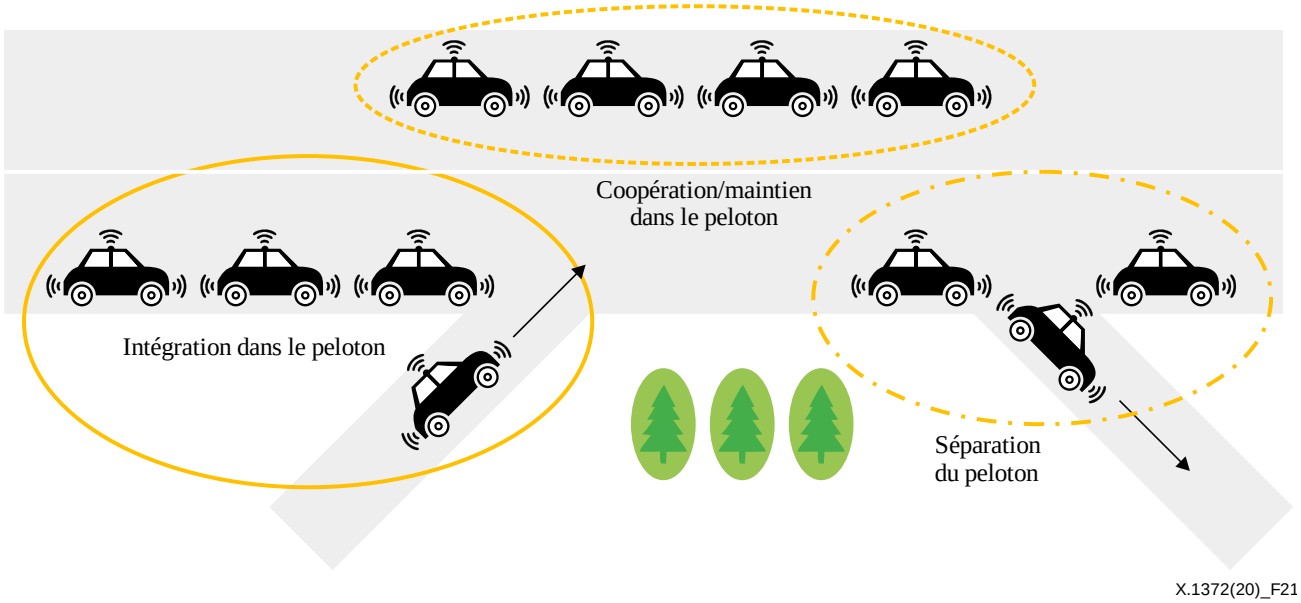


Figure 21 – Cas d'utilisation des pelotons routiers

– Intégration dans le peloton: le véhicule, qui n'est pas membre d'un peloton, avance et se joint au peloton à l'intersection suivante.

– Coopération/maintien dans le peloton: les véhicules appartenant au même peloton doivent communiquer et coopérer entre eux afin de maintenir le peloton et mener à bien des opérations, par exemple laisser passer un véhicule prioritaire, ajuster leur position en fonction de l'itinéraire prévu, traverser des intersections et changer de file.

– Séparation du peloton. Le véhicule quitte le peloton auquel il appartient en prenant une autre voie à l'intersection suivante.

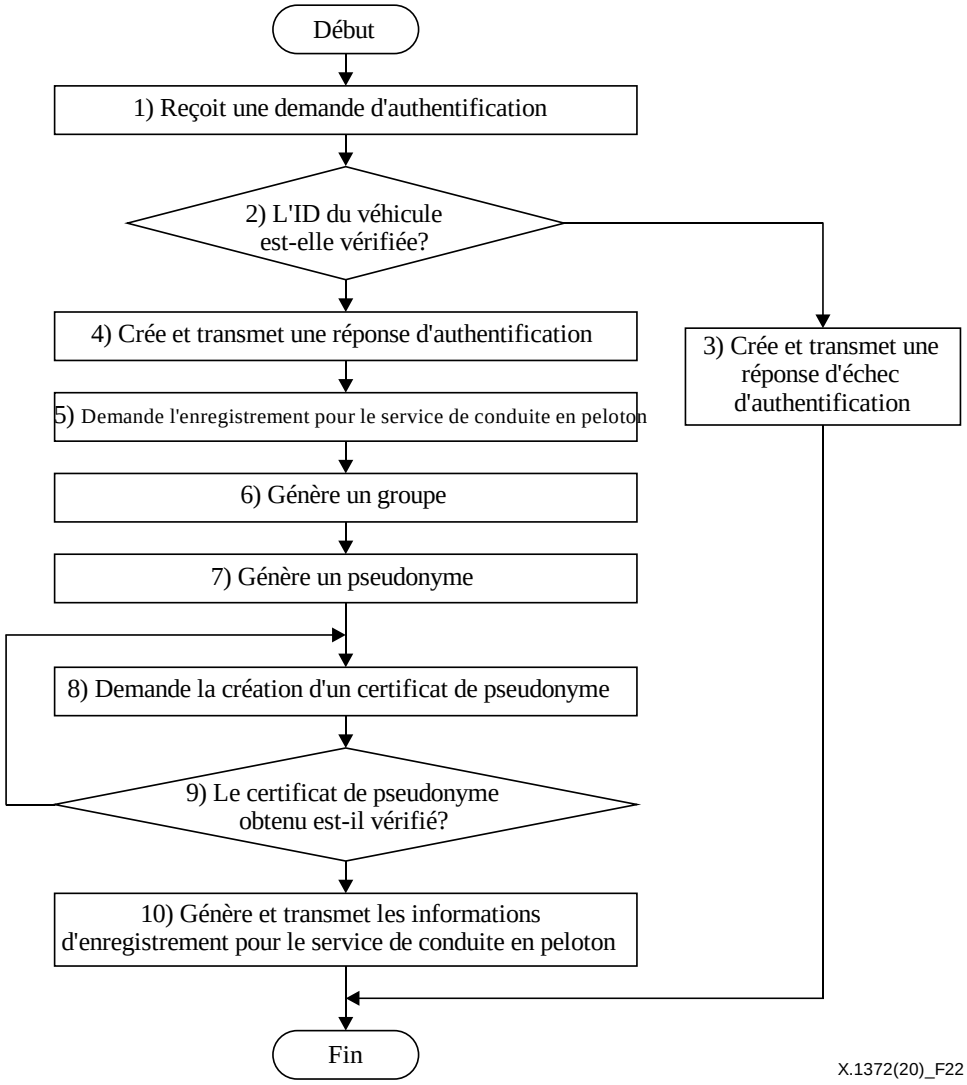


Figure 22 – Procédure d'enregistrement dans un peloton

La Figure 22 montre un exemple d'authentification pour un service de conduite en pelotons. En l'espèce, si une demande d'authentification en vue de l'enregistrement auprès d'un service de conduite en groupe, c'est-à-dire une demande authentification d'un véhicule, est envoyée par un véhicule en mode exécution de service (étape 1), l'identité du véhicule devrait être vérifiée, par exemple à l'aide de l'algorithme de signature numérique d'un système de chiffrement de clé publique (étape 2). Dans ce cas précis, la demande d'authentification du véhicule peut être faite moyennant la transmission, au système du service de conduite en groupe, d'un message signé avec une clé privée du véhicule. À l'issue de la vérification effectuée lors de l'étape 2, s'il est établi que l'identité du véhicule n'est pas valide, le système du service de conduite en groupe génère une réponse d'échec de l'authentification qu'il transmet aux véhicules (étape 3).

