ETSI TS 1DD DDD V0.0.3 (2020-08)

Errata Document for C-ITS Release 1

Release 1

<

**TECHNICAL SPECIFICATION**

Reference

DMI/ITS-205

Keywords

ITS, Release 1

***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 - NAF 742 C

Association à but non lucratif enregistrée à la

Sous-préfecture de Grasse (06) N° 7803/88

***Important notice***

The present document can be downloaded from:
<http://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](http://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>

***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 2020.

All rights reserved.

**DECT**TM, **PLUGTESTS**TM, **UMTS**TM and the ETSI logo are trademarks of ETSI registered for the benefit of its Members.
**3GPP**TM and **LTE**TM 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.

Contents

Intellectual Property Rights 4

Foreword 4

Modal verbs terminology 4

1 Scope 5

2 Impacted Deliverables 5

Corrections for ETSI TS 102 894-2 (V1.3.1): 6

Corrections for ETSI TS 102 941 (V1.3.1): 10

Corrections for ETSI EN 302 637-2 (V1.4.1) 37

Corrections for ETSI EN 302 637-3 (V1.3.1) 43

Corrections for ETSI TS 103 301 (V1.3.1) 51

# Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is 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](https://ipr.etsi.org/)).

Pursuant to the ETSI IPR Policy, no investigation, 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.

# Foreword

This ETSI Errata Document reflects the decisions of the ETSI Technical Body responsible for the referenced ETSI Deliverables, that are not yet published. It has therefore to be noted that for ENs the agreed corrections have not been through the ENAP procedure yet. The Errata Document has been produced by ETSI Technical Committee Intelligent Transport Systems – ETSI TC 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](https://portal.etsi.org/Services/editHelp%21/Howtostart/ETSIDraftingRules.aspx) (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 ETSI Errata Document reflects not yet published decisions of the ETSI Technical Committee Intelligent Transport Systems who are responsible for the referenced ETSI deliverable.

This Errata Document covers C-ITS Release 1

It has to be noted that for deliverables of the type ENs he agreed corrections have not been through the ENAP procedure yet and thus could be subject to changes as part of the ENAP procedure.

Section 2 of this document list the ETSI deliverables and their version number to which corrections are contained in this document

# 2 Impacted Deliverables

Corrections to the following ETSI deliverables are contained in this Errata Document

[1] ETSI TS 102 894-2 (V1.3.1): "Intelligent Transport Systems (ITS); Users and applications requirements; Part 2: Applications and facilities layer common data dictionary".

[2] ETSI TS 102 941 (V1.3.1): "Intelligent Transport Systems (ITS); Security; Trust and Privacy Management".

[3] ETSI EN 302 637-2 (V1.4.1): "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service ".

[4] ETSI EN 302 637-3 (V1.3.1): "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service".

[5] ETSI TS 103 301 (V1.3.1): “Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Facilities layer protocols and communication requirements for infrastructure services; Release 2”

# Corrections for ETSI TS 102 894-2 (V1.3.1):

|  |
| --- |
| **Overview of Change Requests** |
| <Change Requesrt> | <Date> | <Title> |
| CR 102 894-2#001 | 12-07-19 | Correction of ASN.1 definition for Data Element [LanePosition ] |
| CR 102 894-2#002 | 05-08-20 | Harmonize the use of vehicle dimensions between ETSI Documents |
|  |  |  |
|  |  |  |

