NORME INTERNATIONALE

ISO 21177

Première édition
2023-04

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 21177:2023(F)

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 ..... **vi**
Introduction ..... **vii**
1 Domaine d'application **1**
2 Références normatives **1**
3 Termes et définitions **1**
4 Symboles et abréviations **2**
5 Vue d'ensemble **4**
5.1 Description générale, relations avec la sécurité de la couche transport (TLS) et relations avec les spécifications des applications 4
5.2 Objectifs 5
5.3 Architecture et entités fonctionnelles 6
5.4 Pointeurs d'éléments cryptographiques 11
5.5 État et ID de session 11
5.6 Contrôle d'accès et état d'autorisation 12
5.7 Non-répudiation au niveau de l'application 13
5.8 Conventions applicables aux primitives de service 13
6 Flux de processus et diagrammes séquentiels **14**
6.1 Généralités 14
6.2 Vue d'ensemble des flux de processus 14
6.3 Conventions applicables aux diagrammes séquentiels 14
6.4 Configuration 15
6.5 Ouverture de session 17
6.6 Envoi des données 20
6.7 Envoi de la PDU de contrôle d'accès 23
6.8 Réception de la PDU 24
6.9 Extension de session 29
6.9.1 Objectifs 29
6.9.2 Traitement 30
6.10 Courtage de connexions sécurisées 30
6.10.1 Objectifs 30
6.10.2 Prérequis 31
6.10.3 Vue d'ensemble 31
6.10.4 Spécifications détaillées 32
6.11 Fin de session forcée 41
6.12 Clôture de session au niveau de la couche session 43
6.13 Désactivation 44
6.14 Exemple de session sécurisée 45
7 Sous-système de sécurité: interfaces et types de données **46**
7.1 Généralités 46
7.2 État et politique de contrôle d'accès 47
7.3 Authentification renforcée 48
7.3.1 Définition et états possibles 48
7.3.2 États pour l'authentification renforcée du rôle de propriétaire 49
7.3.3 État pour l'authentification renforcée du rôle d'accesseur 50
7.3.4 Utilisation par le contrôle d'accès 50
7.3.5 Méthodes permettant de fournir une authentification renforcée 51
7.3.6 Authentification renforcée avec SPAKE2 51
7.4 Authentification étendue 52
7.5 Requête d'informations sur la gestion de la sécurité 53
7.5.1 Fondement logique 53
7.5.2 Généralités 54
7.6 Types de données 54

7.6.1 Généralités 54
7.6.2 Importations 55
7.6.3 Types de données «facilitateurs » 55
7.6.4 Iso21177AccessControlPdu 55
7.6.5 AccessControlResult 56
7.6.6 ExtendedAuthPdu 56
7.6.7 ExtendedAuthRequest 57
7.6.8 InnerExtendedAuthRequest 57
7.6.9 AtomicExtendedAuthRequest 57
7.6.10 ExtendedAuthResponse 58
7.6.11 ExtendedAuthResponsePayload 58
7.6.12 EnhancedAuthPdu 58
7.6.13 SpakeRequest 59
7.6.14 SpakeResponse 59
7.6.15 SpakeRequesterResponse 59
7.6.16 SecurityMgmtInfoPdu 59
7.6.17 SecurityMgmtInfoRequest 59
7.6.18 EtsiCrlRequest 60
7.6.19 CertChainRequest 60
7.6.20 SecurityMgmtInfoResponse 60
7.6.21 SecurityMgmtInfoErrorResponse 61
7.6.22 EtsiCrlResponse 61
7.6.23 EtsiCtlResponse 61
7.6.24 IeeeCrlResponse 61
7.6.25 CertChainResponse 61
7.6.26 SessionExtensionPdu 62
7.7 Interface App-Sec 63
7.7.1 App-Sec-Configure.request 63
7.7.2 App-Sec-Configure.confirm 65
7.7.3 App-Sec-StartSession.indication 65
7.7.4 App-Sec-Data.request 65
7.7.5 App-Sec-Data.confirm 66
7.7.6 App-Sec-Incoming.request 66
7.7.7 App-Sec-Incoming.confirm 67
7.7.8 App-Sec-EndSession.request 68
7.7.9 App-Sec-EndSession.indication 68
7.7.10 App-Sec-Deactivate.request 69
7.7.11 App-Sec-Deactivate.confirm 69
7.7.12 App-Sec-Deactivate.indication 70
7.8 Interface interne du sous-système de sécurité 70
7.8.1 Généralités 70
7.8.2 Sec-AuthState.request 70
7.8.3 Sec-AuthState.confirm 71

