Norme internationale

ISO 21177

Deuxième édition
2024-03

Systèmes de transport intelligents — Services de sécurité des stations ITS pour l'établissement et l'authentification des sessions sécurisées entre dispositifs de confiance

Intelligent transport systems — ITS station security services for secure session establishment and authentication between trusted devices

Numéro de référence
ISO 21177:2024(fr)

ISO copyright office
Case postale 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Genève
Tél.: +41 22 749 01 11
E-mail: copyright@iso.org
Web: www.iso.org

Publié en Suisse

Sommaire

Page

Avant-propos

L'ISO (Organisation internationale de normalisation) est une fédération mondiale d'organismes nationaux de normalisation (comités membres de l'ISO). L'élaboration des Normes internationales est en général confiée aux comités techniques de l'ISO. Chaque comité membre intéressé par une étude a le droit de faire partie du comité technique créé à cet effet. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'ISO participent également aux travaux. L'ISO collabore étroitement avec la Commission électrotechnique internationale (IEC) en ce qui concerne la normalisation électrotechnique.

Les procédures utilisées pour élaborer le présent document et celles destinées à sa mise à jour sont décrites dans les Directives ISO/IEC, Partie 1. Il convient, en particulier, de prendre note des différents critères d'approbation requis pour les différents types de documents ISO. Le présent document a été rédigé conformément aux règles de rédaction données dans les Directives ISO/IEC, Partie 2 (voir www.iso.org/directives).

L'ISO attire l'attention sur le fait que la mise en application du présent document peut entraîner l'utilisation d'un ou de plusieurs brevets. L'ISO ne prend pas position quant à la preuve, à la validité et à l'applicabilité de tout droit de brevet revendiqué à cet égard. À la date de publication du présent document, l'ISO avait reçu notification qu'un ou plusieurs brevets pouvaient être nécessaires à sa mise en application. Toutefois, il y a lieu d'avertir les responsables de la mise en application du présent document que des informations plus récentes sont susceptibles de figurer dans la base de données de brevets, disponible à l'adresse www.iso.org/brevets. L'ISO ne saurait être tenue pour responsable de ne pas avoir identifié tout ou partie de tels droits de propriété.

Les appellations commerciales éventuellement mentionnées dans le présent document sont données pour information, par souci de commodité, à l'intention des utilisateurs et ne sauraient constituer un engagement.

Pour une explication de la nature volontaire des normes, la signification des termes et expressions spécifiques de l'ISO liés à l'évaluation de la conformité, ou pour toute information au sujet de l'adhésion de l'ISO aux principes de l'Organisation mondiale du commerce (OMC) concernant les obstacles techniques au commerce (OTC), voir www.iso.org/avant-propos.

Le présent document a été élaboré par le comité technique ISO/TC 204, *Systèmes de transport intelligents,* en collaboration avec le comité technique CEN/TC 278, *Systèmes de transport intelligents,* du Comité européen de normalisation (CEN) conformément à l'Accord de coopération technique entre l'ISO et le CEN (Accord de Vienne).

Cette deuxième édition annule et remplace la première édition (ISO 21177:2023), dont elle constitue une révision mineure. Les modifications sont les suivantes.

Les principales modifications sont les suivantes:

— les références croisées à la RFC 8942 ont été remplacées par des références à la RFC 8902 dans l'ensemble du document;

— les informations concernant le ou les brevets exigés pour la mise en œuvre du présent document ont été déplacées de l'Introduction à l'Avant-propos.

Il convient que l'utilisateur adresse tout retour d'information ou toute question concernant le présent document à l'organisme national de normalisation de son pays. Une liste exhaustive desdits organismes se trouve à l'adresse www.iso.org/fr/members.html.

Introduction

Le présent document spécifie les services de sécurité des stations ITS qui assurent l'authenticité de la source ainsi que la confidentialité et l'intégrité des activités des applications se déroulant entre dispositifs de confiance. Les deux dispositifs participant à un échange de données établissent une session cryptographiquement sécurisée. Dans le cadre de l'établissement de cette session, chaque dispositif [ou, plus précisément, chaque entité finale (EE), qui est une application sur le dispositif] reçoit un ou plusieurs certificats numériques cryptographiquement liés à l'autre EE et contenant des déclarations, faites par un tiers de confiance, sur les capacités, les propriétés et les permissions de l'EE. Cela permet à chaque EE de s'assurer des propriétés de l'autre EE dans la session, et donc à chaque EE de prendre des décisions de confiance et de contrôle d'accès concernant les données auxquelles l'autre EE peut accéder, les commandes que l'autre EE peut exécuter, les états que l'autre EE peut modifier et d'autres types d'accès que l'autre EE peut demander. En d'autres termes, les deux EE établissent une relation de confiance dans laquelle chacune a obtenu la confiance de l'autre pour effectuer des actions spécifiques, sans qu'une EE doive autoriser l'autre à avoir un accès arbitraire.

