NORME INTERNATIONALE

ISO 20828

Première édition
2006-07-01

Véhicules routiers — Gestion des certificats de sécurité

Road vehicles — Security certificate management

Numéro de référence
ISO 20828:2006(F)

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

Les Normes internationales sont rédigées conformément aux règles données dans les Directives ISO/CEI, Partie 2.

La tâche principale des comités techniques est d'élaborer les Normes internationales. 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 du présent document 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.

L'ISO 20828 a été élaborée par le comité technique ISO/TC 22, *Véhicules routiers*, sous-comité SC 3, *Équipement électrique et électronique*.

Introduction

Souvent, les données transmises au sein d'un véhicule routier, entre des véhicules routiers ou en provenance ou à destination d'un véhicule doivent être protégées afin de garantir leur confidentialité et leur intégrité. La cryptographie est un excellent moyen pour obtenir ce type de protection. En fonction des exigences de protection, il est possible d'utiliser différentes solutions. Dans certains cas, il est suffisant de verrouiller une liaison de données impliquant un dispositif spécifique, et de la déverrouiller uniquement si un second dispositif a envoyé la bonne clé en réponse à une amorce arbitraire. Le service d'accès de sécurité correspondant est spécifié dans de nombreuses Normes internationales et est très largement utilisé aujourd'hui.

L'ISO 15764 définit une solution de sécurité étendue. Elle ne se borne pas à restreindre l'accès aux données, mais protège aussi les données lorsqu'elles sont transmises à travers la liaison de données. Une protection est assurée contre l'usurpation d'identité, la réinsertion, l'écoute électronique, la manipulation et la répudiation. Avant de démarrer la transmission de données sécurisée, la liaison de données doit être configurée comme une liaison sécurisée. L'ISO 15764 offre les deux méthodes suivantes pour réaliser cela.

a) Les deux dispositifs qui participent à la transmission de données ont une clé cryptographique secrète prédéfinie. Cette clé est utilisée pour établir la liaison sécurisée et exclure tous les tiers qui n'y ont pas accès de toute participation à la liaison sécurisée. Cette méthode est basée sur des clés symétriques et s'applique aux dispositifs ayant une mémoire et une puissance de calcul limitées.

b) La liaison sécurisée peut être établie entre des dispositifs arbitraires, si ces dispositifs ont une clé privée et un certificat de sécurité pour la clé publique correspondante. Cette méthode utilise la cryptographie asymétrique, qui nécessite une mémoire et une puissance de calcul plus élevées au niveau des dispositifs.

Les clés publiques sont des clés cryptographiques qui sont publiquement disponibles et qui sont liées à une clé privée, qui est gardée secrète par le dispositif qui la détient. Il existe les deux manières d'utiliser un couple de clés publique/privée:

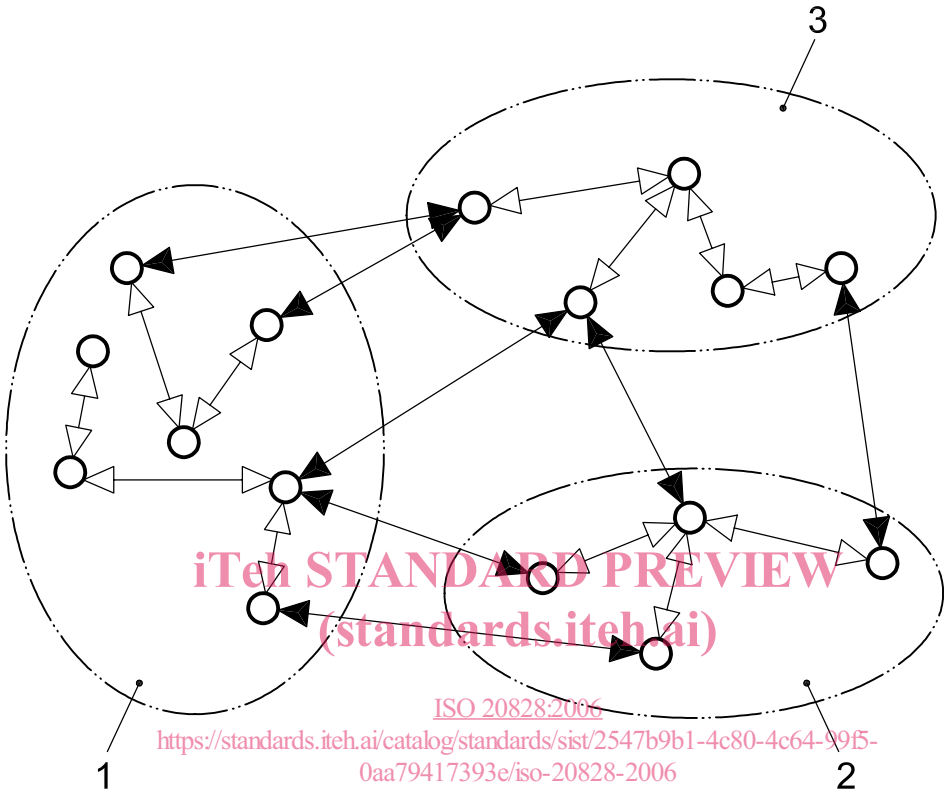
a) le dispositif détenant la clé privée peut ajouter une signature électronique aux données qu'il émet. Cette signature est spécifique aux données émises et ne peut être générée qu'avec la clé privée. Une autre chaîne de données à signer ou une clé privée différente donneraient toutes deux une signature différente. Tout autre dispositif possédant la clé publique correspondante est en mesure de vérifier la signature et donc de confirmer que la chaîne de données provient bien du dispositif qui détient la clé privée et qu'elle n'a pas été modifiée après son émission;

b) tout dispositif possédant la clé publique peut l'utiliser pour crypter des données avant de les envoyer au dispositif détenant la clé privée. Comme les données peuvent uniquement être décryptées en utilisant la clé privée, aucun autre dispositif n'est en mesure d'interpréter correctement les données émises.

Mais comment l'utilisateur de la clé publique sait-il qu'il utilise la bonne clé ? Un tiers malveillant pourrait envoyer sa propre clé publique, en prétendant qu'elle provient d'un dispositif de confiance, et pourrait espérer avoir accès aux transmissions de données sécurisées. Pour chaque domaine de transmissions de données sécurisées, il doit y avoir une (ou plusieurs) autorité(s) qui décide(nt) des dispositifs qui sont dignes de confiance. Cette autorité s'appelle l'autorité de certification (AC, en anglais «CA»). Pour les dispositifs sécurisés, elle délivre des certificats de sécurité qui confirment que la clé publique provient bien de ce dispositif (c'est-à-dire que le dispositif détient la clé privée correspondante). La signature électronique de l'autorité de certification est jointe au certificat, ce qui le rend infalsifiable. Dans le cadre de la procédure pour établir une liaison sécurisée, chacun des dispositifs concernés doit vérifier le certificat de l'autre.

Avec la second méthode spécifiée dans l'ISO 15764, une liaison sécurisée peut être établie entre des dispositifs qui utilisent la clé publique de l'autorité de certification de l'autre. Mais dans bien des cas, on a affaire à des domaines de sécurité différents qui n'ont pas les mêmes autorités chargées de désigner les dispositifs sécurisés, et il est nécessaire de créer des liaisons sécurisées entre des dispositifs appartenant à

des domaines différents, sans connaître les clés publiques des autorités de certification de l'autre domaine. La présente Norme internationale définit comment la confiance entre des dispositifs appartenant à des domaines de sécurité différents peut être établie sur la base des certificats de sécurité. En ce sens, elle élargit le champ d'application de l'ISO 15764.



