ETSI TS 103 601 V2.1.1 (2024-03)

TECHNICAL SPECIFICATION

Intelligent Transport Systems (ITS);
Security;
Security management messages communication requirements and distribution protocols;
Release 2

iTeh Standards
(https://standards.iteh.ai)
Document Preview
ETSI TS 103 601 V2.1.1 (2024-03)
https://standards.iteh.ai/catalog/standards/etsi/60cdfe42-56b6-4a9a-8059-fc33b20f9de7/etsi-ts-103-601-v2-1-1-2024-03

Reference

RTS/ITS-005115

Keywords

ITS, protocol, security

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Important notice

The present document can be downloaded from:
https://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

If you find a security vulnerability in the present document, please report it through our Coordinated Vulnerability Disclosure Program:
https://www.etsi.org/standards/coordinated-vulnerability-disclosure

iTeh Standards
(https://standards.iteh.ai)
Document Preview
ETSI TS 103 601 V2.1.1 (2024-03)
https://standards.iteh.ai/catalog/standards/etsi/60cdfe47-56b6-4a9a-8059-fc3ab20f9de7/etsi-ts-103-601-v2-1-1-2024-03

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.
No recommendation as to products and services or vendors is made or should be implied.
No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.
In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

Copyright Notification

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.
The content of the PDF version shall not be modified without the written authorization of ETSI.
The copyright and the foregoing restriction extend to reproduction in all media.

© ETSI 2024.
All rights reserved.

Contents

iTeh Standards (https://standards.iteh.ai) Document Preview ETSI TS 103 601 V2.1.1 (2024-03) https://standards.iteh.ai/catalog/standards/etsi/60edfe42-5070-4d0a-8059-fe33b20f9de7/etsi-ts-103-601-v2-1-1-2024-03

iTeh Standards
(https://standards.iteh.ai)
Document Preview
ETSI TS 103 601 V2.1.1 (2024-03)
https://standards.iteh.ai/catalog/standards/etsi/60cdfe42-56b6-4a9a-8059-fc33b20f9de7/etsi-ts-103-601-v2-1-1-2024-03

iTeh Standards
(https://standards.iteh.ai)
Document Preview

ETSI TS 103 601 V2.1.1 (2024-03)
https://standards.iteh.ai/catalog/standards/etsi/60cdfe42-56b6-4a9a-8059-fc33b20f9de7/etsi-ts-103-601-v2-1-1-2024-03

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

iTeh Standards
(https://standards.iteh.ai)
Document Preview
ETSI TS 103 601 V2.1.1 (2024-03)
https://standards.iteh.ai/catalog/stan

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Intelligent Transport Systems (ITS).

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

1 Scope

The present document defines communication requirements and profiles to support communications from/to ITS-S stations (e.g. fixed road side ITS-S, mobile ITS-S) for the support of security management services specified in ETSI TS 102 941 [2] (i.e. certificate management, trust and revocation lists distribution).

The present document also defines the related protocol handling for the selected messages as well as the requirements for the lower layer protocol stacks and for the Security Management entity in order to support message dissemination and reception.

2 References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at https://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

iTeh Standards (https://standards.iteh.ai) Document Preview

The following referenced documents are necessary for the application of the present document.

[1] ETSI TS 102 940: "Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management; Release 2".

[2] ETSI TS 102 941: "Intelligent Transport Systems (ITS); Security; Trust and Privacy Management; Release 2".

[3] ETSI TS 103 097: "Intelligent Transport Systems (ITS); Security; Security header and certificate formats; Release 2".

[4] ETSI TS 103 248 (V2.3.1): "Intelligent Transport Systems (ITS); GeoNetworking; Port Numbers for the Basic Transport Protocol (BTP); Release 2".

[5] ETSI TS 103 836-4-1: "Intelligent Transport Systems (ITS); Vehicular communications; GeoNetworking; Part 4: Geographical addressing and forwarding for point-to-point and point-to-multipoint communications; Sub-part 1: Media-Independent Functionality; Release 2".

[6] ETSI TS 102 965: "Intelligent Transport Systems (ITS); Application Object Identifier (ITS-AID); Registration; Release 2".

[7] Recommendation ITU-T X.696: "Information technology - ASN.1 encoding rules: Specification of Octet Encoding Rules (OER)".

[8] IEEE Std 1609.2™-2022: "IEEE Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages".

https://standards.iteh.ai/catalog/standards/etsi/60cdfe42-56b6-4a9a-8059-fc33b20f9de7/etsi-ts-103-601-v2-1-1-2024-03

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] IEEE 802.11™: "IEEE Standard for Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks-Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications".