Les mécanismes spécifiés dans le présent document permettent à chaque EE d'établir des faits de confiance sur l'autre EE. Pour que ces mécanismes puissent être utilisés, la spécification de l'EE doit inclure une politique de contrôle d'accès, indiquant quelles propriétés doivent être connues comme étant vraies sur l'autre EE pour que cette dernière soit autorisée à effectuer des actions particulières. En d'autres termes, le présent document fournit un moyen d'obtenir des informations pertinentes en matière de sécurité, mais l'utilisation de ces informations doit être précisée dans la spécification de l'EE.

La Figure 1 illustre la relation de confiance entre deux dispositifs. Deux dispositifs coopèrent dans le cadre d'une relation de confiance, c'est-à-dire qu'ils échangent des informations avec une protection bidirectionnelle explicite facultative.

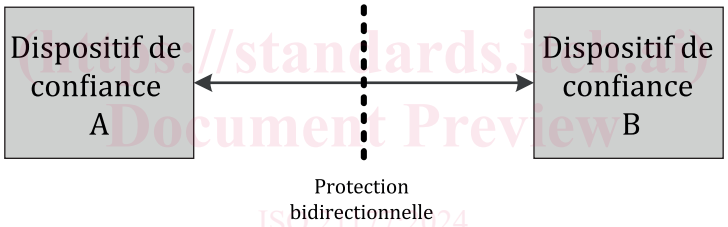


Figure 1 — Interconnexion des dispositifs de confiance

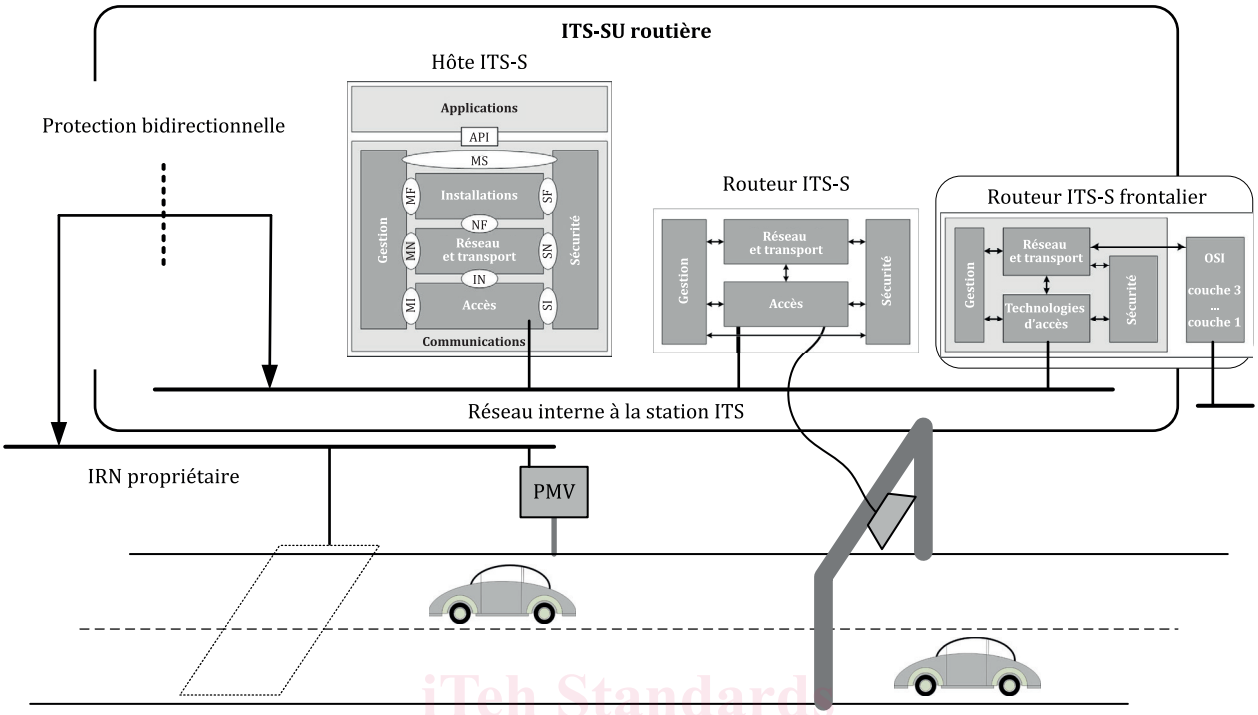
Selon l'ISO 21217, une unité de station ITS (ITS-SU), c'est-à-dire la mise en œuvre physique de la fonctionnalité de la station ITS (ITS-S), est un dispositif de confiance, et une ITS-SU peut être composée d'unités de communication de station ITS (ITS-SCU) interconnectées par le réseau interne à une station ITS. Ainsi, une ITS-SCU est la plus petite entité physique d'une ITS-SU désignée comme un dispositif de confiance.