À l'issue de la vérification effectuée lors de l'étape 2, s'il est établi que l'identité du véhicule est valide, le système du service de conduite en groupe génère une réponse d'authentification pour le véhicule et lui transmet (étape 4).

Lorsque la réponse authentification est reçue, c'est-à-dire une fois l'authentification du véhicule menée à bien, après qu'un usager a fourni et sélectionné les informations d'enregistrement pour le service de conduite en groupe, notamment le type de conduite en groupe, le lieu de départ, la destination, l'heure estimée de départ, l'heure estimée d'arrivée et les étapes souhaitées, le véhicule transmet les informations d'enregistrement correspondante au système du service de conduite en groupe afin de demander l'enregistrement auprès du service de conduite en groupe (étape 5).

Ensuite, si une demande d'enregistrement auprès du service de conduite en groupe, qui comprend les informations d'enregistrement pour la conduite en groupe, est soumise par le véhicule, le système du service de conduite en groupe crée, sur la base des informations d'enregistrement, un groupe composé de véhicules avec la même destination, le même lieu de départ, la même heure estimée d'arrivée, etc., puis stocke/enregistre les informations concernant le groupe en question dans les informations relatives au groupe (étape 6).

En l'espèce, le groupe concerné pourra comprendre au moins un chef de groupe, c'est-à-dire un véhicule de tête, et au moins un membre, c'est-à-dire un véhicule membre. Après cela, le système du service de conduite en groupe attribue un pseudonyme à chaque véhicule du groupe (étape 7), génère un message de demande de certificat afin de demander la création d'un certificat de pseudonyme pour le pseudonyme attribué à chaque véhicule du groupe et transmet le message au centre d'authentification (étape 8).

Le système du service de conduite en groupe vérifie si le certificat de pseudonyme est obtenu ou non auprès du centre d'authentification (étape 9). À l'issue de cette opération, si le certificat de pseudonyme est obtenu, le système du service de conduite en groupe stocke le certificat dans la base de données des informations relatives au groupe. Le certificat de pseudonyme pourra être un message portant la signature numérique du centre d'authentification. Il est possible de garantir la justification du pseudonyme grâce au certificat de pseudonyme. Le pseudonyme est une clé publique attribuée à chaque véhicule par le système du service de conduite en groupe.

Plusieurs pseudonymes peuvent être attribués à chaque véhicule. Étant donné que le pseudonyme ne contient pas d'informations associées à l'identité de chaque véhicule, l'identité du véhicule prenant part à la conduite en groupe n'est pas exposée, afin qu'il soit possible de protéger les informations PII de chaque véhicule du groupe.

Si la notification est reçue, le système du service de conduite en groupe génère les informations d'enregistrement au service de conduite en groupe pour le groupe en question, les stocke dans la base de données correspondante et les transmet à chaque véhicule du groupe (étape 10). En l'espèce, les informations d'enregistrement au service de conduite en groupe peuvent comprendre un identifiant de groupe, un pseudonyme attribué à chaque véhicule, un certificat de pseudonyme pour le pseudonyme, etc. Chaque véhicule, c'est-à-dire chaque utilisateur du véhicule, du groupe en question pour lequel le service de conduite en groupe est enregistré, peut prendre part à la conduite en groupe en communiquant avec les autres véhicules du groupe et en utilisant pour ce faire les informations d'enregistrement au service de conduite en groupe fournies par ledit service.

9.4 Infrastructure PKI de véhicule

Une infrastructure de clé publique (PKI), qui produit et gère des certificats numériques, est nécessaire pour instaurer la confiance entre les participants dans les environnements de communications de véhicule. L'infrastructure PKI de véhicule diffère de l'infrastructure PKI classique en plusieurs points. Le plus important est qu'elle utilise des pseudonymes afin de protéger l'exposition de l'emplacement du véhicule par rapport à l'emplacement du propriétaire. Le nombre de certificats est bien plus élevé que dans le cas d'une infrastructure PKI classique. Par conséquent, l'objectif principal de l'infrastructure PKI de véhicule est d'offrir des méthodes efficaces pour demander des certificats et gérer la révocation.

L'Appendice II présente plus en détail des modèles de référence d'architecture PKI de véhicule.

Appendice I

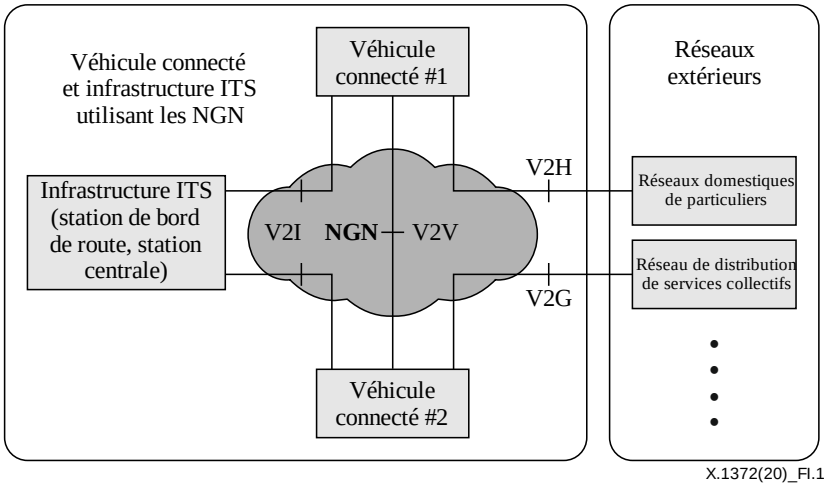
Modèles de référence de communication de véhicule

(Le présent Appendice ne fait pas partie intégrante de la Recommandation.)

