ITUPublications
Recommandations

Union internationale des télécommunications
Secteur de la normalisation

Recommandation

UIT-T X.1383 (03/2023)

SÉRIE X: Réseaux de données, communication entre systèmes ouverts et sécurité

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

---

Exigences de sécurité pour les données classées dans les communications de véhicule à tout

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 (1)	X.1140–X.1149
Sécurité des applications (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.1350–X.1369
Sécurité des systèmes de transport intelligents	**X.1370–X.1399**
Sécurité de la technologie des registres distribués (DLT)	X.1400–X.1429
Sécurité des applications (2)	X.1450–X.1459
Sécurité de la toile (2)	X.1470–X.1489
ÉCHANGE D'INFORMATIONS SUR LA CYBERSÉCURITÉ	
Aperçu général de la cybersécurité	X.1500–X.1519
Échange concernant les vulnérabilités/les états	X.1520–X.1539
Échange concernant les événements/les incidents/l'heuristique	X.1540–X.1549
Échange de politiques	X.1550–X.1559
Heuristique et demande d'informations	X.1560–X.1569
Identification et découverte	X.1570–X.1579
Échange garanti	X.1580–X.1589
Cyberdéfense	X.1590–X.1599
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 œuvre 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
Protection des données	X.1770–X.1789
SÉCURITÉ DES IMT-2020	X.1800–X.1819

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

Recommandation UIT-T X.1383

Exigences de sécurité pour les données classées dans les communications de véhicule à tout

Résumé

La sécurité des données est l'une des considérations les plus importantes pour les communications de véhicule à tout (V2X). Or, dans un environnement à ressources limitées tel que celui des communications embarquées, la protection des données consomme beaucoup de ressources étant donné que des fonctions de chiffrement sont requises.

La Recommandation UIT-T X.1383 classe les données utilisées dans les communications V2X en plusieurs types (par exemple les données relatives aux attributs de l'objet, à l'état du véhicule, à la perception de l'environnement, à la commande du véhicule ou aux services d'application ou encore les données personnelles de l'utilisateur) et attribue trois niveaux de sécurité pour les types de données classées. Sur la base de ces types de données classées et des niveaux de sécurité attribués aux données, la Recommandation énonce des exigences de sécurité pour les données classées dans les communications V2X.

Historique

Édition	Recommandation	Approbation	Commission d'études	ID Unique*
1.0	UIT-T X.1383	03-03-2023	17	11.1002/1000/15108

Mots clés

Données classées, sécurité des données, communications 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.

À la date d'approbation de la présente Recommandation, l'UIT n'avait pas été avisée de l'existence d'une propriété intellectuelle protégée par des brevets ou par des droits d'auteur afférents à des logiciels, et dont l'acquisition pourrait être requise 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 responsables de la mise en œuvre de consulter les bases de données appropriées de l'UIT-T disponibles sur le site web de l'UIT-T à l'adresse http://www.itu.int/ITU-T/ipr/.

TABLE DES MATIÈRES

Recommandation UIT-T X.1383

Exigences de sécurité pour les données classées dans les communications de véhicule à tout

1 Domaine d'application

La présente Recommandation classe les données utilisées dans les communications V2X en plusieurs types et définit un niveau de sécurité pour chaque type de données classées. Sur la base de ces types de données classées, et pour chaque niveau de sécurité, la Recommandation énonce des exigences de sécurité concernant les données classées dans les communications V2X.

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. Toute Recommandation ou autre référence étant sujette 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. La liste des Recommandations de l'UIT-T en vigueur est régulièrement publiée. La référence à un document figurant dans la présente Recommandation ne donne pas à ce document, en tant que tel, le statut d'une Recommandation.

[UIT-T X.1372] Recommandation UIT-T X.1372 (2020), *Lignes directrices relatives à la sécurité des communications de véhicule à tout autre élément (V2X)*.

[UIT-T X.1603] Recommandation UIT-T X.1603 (2018), *Exigences de sécurité des données pour le service de surveillance de l'informatique en nuage*.

[UIT-T X.1641] Recommandation UIT-T X.1641 (2016), *Lignes directrices pour la sécurité des données des clients de services en nuage*.

3 Définitions

3.1 Termes définis ailleurs

La présente Recommandation utilise les termes suivants définis ailleurs:

3.1.1 désensibilisation des données [b-UIT-T X.1217]: processus consistant à dissimuler les données sensibles.

3.1.2 cycle de vie des données [b-UIT-T X.1751]: ensemble du processus de survie après la production des données, y compris la collecte, la transmission, le stockage, l'utilisation (qui englobe l'analyse et la visualisation des données), le partage et la destruction des données.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

ABS système de freinage antipatinage (*anti-skid braking system*)

BSM message de sécurité de base (*basic safety message*)

CAM message de sensibilisation fondé sur la coopération (*cooperative awareness message*)

DoS déni de service (*denial of service*)

GDPR Règlement général sur la protection des données (*general data protection regulation*)

ICV véhicule connecté intelligent (*intelligent connected vehicle*)

TLS sécurité dans la couche de transport (*transport layer security*)

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

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

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

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

V2X véhicule à tout (*vehicle-to-everything*)

5 Conventions

Dans la présente Recommandation:

L'expression "**il est obligatoire**" indique une exigence qui doit être strictement suivie et par rapport à laquelle aucun écart n'est permis pour pouvoir déclarer la conformité à la présente Recommandation.

L'expression "**il est recommandé**" indique une exigence qui est recommandée mais qui n'est pas absolument nécessaire. Cette exigence n'est donc pas indispensable pour déclarer la conformité.

Le terme "**peut**" indique une exigence optionnelle qui est admissible, sans pour autant être en quoi que ce soit recommandée.

L'expression "**il est interdit**" indique une exigence qui doit être strictement suivie et par rapport à laquelle aucun écart n'est permis pour pouvoir déclarer la conformité à la présente Recommandation.