NOTE 1 L'ISO 21217 couvre entièrement la fonctionnalité de l'EN 302 665,[16] qui précède l'ISO 21217.

NOTE 2 Une ITS-SU peut être composée d'ITS-SCU de différents fournisseurs, chaque ITS-SCU étant liée à un centre de configuration et de gestion d'ITS-SCU différent, spécifié dans les normes ISO 24102-2 et ISO 17419. Les communications de gestion interne à la station entre les ITS-SCU d'une même ITS-SU sont spécifiées dans l'ISO 24102-4. La réglementation européenne relative aux C-ITS désigne le «centre de configuration et de gestion d'ITS-SCU» sous l'appellation «exploitant de station STIC», c'est-à-dire l'entité responsable de l'exploitation d'une station C-ITS. Cet exploitant peut être responsable de l'exploitation d'une seule station C-ITS (fixe ou mobile), ou d'une infrastructure C-ITS composée de plusieurs stations C-ITS fixes ou de plusieurs stations ITS mobiles.

Quatre contextes de mise en œuvre des nœuds de communication dans les réseaux de communication des ITS sont identifiés dans l'architecture des stations et des communications ITS de l'ISO 21217, chacun étant composé d'ITS-SU assumant un rôle particulier: personnelle, embarquée, routière ou centrale. Ces ITS-SU sont des nœuds de communication sécurisés par les ITS, conformément à l'ISO 21217, qui participent à une grande variété de services ITS liés, par exemple, au développement durable, à la sécurité routière et à l'efficacité des transports. Voir également la Figure 2, la Figure 3, la Figure 4 et la Figure 5.

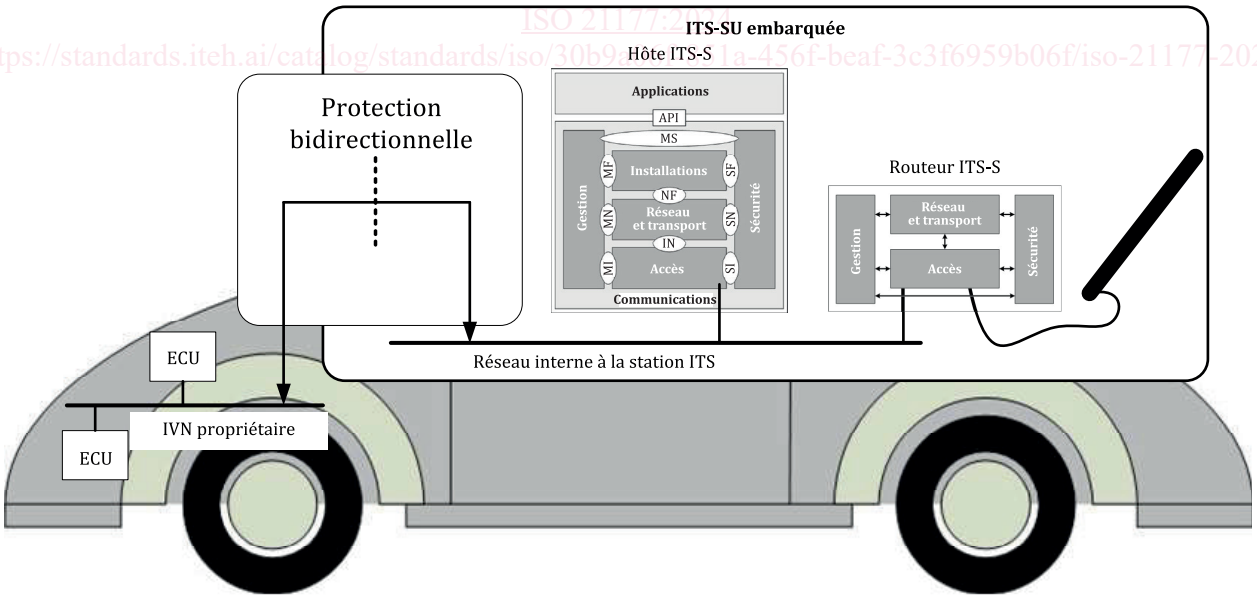
Au cours de la dernière décennie, sont apparus des services ITS nécessitant un accès sécurisé aux données des réseaux de capteurs et de contrôle (SCN), par exemple, des réseaux embarqués (IVN) et des réseaux routiers d'infrastructure (IRN), dont certains nécessitent un accès local sécurisé à des informations périssables; voir la Figure 2 et la Figure 3.