I.1 Cadre UIT-T applicable aux services et applications pour véhicules connectés utilisant les réseaux NGN

Le cadre applicable aux services et applications pour véhicules connectés dans le contexte des réseaux de prochaine génération (NGN) est décrit dans [b-UIT-T Y.2281]. Le véhicule est l'un des composants importants utilisant les capacités de réseau pour les communications de véhicule à infrastructure (V2I), de véhicule à véhicule (V2V) et de véhicule à domicile (V2H). Dans ce contexte, un véhicule connecté peut coopérer avec des réseaux de prochaine génération (NGN) pour prendre en charge des services et applications plus évolués, comme des applications de sécurité routière, des applications se rapportant à la circulation, des services multimédias et la mise en œuvre de ces services en fonction de l'emplacement.

[b-UIT-T Y.2281] identifie la relation entre un réseau NGN et un véhicule connecté ainsi que les exigences compte tenu de la nécessité de prendre en charge des services et applications de véhicules connectés utilisant les réseaux NGN. Elle décrit en outre une architecture cadre des véhicules connectés et de l'infrastructure des systèmes de transport intelligents (ITS) utilisant les réseaux NGN afin d'harmoniser les fonctionnalités de communication des réseaux NGN et des véhicules connectés.

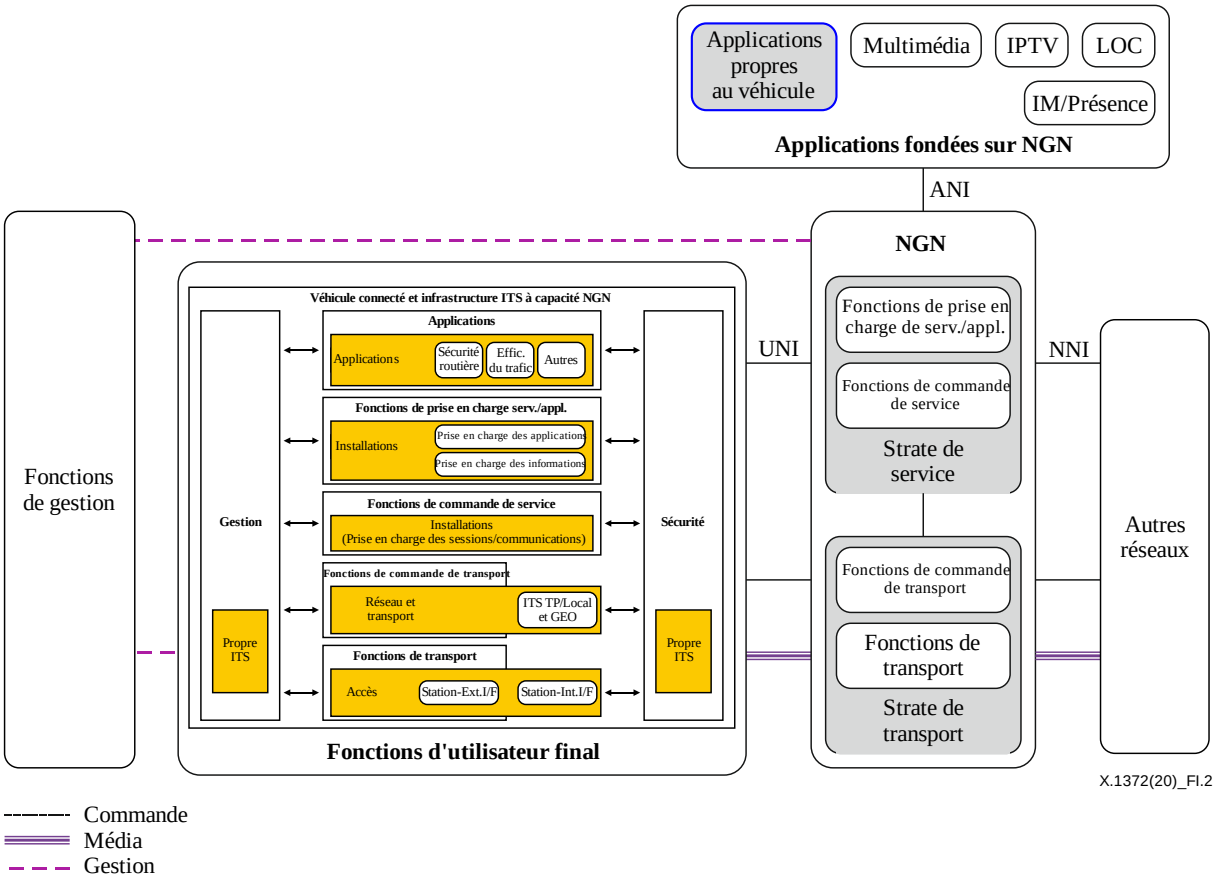


NOTE – Source: [b-UIT-T Y.2281].

Figure I.1 – Modèle général de configuration d'un véhicule connecté et de l'infrastructure ITS

La Figure I.1 présente une configuration modèle selon UIT-T Y.2281 et montre les relations que les véhicules connectés entretiennent avec l'infrastructure ITS, ainsi qu'avec des réseaux extérieurs comme les réseaux domestiques de particuliers et un réseau de distribution de services collectifs utilisant la technologie NGN. Par rapport à d'autres normes relatives aux ITS, [b-UIT-T Y.2281] traite de l'utilisation des NGN dans des environnements ITS. Cette norme définit l'utilisation des réseaux NGN dans les environnements ITS afin de réduire au minimum les problèmes d'interopérabilité entre les communications ITS entre homologues et un réseau public. Ces fonctionnalités d'interopérabilité sont particulièrement importantes pour la prise en charge de la qualité de service, de la mobilité et de la sécurité avec différents services multimédias.

La Figure I.2 présente un aperçu de l'architecture d'un véhicule connecté et d'une infrastructure ITS à capacité NGN coopérant avec un réseau NGN. Le réseau NGN est composé de "fonctions d'utilisateur final", d'une "strate de service", d'une "strate de transport", d'une "strate de gestion" et "d'applications fondées sur NGN". La fonction de véhicule connecté et infrastructure ITS à capacité NGN est située au niveau des fonctions d'utilisateur final du point de vue du réseau NGN. [b-ITU-T Y.2281] décrit la manière dont les applications NGN propres au véhicule, par exemple l'appel d'urgence, sont prises en charge via un réseau NGN.



NOTE – Source: [b-UIT-T Y.2281].