[i.2] ETSI EN 302 890-1: "Intelligent Transport Systems (ITS); Facilities layer function; Part 1: Services Announcement (SA) specification".

[i.3] ISO/IEC 9646-7 (1995): "Information technology - Open Systems Interconnection - Conformance testing methodology and framework - Part 7: Implementation Conformance Statements".

[i.4] ISO/IEC 8824-1:2015: "Information technology -- Abstract Syntax Notation One (ASN.1): Specification of basic notation".

[i.5] ETSI TS 103 836: Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 6: Internet Integration; Sub-part 1: Transmission of IPv6 Packets over GeoNetworking Protocols.

[i.6] C. Fragouli et al: "Network coding: an instant primer", ACM SIGCOMM Computer Communication Review, Vol. 36, No. 1, January 2006, pp 63-68.

[i.7] Pouya Ostovari, Jie Wu, and Abdallah Khreishah: "Network Coding Techniques for Wireless and Sensor Networks", 18 January 2015.

[i.8] Philip A. Chou and Yunnan Wu: "Network Coding for the Internet and Wireless Networks", Microsoft Report MSR-TR-2007-70, June 2007.

[i.9] Farhan Jamil, Anam Javaid, Tariq Umer, Mubashir Husain Rehmani: "A comprehensive survey of network coding in vehicular ad-hoc networks", Wireless Networks, May 2016.

[i.10] Robert H. Morelos-Zaragoza: The Art of Error Correcting Coding, Second Edition, John Wiley & Sons, 2006, ISBN: 0470015586.

[i.11] IETF RFC 6726: "FLUTE - File Delivery over Unidirectional Transport", November 2012.

[i.12] IETF RFC 5651, M. Luby, M. Watson, L. Vicisano: "Layered Coding Transport (LCT) Building Block", October 2009.

[i.13] IETF RFC 5052, M. Watson, M. Luby, and L. Vicisano: "Forward Error Correction (FEC) Building Block", August 2007.

iTeh Standards
(https://standards.iteh.ai)
Document Preview
ETSI TS 103 601 V2.1.1 (2024-03)
https://standards.iteh.ai/catalog/standards/etsi/60edfe42-5b6b-4a9a-8059-fc33b20f9de7/etsi-ts-103-601-v2-1-1-2024-03

3 Definition of terms, symbols, abbreviations and notations

3.1 Terms

For the purposes of the present document, the terms given in ETSI TS 102 940 [1], ETSI TS 102 941 [2] and the following apply:

CTL/CRL Distribution Application: software application supported by an ITS-S that enables a relay service for storing and distribution of CTL/CRL to other ITS-S

Maximum Transmission Unit (MTU): maximum packet size in octets that can be conveyed in one piece over a data link

3.2 Symbols

For the purposes of the present document, the following symbols apply:

N1 number of attempts that an ITS-S is authorized to do after the sending of the EC request. Note that N1 is a non-negative integer ($N1 \geq 0$)

N1 = 0 means that no EC retry is possible

N1 = 1 means that after sending the EC request and not having received the response (because of EC request loss or EC response loss), the ITS-S can use the EC retry service only one time

N2 it is the number of attempts that an ITS-S is authorized to do after the sending of the AT request. Note that N2 is a non-negative integer ($N1 \geq 0$).

N2 = 0 means that no AT retry is possible

N2 = 1 means that after sending the AT request and not having received the response (because of AT request loss or AT response loss), the ITS-S can use the AT retry service only one time

T1 time interval between two successive repeated EC requests that are performed by an ITS-S

T2 life-time duration of the created EC request by the requesting ITS-S

T3 time interval between the reception/storage of the context information of the initial EC Request and the last incoming/repeated EC request received by an EA

T4 time interval between two successive repetitions of the same AT request that are performed by an ITS-S

T5 life-time duration of the created AT by the requesting ITS-S

T6 time interval between the reception/storage of the context information of the initial AT Request and the last incoming/repeated AT request received by an AA

