Norme internationale

ISO 15118-20

Véhicules routiers — Interface de communication entre véhicule et réseau électrique —

Partie 20: Exigences des couches réseau et application de 2ème génération

AMENDEMENT 1: Service RED en CA, service MCS et concept de sécurité amélioré

Road vehicles — Vehicle to grid communication interface —

Part 20: 2nd generation network layer and application layer requirements

AMENDMENT 1: AC DER service, MCS service, and improved security concept

Sample Document
Get the document from standards.iteh.ai

Première édition
2022-04

AMENDEMENT 1
2026-07

Numéro de référence
ISO 15118-20:2022/Amd.1:2026(fr)

© ISO 2026

ISO 15118-20:2022/Amd 1:2026 • https://standards.iteh.ai/catalog/standards/iso/6ad8ce30-396d-4303-a734-c2bccb972d1f/iso-15118-20-2022-amd-1-2026

Sample Document

get full document from standards.iteh.ai



DOCUMENT PROTÉGÉ PAR COPYRIGHT

© ISO 2026

Tous droits réservés.

La présente publication de l'ISO est protégée par le droit d'auteur et demeure la propriété de l'ISO et/ou de ses concédants de licence.

Le contenu de la présente publication de l'ISO est fourni sous licence, et n'est pas vendu. Son utilisation est soumise aux conditions de licence applicables définies par l'ISO, un organisme membre de l'ISO, ou un distributeur tiers agréé.

Sous réserve des besoins liés à sa mise en œuvre ou d'une autorisation expresse prévue aux termes d'une licence distincte, aucune partie de la présente publication de l'ISO ne peut être reproduite, distribuée, modifiée, utilisée ou mise à disposition sous quelque forme ou par quelque moyen que ce soit – électronique ou mécanique, y compris la photocopie, la numérisation, l'enregistrement ou la publication sur des plateformes numériques internes ou externes.

Toute utilisation hors du champ d'application des droits accordés est interdite et peut donner lieu à des poursuites judiciaires.

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

Publié en Suisse

ISO 15118-20:2022/Amd 1:2026 • https://standards.iteh.ai/catalog/standards/iso/6ad8ce30-396d-4303-a734-c2bccb972d1f/iso-15118-20-2022-amd-1-2026

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 propriété revendiqué à cet égard. À la date de publication du présent document, l'ISO n'avait pas 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 de tels droits de propriété et averti de leur existence.

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 le lien suivant: www.iso.org/iso/foreword.html.

Sample Document
get full document from standards.iteh.ai

Le présent document a été établi conjointement par le comité technique ISO/TC 22, *Véhicules routiers*, sous-comité SC 31, *Communication de données*, et par le comité technique IEC/TC 69, *Véhicules électriques destinés à circuler sur la voie publique et chariots de manutention électriques*, en collaboration avec le Comité technique CEN/TC 301 du Comité européen de normalisation (CEN), *Véhicules routiers*, conformément à l'Accord de coopération technique entre l'ISO et le CEN (Accord de Vienne).

Une liste de toutes les parties de la série ISO 15118 se trouve sur le site web de l'ISO.

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/members.html.

© ISO 2026 – Tous droits réservés

ISO 15118-20:2022/Amd 1:2026 • https://standards.iteh.ai/catalog/standards/iso/6ad8ce30-396d-4303-a734-c2bccb972d1f/iso-15118-20-2022-amd-1-2026

Sample Document

get full document from standards.iteh.ai

Véhicules routiers — Interface de communication entre véhicule et réseau électrique —

Partie 20:
Exigences des couches réseau et application de 2ème génération

AMENDEMENT 1: Service RED en CA, service MCS et concept de sécurité amélioré

Article 2, Références normatives

Ajouter les références suivantes à la fin de l'article:

ISO 15118-10:2025, *Véhicules routiers — Interface de communication entre véhicule et réseau électrique — Partie 10: Exigences relatives aux couches physiques et liaison de données pour l'Ethernet à paire unique*

IEC 61851-23-3:2025, *Système de charge par conduction pour véhicules électriques — Partie 23-3: Système d'alimentation en courant continu pour véhicules électriques — Système de recharge mégawatt*

Sample Document
Get full document from standards.iteh.ai

Article 3, Termes et définitions

Ajouter les termes et définitions suivants à la fin de l'article:

3.72
état d'activation de charge
état CE
état conformément à la fonction d'activation de charge définie dans l'IEC 61851-23-3

Note 1 à l'article: L'abréviation «CE» est dérivée du terme anglais développé correspondant «charge enable».

3.73
système de recharge mégawatt
MCS
système de recharge conforme à l'IEC 61851-23-3

Note 1 à l'article: L'abréviation «MCS» est dérivée du terme anglais développé correspondant «megawatt charging system».

3.74
EPS régional
système électrique régional, défini dans l'IEEE 1547

Note 1 à l'article: L'abréviation «EPS» est dérivée du terme anglais développé correspondant «electric power system».