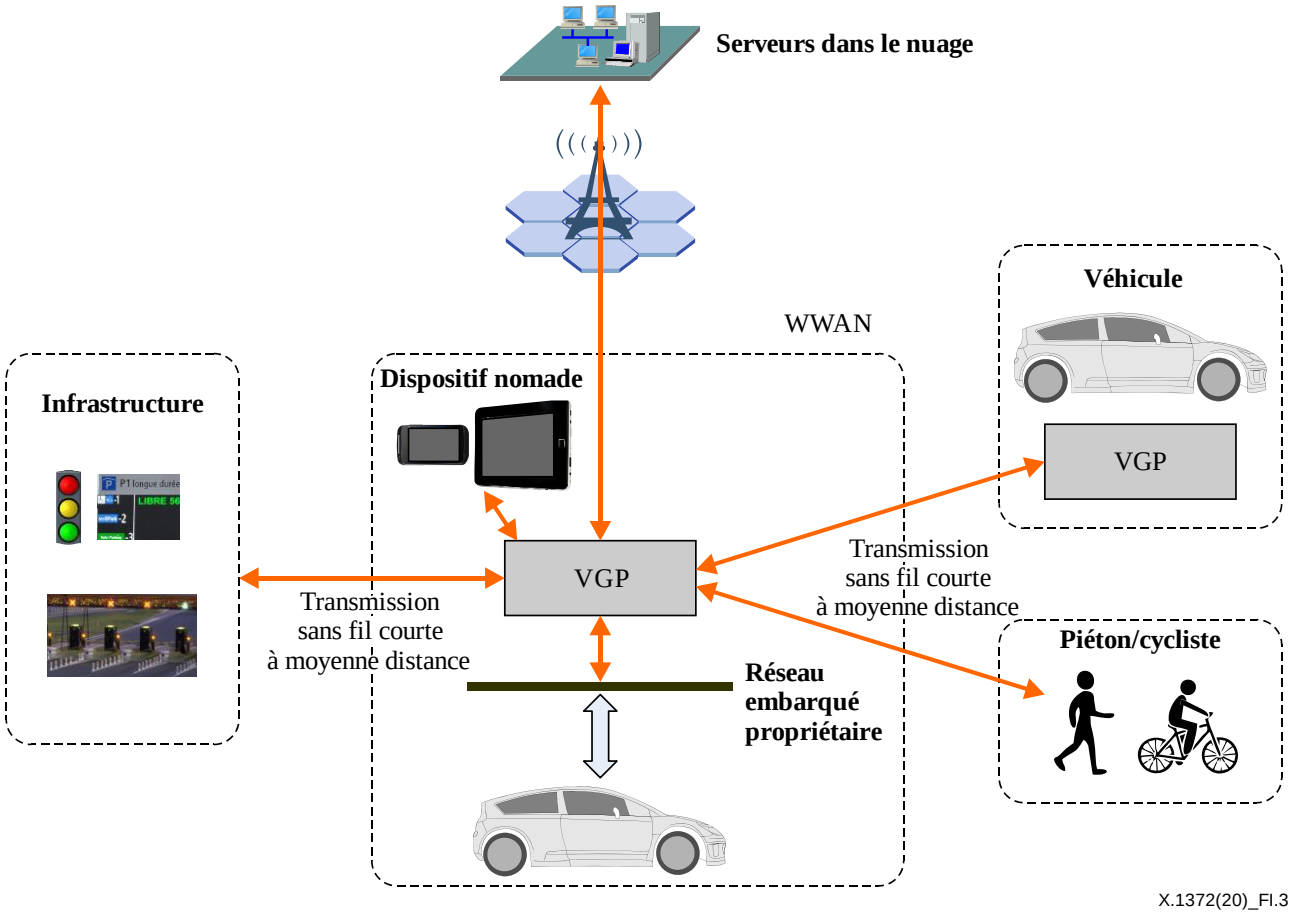
Figure I.2 – Aperçu de l'architecture d'un véhicule connecté et d'une infrastructure ITS à capacité NGN coopérant avec un réseau NGN

Les considérations liées à la sécurité présentées dans [b-UIT-T Y.2281] font référence à [b-UIT-T Y.2201]. Des aspects liés à la sécurité doivent être pris en compte en fonction du réseau qui est connecté au véhicule. Toutefois, [b-UIT-T Y.2281] ne spécifie la sécurité que pour les NGN et les autres cas d'exigences de sécurité ne relèvent pas du domaine application de cette norme.

Le cadre UIT-T applicable aux services et applications pour véhicules connectés utilisant les réseaux NGN porte sur l'adaptation des NGN à l'environnement des véhicules. [b-UIT-T Y.2281] ne spécifie pas les aspects liés à la sécurité de l'environnement des véhicules. L'architecture d'accès hertzien dans l'environnement des véhicules (WAVE) de l'IEEE, décrite dans [b-IEEE WAVE], porte sur une interface radioélectrique à 5,9 GHz étant donné qu'elle ne comprend pas de manière explicite une application permettant de communiquer avec un autre réseau. L'architecture ITS définie par l'ETSI, décrite dans [b-ETSI EN 302 665], fait référence à la couche application qui est une pile de protocoles de communication. Dans la mesure où la couche d'accès fait appel à la norme IEEE 802.x, à la technologie 3G cellulaire et à la technologie Bluetooth, l'architecture ITS de l'ETSI a vocation à prendre en charge de multiples piles de protocoles de réseaux.

I.2 Architecture et entités fonctionnelles des plates-formes de passerelle de véhicule définies par l'UIT-T

L'architecture et les entités fonctionnelles des plates-formes de passerelle de véhicule (VGP) sont étudiées dans le cadre de la Commission d'études 16 de l'UIT-T. L'architecture, le cadre de l'architecture fonctionnelle et les entités fonctionnelles des plates-formes de passerelle de véhicule sont décrits dans [b-UIT-T H.550]. Le terme plate-forme VGP est défini dans [b-UIT-T F.749.1]. Une passerelle VGP est l'assemblage d'équipements TIC et de logiciels à l'intérieur d'un véhicule fonctionnant comme une plate-forme ouverte pour fournir un environnement d'exécution intégré permettant de fournir les services de communication d'une passerelle de véhicule. La plate-forme VGP peut également fournir des services de communication de couche supérieure, par exemple l'interaction avec le conducteur grâce aux services d'accès conducteur-véhicule, etc. Les sous-systèmes destinés uniquement à l'exploitation du véhicule ne sont pas considérés comme faisant partie de la passerelle VGP.



NOTE – Source: [b-UIT-T H.550].