|  |
| --- |
| **CHANGE REQUEST** |
|  | TS 102 894-2 | **Version** | 1.3.1 | **CR** | 1 | **rev** | - |  |
|  |
| **CR Title** | Correction of ASN.1 definition for Data Element [LanePosition ]  |
|  |  |
| **Original Source** | ITS WG1 |
|  |  |
| **Work Item Ref** | RTS/ITS-00168 | **Submission date** | 21/03/2019 |
| **Approving TB**  | TC ITS | **Approval date** | 08/04/2019 |
| **Category:** | F | **Release** | 1 |  |
|  | Use **one** of the following categories:**F** (correction)**A** (correction in an earlier release)**B** (addition of feature) **C** (functional modification of feature)**D** (editorial modification) |  |
|  |  |
| **Reason for change** | In Annex B, ASN.1 definition of LanePosition is not in line with DE definition in Annex A.40 |
|  |  |
| **Consequence if not approved** | Wrong implementation of the base specification for the data element.  |
|  |  |
| **Summary of change** | In Annex A.40, outterHardShoulder should be outerHardShoulderChange LanePosition in Annex B to:LanePosition ::= INTEGER {offTheRoad(-1), innerHardShoulder(0),innermostDrivingLane(1), secondLaneFromInside(2), outerHardShoulder(14) } (-1..14) |
|  |  |
| **Clauses affected** | Annex B, Annex A.40 |
|  |  |
| **Linked Change Requests** |  |  |
|  |  |  |
|  |  |
| **Other comments** | Mantis issue 7789 and decision made in ITSWG1#47 meeting. <http://oldforge.etsi.org/mantis/view.php?id=7789>  |
|  |  |

### A.40 DE\_LanePosition

|  |  |
| --- | --- |
| **Descriptive Name** | LanePosition |
| **Identifier** | DataType\_ 40 |
| **ASN.1 representation** | LanePosition ::= INTEGER {offTheRoad(-1), innerHardShoulder(0),innermostDrivingLane(1), secondLaneFromInside(2), outerHardShoulder(14) } (-1..14) |
| **Definition** | This DE indicates the transversal position information on the road in resolution of lanes, counted from the inside border of the road for a given traffic direction. For example, the innermostDrivingLane corresponds to the left most lane of the carriageway in a country with right-land traffic, and to the right most lane of the carriageway in a left-land traffic (e.g. in UK). The value -1 denotes that the referenced position is outside the road. |
| **Unit** | N/A |
| **Category** | GeoReference information, road topology information |

### Annex B (normative):

### ASN.1 module of the common data dictionary

The ASN.1 module of the common data dictionary shall be as specified as below.

|  |
| --- |
|  |
|  |
|  |
| LanePosition ::= INTEGER {offTheRoad(-1), innerHardShoulder(0),innermostDrivingLane(1), secondLaneFromInside(2), outerHardShoulder(14) } (-1..14) |

|  |
| --- |
| **CHANGE REQUEST** |
|  | ETSI TS 102 894-2 | **Version** | 1.3.1 | **CR** | *2* | **rev** | - |  |
|  |
| **CR Title** | Harmonize the use of vehicle dimensions between ETSI Documents |
|  |  |
| **Original Source** | ITS WG1 |
|  |  |
| **Work Item Ref** | RTS/ITS-00148 | **Submission date** | 02.06.2020 |
| **Approving TB**  | ITS | **Approval date** | 05.08.2020 |
| **Category:** | **F** | **Release** | 1 |  |
|  | Use **one** of the following categories:**F** (correction)**A** (correction in an earlier release)**B** (addition of feature) **C** (functional modification of feature)**D** (editorial modification) |  |
|  |  |
| **Reason for change** | There is an inconsistency between the EN 302 637-2 (CA Service), the TS 102 894-2 (CDD) and the EN 302 890-2 (PoTi). Whereas the CA-Service and the CDD state that the vehicle width DF (Clause B.36 in CA-Service; Clause A.95 in CDD) shall include the width of the vehicle ITS-S with side mirrors included, the PoTi EN (Clause 6.2.2) states that side mirrors are excluded. It is proposed to follow the interpretation of the PoTi EN as the detection of side mirrors is difficult for perception sensors from other vehicles. However, the vehicle width information could be used in data association algorithms. A vehicle following the vehicle ITS-S disseminating the e.g., CAM with this information is likely not to perceive the width including the side mirrors. |
|  |  |
| **Consequence if not approved** | Non-hamonized use of the vehicleWidth DE between different ITS-S due to contradicting specifications |
|  |  |
| **Summary of change** | Change wording in Clause A.95 of TS 102 894-2 to “Width of a vehicle, excluding side mirrors and possible similar extensions. For a vehicle width equal to or greater than6,1 metres, the value shall be set to 61. The value shall be set to 62 if the information is unavailable.” |
|  |  |
| **Clauses affected** | A.95 of TS 102 894-2 |
|  |  |
| **Linked Change Requests** | See above |  |
|  |  |  |
|  |  |
| **Other comments** |  |
|  |  |