© ISO 2026 – Tous droits réservés

ISO 15118-20:2022/Amd 1:2026 • https://standards.iteh.ai/catalog/standards/iso/6ad8ce30-396d-4303-a734-c2bccb972d1f/iso-15118-20-2022-amd-1-2026

3.75
interruption de l'alimentation
interruption de la fourniture de puissance active en régime permanent et transitoire, et limitation de l'échange de puissance réactive

Note 1 à l'article: À l'issue de l'interruption, le VE retourne immédiatement en service sans respecter les règles d'entrée en service.

3.76
ressource énergétique distribuée
RED
source d'énergie électrique qui n'est pas directement connectée à un réseau de production-transport

EXEMPLE Générateurs et technologies de stockage d'énergie capables d'exporter de la puissance active vers le réseau électrique.

Note 1 à l'article: Un système d'interconnexion ou un dispositif RED supplémentaire qui est nécessaire pour assurer la conformité au présent document fait partie d'une RED.

3.77
entrée en service
ensemble de paramètres qui définit les modalités de mise sous tension ou de remise sous tension du système électrique

Note 1 à l'article: Si les valeurs de tension et de fréquence ne se situent pas dans la plage souhaitée, la *ressource énergétique distribuée (RED)* (3.76) ne sera pas autorisée à commencer à injecter de la puissance dans le réseau/système électrique.

3.78
courbe de statisme de la fréquence
courbe paramétrée de la fonction fréquence-watt

Sample Document

Note 1 à l'article: Les paramètres comprennent une bande morte de fréquence (db, *dead band*) et un facteur k sans unité qui définit le taux de variation de la puissance de sortie dû à la variation de fréquence. Cette opération limite la production ou la consommation de puissance active lorsque l'écart entre la fréquence d'alimentation et sa valeur nominale atteint une valeur spécifiée.

3.79
recharge de niveau 1
recharge avec une puissance maximale comprise entre 1 kW et 1,8 kW, par l'intermédiaire d'une prise monophasée normalisée de 120 V en valeur efficace en courant alternatif

Note 1 à l'article: Cette limite de puissance n'est applicable qu'aux États-Unis.

3.80
recharge de niveau 2
recharge avec une puissance maximale comprise entre 3 kW et 22 kW, par l'intermédiaire d'un chargeur en courant alternatif spécifique

Note 1 à l'article: Aux États-Unis, la tension fournie est généralement de 240 V en valeur efficace en courant alternatif alors qu'en Europe, elle est de 230 V en valeur efficace en courant alternatif.

3.81
zone de coupure admise
zone de tension ou de fréquence dans laquelle le VE est autorisé à effectuer une *interruption de l'alimentation* (3.75) et à effectuer *une coupure* (3.88) de la connexion

Note 1 à l'article: La zone est définie par une courbe linéaire segmentée qui marque la limite pour la tension ou la fréquence.

© ISO 2026 – Tous droits réservés

ISO 15118-20:2022/Amd 1:2026 • https://standards.iteh.ai/catalog/standards/iso/6ad8ce30-396d-4303-a734-c2bccb972d1f/iso-15118-20-2022-amd-1-2026

3.82
zone d'interruption momentanée
zone de tension ou de fréquence dans laquelle le VE effectue une *interruption de l'alimentation* (3.75) temporaire d'un système électrique (l'injection de puissance dans ce système) en réponse à une perturbation des tensions applicables ou de la fréquence du système

Note 1 à l'article: Lorsqu'il entre dans cette zone, le VE conserve la capacité de rétablir immédiatement la sortie de fonctionnement au moment où les tensions applicables et la fréquence du système reviennent dans les plages définies.

Note 2 à l'article: La zone est définie par une courbe linéaire segmentée qui marque la limite pour la tension ou la fréquence.

3.83
zone de coupure obligatoire
zone de tension ou de fréquence dans laquelle le VE doit effectuer une *interruption de l'alimentation* (3.75) et une *coupure* (3.88) de la connexion

Note 1 à l'article: La zone est définie par une courbe linéaire segmentée qui marque la limite pour la tension ou la fréquence.

3.84
temps de réponse en boucle ouverte
temps nécessaire pour atteindre 90 % de la nouvelle cible en réponse à la variation progressive du signal d'entrée de commande

3.85
service d'autorisation
paramètre qui indique si une *ressource énergétique distribuée (RED)* (3.76) est autorisée à entrer ou à rester en service

Sample Document

3.86
retour au service
entrée en service (3.77) qui fait suite à une *reprise après coupure* (3.88)

get full document from standards.iteh.ai

3.87
tenue
aptitude à résister aux perturbations de tension ou de fréquence à l'intérieur de limites définies et à continuer à fonctionner comme prévu

3.88
coupure
inhibition du *retour au service* (3.86) immédiat

Note 1 à l'article: Une fois que la *ressource énergétique distribuée (RED)* (3.76) a reçu l'autorisation de reprendre le service, elle doit respecter les règles d'*entrée en service* (3.77).