Figure I.3 – Place de la plate-forme VGP dans le modèle de référence ITS

La Figure I.3 montre le positionnement de la plate-forme VGP dans le modèle de référence de système de transport intelligent (ITS): il existe six grands scénarios, à savoir de véhicule à véhicule, de véhicule à infrastructure, de véhicule à serveur dans le nuage, de véhicule à dispositif nomade, de véhicule à piéton/cycliste et interaction avec le réseau embarqué.

– Le scénario de véhicule à véhicule (V2V) correspond principalement aux scénarios de sécurité et de conduite autonome dans lesquels les véhicules communiquent entre eux.

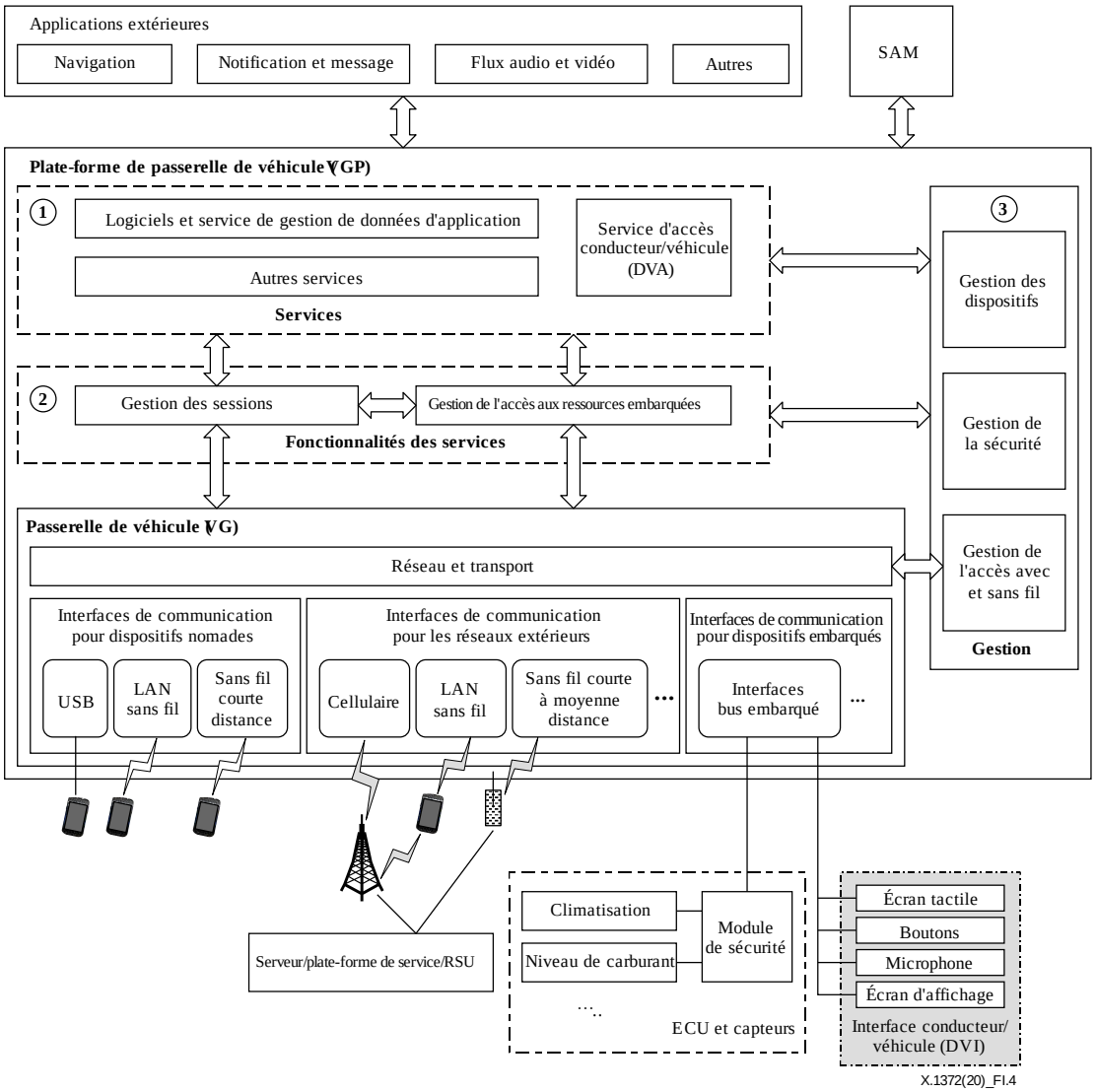
– Le scénario de véhicule à infrastructure (V2I) correspond principalement aux scénarios d'échanges d'informations concernant la sécurité, les télépéages et le trafic dans lesquels les véhicules communiquent avec les infrastructures de bord de route.

– Le scénario de véhicule à serveur dans le nuage correspond principalement aux scénarios d'appel d'urgence et de télématique dans lesquels les véhicules communiquent avec des services en nuage.

– Le scénario de véhicule à dispositif nomade correspond principalement aux scénarios de télécommunication et d'interface utilisateur distant dans lesquels les véhicules se connectent à des dispositifs nomades.

– Le scénario de véhicule à piéton/cycliste correspond principalement au scénario d'avertissement de sécurité dans lesquels des véhicules communiquent avec les dispositifs des piétons/cyclistes.

– Le scénario d'interaction avec le réseau embarqué correspond principalement aux scénarios de diagnostic de véhicule, de collecte de données à distance et de contrôle du véhicule à distance dans lesquels une plate-forme VGP communique avec le réseau embarqué propriétaire.



NOTE – Source: [b-UIT-T H.550].

Figure I.4 – Architecture de haut niveau d'une plate-forme VGP

La Figure I.4 présente l'architecture de haut niveau d'une plate-forme VGP. Les services VGP comprennent les logiciels et un service de gestion de données d'application, un service d'accès conducteur-véhicule et d'autres services (voir le bloc (1) dans la Figure I.4). Les fonctionnalités de service comprennent la gestion des sessions et la gestion de l'accès aux ressources embarquées (voir le bloc (2) dans la Figure I.4). La gestion comprend la gestion des dispositifs, la gestion de la sécurité et la gestion de l'accès avec et sans fil (voir le bloc (3) dans la Figure I.4). Les services prennent en charge des applications extérieures comme la navigation et les infoloisirs pour mener à bien l'établissement de sessions, la conversion de formats de données et les traitements spécifiques.