1. 95 DE\_VehicleWidth

|  |  |
| --- | --- |
| **Descriptive Name** | VehicleWidth |
| **Identifier** | DataType\_ 95 |
| **ASN.1 representation** | VehicleWidth ::= INTEGER {tenCentimeters(1), outOfRange(61), unavailable(62)} (1..62) |
| **Definition** | ~~Width of a vehicle, including side mirrors. For a vehicle width equal to or greater than 6,1 metres, the value shall be set to 61. The value shall be set to 62 if the information is unavailable.~~Width of a vehicle, excluding side mirrors and possible similar extensions. For a vehicle width equal to or greater than 6,1 metres, the value shall be set to 61. The value shall be set to 62 if the information is unavailable. |
| **Unit**  | 0,1 metre |
| **Category** | Vehicle information |

# Corrections for ETSI TS 102 941 (V1.3.1):

|  |
| --- |
| **Overview of Change Requests** |
| <Change Requesrt> | <Date> | <Title> |
| CR 102 941#001 | 12-07-19 | Allowing of DC entries in the ECTL |
| CR 102 941#002 | 17-01-20 | Add definitions of CTL and CRL update fields |
| CR 102 941#003 | 3-07-20 | Add a specification of Link Certificates as TS 102 941 messages for RCAs and TLM, to support the re-keying process of the TLM/ RCA certificates and secure change of trust anchors certificates in corresponding receiving C-ITS trust domain entities |
| CR 102 941#004 | 3-07-20 | The AuthorizationValidationResponse message is encrypted by EA using the symmetric key provided by AA in the AuthorizationValidationRequest message. |
| CR 102 941#005 | 3-07-20 | Move newly defined TS103097 data types from TS 102 941 to TS 103 097 |

|  |
| --- |
| **CHANGE REQUEST** |
|  | ETSI TS 102 941 | **Version** | 1.3.1 | **CR** | 1 | **rev** | - |  |
|  |
| **CR Title** | Allowing of DC entries in the ECTL |
|  |  |
| **Original Source** | ITS WG5 |
|  |  |
| **Work Item Ref** | RTS/ITS-00552 | **Submission date** | 22/03/2019 |
| **Approving TB**  | TC ITS | **Approval date** | 08/04/2019 |
| **Category:** | **F** | **Release** | 1 |  |
|  | Use **one** of the following categories:**F** (correction)**A** (correction in an earlier release)**B** (addition of feature) **C** (functional modification of feature)**D** (editorial modification) |  |
|  |  |
| **Reason for change** | ECTL contains the list of trusted Root certificates but there is no way to download CRLs issued by these Root CAs.Putting DC entries in the ECTL allows distributing the Root CA DC access point URLs. |
|  |  |
| **Consequence if not approved** | The CRL from some PKIs can be not available for all ITS-Ss. Messages from stations, enrolled in these PKIs, shall be considered as untrusted even if these devices are successfully enrolled and authorized by its PKIs. |
|  |  |
| **Summary of change** | 1. Allowing DC entry in ECTL
 |
|  |  |
| **Clauses affected** | **6.3.1 and Annex B.2** |
|  |  |
| **Linked Change Requests** | None |  |
|  |  |  |
|  |  |
| **Other comments** | None |
|  |  |

**6.3.1 Generation and distribution of CTL by TLM**

* delete a Root CA certificate (revoked);
* add, remove or modify DC access points of Root CAs;
* update the TLM certificate after a renewal process (creation of new key and generation of TLM certificates);

…

The CTL issued by the TLM shall contain the following information:

* TLM certificate and optionally link certificate ~~(optional)~~;
* Root CA certificates and optionally link certificates ~~(optional~~);
* CPOC access point.