$T_{\mathrm{P2pctldMax}}$ maximum waiting time before a responder ITS-S which has received a request for a specific CTL or a broadcasting ITS-S starts transmitting the successive segments containing the full CTL, after listening to detect if another ITS-S has not already started to send the same CTL

d repetition duration of the CTL or CRL broadcast transmission in days or in seconds. If d=0 then the list is transmitted only once

f repetition frequency of the CTL or CRL broadcast transmission in millihertz

N_{total} total number of consecutive segments transmitted by the Sender which applies segmentation of the original message, e.g. a FullCtl

iTeh Standards
(https://standards.iteh.ai)
Document Preview
ETSI TS 103 601 V2.1.1 (2024-03)
https://standards.iteh.ai/catalog/standards/etsi/06cdfe42-56b0-4a9a-8059-fe55b20f9de7/etsi-ts-103-601-v2-1-1-2024-03

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

5G-NR	5G New Radio
AA	Authorization Authority
AES	Advanced Encryption Standard
AID	Application Identifier
ALC	Asynchronous layered coding
ASN	Abstract Syntax Notation
AT	Authorization Ticket
B2B	Business to Business

BTP	Basic Transport Protocol
CA	Certification Authority
CAM	Cooperative Awareness Message
CCMS	Cooperative-ITS Certificate Management System
CP	Certificate Policy
CPOC	C-ITS Point Of Contact
CRL	Certificate Revocation List
CTL	Certificate Trust List
CXLDA	CRL/CTL Distribution Application
DC	Distribution Centre
EA	Enrollment Authority
EC	Enrollment Credential
ECTL	European Certificate Trust List
EN	European Norm
FDT	File Delivery Table
FEC	Forward Error Correction
F-PDU	Facilities Layer Protocol Data Unit
GBC	GeoBroadCast
GN	GeoNetworking
GN_SAP	GeoNetworking_Service Access Point
GN6	GeoNetworking over IPv6
GUC	GeoUniCast
HTTP	Hyper Text Transfer Protocol
IP	Internet Protocol
ITS	Intelligent Transport System
ITS-G5	5 GHz wireless communication
ITS-S	Intelligent Transport System - Station
LCT	Layer Coding Transport
MTU	Maximum Transmission Unit
NR	New Radio
OER	Octet Encoding Rules
OID	Object Identification number
P2P	Peer-to-Peer
P2PCXLD	Peer-to-peer CRL/CTL Distribution service
PDU	Protocol Data Unit
PICS	Protocol Implementation Conformance Statement
PKI	Public Key Infrastructure
PSID	Provider Service Identifier
RA	Router Advertisement
RAN	Radio Access Network
RCA	Root Certification Authority
R-ITS-S	Roadside ITS-S
RMT	Reliable Multicast Transport
RSU	Road Side Unit
SAM	Service Advertisement Message
SCH	Service CHannel
SCRM	Segmented CTL Response Message
SHA	Secure Hash Algorithm
SHB	Single Hop Broadcast
SLAAC	StateLess Address Auto-Configuration
SM-PDU	Security Management PDU
TA	Trust Anchor
TCP	Transmission Control Protocol
TLM	Trust List Manager
TS	Technical Specification
UC	Use Case
UPER	Unaligned Packed Encoding Rule
URL	Uniform Resource Locator
V2X	Vehicle to Everything
V-ITS-S	Vehicle ITS-S
WLAN	Wireless Local Area Network

iTeh Standards
(https://standards.iteh.ai)
Document Preview
ETSI TS 103 601 V2.1.1 (2024-03)
https://standards.iteh.ai/catalog/standards/etsi/60cdfe42-56b6-4a9a-8059-fc33b20f9de7/etsi-ts-103-601-v2-1-1-2024-03

3.4 Notations

For the purposes of the present document, the notations given in ETSI TS 102 940 [1] apply.

4 Services description: use cases and requirements

4.1 Certificate provisioning service

4.1.1 Service description

4.1.1.1 Overview

The certificates reloading service consists for an ITS-S to request EC/AT to the PKI in an online and automatic manner. EC requests are not frequent as an ITS-S usually requests one EC at the beginning of its lifecycle and then renews its EC in advance before the end of its key validity period [2]. However, AT are requested much more often. Indeed when an ITS-S has only a few remaining Ats it requests new ones to the PKI.

Figure 1 depicts the service from a V-ITS-S and a R-ITS-S point of view:

1) (Green arrow) - A V-ITS-S is within the radio coverage of a RAN access point that provides Internet connectivity (e.g. cellular base station, Wi-Fi hotspot, R-ITS-S, etc.). The V-ITS-S thus sends its EC/AT request to the PKI via the RAN access point and the Gateway. The PKI processes the request and sends back immediately its response to the V-ITS-S.