Légende

PMV panneau à messages variables

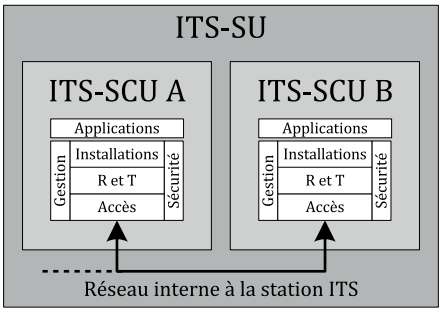
Figure 2 — Exemple d'une ITS-SU routière connectée à un IRN propriétaire



Légende

ECU electronic control unit [unité de contrôle électronique]

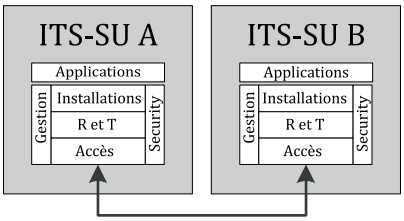
Figure 3 — Exemple d'une ITS-SU embarquée connectée à un IVN propriétaire



Légende

R et T réseau et transport

Figure 4 — Interconnexion des ITS-SCU dans une ITS-SU



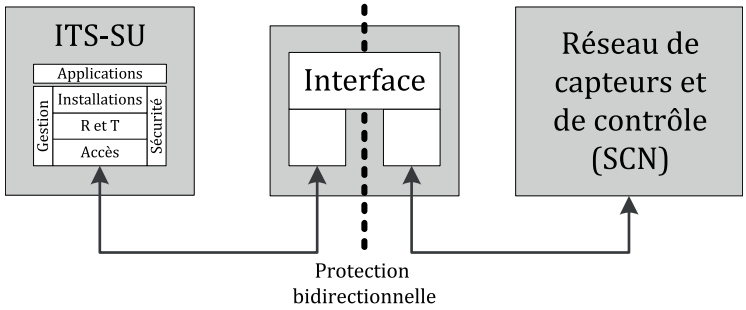
Légende

R et T réseau et transport

Figure 5 — Interconnexion des ITS-SU

En appliquant les moyens de sécurité de base spécifiés dans le présent document, les ITS-SU peuvent établir des sessions d'application sécurisées. L'établissement de sessions nécessite une connaissance préalable d'un partenaire de session ou peut intervenir au moyen d'une annonce de service spécifiée dans l'ISO 22418. En outre, la diffusion de messages est sécurisée par des moyens d'authentification de l'expéditeur de tels messages, applicables au message d'avertissement de service (SAM) spécifié dans l'ISO 16460 et utilisé dans l'ISO 22418. De plus, d'autres moyens de sécurité peuvent être appliqués, par exemple le chiffrement des messages.

Une autre relation de confiance dans le domaine des ITS se déroule entre une ITS-SU composée d'une ou plusieurs ITS-SCU et un réseau de capteurs et de contrôle (SCN). La confiance est obtenue en appliquant des moyens de sécurité dans une interface comme le montre la Figure 6 selon les modalités détaillées dans le présent document.



Légende

R et T réseau et transport

Figure 6 — Interface entre l'ITS-SU et le réseau de capteurs et de contrôle

L'interface présentée à la Figure 6 peut être un dispositif autonome, ou peut être intégrée à l'ITS-SU, ou peut faire partie du SCN. Les «réseaux embarqués» (IVN) et les «réseaux routiers d'infrastructure» (IRN) sont des exemples de SCN.