The CTL issued by the TLM may contain the following information:

* Root CA DC access points.

The CTL issued by the TLM shall not contain any other information.

´

---- Next change --

**Annex B.2**

Table B.3: Allowed combinations of CTL SSPs

| CTL type | Allowed CTL entries | Value |
| --- | --- | --- |
| TLM CTL (ECTL) | * TLM certificate entries;
* Root CA entries;
* DC entry (for CPOC and Root CA DC access points).
 | C8h |
| RootCA CTL | * EA entries;
* AA entries;
* Root CA DC access point entries.
 | 38h |

|  |
| --- |
| **CHANGE REQUEST** |
|  | ETSI TS 102 941 | **Version** | 1.3.1 | **CR** | 2 | **rev** | - |  |
|  |
| **CR Title** | Add definitions of CTL and CRL update fields |
|  |  |
| **Original Source** | ITS WG5 |
|  |  |
| **Work Item Ref** | RTS/ITS-00552 | **Submission date** | 17/12/2019 |
| **Approving TB**  | ITS | **Approval date** | 17/01/2019 |
| **Category:** | **D** | **Release** | 1 |  |
|  | Use **one** of the following categories:**F** (correction)**A** (correction in an earlier release)**B** (addition of feature) **C** (functional modification of feature)**D** (editorial modification) |  |
|  |  |
| **Reason for change** | Clarification of definitions for some fields used in the CTL and CRL data structures is proposed: the definition of thisUpdate and nextUpdate as specified in RFC 5280 is added. |
|  |  |
| **Consequence if not approved** | The issuer of CTL or CRL may not provide values for these dates which are conformant to these definitions and therefore the transmitted information may not be correct and would open attack surfaces on the receiver side. |
|  |  |
| **Summary of change** | Adding definitions of thisUpdate and nextUpdate fields used in CRL/CTL data structures |
|  |  |
| **Clauses affected** | Clause 2.2, clause 3.1 |
|  |  |
| **Linked Change Requests** | None |  |
|  |  |  |
|  |  |
| **Other comments** | None |
|  |  |

### 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.16] IETF RFC 5280 : « Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile »

### 3.1 Terms

For the purposes of the present document, the terms given in ETSI TS 102 731 [1], ETSI TS 102 940 [5], ISO/IEC 15408-2 [i.1] and the following apply:

…………….

**thisUpdate:** this field indicates the issue date of this CRL (as specified in RFC 5280 [i.10])

**nextUpdate**: this field indicates the date by which the next CRL (respectively the next CTL) will be issued. The next CRL (respectively the next CTL) could be issued before the indicated date, but it will not be issued any later than the indicated date (as specified in RFC 5280 [i.16])