Article 4, Termes abrégés

Ajouter les abréviations suivantes à la liste:

CE (Charge Enable)	activation de charge
CL (charge loop)	boucle de recharge
RED	ressource énergétique distribuée (dans le contexte d'un service RED en CA)
MCS	système de recharge mégawatt

© ISO 2026 – Tous droits réservés

ISO 15118-20:2022/Amd 1:2026 • https://standards.iteh.ai/catalog/standards/iso/6ad8ce30-396d-4303-a734-c2bccb972d1f/iso-15118-20-2022-amd-1-2026

Modifier l'abréviation existante «DER» de la manière suivante:

DER (Distinguished Encoding Rules)	règles de codage distinctives (dans le cadre des certificats X.509v3)

5.2

Remplacer l'intégralité du paragraphe, y compris son titre, par le paragraphe suivant:

5.2 Structure des exigences et des dispositions

Le présent document décrit les exigences selon la structure définie ci-dessous. De même, les dispositions importantes qui ne constituent pas des exigences («doit»), mais des autorisations («peut») ou des recommandations («il convient») suivent la structure définie ci-dessous. Chaque exigence ou disposition définie dans le présent document est identifiée par un numéro unique. Cette structure systématique et ordonnée permet au lecteur de trouver facilement l'exigence (la disposition) qu'il recherche.

Le format ci-dessous s'applique aux nouvelles exigences ou dispositions et aux exigences ou dispositions mises à jour:

«[V2G20-«XXXX»]» «formulation de l'exigence/de la disposition», où:

— **«**V2G20**»** représente le présent document;

— «XXXX» correspond au numéro spécifique de l'exigence ou de la disposition, soit un numéro à quatre chiffres à partir de 1 000;

— «formulation de l'exigence/de la disposition» correspond au texte décrivant l'exigence ou la disposition.

— Pour les exigences propres au service RED en CA ou au service MCS exclusivement, un identificateur est ajouté de la manière suivante: «[V2G20-"XXXX"] [RED]» ou «[V2G20-"XXXX"] [MCS]», respectivement.

Sample Document
Get full document from standards.iteh.ai

EXEMPLE 1 **[V2G20-0000]** Ceci est un exemple d'identification qu'il faut/qu'il est admis/qu'il est recommandé de suivre pour les exigences introduites dans le présent document.

Le format suivant s'applique aux exigences tirées de la première édition de l'ISO 15118-2:

[«V2G20»-«YYY»] «formulation de l'exigence/de la disposition», où:

— **«**V2G20**»** représente le présent document;

— «YYY» correspond au numéro spécifique de l'exigence ou de la disposition, déjà défini dans la première édition de l'ISO 15118-2;

— La «formulation de l'exigence/de la disposition» est identique à celle spécifiée dans la première édition de l'ISO 15118-2.

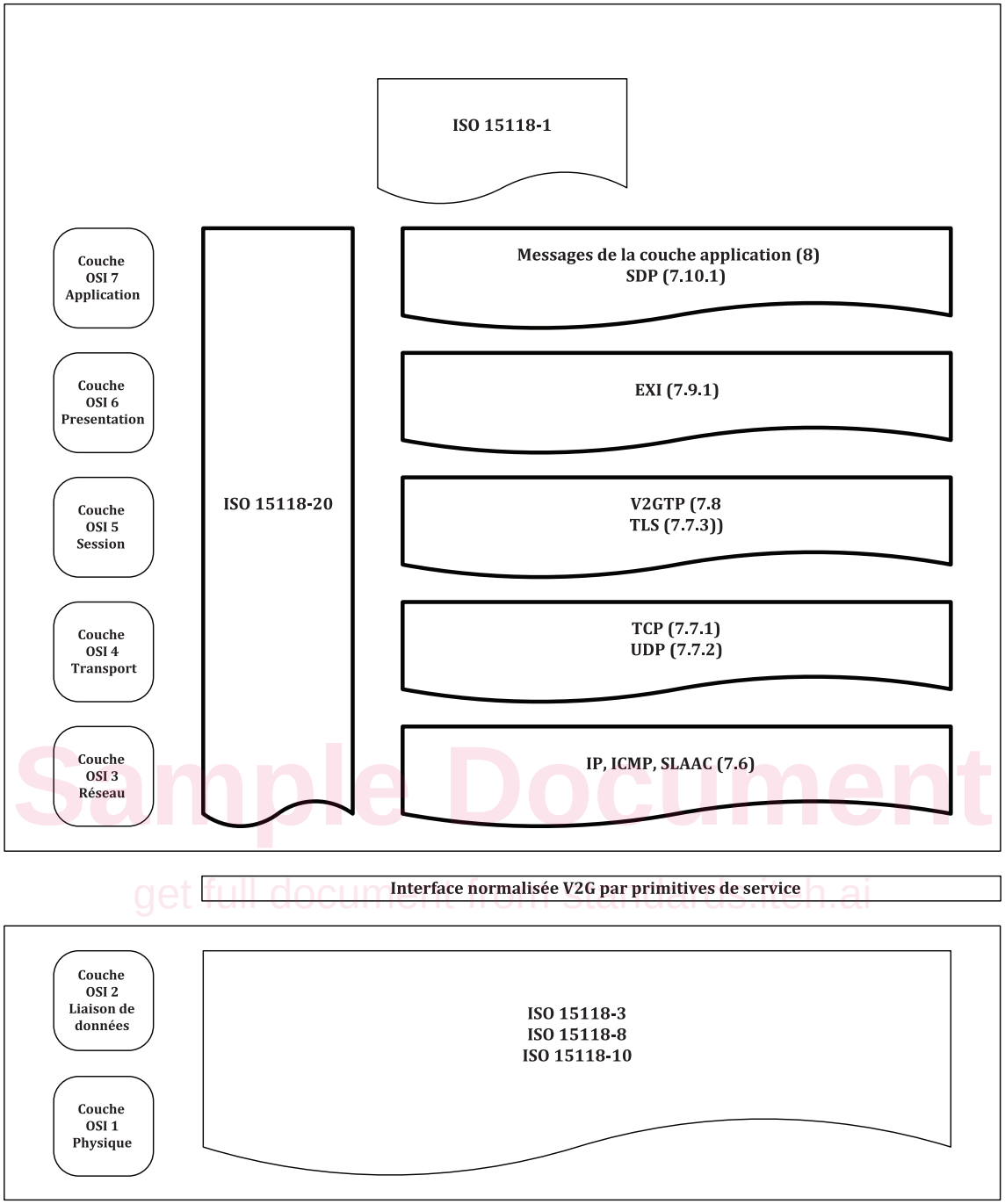
EXEMPLE 2 **[V2G20-000]** Ceci est un exemple d'identification qu'il faut/qu'il est admis/qu'il est recommandé de suivre pour les exigences définies à l'origine dans la première édition de l'ISO 15118-2.