2) (Orange arrows) - A R-ITS-S is connected to the Internet either wired (e.g. optical fibre, Ethernet, etc.) or wirelessly via a RAN access point (e.g. cellular base station, Wi-Fi® hotspot, etc.). The R-ITS-S thus sends its EC/AT request to the PKI directly (wire) or via the RAN access point and the Gateway. The PKI processes the request and sends back immediately its response to the R-ITS-S.

NOTE: In the present document, the RAN Access Point and the Gateway are differentiated. The RAN Access Point is hardware that provides radio access and the Gateway is the relaying software that links the local network with the Internet. However the Gateway may be integrated in the RAN Access Point.

iTeh Standards
(https://standards.iteh.ai)
Document Preview
ETSI TS 103 601 V2.1.1 (2024-03)
https://standards.iteh.ai/catalog/standards/etsi/60cdfe42-56b6-4a9a-8059-fc33b20f9de7/etsi-ts-103-601-v2-1-1-2024-03

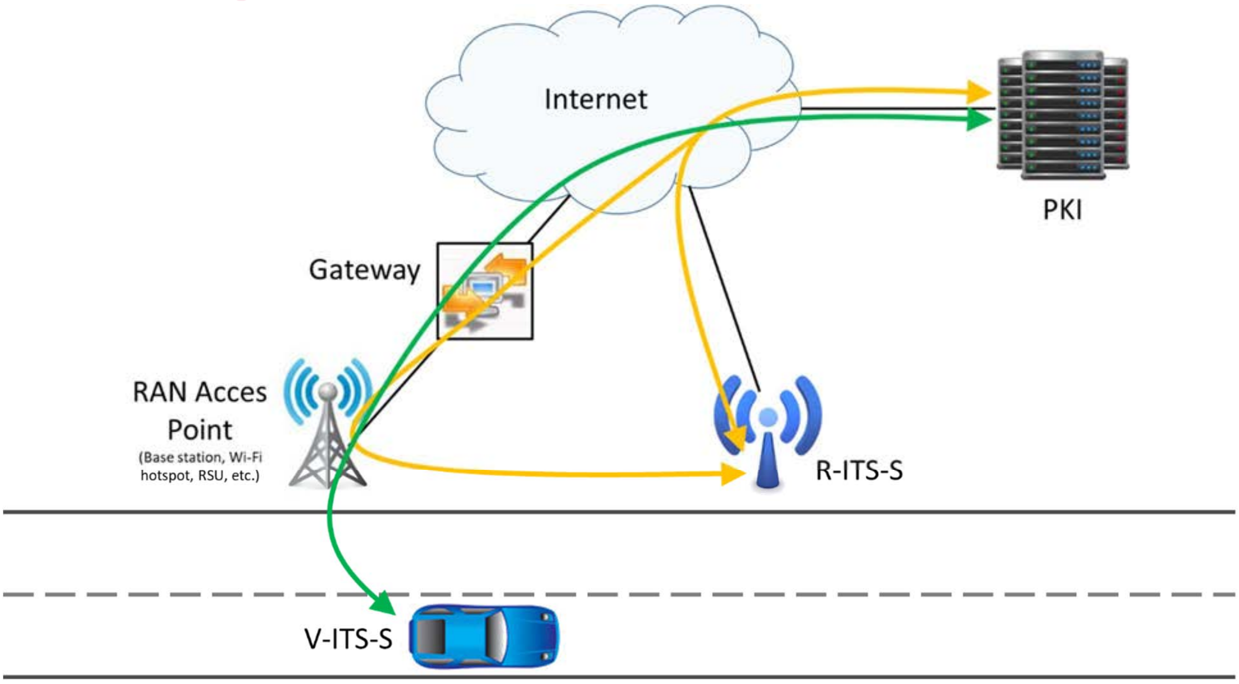

Figure 1: Example of certificates reloading service for a V-ITS-S (green) and a R-ITS-S (orange)

4.1.1.2 UC-SEC-01: EC initial request or re-keying

Use Case ID:	***UC-SEC-01***
Use Case Name:	Enrolment credential initial request or re-keying.
Priority:	Mandatory.
Related Requirement:	ITS-S is registered in the PKI. ITS-S has Ipv6 connectivity.