6 Cycle de vie des données dans les communications V2X

6.1 Cycle de vie des données

Le cycle de vie des données est défini d'après le flux de données dans les activités de l'organisation concernée dans un environnement de communications de véhicule à tout (V2X). D'après la situation effective des communications V2X, le cycle de vie de la sécurité des données est analogue à celui qui est présenté dans la Recommandation [UIT-T X.1641], qui recouvre les étapes décrites ci-après de la collecte, de la transmission, du stockage, de l'utilisation, de la migration, de la destruction et de la sauvegarde et de la restauration des données:

– **Collecte de données**: processus consistant à produire de nouvelles données dans le système interne de l'organisation et à recueillir des données en provenance de l'extérieur. Il existe deux formes de collecte de données dans les communications V2X, l'une concernant les données produites dans les divers processus commerciaux de communications V2X, l'autre concernant les données recueillies par les utilisateurs, partenaires et autres tiers concernés.

– **Transmission de données**: processus par lequel les données circulent d'une entité à une autre au sein de l'organisation. Dans le cadre des communications V2X, la transmission de données consiste principalement dans la réalisation de flux de données liés aux services de communication V2X entre les systèmes et les équipements.

– **Stockage des données**: processus de stockage des données sur support physique ou dans le nuage sous tout format numérique. Cette étape a lieu en général de façon presque simultanée avec celle de la collecte des données.

– **Utilisation des données**: série d'activités, dont la recherche, l'analyse et le traitement de données, menées par les organisations pour les données dynamiques dans le cadre des communications V2X. Une actualisation des données et une production de nouvelles données peuvent intervenir à ce stade.

– **Migration des données**: processus de transfert des données à des tiers extérieurs. Cette étape recouvre l'affichage des données et leur fourniture à des utilisateurs dans le cadre des communications V2X. Elle recouvre aussi le processus de fourniture mutuelle des données au titre de la coopération interentreprises et interinstitutions dans le cadre des communications V2X.

– **Destruction des données**: processus visant à rendre les données indisponibles, définitivement ou temporairement, par des moyens physiques ou techniques. La destruction des données peut être liée à des raisons de coût pour l'entreprise aussi bien qu'à des impératifs extérieurs de conformité ou d'ordre économique. En particulier, s'il existe une réglementation relative à la conservation des données, il convient de considérer que les prestataires de services devraient effacer ou anonymiser comme il se doit les données collectées afin d'empêcher la récupération des données qui ont atteint leur date limite de conservation ou pour lesquelles les utilisateurs n'accordent plus leur consentement.

– **Sauvegarde et restauration des données**: processus consistant à copier tout ou partie des données sur d'autres supports de stockage afin d'éviter la perte de données et de récupérer les données originales à l'aide des données de sauvegarde en cas de perte des données.

6.2 Analyse des menaces

Les données qui interviennent dans les communications V2X doivent aussi faire face à des menaces et des problèmes de sécurité analogues à ceux qui sont répertoriés dans les Recommandations [UIT-T X.1603] et [UIT-T X.1641]. On a récapitulé dans le Tableau 6-1 ci-après une partie de ces menaces et problèmes liés à la sécurité des données dans les communications V2X.

Tableau 6-1 – Menaces et problèmes liés au cycle des données intervenant dans les communications V2X

Cycle de vie des données	Menaces et problèmes en matière de sécurité
Collecte des données	a) Collecte de données sans autorisation b) Vulnérabilité de l'interface d'acquisition c) Usurpation d'identité d) Interception et falsification e) Accès non sécurisé aux services f) Accès non autorisé aux fonctions d'administration
Transmission des données	a) Interception b) Usurpation d'identité c) Écoutes illicites d) Accès non autorisé e) Attaque par déni de service (DoS)
Stockage des données	a) Perte et fuite de données b) Indisponibilité des services
Utilisation des données	a) Utilisation abusive des données b) Menaces internes c) Vulnérabilité du système d) Écoutes illicites
Migration des données	a) Utilisation abusive des données b) Vulnérabilité du système c) Fausse déclaration d) Attaque DoS

Tableau 6-1 – Menaces et problèmes liés au cycle des données intervenant dans les communications V2X

Cycle de vie des données	Menaces et problèmes en matière de sécurité
Destruction des données	a) Usurpation d'identité b) Vulnérabilité du système
Sauvegarde et restauration des données	a) Vulnérabilité du système

7 Données classées et communications V2X

Le présent paragraphe indique la politique de classement des données applicable aux communications V2X. Les six catégories de données – données relatives aux attributs de l'objet, à l'état du véhicule, à la perception de l'environnement, à la commande du véhicule et aux services d'application, et données personnelles de l'utilisateur – sont décrites au § 7.2.

7.1 Identification des données en fonction des scénarios de communications V2X

Les données traitées dans les communications V2X peuvent être identifiées d'après les scénarios des communications effectives. La Recommandation [UIT-T X.1372] classe les scénarios de communications V2X comme suit: communications de véhicule à véhicule (V2V), de véhicule à infrastructure (V2I), de véhicule à dispositif nomade (V2D) et de véhicule à piéton (V2P). Le présent paragraphe décrit les processus de communications et les données correspondant à chaque scénario de communications.

7.1.1 Données intervenant dans les communications V2V

La Recommandation [UIT-T X.1372] répertorie trois scénarios de communications: transmission d'avertissements V2V; communications V2V en mode peloton; et communications V2V en mode balise. Dans un scénario de transmission d'avertissements V2V, un message d'avertissement est transmis d'un véhicule à l'autre. Dans un scénario de communications V2V en mode peloton, des groupes de véhicules échangent entre eux des informations sur l'état des véhicules. Dans un scénario de communications V2V en mode balise, chaque véhicule envoie ses informations sur l'état du véhicule. Le Tableau 7-1 présente les données intervenant dans les communications V2V.

Tableau 7-1 – Données intervenant dans les communications V2V

Catégorie	Scénario	Données
Véhicule à véhicule	Transmission d'avertissements V2V	• Message d'avertissement • Message de sécurité de base (BSM) • Message de sensibilisation fondé sur la coopération (CAM)
	Communications V2V en mode peloton	• BSM • CAM
	Communications V2V en mode balise	• BSM • CAM

Les spécifications techniques du BSM et du CAM sont décrites dans les Documents [b-SAE J2735] et [b-ETSI TS 102 637-2], respectivement.