|  |
| --- |
| **CHANGE REQUEST** |
|  | ETSI TS 102 941 | **Version** | 1.3.1 | **CR** | 3 | **rev** | - |  |
|  |
| **CR Title** | Add a specification of Link Certificates as TS 102 941 messages for RCAs and TLM, to support the re-keying process of the TLM/ RCA certificates and secure change of trust anchors certificates in corresponding receiving C-ITS trust domain entities |
|  |  |
| **Original Source** | ITS WG5 |
|  |  |
| **Work Item Ref** | RTS/ITS-00552 | **Submission date** | 01/07/2020 |
| **Approving TB**  | ITS | **Approval date** | 03.07.2020 |
| **Category:** | **B** | **Release** | 1 |  |
|  | Use **one** of the following categories:**F** (correction)**A** (correction in an earlier release)**B** (addition of feature) **C** (functional modification of feature)**D** (editorial modification) |  |
|  |  |
| **Reason for change** | TS 103 097 link certificates format is deleted and must be replaced by TS 102 941 Link Certificate Messages as required by the EU CCMS CPOC protocol specification  |
|  |  |
| **Consequence if not approved** | Issuing of the link certificate associated to the re-keyed certificate is not possible for the TLM and for the RCAs |
|  |  |
| **Summary of change** | Specification of interfaces for the transmission of Link Certificates, i.e. via the CPOC-RCA and CPOC distribution centre, requirements for the generation of the TLM Link Certificate/ RCA Link Certificate messages and specification of the corresponding ASN.1 modules extension for the new Ts102941 messages. |
|  |  |
| **Clauses affected** | 2.2, 6.4, A.2.1, A.2.2, A.2.3, A.2.4, A.2.8, B.2 |
|  |  |
| **Linked Change Requests** | CR TS 103 097 #0003 CR TS 103 097 #0004 |  |
|  |  |  |
|  |  |
| **Other comments** |  |
|  |  |

## 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.16] Certificate Policy for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS), Release from preparatory phase of C-ITS Delegated Regulation, 13rd March 2019.

NOTE: Available at <https://cpoc.jrc.ec.europa.eu/>

[i.17]  Annex I of CPOC Protocol: Requirements & best practices of TLM certificates, RCA certificates and the ECTL

NOTE: Available at <https://cpoc.jrc.ec.europa.eu/>

#### **Editor Note: To be added after end of clause 6.3**

## 6.4 Generation and distribution of TLM / RCA Link Certificates

### 6.4.1 General

The main objective of link certificates is the update of trust anchors (RCA, TLM) in all C-ITS entities: Link certificates are used to change trust anchors certificates in an integrity/authenticated protected way.

According to the Certificate Policy document ([i.16]), the TLM shall regularly re-keys its TLM Certificate. Each time the TLM is re-keying its certificate, it shall generate the TLM Link Certificate message as specified in clause 6.4.2.1. The TLM shall provide the pair of new re-keyed TLM Certificate and corresponding TLM Link Certificate to all participants of the C-ITS Trust Domain via the CPOC distribution centre (CPOC-WEB).

NOTE 1: The TLM is publishing the pair of new re-keyed TLM certificate and corresponding TLM Link Certificate across the interface at reference point S12 as specified in ETSI TS 102 940 clause 7.1 [5]). This information is made available in read access to all participants of the C-ITS Trust Domain, including PKI authorities, ITS-Stations, Manufacturers / Operators.

For the creation of a new Root CA, after issuing its Root CA certificate it shall follow the initial enrolment of a new RCA to the CPOC to get the approval of the CPA (via the initial application form process).

According to the Certificate Policy [i.16], the Root CA shall change its RCA certificate regularly via a re-keying process. When re-keying its certificate, the RCA may generate the linkage information to its current valid RCA certificate using the RCA Link Certificate message specified in clause 6.4.2.2.

If the RCA follows the re-enrolment process, it shall provide the pair of new rekeyed RCA certificate and corresponding RCA Link Certificate to the CPOC via the CPOC-RCA interface (CPOC-ENTRY). Otherwise, the full initial application form process (like initial enrolment of a new RCA) is applied.

NOTE 2: The RCA is publishing the new re-keyed RCA certificate and (optional) corresponding RCA Link Certificate across the interface at reference point S11 as specified in ETSI TS 102 940 clause 7.1 [5]).

NOTE 3: The Annex I of CPOC protocol [i.17] presents different use cases on how re-keying process of RCA certificates are managed in the EU CCMS. The detailed specification of the enrolment/ re-enrolment processes is out of the scope of the present document.