Primary Actor	ITS-S.
Description	ITS-S requests an EC to the EA. After verification, the EA replies positively by sending back the requested EC to the ITS-S.
Preconditions	ITS-S has its canonical key pair, a canonical identifier, the URL of the EA and the EA certificate. ITS-S is already registered in EA database. ITS-S has Ipv6 connectivity. If a wireless connectivity is used, the ITS-S shall be under the radio coverage of an access point that provides Ipv6 connectivity.
Success End Condition	ITS-S receives its EC from the EA.
Failed End Condition	ITS-S does not receive its EC.
Involved components	Security layer.
Main Success Scenario	1) ITS-S creates the EC request and sends it to the EA. 2) The EA verifies the EC request (as specified in ETSI TS 102 941 [2]) and sends the EC response to the ITS-S. 3) ITS-S receives its EC delivered by the EA.
Extensions	None.
Variations (Alternatives)	If the ITS-S does not receive a response from the EA, it may resume the same EC request to the EA until a maximum retry threshold or maximum delay is reached. Notice that the ITS-S may select another communication profile to resend its request. If the above procedure failed and the ITS-S has still not received its EC and its current EC has expired, the ITS-S notifies the user or the manufacturer/device operator about the situation.
Includes	

Security Characteristics			
Authentication	Yes	Integrity	Yes
Confidentiality	Yes	Authorization	Yes
Anonymity privacy	No	Pseudonymity privacy	No
Availability	Yes	Plausibility	No
Auditability (Accountability)	Yes	Jurisdictional Access	-

4.1.1.3 UC-SEC-02: AT reloading

Use Case ID:	***UC-SEC-02***
Use Case Name:	Authorization ticket reloading.
Priority:	Mandatory.
Related Requirement:	ITS-S is registered in the PKI. ITS-S has a valid EC. ITS-S has Ipv6 connectivity.

Primary Actor	ITS-S.
Description	ITS-S requests an AT to the AA. After verifications, the AA replies positively by sending back the requested AT to the ITS-S.
Preconditions	ITS-S has its canonical key pair, a canonical identifier, its EC certificate and associated private key, the URL of the AA and the AA certificate. ITS-S is already registered in EA database. ITS-S has Ipv6 connectivity. If wireless connectivity is used, the ITS-S shall be under the radio coverage of an access point that provides Ipv6 connectivity.
Success End Condition	ITS-S receives its AT from the AA.
Failed End Condition	ITS-S does not receive its AT.
Involved components	Security layer.

iTeh Standards
(https://standards.iteh.ai)
Document Preview
ETSI TS 103 601 V2.1.1 (2024-03)
https://standards.iteh.ai/catalog/standards/etsi/60c6fe42-56b6-4a9a-8059-[illegible]20f9de7/etsi-ts-103-601-v2-1-1-2024-03

Main Success Scenario	1) ITS-S creates the AT request and sends it to the AA. 2) The AA verifies the AT request (as specified in ETSI TS 102 941 [2]) and sends the AT reply to the ITS-S. 3) ITS-S receives its AT delivered by the AA.
Extensions	None.
Variations (Alternatives)	If the ITS-S does not receive a response from the AA, it may resume the same AT request to the AA until a maximum retry threshold or maximum delay is reached. Notice that the ITS-S may select another communication profile to resend its request. If the above procedure failed and the ITS-S has still not received its AT, the ITS-S may create a new AT request and sends it to another AA.
Includes	

Security Characteristics			
Authentication	Yes	Integrity	Yes
Confidentiality	Yes	Authorization	Yes
Anonymity privacy	No	Pseudonymity privacy	Yes
Availability	Yes	Plausibility	No
Auditability (Accountability)	Yes	Jurisdictional Access	-

4.1.1.4 Use cases and communication profiles mapping

Table 1 summarizes the communication profiles that can be used for each use case. Details of the communication profiles are provided in clause 6 of the present document.

Table 1: Mapping between use cases and communication profiles

		CPS_001	**CPS_002**	**CPS_003**	**CPS_004**
UC-SEC-01	**R-ITS-S**		X		
	V-ITS-S	X (see note)	X		
UC-SEC-02	**R-ITS-S**		X		
	V-ITS-S	X	X		
NOTE: CPS_001 cannot be used to request the first EC as the ITS-S has no AT yet to sign the GN packet.					

iTeh Standards (https://standards.iteh.ai) Document Preview ETSI TS 103 601 V2.1.1 (2024-03) https://standards.iteh.ai/catalog/standards/etsi/60cdfe42-56b6-4a9a-8059-fc33b20f9de7/etsi-ts-103-601-v2-1-1-2024-03

4.1.2 Requirements

4.1.2.1 Security requirements

The PKI management protocols shall satisfy the following basic set of security objectives:

- **Authentication/authorization control:** authentication consists to be sure of the identity which sends data. Authorization control is the verification of an access policy, based on a trusted authentication. Authenticate all entities participating in the protocol is required to prevent illegitimate persons to enter in the system, or to access some unauthorized resources or services.