7.1.2 Données intervenant dans les communications V2I

La Recommandation [UIT-T X.1372] répertorie deux scénarios de communication V2I: les avertissements V2I et l'échange d'informations V2I. Le scénario des avertissements V2I concerne l'échange de messages d'avertissement entre un véhicule et des infrastructures. Dans le cadre de l'échange d'informations V2I, un véhicule et une infrastructure communiquent entre eux pour actualiser les informations sur le trafic et/ou les informations relatives aux services d'infoloisirs. Le Tableau 7-2 présente les données intervenant dans les communications V2I.

Tableau 7-2 – Données intervenant dans les communications V2I

Catégorie	Scénario	Données
Véhicule à infrastructure	Avertissements V2I	• Messages d'avertissement
	Échange d'informations V2I	• Affichage embarqué • Informations embarquées • Informations sur la phase des signaux • Informations sur la durée des feux de circulation • État de la chaussée • Conditions météorologiques • Conditions de visibilité • Informations sur les travaux routiers

7.1.3 Données intervenant dans les communications V2D

Dans un scénario de communications V2D, un véhicule communique avec un dispositif nomade tel qu'un smartphone, un ordinateur portable ou un système de navigation embarqué. La Recommandation [UIT-T X.1372] répertorie deux scénarios de communications V2D: les communications V2D par liaison indirecte et les communications V2D par liaison directe. La différence entre ces scénarios est le mode de communication, l'un et l'autre traitant les mêmes types de données. Les communications V2P sont considérées comme un cas particulier de communications V2D dans la Recommandation [UIT-T X.1372]. Le Tableau 7-3 présente les données intervenant dans les communications V2D.

Tableau 7-3 – Données intervenant dans les communications V2D

Catégorie	Scénario	Données
Véhicule à dispositif nomade	Communications V2D par liaison indirecte/directe	• Données sur le matériel concernant le véhicule • Données sur les logiciels concernant le véhicule • Données sur le matériel concernant les dispositifs • Données sur les logiciels concernant les dispositifs • Données relatives aux plates-formes de services • Données de services liées aux applications

7.2 Classement des données

Le présent paragraphe décrit le classement des données pour ce qui est données traitées dans le cadre des communications V2X.

Les données liées aux communications V2X sont prises en compte afin de répondre aux exigences de lois et règlements relatifs à la protection des données personnelles tels que le règlement général sur la protection des données (RGPD), et les données décrites dans la présente Recommandation ne peuvent renvoyer à des informations se rapportant à une personne spécifique ou identifiable.

7.2.1 Données relatives aux attributs de l'objet

Les données relatives aux attributs de l'objet renvoient aux attributs des entités participant aux communications V2X, qui peuvent être subdivisées en trois types: véhicules, dispositifs mobiles et plates-formes de services en nuage:

– Les données relatives aux attributs des véhicules renvoient aux propriétés des véhicules, entre autres la marque, le type, le logo, la couleur, etc.

– Les données relatives aux attributs des dispositifs mobiles renvoient à des propriétés du dispositif mobile comme la marque, le type, la couleur, etc.

– Les données relatives aux attributs des plates-formes de services concernent des propriétés liées à la plate-forme de services comme la révision, la fabrication, etc.

7.2.2 Données relatives à l'état du véhicule

Les données relatives à l'état du véhicule renvoient à des informations sur l'état des véhicules qui sont étroitement liées aux services d'information utilisés dans les communications V2X. Elles portent sur l'état et les paramètres de fonctionnement des systèmes du véhicule: système de groupe motopropulseur, système de châssis, système de sécurité, système de carrosserie, système de confort et système électrique.

Plus précisément, les données relatives à l'état du véhicule comprennent les informations provenant du système de contrôle embarqué (entre autres, le signal de la commande de la pompe à carburant, l'alarme du capteur de pression d'air, le signal physique du frein moteur, etc.), du système de transmission (dont le couple, le taux de consommation de carburant, etc.), du système de refroidissement (comme la température du liquide de refroidissement), du système de boîte de vitesses (données de démarrage et d'accélération du véhicule, etc.), du système de sécurité (comme l'état des coussins gonflables et de l'utilisation des ceintures de sécurité, etc.), du système de châssis (données relatives à l'état du réseau de bord, du système de direction, du freinage ABS, du contrôle de la pression des pneus, etc.), du système de confort (données relatives à l'ouverture de la climatisation, au réglage des sièges, au système des vitres, à l'utilisation de l'éclairage, etc.) et des autres systèmes auxiliaires.

Sur la base de la description de l'état de fonctionnement du véhicule, on peut répartir les données sur l'état du véhicule en deux types: données sur l'état du véhicule en mouvement et données sur l'état du véhicule à l'arrêt.

– Les données sur l'état du véhicule en mouvement concernent l'état de fonctionnement des systèmes du véhicule (par exemple dans le cas du système de climatisation, qui dépend de la température et de l'humidité à l'intérieur du véhicule).

– Les données sur l'état du véhicule à l'arrêt concernent l'état des systèmes de confort (état de la climatisation, par exemple), des systèmes de sécurité (état de l'utilisation des ceintures de sécurité), etc.

7.2.3 Données relatives à la perception de l'environnement

Les données relatives à la perception de l'environnement concernent principalement l'environnement extérieur des véhicules et recouvrent l'information provenant des équipements externes, des terminaux ou des piétons (en rapport avec les communications entre véhicules ou les interactions des services d'information dans le cadre des communications V2X), notamment sur la vitesse, les feux de circulation et l'infrastructure routière dans le cadre des communications entre véhicules. Les informations recueillies par les radars de vitesse et les caméras concernant l'infrastructure routière, le sens de la conduite et du déplacement, l'état de la conduite et du déplacement, la vitesse, la distance, les données relatives à un éventuel état de collision ou à son absence, et les données relatives aux stations de recharge (pour batteries) et à d'autres équipements acquis pour les véhicules électriques, qui font également partie des données relatives à la perception de l'environnement.