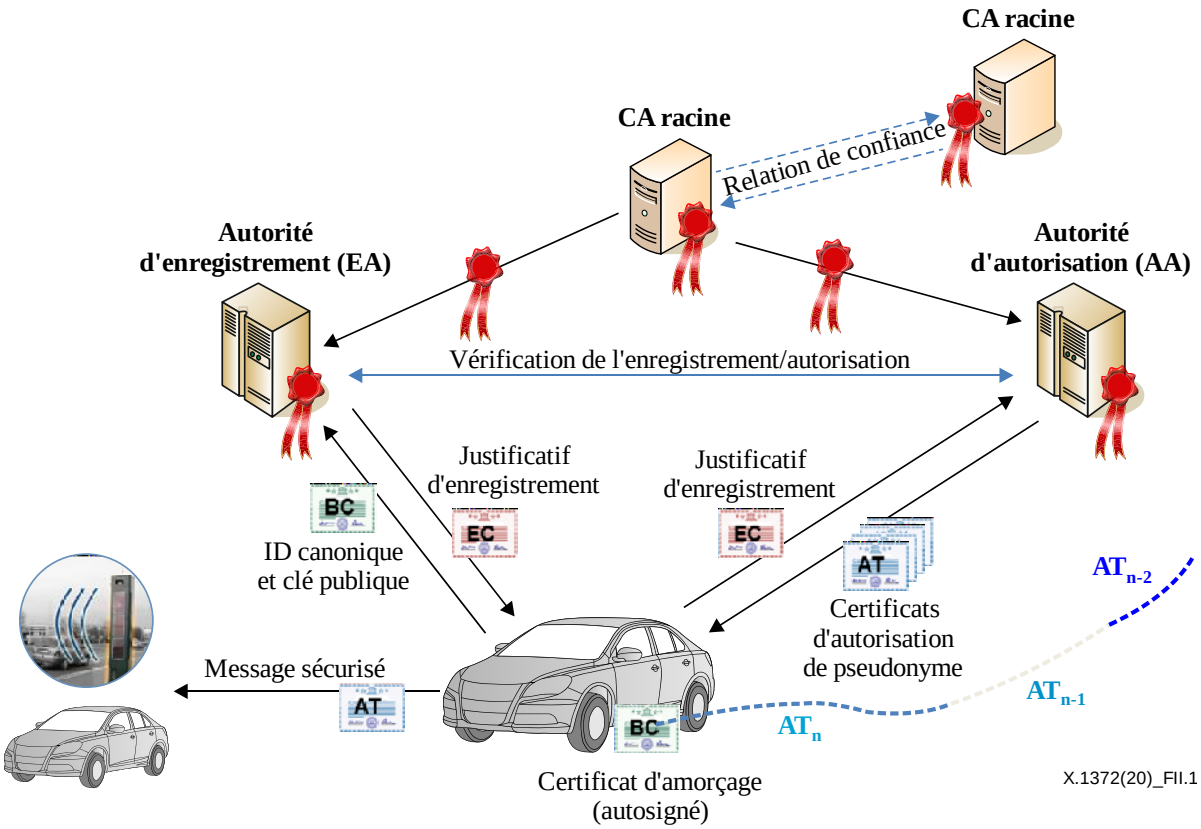
La question de la sécurité sur les passerelles VGP est décrite comme faisant partie de la couche de gestion dans [b-UIT-T H.550]. Une description générique de la fonction de sécurité fait l'objet du paragraphe 8.4.1 de [b-UIT-T H.550], intitulé "Gestion de la sécurité". Cette fonction comprend la gestion de la sécurité pour la couche d'accès, qui comprend elle-même la couche de transport et de réseau, et la gestion de la sécurité pour les services/applications.

Appendice II

Modèles de référence d'infrastructure PKI de véhicule

(Le présent Appendice ne fait pas partie intégrante de la Recommandation.)

Les fonctionnalités de sécurité des communications ITS actuelles comprennent l'authentification des messages, qui a une incidence sur la confidentialité pour les véhicules et les lecteurs. Au niveau européen, l'Institut européen des normes de télécommunication (ETSI) a défini un mécanisme d'authentification des messages fondé sur l'utilisation d'une infrastructure de clé publique comme l'infrastructure PKI de véhicule comme indiqué dans la Figure II.1.



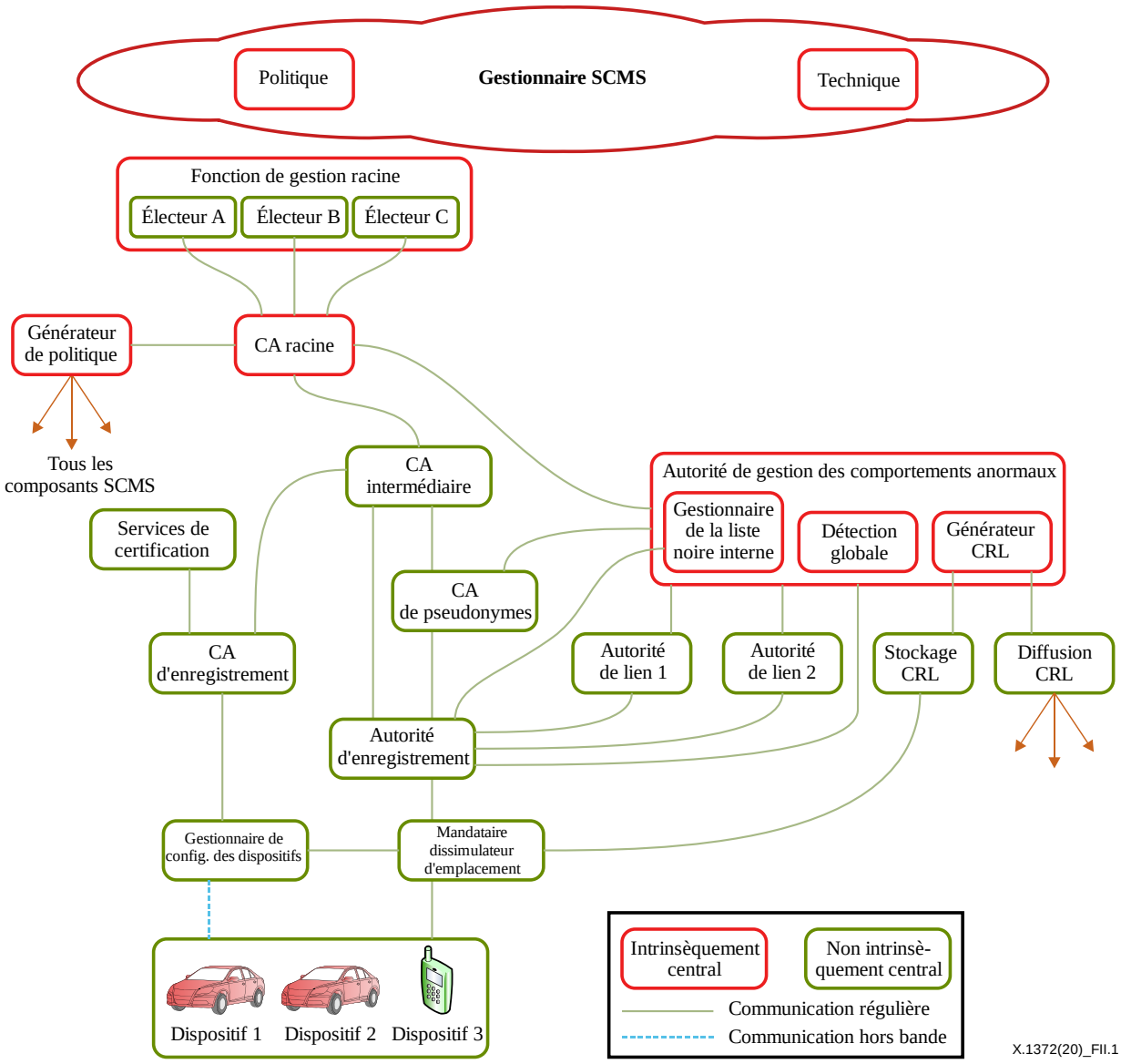
NOTE – Source: [b-ETSI TS 102 940].