- **Integrity:** the integrity of all transmitted data is important to ensure that the contents of the received data are not altered.

- **Confidentiality/Privacy:** the enrolment/authorization request data and the delivered certificates in responses shall only be accessed by authorized entities. The real identity of ITS Station has to be protected, by cryptographic mechanisms and depending on the type of data sent.

- **Non-repudiation/Traceability:** non-repudiation is necessary to prevent ITS Station or others entities from denying the transmission or the content of their messages. Traceability, which is the warranty that an entity cannot refute the emission or reception of information, is also extremely important.

- **Unlinkability:** ability of a user to make multiple uses of resources or services without others being able to link these uses together.

- **Anonymity:** ability of a user to use a resource or service without disclosing the user's identity.

4.2 CTL distribution service

4.2.1 Service description

4.2.1.1 Overview

Within the CCMS framework, the CTL or ECTL is generated and issued by the Root CA or the TLM and published by a DC or CPOC to be made available to all the participants of the trusted C-ITS system, as specified in ETSI TS 102 940 [1]. The issuance of a new CTL (or ECTL) should be done periodically as well as on specific conditions triggered by a security management event or a security incident such as the revocation of an entity of the CCMS.

For each new update of the CTL issued by a Root CA, the Root CA shall provide the base CTL information (fullCTL) and the corresponding Delta CTL (deltaCTL) following the data structures' format specified in ETSI TS 102 941 [2].

For each new update of the ECTL issued by the TLM, the TLM shall provide the base CTL information (fullCTL) and the corresponding Delta CTL (deltaCTL) following the data structures' format specified in ETSI TS 102 941 [2].

The receiving C-ITS stations shall maintain and store the latest certificate trust lists to apply signature and certificate chain validation on received messages (as specified in ETSI TS 103 097 [3]). The transmission and distribution process of certificate trust lists to all the C-ITS stations and to the CCMS entities should be provided efficiently and in a timely manner.

For interoperability purpose, ETSI TS 102 941 [2] specifies the interface with the DC to distribute the base CTL and corresponding delta CTL information and the interface with the CPOC to distribute the base ECTL and corresponding delta ECTL information. In ETSI TS 102 941 [2], clause D.1, a basic mandatory protocol is specified using HTTP v1.1 GET. Other optional protocols may be proposed e.g. for broadcasting over a short-range wireless communication or other radio broadcasting technologies (e.g. LTE, 5G, satellite or terrestrial broadcast system).

4.2.1.2 UC-SEC-03: On demand request of a FullCTL

This use case allows an ITS-S to update its certificate trust list information by requesting the Full CTL to the corresponding CPOC (which distributes the ECTL published by a TLM) or DC (which distributes the CTL published by a RCA).

In this use case, the ITS-S shall use the communication profile as specified in ETSI TS 102 941 [2], clause D.1. It is agnostic from the underlying communication medium.

iTeh Standards (https://standards.iteh.ai) Document Preview ETSI TS 103 601 V2.1.1 (2024-03) https://standards.iteh.ai/catalog/standards/etsi/60edfe42-56b6-4a9a-8059-fc33b20f9de7/etsi-ts-103-601-v2-1-1-2024-03

Use Case ID:	***UC-SEC-03***
Use Case Name:	Get Certificate Trust List.
Priority:	Mandatory.
Related Requirement:	V-ITS-S or R-ITS-S stores CPOC or DC access point received at initialization or via the prior base ECTL or CTL. V-ITS-S or R-ITS-S has an available cellular network connection (3G/4G, LTE or 5G NR) or a short-range wireless interface to a RSU providing internet communication.

Primary Actor	ITS station.
Description	ITS Station wants to update the signed list of trusted PKI authorities published by the TLM (ECTL) or the CTL published by its own Root CA or by other Root CAs (CTL distributed by a Distribution Centre).
Preconditions	-
Success End Condition	ITS station received the latest (base) CTL or ECTL and was able to check its validity and store it in its local secure memory storage.
Failed End Condition	-
Involved components	CPOC or DC, Security layer of the ITS-S, HTTP over TCP-IP, cellular or ITS-G5 communication via a R-ITS-S connected to Internet.
Main Success Scenario	1) ITS Station sends request to CPOC or DC. The communication profile is specified in ETSI TS 102 941 [2], clause D.1 and figure C.1 for cellular communication stack. 2) CPOC or DC returns CTL.