

---

---

**Véhicules routiers — Communications  
entre un véhicule et un équipement externe  
pour le diagnostic relatif aux émissions —**

Partie 7:

**Sécurité de la liaison de données**

iTeh STANDARD PREVIEW

*Road vehicles — Communication between vehicle and external equipment  
for emissions-related diagnostics —*

*Part 7: Data link security*

ISO 15031-7:2001

<https://standards.iteh.ai/catalog/standards/sist/dd8d6e39-a6f7-4406-b8d4-5598d9d107cb/iso-15031-7-2001>



**PDF – Exonération de responsabilité**

Le présent fichier PDF peut contenir des polices de caractères intégrées. Conformément aux conditions de licence d'Adobe, ce fichier peut être imprimé ou visualisé, mais ne doit pas être modifié à moins que l'ordinateur employé à cet effet ne bénéficie d'une licence autorisant l'utilisation de ces polices et que celles-ci y soient installées. Lors du téléchargement de ce fichier, les parties concernées acceptent de fait la responsabilité de ne pas enfreindre les conditions de licence d'Adobe. Le Secrétariat central de l'ISO décline toute responsabilité en la matière.

Adobe est une marque déposée d'Adobe Systems Incorporated.

Les détails relatifs aux produits logiciels utilisés pour la création du présent fichier PDF sont disponibles dans la rubrique General Info du fichier; les paramètres de création PDF ont été optimisés pour l'impression. Toutes les mesures ont été prises pour garantir l'exploitation de ce fichier par les comités membres de l'ISO. Dans le cas peu probable où surviendrait un problème d'utilisation, veuillez en informer le Secrétariat central à l'adresse donnée ci-dessous.

**iTeh STANDARD PREVIEW**  
**(standards.iteh.ai)**

[ISO 15031-7:2001](https://standards.iteh.ai/catalog/standards/sist/dd8d6e39-a6f7-4406-b8d4-5598d9d107cb/iso-15031-7-2001)

<https://standards.iteh.ai/catalog/standards/sist/dd8d6e39-a6f7-4406-b8d4-5598d9d107cb/iso-15031-7-2001>

© ISO 2001

Droits de reproduction réservés. Sauf prescription différente, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de l'ISO à l'adresse ci-après ou du comité membre de l'ISO dans le pays du demandeur.

ISO copyright office  
Case postale 56 • CH-1211 Geneva 20  
Tel. + 41 22 749 01 11  
Fax. + 41 22 749 09 47  
E-mail [copyright@iso.ch](mailto:copyright@iso.ch)  
Web [www.iso.ch](http://www.iso.ch)

Imprimé en Suisse

## 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 (CEI) en ce qui concerne la normalisation électrotechnique.

Les Normes internationales sont rédigées conformément aux règles données dans les Directives ISO/CEI, Partie 3.

Les projets de Normes internationales adoptés par les comités techniques sont soumis aux comités membres pour vote. Leur publication comme Normes internationales requiert l'approbation de 75 % au moins des comités membres votants.

L'attention est appelée sur le fait que certains des éléments de la présente partie de l'ISO 15031 peuvent faire l'objet de droits de propriété intellectuelle ou de droits analogues. L'ISO ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de propriété et averti de leur existence.

La Norme internationale ISO 15031-7 a été élaborée par le comité technique ISO/TC 22, *Véhicules routiers*, sous-comité SC 3, *Équipement électrique et électronique*.

L'ISO 15031 comprend les parties suivantes, présentées sous le titre général *Véhicules routiers — Communications entre un véhicule et un équipement externe pour le diagnostic relatif aux émissions*:

- *Partie 1: Informations générales* [ISO 15031-7:2001](https://standards.iteh.ai/catalog/standards/sist/dd8d6e39-a6f7-4406-b8d4-5598d9d107cb/iso-15031-7-2001)
- *Partie 2: Termes, définitions, abréviations et acronymes*
- *Partie 3: Connecteur de diagnostic et circuits électriques associés, spécifications et utilisation*
- *Partie 4: Dispositif d'essai externe*
- *Partie 5: Services de diagnostic*
- *Partie 6: Définition des codes d'anomalie*
- *Partie 7: Sécurité de la liaison de données*

## Introduction

L'ensemble des différentes parties de l'ISO 15031 fournit un tout cohérent et homogène de spécifications destiné à faciliter le diagnostic relatif aux émissions. Les parties 2 à 7 sont basées sur les pratiques recommandées de la Society of automotive engineers (SAE). La présente partie de l'ISO 15031 est basée sur la SAE J2186:1996, *Sécurité de la liaison de données électrique électronique*.