### 6.4.2 Generation of Link Certificate Messages

#### 6.4.2.1 Generation of Link Certificate Message by the TLM

When the TLM is re-keying its certificate, the TLM generates its “new” re-keyed certificate (tlmCertificate of type EtsiTs103097Certificate)following the TLM certificate profile as specified in TS 103 097 [3] and generates a TLM Link Certificate. This message is a signed “link certificate” which is to be used to establish the trust continuity of the TLM certificate when this continuity is not established directly using the ECTL.

The following functional requirements shall be satisfied:

* The TlmLinkCertificateMessage shall be a signed message using the private key corresponding to the public key contained in the “old” current valid TLM certificate.
* The TLM old certificate shall have the permissions to sign the TLM link certificate message. Its appPermissions shall contain the CTL Service ITS-AID (0x02 70 / decimal 624) and the TLM CTL SSPs (bit at position 0 (80h) set to 1) as specified in clause B.2.
* The content of the TlmLinkCertificateMessage message shall be as described in figure 23. The specification of the TlmLinkCertificateMessage message using ASN.1 [6], [7] shall be as specified in clause A.2.2.

To create a TLM Link Certificate message, the TLM shall follow this process:

* An EtsiTs102941Data structure is built, containing:
* version is set to v1 (integer value set to 1);
* a linkCertificateTlm of type ToBeSignedLinkCertificateTlm is built with:
* expiryTime is the time at which the link certificate message expires. It shall be equal to the end of the validity period of the TLM certificate that signs the message;
* certificateHash is the hash of the “new” generated TLM certificate, tlmCertificate.
	+ - If the TLM certificate has an issuer field of choice self and the corresponding hash algorithm is sha256, the hash value is calculated using the HashedData structure of choice sha256HashedData and the input data to the hash function is set to the COER-encoding of the tlmCertificate;
		- If the TLM certificate has an issuer field of choice self and the corresponding hash algorithm is sha384, the hash value is calculated using the HashedData structure of choice sha384HashedData. The input data to the hash function is set to the COER-encoding of the tlmCertificate.

NOTE 1: To be compliant to the CP [i.16], the TLM certificate is a self-signed certificate containing an IssuerIdentifier of value ‘self’ with corresponding hash value set to sha384 and containing a verification key of type ecdsaBrainpoolP384r1.

NOTE 2: The extension to the ASN.1 HashedData structure is required as specified in TS 103 097 Annex A.2.2 [3].

* An EtsiTs103097Data-Signed structure is built, containing: hashId, tbsData, signer and signature:
* the hashId shall indicate the hash algorithm of the TLM “old” certificate;
* in tbsData:
* the payload shall contain the previous EtsiTs102941Data structure;
* in the headerInfo:
* the psid shall be set to the value of "Certificate Trust List service" as assigned in ETSI TS 102 965 [19];
* the generationTime shall be present and set to the time at which the link certificate message is generated;
* all other components of the component tbsdata.headerInfo not used and absent;
* the signer is declared as a digest, containing the hashedId8 of the “old” current valid TLM certificate;
* the signature over the tbsData computed using the currently valid private key corresponding to “old” TLM certificate.

#### 6.4.2.2 Generation of Link Certificate Message by a Root CA

Figure 23: Message TlmLinkCertificateMessage

When a RCA is re-keying its certificate, the RCA generates its “new” re-keyed certificate (rcaCertificate of type EtsiTs103097Certificate)following the RCA certificate profile as specified in TS 103 097 [3]. The RCA generates a signed RCA Link Certificate message and transmits it with the new RCA certificate at the CPOC-RCA interface (CPOC-ENTRY) to establish that it is the successor to an existing RCA certificate. The link certificate is a signed message which ensures the trust migration from a current valid self-signed certificate (denoted as the “old” certificate in Figure Y) to the “new” self-signed one.