Les cas d'utilisation connexes de ces services ITS ont été largement dérivés des exigences réglementaires et des besoins opérationnels des ITS, et comprennent:

— un accès sécurisé en temps réel aux données périssables liées au véhicule pour les applications de sécurité des personnes et des biens, comme la prévention des collisions, le freinage d'urgence électronique et la détermination des événements;

— un accès local sécurisé à des données détaillées en temps réel pour des applications d'efficacité (gestion du trafic), par exemple, l'interaction aux intersections, la prévention des embouteillages et les priorités dynamiques;

— la protection des données privées, par exemple, en conformité avec le «Règlement général sur la protection des données» (RGPD)[18] européen;

— un accès local à des données certifiées en temps réel pour des applications de développement durable, par exemple, des zones d'émission dynamiques (zones contrôlées telles qu'elles sont actuellement normalisées par le CEN/TC 278), des priorités aux intersections basées sur les émissions, et des réglages interactifs optimaux des véhicules pour minimiser la consommation de carburant.

De nombreux cas d'utilisation des services ITS ont été identifiés pour lesquels l'échange en temps réel d'informations périssables entre des ITS-SU proches les unes des autres est essentiel, et ce nombre est appelé à croître (voir l'architecture nationale de référence ITS des États-Unis[19] par exemple). Il est essentiel qu'en fin de compte, toutes les ITS-SU d'une zone donnée puissent participer à ces services distribués. Il faut donc que les ITS-SU embarquées aient un accès en temps réel aux données des véhicules et que les ITS-SU routières aient un accès en temps réel aux données des infrastructures. Toutes les ITS-SU doivent être capables d'effectuer des mises à jour sécurisées des logiciels.

Selon l'ISO 21217, l'ITS-SCU d'une ITS-SU peut communiquer avec des dispositifs qui, au sens strict, ne sont pas conformes à l'architecture spécifiée par l'ISO 21217. Toutefois, pour que les communications soient reconnues dignes de confiance, un niveau minimum de mesures de sécurité doit être partagé entre une ITS-SCU et un tel dispositif externe. Un nœud Internet ou un nœud dans un réseau de capteurs et de contrôle sont des exemples de tels dispositifs externes. Le présent document suppose que les processus d'application ITS-S fonctionnant sur des ITS-SU reçoivent des certificats délivrés par une autorité de certification (CA), et que la CA est un tiers de confiance dans le sens où, avant de délivrer le certificat au processus d'application ITS-S, elle s'assure que l'ITS-SU sur laquelle réside le processus d'application ITS-S satisfait aux exigences de sécurité minimales pour cette application. Cela permet aux processus d'application ITS-S homologues qui constatent qu'un processus d'application ITS-S possède un certificat valide de s'assurer dans une certaine mesure que le processus d'application ITS-S est effectivement sécurisé et digne de confiance.

L'objet du présent document est donc triple.

1) Spécification des services de sécurité des stations ITS pour établir la confiance entre les processus d'application ITS-S exécutés sur différentes ITS-SCU d'une même ITS-SU, c'est-à-dire établir une plateforme de traitement de confiance, en tenant compte également de la confiance à l'intérieur d'une ITS-SCU:
   — protection des applications contre les actions d'autres applications;
   — protection des informations partagées;
   — protection des ressources de traitement partagées, telles que les logiciels et le matériel de communication, avec notamment des méthodes de hiérarchisation et de restriction d'accès.
2) Spécification des services de sécurité des stations ITS pour établir la confiance entre les processus d'application ITS-S exécutés sur une même ITS-SU.
3) Extension de ces services de sécurité ITS pour établir la confiance entre une ITS-SCU et des dispositifs faisant partie d'un réseau de capteurs et de contrôle.

Ces services de sécurité comprennent, par exemple, les fonctions de sécurité de base de:

a) l'authentification et l'autorisation;

b) la confidentialité et le respect de la vie privée;

c) l'intégrité des données;

d) la non-répudiation.

Les tâches liées aux communications sont:

e) l'établissement de sessions sécurisées pour les communications bidirectionnelles, par exemple basées sur l'avertissement de service spécifié par l'ISO 22418;

f) l'authentification d'un expéditeur de messages radiodiffusés, par exemple CAM, DENM, BSM, SPaT, MAP, FSAM, WSA, etc.;

g) le chiffrement de messages.

NOTE 3 Les tâches f) et g) ci-dessus relatives aux communications sont déjà spécifiées dans d'autres normes, voir l'IEEE 1609.2 et plusieurs normes connexes de l'ETSI, par exemple.