7.2.4 Données relatives à la commande du véhicule

Les données relatives à la commande du véhicule ont trait à la commande du véhicule dans le cadre des communications V2X et relèvent de trois sous-types principaux, à savoir les données relatives à la commande de véhicule pour la conduite automatique/la conduite assistée intelligente, pour la commande à distance et pour la conduite à distance:

– Les données relatives à la commande de véhicule pour la conduite automatique/la conduite assistée intelligente sont les données des instructions de commande liées à la conduite automatique ou à la conduite assistée intelligente. Ces données reposent sur le traitement effectué par les systèmes de perception de l'environnement et de décision intelligente et servent à la production des données de comportement pour la commande intelligente des véhicules, liées au freinage ou au train roulant, au changement de vitesses automatique et à la commande intégrée du châssis.

– Les données relatives à la commande de véhicule pour la commande à distance se rapportent aux instructions fournies aux véhicules par des applications, des plates-formes de service, etc. et comprennent également les données relatives au verrouillage/déverrouillage des portes à distance, à la climatisation à distance, à l'activation à distance des vitres et des éclairages, etc.

– Les données relatives à la commande de véhicule pour la conduite à distance renvoient aux cas d'utilisation de la conduite à distance, qui peuvent être subdivisés en deux, avec d'une part, les cas d'utilisation dans lesquels le conducteur à distance est un humain et, d'autre part, les cas où le conducteur à distance possible est un "nuage". Les données relatives à la commande de véhicule pour la conduite à distance se rapportent à des flux vidéo à l'extérieur des véhicules visant à montrer l'environnement autour d'un véhicule sur la voie ou des flux audio à l'extérieur du véhicule fournis à un conducteur à distance pour l'aider à prendre des décisions. Les données destinées à la conduite à distance peuvent également renvoyer à un flux vidéo ou audio à l'intérieur du véhicule, fournis au conducteur à distance à des fins de surveillance. En outre, les données relatives à la commande de véhicule pour la conduite à distance concernent les données relatives aux instructions de commande à distance fournies par le conducteur à distance au véhicule. À titre d'exemple, des instructions concernant l'accélération ou la manœuvre peuvent être générées et envoyées lorsqu'elles sont déclenchées par un événement commandé, tel qu'une instruction de freinage [b-ETSI TR 126 985], [b-3GPP TR 22.886].

7.2.5 Données relatives aux services d'application

Les données relatives aux services d'application concernent l'application de l'interaction des informations dans le cadre des communications V2X. Elles recouvrent les données liées aux services d'information dans le cadre des communications V2X, outre les données relatives aux attributs de l'objet, à l'état du véhicule, à la perception de l'environnement et à la commande du véhicule, et les données personnelles des utilisateurs, dont les données des systèmes d'infoloisirs, les données de gestion et de suivi concernant la sécurité routière et les données de service liées au véhicule, etc.:

– Les données d'information et de loisirs sont liées aux services de loisirs assurés dans le cadre des communications V2X, dont le téléchargement de contenus multimédias, la navigation sur des sites web et l'abonnement à des services de diffusion destinés à une certaine population, ainsi que les prévisions météorologiques, etc.

– Les données de gestion et de contrôle sur la sécurité routière concernent la sécurité routière et la gestion du trafic, notamment l'alerte précoce en matière de sécurité routière, les secours d'urgence, le suivi et la gestion à distance des véhicules, etc.

– Les données sur les services liés aux véhicules concernent des services après-vente assurés dans le contexte des communications V2X comme l'entretien des véhicules, la gestion des véhicules d'occasion, l'assurance financière et le commerce électronique connexe. À titre d'exemple, la fréquence d'entretien de certains types de pièces automobiles de telle ou telle marque de véhicules fait partie des données sur les services liés aux véhicules.

7.2.6 Données personnelles de l'utilisateur

Les données personnelles de l'utilisateur renvoient aux informations personnelles concernant l'utilisateur qui sont utilisées et/ou produites dans le cadre des communications V2X. Le classement et la protection des données personnelles de l'utilisateur ne sont pas abordés dans le présent paragraphe.

En conséquence, si les données mentionnées dans le Tableau 7-4 à titre d'exemple correspondent aux données personnelles de l'utilisateur visées dans les lois relatives à la protection de la vie privée ou des règlements comme le GDPR, alors le texte législatif ou réglementaire en question prévaudra sur la politique de classement.

7.3 Niveaux de sécurité des données

En fonction de ces facteurs, conjugués aux objectifs de sécurité des données, à l'importance des données considérées et aux conséquences des incidents de sécurité éventuels, chaque catégorie de données peut être classée selon trois niveaux:

– Le **niveau 1** (données moins protégées) concerne des données accessibles au public dans le cadre des communications V2X comme la version du logiciel de la plate-forme V2X.

– Le **niveau 2** (données moyennement protégées) concerne des données qu'il est impératif de protéger par des mesures de sécurité, dont les données de véhicule acquises dans le cadre des communications V2V, le compte de connexion et le mot de passe pour les communications V2X.

– Le **niveau 3** (données très protégées) concerne des données qu'il est impératif de protéger davantage que celles du niveau 2 (données moyennement protégées) dans le cadre des communications V2X, parmi lesquelles les informations relatives aux transactions financières dans le cadre des communications V2D, les données de performance essentielles des véhicules et les données d'authentification de l'identité liées aux communications V2X.

Par données confidentielles, on entend uniquement les données confidentielles des entreprises associées aux communications V2X, les informations personnelles des utilisateurs n'entrant pas ici en ligne de compte.

On trouvera au Tableau 7-4 des renseignements détaillés sur les niveaux de sécurité des données dans le cadre des communications V2X et des exemples connexes.