Article 6

Remplacer la Figure 2 par la figure suivante:

© ISO 2026 – Tous droits réservés

ISO 15118-20:2022/Amd 1:2026 • https://standards.iteh.ai/catalog/standards/iso/6ad8ce30-396d-4303-a734-c2bccb972d1f/iso-15118-20-2022-amd-1-2026



Sample Document
get full document from standards.iteh.ai

Figure 2 — Aperçu général des documents relatifs à la communication entre véhicule et réseau électrique

7.3.2

Remplacer le Tableau 2 par le tableau suivant:

© ISO 2026 – Tous droits réservés

ISO 15118-20:2022/Amd 1:2026 • https://standards.iteh.ai/catalog/standards/iso/6ad8ce30-396d-4303-a734-c2bccb972d1f/iso-15118-20-2022-amd-1-2026

Tableau 2 — Exemples d'extensions de certificat

Extensions de certificat	Description
Key usage (Utilisation de la clé)	Utilisation de la clé privée correspondante (par exemple signature numérique, non-répudiation, chiffrement de clé, etc.)
	Autre spécification d'utilisation de clé en utilisant des OID, par exemple:
	— authentification du serveur (1.3.6.1.5.5.7.3.1); — authentification du client (1.3.6.1.5.5.7.3.2).
	NOTE Parfois, les valeurs suivantes sont ici également codées:
Extended Key Usage (Utilisation étendue de la clé)	— Netscape SGC (1.3.6.1.4.1.311.10.3.3); — Microsoft SGC (2.16.840.1.113730.4.1).
	SGC signifie «Server Gated Crypto» et indique que le serveur peut également utiliser une cryptographie forte pour la connexion avec le navigateur du client. Cette extension a été utilisée au moment du contrôle d'exportation de cryptographie forte pour permettre à un site web financier d'assurer une protection appropriée du transfert de données.
CRL distribution point (Point de diffusion de CRL)	Emplacement pour extraire des listes de révocation de certificats
OCSP	Emplacement de récupération du protocole OCSP. Voir IETF RFC 6960 mise à jour par l'IETF RFC 8954 pour plus d'informations.
Authority information (Informations relatives à l'autorité)	Informations supplémentaires relatives à l'autorisation
Subject alternative name (Autre nom du sujet)	Autres noms de l'entité
Basic constraint = CA (Contrainte de base = AC)	Vrai si le certificat est un certificat racine ou un certificat de sous-AC.
Subject information (Informations sur le sujet)	Informations complémentaires sur le sujet

Sample Document
get full document from standards.iteh.ai

Remplacer la NOTE 8 par ce qui suit:

NOTE 8 De plus, la longueur de clé de 456 bits est utilisée avec certaines courbes dans le cadre de l'application du présent document. Si une entité V2G peut gérer et utiliser des clés de 521 bits, elle peut également être en mesure de gérer et d'utiliser des clés de 456 bits.

Ajouter le nouvel alinéa suivant sous la NOTE 14 à l'exigence [V2G20-1234]:

Dans le présent document, la taille des certificats est inférieure ou égale à 1 600 octets. Cette limite tient compte des contraintes de ressources dans les systèmes embarqués. Pour réduire la taille des certificats, des aspects sont à prendre considération: par exemple, il faut être prudent lors de l'ajout de longues URL, de caractères de 4 octets dans les noms distinctifs ou de politiques de certification multiples, car ces éléments peuvent augmenter la taille du certificat de manière significative. Il peut être nécessaire de n'en utiliser qu'un, soit CRLDistributionPoints, soit AuthorityInfoAccess, et pas les deux, si du fait de l'inclusion des deux, la taille du certificat dépasse 1 600 octets.

Remplacer l'exigence [V2G20-1004] par les nouvelles exigences et la nouvelle note suivantes:

[V2G20-3000] Les parties utilisatrices doivent s'assurer que les certificats sont valides exclusivement dans les limites de la durée de validité du certificat de leur émetteur.