Légende

1 domaine de sécurité 1

2 domaine de sécurité 2

3 domaine de sécurité 3

liaisons sécurisées internes couvertes par l'ISO 15764

liaisons sécurisées externes couvertes par l'ISO 20828

Figure 1 — Comment l'ISO 20828 élargit le champ d'application de l'ISO 15764

L'objectif principal de la présente Norme internationale est la gestion des certificats. De nombreux domaines de sécurité basés sur des certificats ont déjà été définis dans une grande variété de contextes. La tâche d'une gestion des certificats de sécurité pour les véhicules routiers est de définir un cadre dans lequel ces domaines de sécurité puissent interagir, de sorte que des liaisons sécurisées puissent être établies entre un domaine et un autre. Par exemple, il peut y avoir des domaines de sécurité spécifiques pour des constructeurs automobiles différents, pour des autorités publiques chargées des tachygraphes ou de tout autre composant réglementé sur le véhicule, pour les fournisseurs de services informatiques, les réparateurs et les revendeurs agréés, les équipes d'intervention d'urgence et les gestionnaires de flotte. Il convient que ce cadre les couvre tous.

Quand on définit ce cadre de sécurité, il convient de prendre en considération les exigences particulières suivantes liées à l'environnement des véhicules routiers.

— Il n'est pas nécessaire d'avoir une infrastructure globale devant être partagée par tous les systèmes de sécurité. Par exemple, on ne peut pas s'attendre à ce que des bases de données partagées soient installées en vue d'un accès de la part des dispositifs concernés.

— Il doit être possible d'intégrer facilement et sans modifications importantes les systèmes de sécurité qui existent dans les différents domaines.

— Le cadre de sécurité supplémentaire ne doit pas affecter la sécurité de chaque domaine.

— Des dispositifs ayant des niveaux de sécurité différents sont considérés. Il convient que la violation de la sécurité d'un dispositif bénéficiant d'une faible protection n'affecte pas la sécurité des autres dispositifs.

— Il convient de rendre possible l'utilisation du cadre même par des dispositifs ayant des ressources limitées. Cela signifie qu'il est recommandé que les dispositions requises par ce cadre soient faciles à traiter.

Le cas particulier des dispositifs mobiles ayant un accès limité et non permanent à des installations de communication est pris en considération.

Véhicules routiers — Gestion des certificats de sécurité

1 Domaine d'application

La présente Norme internationale établit des pratiques uniformes pour la délivrance et la gestion de certificats de sécurité destinés à être utilisés dans des applications d'infrastructure à clé publique. En supposant que toutes les entités, ayant l'intention de réaliser un échange de données sécurisé avec d'autres entités sur la base de clés publiques et privées, soient en mesure de fournir leur propre certificat, le système de gestion des certificats garantit que les entités reçoivent toutes les informations complémentaires requises pour établir une relation de confiance avec d'autres entités, à partir d'une unique source et dans un format simple et unifié. La gestion des certificats est flexible en ce qui concerne les relations entre les autorités de certification (AC, en anglais «CA»), puisqu'elle ne requiert pas de structure hiérarchique. Elle ne prescrit pas des annuaires centralisés ou d'autres solutions similaires, car elle est accessible par toutes les entités concernées. Ces propriétés font que le système de gestion est optimisé pour les applications dans le domaine automobile.

La présente Norme internationale décrit le rôle et les responsabilités de l'autorité de certification en matière de délivrance et de distribution des certificats. Elle spécifie comment traiter la validité des certificats et les politiques de certificats. Chaque entité doit au préalable s'assurer qu'elle peut réellement faire confiance à une autre entité au moment où elle envisage d'échanger des données d'un certain type avec cette dernière.

La présente Norme internationale prescrit un format de certificat, qui est une déclinaison particulière du célèbre certificat X.509 selon l'ISO/CEI 9594-8. Elle spécifie la structure et l'utilisation de chaque composant du certificat afin qu'il soit conforme à la gestion de certificats définie.