Figure II.1 –Infrastructure PKI de véhicule définie par l'ETSI

Le point de départ de la chaîne de confiance des certificats est l'autorité de certification racine (RCA); elle signe les certificats des autres autorités telles qu'une autorité d'autorisation (AA) ou une autorité d'enregistrement (EA) et produit et tient à jour la liste de révocation des certificats (CRL), qui est la liste des autorités révoquées. Dans un contexte opérationnel, une autorité RCA est gérée par un acteur qui peut garantir un niveau de confiance élevée et stable et qui est suffisamment fédérateur, par exemple un état ou un groupe d'états. L'autorité d'enregistrement est l'autorité qui délivre les certificats d'enregistrement (EC) et valide les demandes de tickets d'autorisation (AT). L'autorité d'autorisation est un tiers de confiance qui fournit les tickets AT aux stations ITS. Elle ne connaît pas l'identité de la station ITS et s'appuie sur l'autorité d'enregistrement pour vérifier si la station en question est autorisée ou non à avoir le ticket AT. La demande de ticket AT contient l'identité de l'autorité d'enregistrement auprès de laquelle la station ITS est enregistrée.

Cette architecture vise à assurer la protection de la vie privée dans le cas des stations ITS et à éviter le traçage: l'autorité d'enregistrement connaît l'identité de la station ITS mais ne connaît pas les certificats de pseudonyme (tickets AT) qu'elle utilise, tandis que l'autorité d'autorisation connaît le certificat de pseudonyme de la station ITS mais ne connaît pas son identité. Une station ITS s'enregistre elle-même auprès de l'autorité d'enregistrement et obtient un certificat d'enregistrement. Ce certificat est utilisé pour demander des identités de pseudonyme (tickets AT) à l'autorité d'autorisation: lorsqu'une station ITS demande un ticket AT, elle envoie, dans le message de demande, son identité chiffrée avec le certificat d'enregistrement et l'identité de l'autorité d'enregistrement. L'autorité d'autorisation reçoit la demande pseudonyme, lit l'identifiant de l'autorité d'enregistrement et vérifie le point d'accès de l'autorité d'enregistrement pour valider la demande de ticket AT. L'autorité d'enregistrement vérifie le certificat d'enregistrement de la station ITS et valide (ou non) les demandes. Si la demande est validée, l'autorité d'autorisation génère et envoie le ticket AT à la station ITS.

Par ailleurs, le Crash Avoidance Metrics Partnership (CAMP) a présenté un système de gestion des justificatifs de sécurité (SCMS) afin de sécuriser les communications V2X (voir [b-SCMS]). Actuellement au stade expérimental, ce système fondé sur l'infrastructure PKI pour assurer la sécurité V2X est en cours de validation. Le système SCMS prend en charge l'amorçage, la fourniture de certificats, le signalement des comportements anormaux et la révocation.



NOTE – Source: [b-SCMS].

Figure II.2 – Architecture PKI-V définie par le partenariat CAMP

La Figure II.2 présente un aperçu de l'architecture SCMS. Les relations entre les différents composants SCMS sont représentées par des traits pleins, et tous les composants envoyant des informations ou des certificats à d'autres sont indiqués.

Les principaux composants du système SCMS sont les suivants:

– Autorité de certification d'enregistrement (ECA): publie les certificats d'enregistrement pour un dispositif et peut être utilisée pour demander des certificats de pseudonyme pour différentes régions géographiques, différents fabricants ou différents types de dispositif.

– Autorité de certification intermédiaire (ICA): autorité de certification secondaire dont le rôle est d'éviter que l'autorité de certification racine soit surchargée et son certificat est publié par l'autorité de certification racine.

– Autorité de lien (LA): génère les valeurs préalables de lien figurant dans les certificats afin de permettre une révocation efficace. De plus, il y a plusieurs autorités de lien afin d'éviter que l'opérateur d'une autorité de lien établisse des liens entre les certificats appartenant à un dispositif donné.

– Mandataire dissimulateur d'emplacement (LOP): modifie l'adresse source afin de cacher l'emplacement du dispositif à l'origine d'une demande et empêche l'établissement de liens entre les adresses réseau et les emplacements.

– Autorité de gestion des comportements anormaux (MA): reçoit et traite les signalements de comportement anormal envoyés par les dispositifs afin d'identifier les possibles comportements anormaux ou dysfonctionnements. En outre, elle révoque le certificat du dispositif et le met sur la liste CRL. Elle lance en outre le processus de rattachement d'un identifiant de certificat aux certificats d'enregistrement correspondants et d'inscription sur la liste noire interne de l'autorité d'enregistrement.

– Générateur de politique (PG): tient à jour le fichier général des politiques pour l'autorité d'enregistrement, qui contient les informations générales de configuration, et le fichier global de chaîne de certificats, qui contient toutes les chaînes de confiance du système SCMS.

– Autorité de certification des pseudonymes (PCA): délivre les certificats de pseudonyme à court terme, d'identification et d'application aux dispositifs. Chaque autorité PCA se limite à une région géographique, à un fabricant ou à un type de dispositif.

– Autorité d'enregistrement (RA): valide et traite les demandes envoyées par le dispositif et s'assure que les dispositifs révoqués ne sont pas en mesure de publier de nouveaux certificats de pseudonyme. En outre, l'autorité d'enregistrement ne délivre pas plus d'un ensemble de certificats pour une période donnée à un dispositif. Enfin, l'autorité d'enregistrement brassera les demandes ou les rapports avant d'envoyer les demandes de signature des certificats de pseudonymes à l'autorité PCA ou de faire suivre l'information à l'autorité de gestion des comportements anormaux.