Tableau 7-4 – Exemples de niveaux de sécurité des données dans le cadre des communications V2X

Catégorie des données dans le cadre des communications V2X		**Niveau de sécurité des données dans le cadre des communications V2X**	**Exemples**
Données relatives aux attributs de l'objet	Données relatives aux attributs du véhicule	Niveau 1	Marque, type, logo ou couleur d'un véhicule.
		Niveau 2	Paramètres de performance de tel ou tel type de véhicule.
		Niveau 3	Données de configuration matérielle et logicielle propres à tel ou tel type de véhicule.
	Données relatives aux attributs du dispositif mobile	Niveau 1	Marque, type, logo ou couleur d'un terminal mobile.
		Niveau 2	Données sur l'état des équipements en rapport avec certaines fonctions importantes dans le cadre des communications V2X.
		Niveau 3	Paramètres de fonctionnement essentiels et informations de configuration de tel ou tel dispositif mobile.
	Données relatives aux attributs de la plate-forme de services en nuage	Niveau 1	Type et nom d'une plate-forme de services en nuage.
		Niveau 2	Informations relatives au matériel, au système d'exploitation ou au logiciel d'une application.
		Niveau 3	Paramètres de fonctionnement essentiels et informations de configuration de tel ou tel dispositif mobile d'une plate-forme de services.
Données relatives au statut du véhicule	Données relatives au statut du véhicule en mouvement	Niveau 1	État d'un système de climatisation. Température intérieure des véhicules.
		Niveau 2	État de fonctionnement des coussins gonflables et des ceintures de sécurité, etc. Données perçues par des capteurs du véhicule qui concernent des aspects importants pour le maniement du véhicule comme la pression des pneus.
		Niveau 3	Principaux indicateurs techniques sur le fonctionnement du véhicule. Données perçues par des capteurs du véhicule qui concernent des aspects importants pour le maniement du véhicule, notamment les données provenant des capteurs de collision.
	Données relatives au statut du véhicule à l'arrêt	Niveau 1	Fréquence d'utilisation d'un système de climatisation au cours d'une certaine période.
		Niveau 2	Consommation moyenne de carburant d'un véhicule.
		Niveau 3	Données confidentielles du système du véhicule.

Tableau 7-4 – Exemples de niveaux de sécurité des données dans le cadre des communications V2X

Catégorie des données dans le cadre des communications V2X		Niveau de sécurité des données dans le cadre des communications V2X	Exemples
Données relatives à la perception de l'environnement	Données relatives à la perception de l'environnement extérieur du véhicule	Niveau 1	Type de chaussée (voie rapide ou route de campagne ou trottoir), état de la chaussée (intacte ou humide ou glissante), limitation de vitesse, informations sur la répartition et l'état des feux de signalisation, informations sur l'état des feux de signalisation, les embouteillages, les accidents de la circulation, etc.
		Niveau 2	Dans le scénario des communications de véhicule à véhicule, les informations après désensibilisation concernant les véhicules à proximité, notamment sur l'emplacement physique, la longitude et la latitude, l'heure de mise à jour, la vitesse de conduite, la marche avant ou le changement de voie. Dans le scénario des communications de véhicule à piéton, les données après désensibilisation concernant par exemple l'emplacement, la distance, la vitesse et l'état de mouvement des piétons à proximité, et le risque de collision.
		Niveau 3	Dans le scénario des communications de véhicule à véhicule, les données après désensibilisation des véhicules adjacents pendant une certaine période, concernant des aspects comme l'itinéraire, l'emplacement, l'heure, le stationnement, etc.
Données relatives à la commande du véhicule	Données relatives à la commande de véhicule pour la conduite automatique /la conduite assistée intelligente	Niveau 1	Données sonores apportant des indications dans le cadre du système d'aide à la marche arrière.
		Niveau 2	Dans l'application de maintien dans la voie du système de conduite assistée intelligente, lorsque le véhicule a tendance à dévier de sa voie, des données de commande d'avertissement concernant par exemple l'instabilité de la commande de direction ou l'indication d'un feu rouge ou d'un feu vert au tableau de bord sont envoyées.
		Niveau 3	Instructions de confirmation du système de stationnement intelligent en stationnement automatique.
		Niveau 1	Données de lecture générales relatives au suivi à distance des communications V2X.
		Niveau 2	Instruction visant à démarrer un véhicule ou à en engager la manœuvre à distance.

Tableau 7-4 – Exemples de niveaux de sécurité des données dans le cadre des communications V2X

Catégorie des données dans le cadre des communications V2X		Niveau de sécurité des données dans le cadre des communications V2X	Exemples
	Données relatives à la commande de véhicule pour la commande à distance	Niveau 3	Mise en œuvre d'instructions relatives à la commande à distance de plusieurs véhicules, notamment d'une flotte, au moyen de la plate-forme de services de communications V2X.
	Données relatives à la commande de véhicule pour la conduite à distance	Niveau 1	Flux vidéo et flux audio à l'intérieur d'un véhicule dont les impératifs concernant la durée de transmission peuvent être plus souples que ceux applicables aux flux vidéo et audio à l'extérieur du véhicule, et qui peuvent être utilisés par le conducteur à distance pour suivre la situation à l'intérieur du véhicule.
		Niveau 2	Flux audio à l'extérieur d'un véhicule pouvant être fournis à un conducteur à distance pour transmettre les sons et les coups de klaxon produits par les autres véhicules.
		Niveau 3	Les capteurs ou les dispositifs de restitution, comme les écrans d'affichage ou les systèmes audio, sont utilisés pour les instructions de manœuvre fournies par le conducteur à distance. Les instructions devraient être fournies avec une grande fiabilité et un faible temps de latence et doivent être prises en compte, en particulier lorsqu'elles sont liées à un évènement d'alarme (par exemple l'instruction de freinage). Données des capteurs vidéo (caméra) et audio (microphone) (il peut également s'agir de données de capteurs radar ou lidar) visant à enregistrer des sons ou des vidéos extérieurs pour l'identification avancée et non visuelle des obstacles sur la route, comme les véhicules de secours, les piétons, etc. Les données des capteurs de l'état du véhicule (accélération, vitesse, direction, position, etc.) peuvent être envoyées à intervalles fixes par le véhicule au conducteur à distance, avec une grande fiabilité, dans la mesure où certains flux de capteurs peuvent être essentiels au bon déroulement de la conduite.
	Données des systèmes d'infoloisirs	Niveau 1	Données des émissions de radio
		Niveau 2	Relevés de navigation des achats en ligne après désensibilisation