2 Références normatives

Les documents de référence suivants sont indispensables pour l'application 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).

ISO 3779, *Véhicules routiers — Numéro d'identification des véhicules (VIN) — Contenu et structure*

ISO 3780, *Véhicules routiers — Code d'identification mondiale des constructeurs (WMI)*

ISO/CEI 8824-1, *Technologies de l'information — Notation de syntaxe abstraite numéro 1 (ASN.1) — Partie 1: Spécification de la notation de base*

ISO/CEI 8824-2, *Technologies de l'information — Notation de syntaxe abstraite numéro 1 (ASN.1) — Partie 2: Spécification des objets informationnels*

ISO/CEI 8824-3, *Technologies de l'information — Notation de syntaxe abstraite numéro 1 (ASN.1) — Partie 3: Spécification des contraintes*

ISO/CEI 9594-2, *Technologies de l'information — Interconnexion de systèmes ouverts (OSI) — Partie 2: L'annuaire: Les modèles*

ISO/CEI 9594-8, *Technologies de l'information — Interconnexion de systèmes ouverts (OSI) — Partie 8: L'annuaire: Cadre général des certificats de clé publique et d'attribut*

ISO/CEI 15408-3, *Technologies de l'information — Techniques de sécurité — Critères d'évaluation pour la sécurité TI — Partie 3: Exigences d'assurance de sécurité*

ISO 15764, *Véhicules routiers — Sécurité étendue de liaison de données*

IETF RFC 3279, *Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, R. Housley, W. Polk, W. Ford, D. Solo, April 2002*

IETF RFC 3280, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, W. Polk, R. Housley, L. Bassham, April 2002*

3 Termes et définitions

Pour les besoins du présent document, les termes et définitions donnés dans l'ISO/CEI 9594-8, l'ISO 15764 ainsi que les suivants s'appliquent.

3.1
certificat
certificat à clé publique tel que défini dans l'ISO/CEI 9594-8, comprenant des informations complémentaires telles que spécifiées dans la présente Norme internationale

3.2
validité du certificat
attribution d'un des deux états «valide» ou «invalide» à un certificat par son émetteur, qui garantit uniquement que le certificat peut être utilisé pour instaurer une relation de confiance entre des entités finales s'il est valide

3.3
liste des autorités de certification
LAC
liste tenue à jour par une AC pour une de ses clés publiques, la clé privée correspondante étant utilisée pour signer des certificats, contenant des informations sur d'autres AC ayant émis des certificats d'AC avec cette clé publique qui est la clé publique du sujet, et des informations sur ces certificats d'AC

3.4
chemin de certification
séquence ordonnée d'AC différentes, avec leurs clés publiques et les certificats d'AC émis par elles et signés avec la clé privée correspondante, dans laquelle chaque clé publique du sujet dans un de ces certificats d'AC est la clé publique de l'AC suivante dans la séquence

3.5
informations sur le chemin de certification
ICC
informations tenues à jour par une AC pour une de ses clés publiques, la clé privée correspondante étant utilisée pour signer des certificats comprenant des informations sur tous les chemins de certification commençant à cette AC avec un certificat d'AC signé par cette clé privée, et comprenant des informations de validité sur les certificats d'AC dans les chemins de certification et sur les certificats émis pour les entités finales par une des AC dans les chemins de certification et signés avec la clé privée correspondant à sa clé publique

3.6
confirmation de confiance
informations accessibles sans restrictions qui permettent à une entité de vérifier qu'elle peut faire confiance à une autre entité

3.7
entité finale
entité impliquée dans l'établissement d'un échange de données sans être installée auprès d'une AC

3.8
entité
équipement technique, protégé contre tout accès de la part de tiers, qui est capable d'échanger des données sur une liaison de communication à laquelle des tiers peuvent avoir accès