Systèmes de transport intelligents — Services de sécurité des stations ITS pour l'établissement et l'authentification des sessions sécurisées entre dispositifs de confiance

1 Domaine d'application

Le présent document contient les spécifications d'un ensemble de services de sécurité des stations ITS nécessaires pour garantir l'authenticité de la source et l'intégrité des informations échangées entre des entités de confiance, c'est-à-dire:

— entre des dispositifs exploités en tant qu'entités délimitées gérées de manière sécurisée, c'est-à-dire les «unités de communication de station ITS» (ITS-SCU) et les «unités de station ITS» (ITS-SU) comme spécifié dans l'ISO 21217; et

— entre les ITS-SU (composées d'une ou plusieurs ITS-SCU) et les entités de confiance externes telles que les réseaux de capteurs et de contrôle.

Ces services comprennent l'authentification et l'établissement de sessions sécurisées, nécessaires pour échanger des informations dans le cadre d'une relation de confiance et de manière sécurisée.

Ces services sont essentiels pour de nombreux services et applications de systèmes de transport intelligents (ITS), notamment les applications de sécurité revêtant un caractère d'urgence, la conduite automatisée, la gestion à distance des stations ITS (ISO 24102-2), et les services routiers liés aux infrastructures.

2 Références normatives

Les documents suivants sont cités dans le texte de sorte qu'ils constituent, pour tout ou partie de leur contenu, des exigences du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

ETSI TS 102 941, *Intelligent Transport Systems (ITS); Security; Trust and Privacy Management (disponible en anglais seulement)*

ETSI TS 103 097, *Intelligent Transport Systems (ITS); Security; Security header and certificate formats (disponible en anglais seulement)*

IEEE 1609.2, *incluant l'Amendement 1, IEEE Standard for Wireless Access in Vehicular Environments — Security Services for Applications and Management Messages (disponible en anglais seulement)*

IEEE 1003.1:2017, *IEEE Standard for Information Technology –Portable Operating System Interface (POSIX(R)) Base Specifications, Issue 7 (disponible en anglais seulement)*

3 Termes et définitions

Pour les besoins du présent document, les termes et définitions suivants s'appliquent.

L'ISO et l'IEC tiennent à jour des bases de données terminologiques destinées à être utilisées en normalisation, consultables aux adresses suivantes:

— ISO Online browsing platform: disponible à l'adresse https://www.iso.org/obp

— IEC Electropedia: disponible à l'adresse https://www.electropedia.org/

3.1
PDU de contrôle d'accès
unité de données de protocole (PDU) générée par le sous-système de sécurité afin d'établir le statut d'autorisation d'un processus d'application ITS-S homologue

3.2
politique de contrôle d'accès
source de données déterminant quel accès aux ressources est autorisé par les applications homologues

3.3
application
entité fonctionnelle, c'est-à-dire un processus d'application ITS-S

Note 1 à l'article: Dans le présent document, le terme «application» en langage naturel est utilisé comme synonyme du terme «processus d'application ITS-S» spécifié dans l'ISO 21217.

3.4
élément cryptographique
clés cryptographiques et éléments qui y sont associés

Note 1 à l'article: Le matériel cryptographique désigne soit une clé secrète pour un algorithme symétrique, soit une clé privée pour un algorithme asymétrique et la clé publique ou le certificat associé

3.5
pointeur d'élément cryptographique
référence à un élément cryptographique permettant l'utilisation de ce dernier dans des opérations cryptographiques (signature, vérification, chiffrement, déchiffrement)

3.6
ITS-AID de négociation
identifiant de l'application ITS (ITS-AID) apparaissant dans le SignedData HeaderInfo des messages TLS (Transport Layer Security) signés dans le cadre de la poignée de main TLS qui a démarré une session sécurisée

3.7
ressources
entité fonctionnelle constituant les points d'extrémité de l'activité du processus d'application ITS-S

3.8
sous-système de sécurité
entité fonctionnelle fournissant une fonctionnalité de sécurité destinée à être utilisée par un processus d'application ITS-S

3.9
couche d'adaptation de sécurité
entité fonctionnelle fournissant une fonctionnalité de multiplexage et de démultiplexage pour les données et les commandes de contrôle de session

3.10
service de session sécurisée
entité fonctionnelle assurant la confidentialité, l'intégrité, l'authentification, la garantie de livraison dans l'ordre et la protection contre le rejeu des datagrammes qui sont transmis par son intermédiaire