Tableau 7-4 – Exemples de niveaux de sécurité des données dans le cadre des communications V2X

<table>
<tr><th colspan="2">Catégorie des données dans le cadre des communications V2X</th><th>Niveau de sécurité des données dans le cadre des communications V2X</th><th>Exemples</th></tr>
<tr><td rowspan="6">Données relatives aux services d'application</td><td></td><td>Niveau 3</td><td>Enregistrements audio et vidéo après désensibilisation dans les applications de services d'information</td></tr>
<tr><td rowspan="3">Données de gestion et de contrôle sur la sécurité routière</td><td>Niveau 1</td><td>Alertes sur les embouteillages, données d'alerte en temps réel sur les accidents de la circulation, etc.</td></tr>
<tr><td>Niveau 2</td><td>Données d'avertissement de collision entre véhicules à la suite du stationnement d'un véhicule devant un autre véhicule de la file</td></tr>
<tr><td>Niveau 3</td><td>Données de télésurveillance des véhicules dans la circulation routière.</td></tr>
<tr><td rowspan="3">Données de services liées au véhicule</td><td>Niveau 1</td><td>Après désensibilisation, enregistrement des données sur le comportement d'utilisation du système d'infoloisirs, concernant l'utilisation, le fonctionnement et d'autres informations du système d'infoloisirs du véhicule.</td></tr>
<tr><td>Niveau 2</td><td>Après désensibilisation, données relatives au comportement de conduite du véhicule.</td></tr>
<tr><td>Niveau 3</td><td>Données après désensibilisation, dont les préférences personnelles et les habitudes de comportement du propriétaire du véhicule, d'après la durée du trajet, l'itinéraire, la localisation et les données sur le comportement d'utilisation du système d'infoloisirs, ou les principaux paramètres du véhicule en fonction de l'état de celui-ci et des données sur la perception de l'environnement, etc.</td></tr>
<tr><td>Données personnelles de l'utilisateur</td><td>s.o.</td><td>s.o.</td><td>s.o.</td></tr>
<tr><td colspan="4">Description du contenu du Tableau 7-4:
1) s.o.: sans objet
2) Les données après désensibilisation dont il est question dans le Tableau 7-4 ne peuvent, une fois anonymisées, rendues floues et traitées par d'autres moyens techniques, identifier directement ou indirectement les personnes ou indiquer leurs informations personnelles. Les méthodes de désensibilisation des données sont notamment l'anonymat, la désidentification, la diversité, la suppression des données, la perturbation des données, la confidentialité différentielle, etc. L'organisation liée aux communications V2X doit prendre les mesures de désensibilisation des données qui s'imposent à l'issue d'un examen complet des caractéristiques des sujets de données, du degré de sensibilité des données et des critères d'exploitation des données.</td></tr>
</table>

8 Exigences de sécurité

Le présent paragraphe énonce les exigences de sécurité élémentaires, intermédiaires et avancées, que l'on a définies selon une correspondance stricte avec les données des niveaux 1 à 3.

8.1 Niveaux d'exigences de sécurité

D'après le classement des catégories de données, on a spécifié des méthodes ou des mesures de sécurité pour chaque niveau. Trois niveaux de sécurité peuvent être adoptés: les exigences de sécurité élémentaires, les exigences de sécurité intermédiaires et les exigences de sécurité avancées. En général, les exigences de sécurité élémentaires ont pour objet de protéger le niveau 1 (données moins protégées), les exigences de sécurité intermédiaires de protéger le niveau 2 (données moyennement protégées) et les exigences de sécurité avancées de protéger le niveau 3 (données très protégées). Le Tableau 8-1 présente les exigences de sécurité en fonction du niveau de sécurité des données liées aux communications V2X.

Les entreprises peuvent aussi opter pour certaines mesures de sécurité en fonction de leur propre situation ou de la confidentialité des données.

Tableau 8-1 – Exigences de sécurité en fonction du niveau de sécurité des données liées aux communications V2X

Niveau de sécurité des données liées aux communications V2X	Niveau des exigences de sécurité		
	Élémentaire	**Intermédiaire**	**Avancé**
Niveau 1 (données moins protégées)	*	s.o.	s.o.
Niveau 2 (données moyennement protégées)	*	*	s.o.
Niveau 3 (données très protégées)	*	*	*
*: couvert; s.o.: sans objet.			

8.2 Exigences de sécurité élémentaires

1) Collecte des données

- Les données utilisées dans les communications V2X devraient être classées d'après l'ensemble de critères suivant: objectifs de sécurité des données, importance des données et conséquences des incidents de sécurité possibles.
- Le principe de minimisation doit être suivi dans le processus de collecte des données. Seules les données relatives aux fonctions d'entreprise peuvent être recueillies.
- Les données recueillies doivent être classées et administrées d'après les méthodes de classement des données et autres décrites aux paragraphes 6 et 7. Des mesures de sécurité différentes devraient être formulées et appliquées pour les différents niveaux de données.

2) Transmission des données

- Les exigences de sécurité globalement applicables à la transmission des données dans les communications V2X ne devraient pas être inférieures à celles du réseau de communications général.

- Des stratégies et mesures de sécurité de transmission des données différentes devraient être adoptées pour les différents aspects (catégories de données, processus d'entreprise et risques de sécurité) des scénarios de communication V2X.
- Des protocoles de sécurité tels que le TLS (sécurité dans la couche de transport) devraient être utilisés pour garantir la sécurité de la transmission des données dans les scénarios de communications entre le véhicule et les autres entités.
- Il devrait pouvoir être détecté que les données ont été corrompues lors de la transmission.