EXEMPLE 1 Un véhicule a un certain nombre d'unités de contrôle électroniques (UCE, en anglais «ECU») reliées par un réseau de communication interne. Par le biais d'une passerelle, ce réseau de communication est raccordé à une liaison de communication externe mobile. Le constructeur du véhicule peut protéger le réseau de communication interne contre tout accès de la part de tiers. Ensuite, la sécurité des données sur la liaison de communication externe peut être assurée par la passerelle, en laissant les données échangées sur le réseau interne sans protection ultérieure. Dans ce cas, l'intégralité du véhicule, représenté par la passerelle, peut être considérée comme une entité.

EXEMPLE 2 Dans le véhicule décrit ci-dessus, il peut y avoir une UCE qui a besoin d'échanger des données sensibles avec un dispositif externe en utilisant le réseau de communication interne, la passerelle et le réseau de communication externe. Pour ces données, le niveau de protection sur le réseau de communication interne peut être considéré comme trop faible. L'UCE sera alors considérée comme une entité distincte qui assure un niveau de sécurité des données plus élevé que si elle s'était basée sur la passerelle.

3.9
confiance initiale
confiance d'une entité envers une autre entité, qui est basée sur les connaissances directes au sujet de cette autre entité et non pas sur des informations reçues de la part de tiers

3.10
émetteur (d'un certificat)
entité identifiée dans un certificat et qui a signé le certificat

NOTE Selon la présente Norme internationale, l'émetteur d'un certificat est toujours une AC.

3.11
certificat de chemin

clé publique d'une AC, avec les informations supplémentaires selon la présente Norme internationale, rendue infalsifiable en la signant avec la clé privée d'une autre AC, confirmant l'existence de chemins de certification aboutissant au propriétaire de la clé publique

3.12
sujet (d'un certificat)
entité identifiée dans un certificat et qui détient la clé publique

4 Symboles et abréviations

Pour les besoins de la présente Norme internationale, les abréviations suivantes s'appliquent.

L'abréviation après «ou» est celle de l'anglais. L'abréviation unique est reprise de l'anglais.

AC ou CA	Autorité de certification
LAC ou CAL	Liste des autorités de certification
ICC ou CPI	Informations sur le chemin de certification
RCD ou DER	Règles de codage distinguées
UCE ou ECU	Unité de contrôle électronique
VIN	Numéro d'identification des véhicules
WMI	Code d'identification mondiale des constructeurs

5 Principes de gestion des certificats

5.1 Établissement d'une relation de confiance

5.1.1 Classes de sécurité

Les entités qui prévoient d'échanger des données sensibles ne doivent échanger ces données qu'après avoir établi une relation de confiance entre elles. La présente Norme internationale spécifie comment cette confiance peut être établie.

Chaque entité peut prendre des mesures appropriées pour protéger les données sensibles qu'elle traite et fera confiance à ces mesures. Dès que les données sensibles sont échangées entre des entités, cela ne suffit plus: il est nécessaire que l'autre entité soit impliquée dans la protection et qu'elle garantisse de prendre des mesures de sécurité appropriées pour protéger les données. L'établissement d'une relation de confiance signifie que l'entité qui fait confiance est convaincue que l'autre entité prend les mesures de sécurité appropriées concernant les données sensibles.

Pour spécifier la confiance requise, les données qui doivent être échangées entre deux entités doivent être classées selon les quatre classes de sécurité suivantes:

Classe 0: Aucune protection

Les données échangées ne sont pas sensibles, ce qui exclut toute menace en matière de sécurité. Ces données peuvent être échangées sans qu'aucune relation de confiance n'ait été établie.