© ISO 2026 – Tous droits réservés

ISO 15118-20:2022/Amd 1:2026 • https://standards.iteh.ai/catalog/standards/iso/6ad8ce30-396d-4303-a734-c2bccb972d1f/iso-15118-20-2022-amd-1-2026

NOTE 15 Il est prévu que l'AC n'émette que des certificats valides exclusivement dans les limites de la durée de validité de son propre certificat.

[V2G20-3001] Lors de la validation des certificats, le CCVE et le CCIR doivent s'assurer que la [V2G20-3000] est respectée.

Remplacer le premier point de la NOTE 20 (ancienne numérotation) par ce qui suit:

NOTE 20 [...].

a) Le contenu du certificat feuille n'a pas été modifié après sa délivrance. Cela signifie qu'il est possible de vérifier et confirmer la signature jusqu'au niveau d'ancre de confiance, et donc l'intégrité du contenu signé.

— [...].

Renuméroter l'ancienne NOTE 15 et les notes suivantes, en commençant par le numéro 16.

7.3.2.1

Remplacer l'exigence [V2G20-2327] et la NOTE 3 par ce qui suit:

[V2G20-3002] Le certificat signataire OCSP utilisé pour signer la réponse OCSP pour l'état du certificat CCIR doit être généré à l'aide d'une chaîne de certification utilisant comme ancre de confiance le même certificat AC racine V2G que le certificat CCIR dont l'état est en cours de vérification, ou utilisant comme ancre de confiance l'un des certificats AC racine V2G dont le CCVE a inclus le DN dans l'extension «certificate_authorities» qu'il a envoyée dans le message «ClientHello». Voir Figure 5 pour une représentation graphique. Voir Annexe H pour plus de détails. Voir H.1.6 pour des exemples de structure de certificat. Voir Annexe B pour plus d'informations sur le profil de certificat.

Sample of document
get full document from standards.iteh.ai

NOTE 3 Le présent document ne prescrit pas l'utilisation d'une AC racine V2G particulière. Dans le cas où plusieurs AC racine V2G sont disponibles dans une région, une bonne pratique consiste à faire en sorte que le certificat signataire OCSP qui signe la réponse OCSP pour le certificat CCIR (ou le ou les certificats de sous-AC de la chaîne de certification CCIR) se lie à l'AC racine V2G qui signe la chaîne de certification CCIR que le CCIR transmet au CCVE pour cette prise de contact TLS particulière. Cela ne relève cependant pas du domaine d'application du présent document.

Remplacer les exigences [V2G20-2330] et [V2G20-2332] par les nouvelles exigences suivantes, respectivement:

[V2G20-3003] Le certificat signataire OCSP utilisé pour signer la réponse OCSP pour l'état du certificat de contrat doit être généré à l'aide d'une chaîne de certification utilisant le même certificat AC racine du FSME ou le même certificat AC racine V2G que l'ancre de confiance du certificat de contrat dont l'état est en cours de vérification. Voir Figure 6 pour une représentation graphique. Voir Annexe H pour plus de détails. Voir H.1.6 pour des exemples de structure de certificat. Voir Annexe B pour plus d'informations sur le profil de certificat.

[V2G20-3004] Le certificat signataire OCSP utilisé pour signer la réponse OCSP pour l'état du certificat de véhicule doit être généré à l'aide d'une chaîne de certification utilisant le même certificat AC racine de FEO ou le même certificat AC racine V2G que l'ancre de confiance du certificat de véhicule dont l'état est en cours de vérification. Voir Figure 7 pour une représentation graphique. Voir Annexe H pour plus de détails. Voir H.1.6 pour des exemples de structure de certificat. Voir Annexe B pour plus d'informations sur le profil de certificat.

© ISO 2026 – Tous droits réservés

ISO 15118-20:2022/Amd 1:2026 • https://standards.iteh.ai/catalog/standards/iso/6ad8ce30-396d-4303-a734-c2bccb972d1f/iso-15118-20-2022-amd-1-2026

Remplacer la NOTE 10 par ce qui suit:

NOTE 10 Le présent document ne prescrit pas l'utilisation d'une AC racine V2G particulière. Dans le cas où plusieurs AC racine V2G sont disponibles dans une région, une bonne pratique consiste à faire en sorte que le certificat signataire OCSP qui signe la réponse OCSP pour le certificat de véhicule (ou le ou les certificats de sous-AC de la chaîne de certification du véhicule) se lie à l'AC racine V2G qui signe la chaîne de certification du véhicule dont l'état est en cours de vérification. Cela ne relève cependant pas du domaine d'application du présent document.

Remplacer l'exigence [V2G20-2334] et la NOTE 12 par ce qui suit:

[V2G20-3005] Le certificat signataire OCSP utilisé pour signer la réponse OCSP pour l'état du certificat de fourniture du FEO doit être généré à l'aide d'une chaîne de certification utilisant comme ancre de confiance le même certificat AC racine de FEO ou le même certificat AC racine V2G que le certificat de fourniture du FEO dont l'état est en cours de vérification. Voir Figure 7 pour une représentation graphique. Voir Annexe H pour plus de détails. Voir H.1.6 pour des exemples de structure de certificat. Voir Annexe B pour plus d'informations sur le profil de certificat.