## iTeh STANDARD PREVIEW (standards.iteh.ai)

[ISO 15031-7:2001](https://standards.iteh.ai/catalog/standards/sist/dd8d6e39-a6f7-4406-b8d4-5598d9d107cb/iso-15031-7-2001)

<https://standards.iteh.ai/catalog/standards/sist/dd8d6e39-a6f7-4406-b8d4-5598d9d107cb/iso-15031-7-2001>

# Véhicules routiers — Communications entre un véhicule et un équipement externe pour le diagnostic relatif aux émissions —

## Partie 7: Sécurité de la liaison de données

### 1 Domaine d'application

La présente partie de l'ISO 15031 donne des lignes directrices pour la protection des modules des véhicules contre toute intrusion «non autorisée» au moyen d'une liaison de données de diagnostic du véhicule. Ces mesures de sécurité offrent aux constructeurs de véhicules la souplesse nécessaire pour leur permettre d'adapter leurs mesures de sécurité à leurs propres besoins spécifiques, sans exclure d'autres mesures additionnelles.

La présente partie de l'ISO 15031 s'applique aux véhicules à moteur dont les modules concernés sont ceux dont le contenu de la mémoire intégrée peut être modifié de l'extérieur du module électronique par l'intermédiaire d'une liaison de transmission de données de diagnostic. Une telle modification pourrait causer une détérioration de l'électronique ou d'autres composants du véhicule, compromettant la conformité du véhicule aux exigences gouvernementales prévues par la loi ou l'intérêt du constructeur du véhicule eu égard à la sécurité.

[ISO 15031-7:2001](https://standards.iteh.ai/catalog/standards/sist/dd8d6e39-a6f7-4406-b8d4-5598d9d107cb/iso-15031-7-2001)

<https://standards.iteh.ai/catalog/standards/sist/dd8d6e39-a6f7-4406-b8d4-5598d9d107cb/iso-15031-7-2001>

### 2 Référence normative

Le document normatif suivant contient des dispositions qui, par suite de la référence qui y est faite, constituent des dispositions valables pour la présente partie de l'ISO 15031. Pour les références datées, les amendements ultérieurs ou les révisions de ces publications ne s'appliquent pas. Toutefois, les parties prenantes aux accords fondés sur la présente partie de l'ISO 15031 sont invitées à rechercher la possibilité d'appliquer l'édition la plus récente du document normatif indiqué ci-après. Pour les références non datées, la dernière édition du document normatif en référence s'applique. Les membres de l'ISO et de la CEI possèdent le registre des Normes internationales en vigueur.

ISO/TR 15031-2:—<sup>1)</sup>, *Véhicules routiers — Communications entre un véhicule et un équipement externe pour le diagnostic relatif aux émissions — Partie 2: Termes, définitions, abréviations et acronymes.*

### 3 Termes et définitions

Pour les besoins de la présente partie de l'ISO 15031, les termes et définitions donnés dans l'ISO/TR 15031-2 et les suivants s'appliquent.

#### 3.1

##### fonctions non protégées

fonctions de diagnostic standards qui sont fournies par les constructeurs de véhicules et régies et protégées par le contrôleur du véhicule

EXEMPLE      Reprogrammation d'éléments sélectionnés tels que l'effacement de codes défaut.

1) À publier.

3.2

**fonctions protégées**

fonctions soumises à des restrictions, dont l'accès nécessite le déverrouillage du contrôleur du véhicule

EXEMPLE Programmation des systèmes d'émission du véhicule tels que cartographies carburant/allumage, antivol et compteur kilométrique.

3.3

**graine**

valeur de données pseudo-aléatoire transmise d'un contrôleur embarqué à un dispositif d'essai externe et traitée par l'algorithme de sécurité pour produire la clé

3.4

**clé**

valeur de données donnant accès aux fonctions protégées, transmise du dispositif d'essai externe au contrôleur embarqué en réponse à la graine

3.5

**fausse tentative d'accès**

**FAA<sup>2)</sup>**

clé incorrecte reçue par le contrôleur embarqué

3.6

**délai entre tentatives**

**DT<sup>3)</sup>**

période qui sépare deux tentatives d'accès

ITeH STANDARD PREVIEW  
(standards.iteh.ai)

**4 Exigences techniques**

[ISO 15031-7:2001](#)

**4.1 Généralités**

<https://standards.iteh.ai/catalog/standards/sist/dd8d6e39-a6f7-4406-b8d4-5598d9d107cb/iso-15031-7-2001>

Le déverrouillage correct du contrôleur du véhicule est une condition préalable pour accéder à certaines fonctions critiques du contrôleur embarqué.

NOTE La présente partie de l'ISO 15031 ne cherche pas à définir les fonctions ou les informations qui doivent être protégées, laissant ceci au constructeur du véhicule.

Le seul accès au contrôleur embarqué qui soit autorisé en mode verrouillé se fait par l'intermédiaire du logiciel spécifique au produit. Cela permet à ce logiciel de se protéger lui-même et de protéger le reste du système de commande du véhicule contre toute intrusion non autorisée. Des fonctions embarquées différentes peuvent être protégées par des combinaisons «graine/clé» distinctes.

Les mesures de sécurité ne doivent pas empêcher les communications normales de diagnostic entre le dispositif externe et le contrôleur embarqué.

**4.2 Caractéristiques de sécurité**

Ces mesures de sécurité peuvent être intégrées dans tout protocole de communication. Des commandes spéciales doivent être envoyées via la liaison de transmission de diagnostic pour déverrouiller le contrôleur embarqué.