Classe 1: Protection de confidentialité

Il existe un risque de mauvaise utilisation de données sensibles par des tiers. L'émetteur des données a la responsabilité d'assurer la confidentialité. L'émetteur doit

— envoyer ces données uniquement aux destinataires qui ont le droit d'y avoir accès,

— envoyer ces données uniquement aux destinataires qui gardent la confidentialité. Cela comprend le fait qu'ils ne retransmettent pas des données qui sont identifiées comme interdites de réacheminement, et qu'ils ne réacheminent ces données qu'à des destinataires qui sont soumis aux mêmes règles de confidentialité, et

— lorsqu'il envoie les données, les protéger de manière qu'aucun tiers non autorisé ne puisse deviner le contenu des données ou leur signification.

Pour agir en conformité avec ces règles, l'émetteur doit établir une relation de confiance avec le destinataire des données. Une entité en qui l'émetteur n'a pas confiance n'a pas le droit d'avoir accès à des données de classe 1. La confiance doit s'étendre au fait que cette entité garde confidentielles les données de classe 1.

Classe 2: Protection de l'intégrité

Des fausses données risquent d'entraîner des conséquences néfastes pour le destinataire de données sensibles s'il les utilise. Le destinataire des données a la responsabilité de vérifier l'intégrité des données. Le destinataire doit

— utiliser uniquement les données reçues d'un émetteur qui a le droit de les envoyer,

— utiliser uniquement les données qui proviennent de l'émetteur ou d'une entité soumise aux mêmes règles d'intégrité que l'émetteur (y compris concernant la protection de l'intégrité sur le chemin entre cette entité et l'émetteur), et

— utiliser les données uniquement après avoir vérifié que l'intégrité est assurée de l'émetteur jusqu'au destinataire. L'intégrité signifie que les données sont envoyées de l'entité qu'elles désignent comme l'émetteur, ont été générées dans des circonstances appropriées pour l'utilisation prévue et n'ont pas été manipulées sur leur trajet jusqu'au destinataire.

Pour agir en conformité avec ces règles, le destinataire doit établir une relation de confiance avec l'émetteur des données. Une entité en qui le destinataire n'a pas confiance n'a pas le droit d'envoyer des données de classe 2. La confiance doit s'étendre au fait que cette entité n'envoie que des données de classe 2 confidentielles qui proviennent de l'entité ou d'une autre entité de confiance.

Classe 3: Protection de la confidentialité et de l'intégrité

Combinaison de la classe 1 et de la classe 2. L'émetteur et le destinataire des données doivent appliquer les règles de la classe 1 et de la classe 2. Les deux entités doivent être capables de se faire confiance.

5.1.2 Extension de la confiance

Pour l'échange de données de classe 1, 2 et 3, une relation de confiance doit être établie entre les deux entités. Pour ce faire, la méthode spécifiée dans la présente Norme internationale suppose que la confiance a les propriétés fondamentales suivantes:

— elle est orientée: si l'entité A fait confiance à l'entité B, cela n'implique pas automatiquement que l'entité B fasse confiance à l'entité A. Par conséquent, la méthode pour établir une relation de confiance doit être appliquée dans le sens dans lequel la confiance est requise en fonction de la classe des données;

— elle est transitive: si l'entité A fait confiance à l'entité B et que l'entité B fasse confiance à l'entité C, alors l'entité A peut faire confiance à l'entité C.

La seconde propriété permet d'étendre à d'autres entités la confiance qui existe entre des entités. Cette extension ne fonctionne que dans les conditions suivantes:

— au départ, il existe une certaine confiance qui n'a pas été établie par le biais d'un tel processus d'extension. Cette confiance est appelée la confiance initiale;

— la confirmation de la relation de confiance établie de l'entité B à l'entité C est mise à la disposition de toute entité A qui souhaite étendre à l'entité C sa confiance en l'entité B. L'entité A doit être en mesure de vérifier cette confirmation.

Une entité A ne doit étendre à l'entité C la confiance qu'elle a en l'entité B que si elle obtient la confirmation du fait que B fait confiance à C et après avoir contrôlé avec succès cette confirmation. Ce cas est illustré à la Figure 2.