3) Stockage des données

- Pour les données stockées dans les terminaux des véhicules et les plates-formes de service, il convient d'adopter des mécanismes de cryptage des données au niveau des équipements et des systèmes associés aux communications V2X. Des paramètres comme l'algorithme, la force et le mode du cryptage devraient être pris en charge par une configuration facultative.
- Il devrait être possible de garantir la sécurité des données du cache dans la plate-forme de service ou le système du véhicule. Les données stockées dans le système de cache devraient être cryptées.
- Pour les données stockées dans les terminaux de véhicules et les plates-formes de services, il convient d'adopter des mécanismes de contrôle de l'accès aux données pour en empêcher l'accès, la modification et la suppression non autorisés, ainsi que l'accès aux informations transversales.
- Il devrait être possible de vérifier l'intégrité des données lors du processus de stockage pour empêcher que des données ne soient altérées, supprimées ou insérées. Une alerte devrait être envoyée à l'utilisateur lorsque l'intégrité des données est détruite.

4) Utilisation des données

- Le traitement des données devrait être limité à ce qui est autorisé et au strict minimum des besoins opérationnels.
- L'utilisation des données devrait être soumise à autorisation et à vérification.
- Les buts et la portée de l'utilisation des données devraient être conformes aux prescriptions des lois et règlements nationaux applicables.
- Au cours de l'analyse et de l'extraction des données, les données sources et les résultats de l'extraction devraient être signés pour empêcher que les données ne soient supprimées ou altérées par malveillance ou utilisées sans restriction.
- Des mesures d'administration et des mesures techniques devraient être adoptées pour le transfert ou l'exportation de données entre dispositifs, systèmes et plates-formes de l'Internet des véhicules, afin d'en garantir la sécurité.

5) Migration des données

- Il devrait être procédé à une évaluation des capacités de sécurité avant la migration des données afin de garantir la sécurité de la migration.
- Il convient de garantir la continuité des activités et des applications lors de la migration de données entre différents dispositifs de données.
- Un plan de migration devrait être établi, la faisabilité de celui-ci et les risques connexes devraient être évalués, et les mesures correspondantes de maîtrise des risques devraient être élaborées ensuite afin de préparer la migration des données.

6) Destruction des données

- Une stratégie et un système de gestion devraient être établis concernant la destruction des données afin de préciser l'objet de la destruction et le processus connexe. Un mécanisme d'examen et d'approbation devrait être établi concernant la destruction des données, et des fonctions devraient être instituées pour assurer la supervision du processus de destruction.
- Des mesures devraient être prévues pour supprimer les données qui ont atteint leur date limite de conservation ou détruire immédiatement les données pour lesquelles les utilisateurs n'accordent plus leur consentement.
- Des mesures devraient être prévues pour faciliter la suppression des données restantes à l'issue de la migration des données ou des données devenues caduques.
- Des mesures devraient être prévues pour supprimer toutes les copies des données de sauvegarde.

7) Sauvegarde et restauration des données

- Des mécanismes de sauvegarde et de récupération des données devraient être établis avant la migration des données.
- La sauvegarde et la récupération des données locales devraient être assurées.
- Un mécanisme de sauvegarde régulière de l'ensemble des données devrait être mis en place, et le cycle recommandé ne devrait pas être inférieur à une sauvegarde par semaine.
- Les données de sauvegarde devraient faire l'objet des mêmes droits de contrôle de l'accès et des mêmes exigences de stockage sécurisé que les données d'origine.

8.3 Exigences de sécurité intermédiaires

Les exigences de sécurité intermédiaires consistent dans une série de surensembles des exigences de sécurité élémentaires. Les exigences ci-après seront ajoutées par rapport aux exigences de sécurité élémentaires de chaque phase du cycle de vie des données:

1) Collecte des données

Outre les exigences de sécurité élémentaires, les exigences ci-après devraient aussi être remplies:

- Lors de la collecte des données de niveau 2, les données originales devraient être sauvegardées afin d'éviter l'omission et la perte de données.
- Des mécanismes d'identification devraient être adoptés afin de garantir l'authenticité de la collecte des données.
- Des mécanismes de vérification des données devraient être adoptés afin de garantir l'intégrité de la collecte des données.

2) Transmission des données

Outre les exigences de sécurité élémentaires, les exigences ci-après devraient aussi être remplies:

- Un réseau privé ou un réseau privé virtuel devraient être adoptés pour la transmission des données de la plate-forme principale de services automobiles et de l'Internet des véhicules afin d'en assurer l'isolement par rapport à l'Internet.
- Dans le cadre des communications V2V/V2I, un certificat d'identité de confiance, capable de vérifier l'identité du nœud de transmission des données, devrait être prévu, et les informations d'authentification ne devraient pas divulguer d'informations confidentielles.

- Le véhicule devrait être capable d'identifier les demandes de connexion illicites en provenance de réseaux cellulaires de manière à filtrer les paquets malveillants.
- Pour les données de niveau 2, dont les données d'instructions de commande à distance, la fiabilité de la source de données devrait être vérifiée pour faire en sorte que les données ne soient pas falsifiées.

3) Stockage des données

Outre les exigences de sécurité élémentaires, les exigences ci-après devraient aussi être remplies:

- L'intégrité des données devrait pouvoir être vérifiée lors du processus de stockage pour empêcher que des données ne soient altérées, supprimées ou insérées, et les mesures de restauration nécessaires devraient être prévues pour les cas où l'intégrité des données est détruite.
- Des informations d'identification devraient être définies pour les fichiers de données stockés dans le véhicule connecté intelligent (ICV), les plates-formes de service et les applications pour éviter que ces fichiers ne soient utilisés dans des dispositifs et systèmes non autorisés.
- Pour ce qui est du système de mise en cache de la plate-forme de services, dans le cadre des communications V2X, des enregistrements opérationnels spécifiques devraient être conservés afin de protéger les données mises en cache du niveau 2.
- L'ensemble du processus de gestion du journal de données devrait être conçu de façon à pouvoir prévenir les menaces de répudiation des données.