NOTE 12 Le présent document ne prescrit pas l'utilisation d'une AC racine V2G particulière. Dans le cas où plusieurs AC racine V2G sont disponibles dans une région, une bonne pratique consiste à faire en sorte que le certificat signataire OCSP qui signe la réponse OCSP pour le certificat de fourniture du FEO (ou le ou les certificats de sous-AC de la chaîne de certification de fourniture du FEO) se lie à l'AC racine V2G qui signe la chaîne de certification de fourniture du FEO dont l'état est en cours de vérification. Cela ne relève cependant pas du domaine d'application du présent document.

7.3.4

Supprimer les exigences suivantes: [V2G20-1235] et [V2G20-2646].

Sample Document
get full document from standards.iteh.ai

7.4

Ajouter les nouvelles exigences et la nouvelle NOTE suivantes à la fin de ce paragraphe (sous la Figure 9):

[V2G20-3006] [MCS] Dans le cas d'un service MCS ou MCS_BPT: si le CCVE a transmis le message SessionStopReq avec un paramètre ChargingSession défini sur «Pause», il doit interrompre la liaison de données (D-LINK_PAUSE.request ()) après réception du message SessionStopRes avec un paramètre ResponseCode défini sur «OK» et suivre les exigences de veille et de réactivation définies dans l'ISO 15118-10:2025, 7.6.

[V2G20-3007] [MCS] Dans le cas d'un service MCS ou MCS_BPT: si le CCIR a reçu le message SessionStopReq avec un paramètre ChargingSession défini sur «Pause», il doit interrompre la liaison de données (D-LINK_PAUSE.request ()) après envoi du message SessionStopRes avec un paramètre ResponseCode défini sur «OK» et suivre les exigences de veille et de réactivation définies dans l'ISO 15118-10:2025, 7.6.

NOTE 3 Les exigences [V2G20-1227] et [V2G20-1777] ne sont pas applicables aux services MCS et MCS_BPT.

7.5

Remplacer la deuxième phrase du premier alinéa par ce qui suit:

L'ISO 15118-3, l'ISO 15118-8 et l'ISO 15118-10 donnent d'autres informations sur la couche liaison de données à couvrir.

Ajouter la nouvelle exigence suivante à la fin de ce paragraphe:

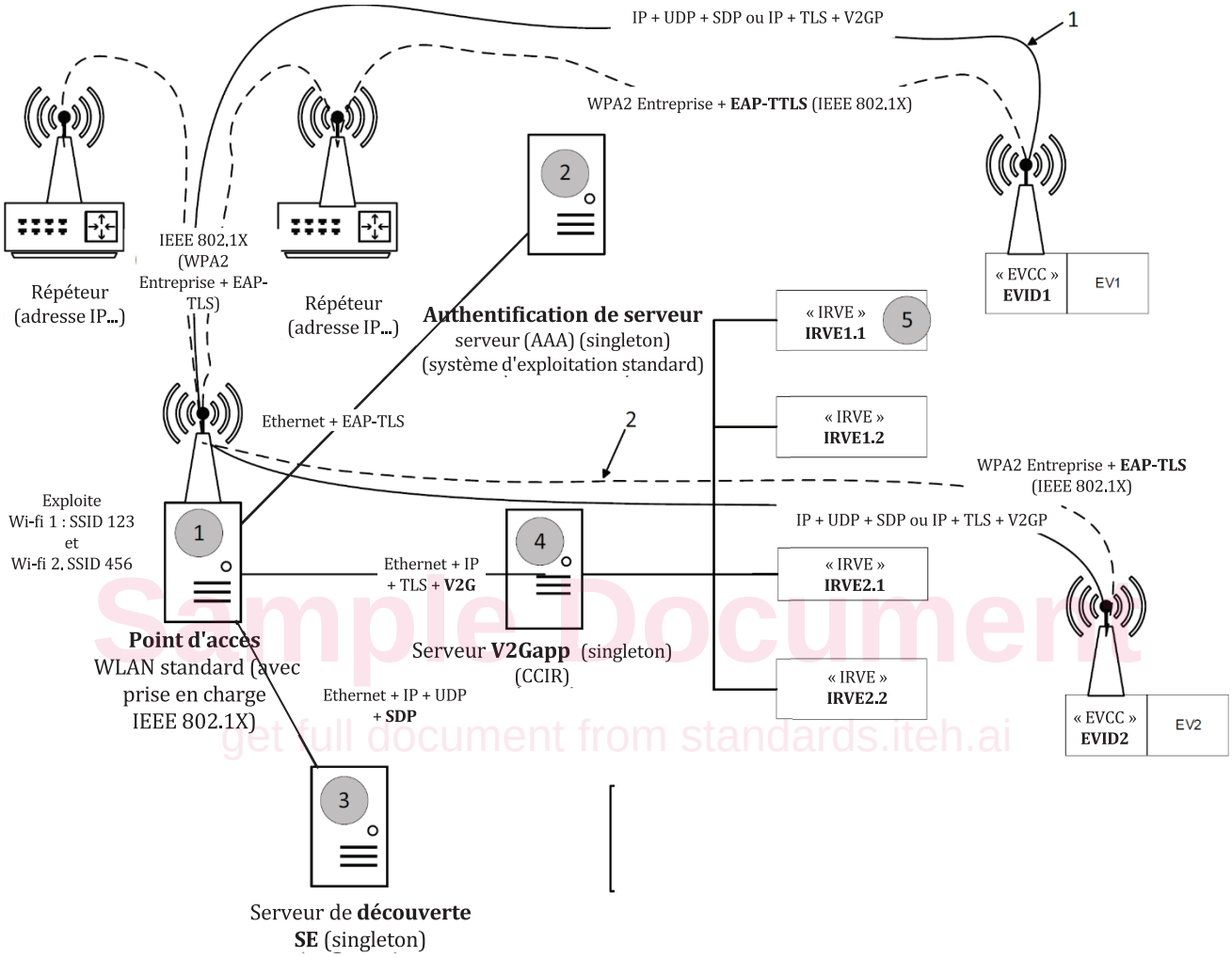
© ISO 2026 – Tous droits réservés

ISO 15118-20:2022/Amd 1:2026 • https://standards.iteh.ai/catalog/standards/iso/6ad8ce30-396d-4303-a734-c2bccb972d1f/iso-15118-20-2022-amd-1-2026

[V2G20-3008] [MCS] Si une entité V2G communique par 10BASE-T1S, elle doit être conforme à l'ISO 15118-10.

7.5.1.2

Remplacer la Figure 10 par la figure suivante:



Légende

1 protocole de communication de la couche application

2 protocole de communication IEEE 802.1X

Figure 10 — Exemple IEEE 802.1X avec authentification de serveur pour le TPSF

7.7.3.3

Ajouter la nouvelle NOTE suivante après la NOTE 8 sous la [V2G20-2368]:

NOTE 9 Bien que cette exigence spécifie l'utilisation des RDN du champ Issuer des certificats racine, conformément à l'IETF RFC 5280:2008, 4.1.2.4 (mise à jour par l'IETF RFC 6818, l'IETF RFC 8398 et l'IETF RFC 8399) pour les certificats racine, il convient que ces RDN soient les mêmes pour le champ Issuer et le champ Subject.

Remplacer les exigences [V2G20-2369] et [V2G20-2370] par les nouvelles exigences suivantes, respectivement:

Sample Document
get full document from standards.iteh.ai

© ISO 2026 – Tous droits réservés

ISO 15118-20:2022/Amd 1:2026 • https://standards.iteh.ai/catalog/standards/iso/6ad8ce30-396d-4303-a734-c2bccb972d1f/iso-15118-20-2022-amd-1-2026

[V2G20-3373] Si aucun certificat AC racine V2G ni aucun certificat AC racine privée de l'EP ne sont disponibles dans le CCVE, l'extension «certificate_authorities» ne doit pas être présente dans le message «ClientHello».

[V2G20-3374] Tant que le CCVE est en CPM4PE, il ne doit pas inclure l'extension «certificat_authorities» dans le message «ClientHello», que le CCVE dispose ou non d'un ou de plusieurs certificats AC racine V2G et d'un ou de plusieurs certificats AC racine privée de l'EP. Voir H.2.2.3 pour plus d'informations sur le CPM4PE.

Supprimer l'exigence suivante: [V2G20-2371]

Remplacer les exigences [V2G20-2378] et [V2G20-2379] par les nouvelles exigences suivantes, respectivement:

[V2G20-3375] Si le CCVE n'a fourni aucune indication des racines disponibles conformément à la **[V2G20-3373]**, un CCIR public doit envoyer dans le message «ServerHello» sa propre chaîne de certification (chaîne de certification CCIR) ainsi que tous les éventuels co-certificats nécessaires jusqu'à une racine (à l'exclusion du certificat racine lui-même) de son choix.

[V2G20-3376] Si le CCVE fournit une liste des racines disponibles conformément à la [V2G20-1006], le CCIR public doit suivre l'IETF RFC 5280:2008, 7.1, mise à jour par l'IETF RFC 6818, l'IETF RFC 8398 et l'IETF RFC 8399, pour utiliser les «DistinguishedNames» reçus (voir [V2G20-1006]) afin de choisir une chaîne de certification CCIR provenant de l'un des «DistinguishedNames» reçus et de la fournir au CCVE dans un message «ServerHello» défini dans l'IETF RFC 8446.

Sample Document
get full document from standards.iteh.ai

Remplacer les exigences [V2G20-2383] et [V2G20-2384] par les nouvelles exigences suivantes, respectivement:

[V2G20-3377] Si le CCVE fournit une liste des racines disponibles conformément à la [V2G20-1006], le CCIR privé doit suivre l'IETF RFC 5280:2008, 7.1, mise à jour par l'IETF RFC 6818, l'IETF RFC 8398 et l'IETF RFC 8399, pour utiliser les «DistinguishedNames» reçus (voir [V2G20-1006]) afin de choisir une chaîne de certification EP provenant de l'un des «DistinguishedNames» reçus et de la fournir au CCVE dans un message «ServerHello» défini dans l'IETF RFC 8446.