8 Couche d'adaptation: interfaces et types de données 72
8.1 Généralités 72
8.2 Types de données 73
8.2.1 Généralités 73
8.2.2 Iso21177AdaptorLayerPDU 73
8.2.3 Apdu 74
8.2.4 AccessControl 74
8.2.5 TlsClientMsg1 74
8.2.6 TlsServerMsg1 74
8.3 Interface App-AL 74
8.3.1 App-AL-Data.request 74
8.3.2 App-AL-Data.confirm 75
8.3.3 App-AL-Data.indication 75
8.3.4 App-AL-EnableProxy.request 76
8.4 Interface Sec-AL 78

8.4.1 Sec-AL-AccessControl.request 78
8.4.2 Sec-AL-AccessControl.confirm 78
8.4.3 Sec-AL-AccessControl.indication 78
8.4.4 Sec-AL-EndSession.request 79
8.4.5 Sec-AL-EndSession.confirm 79

9 Services de session sécurisée 79
9.1 Généralités 79
9.2 Interfaces App-Sess 80
9.2.1 App-Sess-EnableProxy.request 80
9.3 Interface Sec-Sess 80
9.3.1 Sec-Sess-Configure.request 80
9.3.2 Sec-Sess-Configure.confirm 83
9.3.3 Sec-Sess-Start.indication 83
9.3.4 Sec-Sess-EndSession.indication 83
9.3.5 Sec-Sess-Deactivate.request 84
9.3.6 Sec-Sess-Deactivate.confirm 84
9.4 Interface AL-Sess 84
9.4.1 AL-Sess-Data.request 84
9.4.2 AL-Sess-Data.confirm 85
9.4.3 AL-Sess-Data.indication 85
9.4.4 AL-Sess-EndSession.request 86
9.4.5 AL-Sess-EndSession.confirm 86
9.4.6 AL-Sess-ClientHelloProxy.request 86
9.4.7 AL-Sess-ClientHelloProxy.indication 87
9.4.8 AL-Sess-ServerHelloProxy.request 88
9.4.9 AL-Sess-ServerHelloProxy.indication 88
9.5 Mécanismes autorisés 89
9.5.1 TLS 1.3 89
9.5.2 DTLS 1.3 90

Annexe A (informative) **Scénarios d'utilisation 91**

Annexe B (normative) **Module ASN.1 ..... 99**

Annexe C (normative) **Type fonctionnel de PDU d'extension de session 100**

Annexe D (normative) **Autorisation du propriétaire 101**

Bibliographie 105

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'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. Les détails concernant les références aux droits de propriété intellectuelle ou autres droits analogues identifiés lors de l'élaboration du document sont indiqués dans l'Introduction et/ou dans la liste des déclarations de brevets reçues par l'ISO (voir www.iso.org/brevets).

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 première édition de l'ISO 21177 annule et remplace l'ISO/TS 21177:2019, qui a fait l'objet d'une révision technique.

Les principales modifications sont les suivantes:

— les propositions de modification présentées dans l'ISO/TR 21186-3:2021 ont été incorporées, y compris:

  — ajout de la fonctionnalité de demande de CRL;

  — ajout de la fonctionnalité d'extension de session;

— des améliorations rédactionnelles ont été apportées afin d'améliorer la lisibilité et la clarté, notamment:

  — révision de la Figure 7, renumérotée en Figure 8;

  — insertion d'une nouvelle Figure 7.

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.

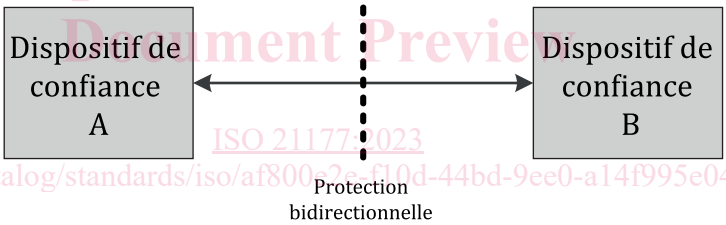

Figure 1 — Interconnexion des dispositifs de confiance

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-SCUs) 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-SUs 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