4) Utilisation des données

Outre les exigences de sécurité élémentaires, les exigences ci-après devraient aussi être remplies:

- Pour la recherche des données du niveau 2, un traitement flou devrait être appliqué à des opérations comme la recherche, l'affichage extérieur et les statistiques.
- L'utilisation des données du niveau 2 devrait être auditée et un journal d'audit devrait être produit.

5) Migration des données

Outre les exigences de sécurité élémentaires, les exigences ci-après devraient aussi être remplies:

- Un plan de migration devrait être établi, la faisabilité de celui-ci et les risques connexes devraient être évalués, et les mesures correspondantes de maîtrise des risques devraient être élaborées ensuite afin de préparer la migration des données.

6) Destruction des données

Outre les exigences de sécurité élémentaires, les exigences ci-après devraient aussi être remplies:

- Il devrait être veillé à ce que l'espace de stockage des ressources liées aux communications V2X – fichiers, répertoires, données de la base de données, etc. – ne soit pas libéré ou réattribué à d'autres utilisateurs tant que ces ressources ne sont pas complètement effacées.
- En ce qui concerne le terminal embarqué, afin d'éviter les fuites de données liées au remplacement de composants du véhicule, il devrait être prévu une fonction d'effacement des données du terminal du véhicule, pour faire en sorte que ces données ne puissent pas être récupérées.

7) Sauvegarde et restauration des données

Outre les exigences de sécurité élémentaires, les exigences ci-après devraient aussi être remplies:

- Pour les données de sauvegarde locales ou distantes, une sauvegarde complète des données doit être effectuée au moins une fois par semaine, et les sauvegardes incrémentielles doivent faire l'objet d'une sauvegarde au moins une fois par jour. En outre, un mécanisme de sauvegardes multiples doit être mis en place.
- Les données de sauvegarde doivent être cryptées et stockées.

8.4 Exigences de sécurité avancées

Les exigences de sécurité avancées consistent dans une série de surensembles des exigences de sécurité élémentaires. Outre les exigences de sécurité intermédiaires de chaque phase du cycle de vie des données, les exigences ci-après devraient être adoptées:

1) Collecte des données

- Les exigences de protection sont identiques à celles qui relèvent des exigences de sécurité intermédiaires.

2) Transmission des données

Outre les exigences de sécurité intermédiaires, les exigences ci-après devraient aussi être remplies:

- Toute atteinte à l'intégrité des données devrait être détectée pendant la transmission, et il convient de prendre les mesures nécessaires pour récupérer les données après la détection d'une atteinte à leur intégrité.
- Concernant les données confidentielles du niveau 3, il convient d'adopter l'authentification mutuelle pour répondre aux menaces de falsification et de fuite de données découlant de l'usurpation de l'identité d'entités externes.

3) Stockage des données

Outre les exigences de sécurité intermédiaires, les exigences ci-après devraient aussi être remplies:

- Il convient d'adopter un dispositif de stockage matériel sécurisé par cryptage afin de garantir la confidentialité des données confidentielles des véhicules, des plates-formes de service, des applications de terminaux mobiles intelligents et des infrastructures routières.
- Il devrait être possible de vérifier l'intégrité des données au cours du processus de stockage afin d'empêcher que des données ne soient altérées, supprimées ou insérées, et les mesures de restauration nécessaires devraient être prévues pour les cas où l'intégrité des données est détruite.

4) Utilisation des données

Outre les exigences de sécurité intermédiaires, les exigences ci-après devraient aussi être remplies:

- L'agrément de l'autorité d'exploitation secondaire devrait être effectué selon un mode d'autorisation multi-personnes.
- Il convient d'isoler les corrélations de données pour éviter les fuites de données imputables à l'analyse de l'association des données pour les données stockées dans les différents systèmes, plates-formes ou applications.
- La désensibilisation dynamique devrait être favorisée dans le cadre de l'utilisation de données confidentielles.

5) Migration des données

Les exigences de protection sont identiques à celles qui relèvent des exigences de sécurité intermédiaires.

6) Destruction des données

Outre les exigences de sécurité intermédiaires, les exigences ci-après devraient aussi être remplies:

- Il convient de fournir des moyens permettant d'empêcher toute récupération des données détruites.

7) Sauvegarde et restauration des données

Outre les exigences de sécurité intermédiaires, les exigences ci-après devraient aussi être remplies:

- Des mesures d'authentification, notamment de l'identité, devraient être prises à titre de sécurité pour faire en sorte que les opérations de sauvegarde et de récupération des données locales et distantes ne puissent être effectuées que si les utilisateurs autorisés en ont connaissance ou sous le contrôle de ces derniers.

Bibliographie

[b-UIT-T X.1217] Recommandation UIT-T X.1217 (2021), *Lignes directrices relatives à l'utilisation de renseignements sur les menaces dans le cadre de l'exploitation des réseaux de télécommunication*.

[b-UIT-T X.1751] Recommandation UIT-T X.1751 (2020), *Lignes directrices relatives à la sécurité de la gestion du cycle de vie des mégadonnées par les opérateurs de télécommunication*.

[b-3GPP TR 22.886] 3GPP TR 22.886 V16.2.0 (2018), *Study on enhancement of 3GPP Support for 5G V2X Services (Release 16)* (Étude relative à l'amélioration de l'appui fourni par 3GPP pour les services de véhicule à tout autre élément fondés sur la 5G (publication 16)).

[b-ETSI TR 126 985] ETSI TR 126 985 V16.0.0 (2020), *5G Vehicle-to-everything (V2X) Media handling and interaction (3GPP TR 26.985 version 16.0.0 Release 16*) (Traitement et interactions des médias pour la communication de véhicule à tout autre élément fondée sur la 5G (3GPP TR 26.985 version 16.0.0, publication 16)).

[b-ETSI TS 102 637-2] ETSI TS 102 637-2 (2011), *Systèmes de transport intelligents (ITS); Communications des véhicules; Ensemble d'applications de base; Partie 2: Spécification du service de base coopératif de sensibilisation*.

[b-SAE J2735] *Dictionnaire des séries de messages pour les communications de véhicule à tout autre élément*, (juillet 2020).

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	Équipements 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

Publié en Suisse
Genève, 2023