– Autorité de certification racine (RCA): premier et dernier élément de la chaîne de certification dans le système SCMS. Elle délivre les certificats pour les autorités racines intermédiaires, les générateurs de politique et les autorités de gestion des comportements anormaux.

Bibliographie

[b-UIT-T F.749.1] Recommandation UIT-T F.749.1 (2015), Exigences fonctionnelles pour les passerelles de véhicule.

[b-UIT-T H.550] Recommandation UIT-T H.550 (2017), *Architecture et entités fonctionnelles des plates-formes de passerelle de véhicule.*

[b-UIT-T X.509] Recommandation UIT-T X.509 (2019), *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: cadre général des certificats de clé publique et d'attribut.*

[b-UIT-T X.641] Recommandation UIT-T X.641 (1997), *Technologies de l'information – Qualité de service: cadre général.*

[b-UIT-T X.800] Recommandation UIT-T X.800 (1991), *Architecture de sécurité pour l'interconnexion en systèmes ouverts d'applications du CCITT.*

[b-UIT-T X.813] Recommandation UIT-T X.813 (1996), *Technologies de l'information – Interconnexion des systèmes ouverts – Cadres de sécurité dans les systèmes ouverts: non-répudiation.*

[b-UIT-T X.1252] Recommandation UIT-T X.1252 (2010), *Termes et définitions de base relatifs à la gestion d'identité.*

[b-UIT-T X.1371] Recommandation UIT-T X.1371 (2019), *Menaces pour la sécurité des véhicules connectés*.

[b-UIT-T Y.2201] Recommandation UIT-T Y.2201 (2009), *Spécifications et capacités des réseaux de prochaine génération de l'UIT-T.*

[b-UIT-T Y.2281] Recommandation UIT-T Y.2281 (2011), *Cadre applicable aux services et applications pour véhicules connectés utilisant les réseaux NGN*.

[b-ETSI EN 302 665] ETSI EN 302 665 V1.1.1 (2010-09), Intelligent Transport Systems (ITS); Communications Architecture.
<https://www.etsi.org/deliver/etsi_en/302600_302699/302665/01.01.01_60/en_302665v010101p.pdf>

[b-ETSI TS 102 940] ETSI TS 102 940 V1.3.1 (2018-04), *Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management.*
<https://www.etsi.org/deliver/etsi_ts/102900_102999/102940/01.03.01_60/ts_102940v010301p.pdf>

[b-IEEE WAVE] IEEE Std. 1609.2 (2016), *Norme de l'IEEE pour l'accès hertzien dans l'environnement des véhicules – Services de sécurité pour les messages d'applications et de gestion.*

[b-ISO 13185-1] ISO/TR 13185-1 (2012), *Systèmes intelligents de transport – Interface véhicule pour la fourniture et le support de services ITS – Partie 1: Informations générales et définition des cas d'utilisation.*

[b-OVERSEE] Open Vehicular Secure Platform, OVERSEE Project. (Site web).
<https://www.oversee-project.com/>

[b-RITA] Département des transports des États-Unis, FHWA-JPO-11-130 (2011), *An Approach to Communications Security for a Communications Data Delivery System for V2V/V2I Safety: Technical Description and Identification of Policy and Institutional Issues*.
<https://rosap.ntl.bts.gov/view/dot/3334/Share>

[b-SCMS] Crash Avoidance Metrics Partners (CAMP LLC) Vehicle Safety Communications 5 (VSC5) Consortium, *Security Credential Management System Proof-of-Concept Implementation, EE Requirements and Specifications Supporting SCMS Software Release 1.1*, 4 mai 2016. <https://www.its.dot.gov/pilots/pdf/SCMS_POC_EE_Requirements.pdf>

[b-UNECE GRVA] Document informel GRVA-01-17 du Secrétariat des Nations Unies, *Draft recommendation on cyber security of the Task Force on Cyber Security and Over-the-air issues of UNECE WP.29 GRVA*.

[b-US DOT] Département des transports des États-Unis, Safety Pilot Program. <https://www.its.dot.gov/research_archives/safety/safety_pilot_plan.htm>

[b-USDOTHS812014] Département des transports des États-Unis, National Highway Traffic Safety Administration, DOT HS 812 014 (2014), *Vehicle-to-Vehicle Communications: Readiness of V2V Technology for Application*. <https://www.nhtsa.gov/staticfiles/rulemaking/pdf/V2V/Readiness-of-V2V-Technology-for-Application-812014.pdf>

[b-US GOV] Sénateur du Massachusetts (États-Unis), Edward J, Markey, Staff Report (2015), *Tracking & Hacking: Security & Privacy Gaps Put American Drivers at Risk*. <http://www.markey.senate.gov/imo/media/doc/2015-02-06_MarkeyReport-Tracking_Hacking_CarSecurity%202.pdf>

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série D	Principes de tarification et de comptabilité et questions de politique générale et d'économie relatives aux télécommunications internationales/TIC
Série E	Exploitation générale du réseau, service téléphonique, exploitation des services et facteurs humains
Série F	Services de télécommunication non téléphoniques
Série G	Systèmes et supports de transmission, systèmes et réseaux numériques
Série H	Systèmes audiovisuels et multimédias
Série I	Réseau numérique à intégration de services
Série J	Réseaux câblés et transmission des signaux radiophoniques, télévisuels et autres signaux multimédias
Série K	Protection contre les perturbations
Série L	Environnement et TIC, changement climatique, déchets d'équipements électriques et électroniques, efficacité énergétique; construction, installation et protection des câbles et autres éléments des installations extérieures
Série M	Gestion des télécommunications y compris le RGT et maintenance des réseaux
Série N	Maintenance: circuits internationaux de transmission radiophonique et télévisuelle
Série O	Spécifications des appareils de mesure
Série P	Qualité de transmission téléphonique, installations téléphoniques et réseaux locaux
Série Q	Commutation et signalisation et mesures et tests associés
Série R	Transmission télégraphique
Série S	Equipements terminaux de télégraphie
Série T	Terminaux des services télématiques
Série U	Commutation télégraphique
Série V	Communications de données sur le réseau téléphonique
Série X	**Réseaux de données, communication entre systèmes ouverts et sécurité**
Série Y	Infrastructure mondiale de l'information, protocole Internet, réseaux de prochaine génération, Internet des objets et villes intelligentes
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication

Imprimé en Suisse
Genève, 2020