[V2G20-3378] Si le CCVE n'a fourni aucune indication des racines disponibles conformément à la **[V2G20-3373]**, un CCIR privé qui n'est pas en mode CPM4PE doit envoyer dans le message «ServerHello» sa propre chaîne de certification (chaîne de certification EP) ainsi que tous les éventuels co-certificats nécessaires jusqu'à une racine (à l'exclusion du certificat racine lui-même) de son choix.

Remplacer l'exigence [V2G20-2388] par ce qui suit:

[V2G20-3379] Étant donné que le CCVE a utilisé l'extension «status_request» pour demander une réponse OCSP pour la chaîne de certification transmise par le CCIR public, il doit inclure une réponse OCSP pour chaque certificat de la chaîne de certification envoyée par le CCIR public dans le message «Certificate». Voir IETF RFC 6960 (mise à jour par l'IETF RFC 8954) et IETF RFC 8446 pour plus d'informations.

© ISO 2026 – Tous droits réservés

ISO 15118-20:2022/Amd 1:2026 • https://standards.iteh.ai/catalog/standards/iso/6ad8ce30-396d-4303-a734-c2bccb972d1f/iso-15118-20-2022-amd-1-2026

Remplacer l'exigence [V2G20-2391] par ce qui suit:

[V2G20-3380] Étant donné que le CCVE a utilisé l'extension «status_request» pour demander une réponse OCSP pour la chaîne de certification transmise par le CCIR privé, si le CCIR privé prend en charge PnC, il doit inclure une réponse OCSP pour chaque certificat de la chaîne de certification envoyée par le CCIR privé dans le message «Certificate». Voir IETF RFC 6960 (mise à jour par l'IETF RFC 8954) et IETF RFC 8446 pour plus d'informations.

Remplacer la NOTE 21 sous la [V2G20-1008] par ce qui suit:

NOTE 21 Comme cela est défini dans l'IETF RFC 6960 (mise à jour par l'IETF RFC 8954), un répondeur OCSP peut être soit la sous-AC elle-même, soit une entité directement signée par la sous-AC/l'AC racine correspondante à l'aide d'une paire de clés assorties d'un fanion d'utilisation de clé étendu spécifique dans le certificat.

Remplacer les exigences [V2G20-2404] et [V2G20-2405] par les nouvelles exigences suivantes, respectivement:

[V2G20-3381] Si aucun certificat AC racine V2G ni aucun certificat AC racine du FEO ne sont disponibles dans le CCIR public ou le CCIR privé qui n'est pas en mode CPM4PE, l'extension «certificate_authorities» ne doit pas être présente dans le message «CertificateRequest».

[V2G20-3382] Un CCIR privé en mode CPM4PE ne doit pas inclure l'extension «certificate_authorities» dans le message «CertificateRequest». Voir H.2.2.3 pour plus d'informations sur le CPM4PE.

Sample Document
get full document from standards.iteh.ai

Ajouter la nouvelle NOTE suivante après la NOTE 29 sous la [V2G20-2403]:

NOTE 30 Bien que cette exigence spécifie l'utilisation des RDN du champ Issuer des certificats racine, conformément à l'IETF RFC 5280:2008, 4.1.2.4 (mise à jour par l'IETF RFC 6818, l'IETF RFC 8398 et l'IETF RFC 8399) pour les certificats racine, il convient que ces RDN soient les mêmes pour le champ Issuer et le champ Subject.

Remplacer les exigences [V2G20-2426], [V2G20-2427] et [V2G20-2428] par les nouvelles exigences suivantes, respectivement:

[V2G20-3383] Si le CCIR fournit une liste des racines disponibles conformément à la [V2G20-2401] ou à la [V2G20-2402], le CCVE doit suivre l'IETF RFC 5280:2008, 7.1, mise à jour par l'IETF RFC 6818, l'IETF RFC 8398 et l'IETF RFC 8399, pour utiliser les «DistinguishedNames» reçus (voir [V2G20-2401]) afin de choisir une chaîne de certification du véhicule provenant de l'un des «DistinguishedNames» reçus et de la fournir au CCIR dans un message «Certificate» défini dans l'IETF RFC 8446.

[V2G20-3384] Si le CCIR public n'a fourni aucune indication des racines disponibles conformément à la **[V2G20-3381]**, le CCVE doit envoyer un message «Certificate» contenant sa propre chaîne de certification (chaîne de certification du véhicule) ainsi que tous les éventuels co-certificats nécessaires jusqu'à la racine correspondante (à l'exclusion du certificat racine lui-même) de son choix.

[V2G20-3385] Si le CCIR privé n'a fourni aucune indication des racines disponibles conformément à la **[V2G20-3381]**, un CCVE qui n'est pas en mode CPM4PE doit envoyer un message «Certificate» contenant sa propre chaîne de certification (chaîne de certification du véhicule) ainsi que tous les éventuels co-certificats nécessaires jusqu'à la racine correspondante (à l'exclusion du certificat racine lui-même) de son choix.

© ISO 2026 – Tous droits réservés

ISO 15118-20:2022/Amd 1:2026 • https://standards.iteh.ai/catalog/standards/iso/6ad8ce30-396d-4303-a734-c2bccb972d1f/iso-15118-20-2022-amd-1-2026