Les trois paramètres suivants doivent régir l'accès de sécurité au contrôleur embarqué et la fonction protégée.

---

2) False Access Attempt

3) Delay Time

- a) La graine et la clé doivent avoir chacune une longueur minimale de deux octets. Le choix d'un nombre minimum d'octets aboutit à un niveau minimum de sécurité. Il est conseillé d'utiliser quatre octets ou plus lorsqu'on exige des niveaux de sécurité supérieurs. La responsabilité de la relation entre la valeur graine et la clé incombe au constructeur du véhicule. Il peut exister des relations graine/clé multiples pour accéder à différentes fonctions d'un contrôleur ou à différents systèmes d'un même véhicule.
- b) Le nombre des fausses tentatives d'accès (FAA) doit être de deux au maximum avant le déclenchement du délai entre tentatives (DT). Le constructeur du véhicule peut définir un nombre réduit de FAA pour une meilleure adaptation à ses besoins spécifiques. Lorsque la clé reçue par le contrôleur n'est pas la bonne, l'opération est considérée comme une FAA, mais si l'accès est refusé pour une autre raison, elle n'est pas considérée comme telle.
- c) Le DT doit être au minimum de 10 s; le constructeur du véhicule peut définir un DT plus long pour une meilleure adaptation à ses besoins spécifiques, y compris un DT qui augmente avec le nombre de FAA.

La divulgation de la relation graine/clé doit être limitée aux personnes autorisées par le constructeur du véhicule.

**AVERTISSEMENT — Il convient de prendre toutes les précautions nécessaires au moment du choix de la valeur de chacun des paramètres car leur combinaison détermine le niveau de sécurité d'une application ou d'un système.**

### 4.3 Exigences fonctionnelles

Deux couples de messages de communication demande/réponse doivent être utilisés pour déverrouiller la fonction embarquée protégée.

NOTE La présente partie de l'ISO 15031 ne définit pas le contenu spécifique du message, laissant ceci au constructeur du véhicule.

- **Demande 1/Réponse 1.** Le dispositif externe doit demander au contrôleur embarqué de déverrouiller la fonction protégée souhaitée en envoyant une Demande 1. Le contrôleur doit répondre en envoyant une graine avec la Réponse 1. Une graine zéro doit indiquer que le contrôleur est actuellement déverrouillé.
- **Demande 2/Réponse 2.** Le dispositif externe doit répondre en renvoyant au contrôleur un numéro de clé avec la Demande 2. Le contrôleur doit comparer cette clé à la clé définie de façon interne et envoyer la Réponse 2. Si les deux numéros coïncident, le contrôleur autorisera l'accès du dispositif externe à la fonction protégée (c'est-à-dire qu'il déverrouillera cette fonction). Si le nombre admis de FAA est atteint sans que les numéros de clé ne coïncident (fausse tentative), le contrôleur déclenchera le DT avant d'autoriser d'autres tentatives.

Le DT doit être également exigé à chaque mise sous tension du contrôleur et de la fonction.

La fonction doit déclencher automatiquement le DT avant de demander une nouvelle graine, quelle que soit la raison de cette demande.

Les trois réponses suivantes du contrôleur embarqué doivent être décodées par le dispositif externe.

- a) **Accepté:** le contrôleur a déverrouillé son accès.
- b) **Clé non valide:** la tentative d'accès a été rejetée car le contrôleur a déterminé que la clé n'était pas la bonne; il s'agit d'une fausse tentative d'accès (FAA).
- c) **Erreur de processus:** la tentative d'accès a été rejetée pour des raisons autres que la réception d'une mauvaise clé; ceci ne doit pas être compté comme une FAA.

Chacune des conditions suivantes doit aboutir à l'interruption de l'accès de sécurité, en verrouillant la fonction protégée:

- chaque mise sous tension du contrôleur;

## ISO 15031-7:2001(F)

- mise du produit en mode de fonctionnement normal;
- autres conditions laissées à la discrétion du constructeur du véhicule.

En cas de tentative faite pour communiquer avec un contrôleur embarqué verrouillé et pour accéder à une fonction protégée, le contrôleur peut renvoyer une réponse spéciale indiquant qu'il est verrouillé et qu'il ne peut pas répondre comme demandé.

## iTeh STANDARD PREVIEW (standards.iteh.ai)

[ISO 15031-7:2001](https://standards.iteh.ai/catalog/standards/sist/dd8d6e39-a6f7-4406-b8d4-5598d9d107cb/iso-15031-7-2001)

<https://standards.iteh.ai/catalog/standards/sist/dd8d6e39-a6f7-4406-b8d4-5598d9d107cb/iso-15031-7-2001>

**iTeh STANDARD PREVIEW**  
**(standards.iteh.ai)**

ISO 15031-7:2001

<https://standards.iteh.ai/catalog/standards/sist/dd8d6e39-a6f7-4406-b8d4-5598d9d107cb/iso-15031-7-2001>