The following functional requirements shall be satisfied:

* A Double Signed RCA Link Certificate Message shall be created as specified in this clause. The two steps are:
	+ the “old” CA creates an EtsiTs102941Data of choice singleSignedLinkCertificateRca containing the ToBeSignedLinkCertificateRca(containing the hash of the new root certificate) and signs it.
	+ the “new” CA creates an EtsiTs102941Data of choice doubleSignedLinkCertificateRca containing the RcaSingleSignedLinkCertificateMessage and signs it.
* Both the old and the new RCA certificates shall have the permissions to sign the RCA link certificate messages (singleSignedLinkCertificateRca and doubleSignedLinkCertificateRca). RCA certificates’s appPermissions shall contain the CTL Service ITS-AID (0x02 70 / decimal 624) and one of the RCA CTL SSPs bits at position 2 (20h) or position 3 (10h) shall be set to 1 as specified in clause B.2.
* The content of the RcaSingleSignedLinkCertificateMessage structure is depicted in figure 24 and the content of the RcaDoubleSignedLinkCertificateMessage is depicted in figure 25. The specification of the RcaDoubleSignedLinkCertificateMessage message using ASN.1 [6], [7] shall be as specified in clause A.2.2.

To create a Double Signed RCA Link Certificate message, the RCA shall follow this process:

* Single Signed RCA Link certificate Message: An EtsiTs102941Data structure is built, containing:
* version is set to v1 (integer value set to 1);
* a singleSignedlinkCertificateRca of type ToBeSignedLinkCertificateRca is built with:
* expiryTime is the time at which the link certificate message expires. It shall be equal to the end of the validity period of the RCA certificate that signs the message;
* certificateHash is the hash of the “new” generated RCA certificate, rcaCertificate.
	+ - If the RCA certificate has an issuer field of choice self and the corresponding hash algorithm is sha256, the hash value is calculated using the HashedData structure of choice sha256HashedData and the input data to the hash function is set to the COER-encoding of the rcaCertificate;
		- If the RCA certificate has an issuer field of choice self and the corresponding hash algorithm is sha384, the hash value is calculated using the HashedData structure of choice sha384HashedData. The input data to the hash function is set to the COER-encoding of the rcaCertificate.

NOTE 1: To be compliant to the CP [i.16], the RCA certificate is a self-signed certificate containing an IssuerIdentifier of value ‘self’ with corresponding hash value set to sha256 or to sha384 and containing a verification key of type ecdsaNistP256, ecdsaBrainpoolP256r1 or ecdsaBrainpoolP384r1.

NOTE 2: The extension to the ASN.1 HashedData structure is required as specified in TS 103 097 Annex A.2.2 [3].

* An EtsiTs103097Data-Signed structure of type RcaSingleSignedLinkCertificateMessage is built (see Figure Y), containing: hashId, tbsData, signer and signature:
* the hashId shall indicate the hash algorithm of the RCA “old” certificate;
* in tbsData:
* the payload shall contain the previous EtsiTs102941Data structure;
* in the headerInfo:
* the psid shall be set to the value of "Certificate Trust List service" as assigned in ETSI TS 102 965 [19];
* the generationTime shall be present and set to the time at which the link certificate message is generated;
* all other components of the component tbsdata.headerInfo not used and absent;
* the signer is declared as a digest, containing the hashedId8 of the “old” current valid RCA certificate;
* the signature over the tbsData computed using the currently valid private key corresponding to “old” RCA certificate.
* Double Signed RCA Link certificate Message: An EtsiTs102941Data structure is built, containing:
* version is set to v1 (integer value set to 1);
* the content is set to the previous signed data structure of type RcaSingleSignedLinkCertificateMessage.
* An EtsiTs103097Data-Signed structure of type RcaSingleSignedLinkCertificateMessage is built (see Figure Y), containing: hashId, tbsData, signer and signature:
* the hashId shall indicate the hash algorithm of the RCA “new” certificate;
* in tbsData:
* the payload shall contain the previous EtsiTs102941Data structure;
* in the headerInfo:
* the psid shall be set to the value of "Certificate Trust List service" as assigned in ETSI TS 102 965 [19];
* the generationTime shall be present and set to the time at which the link certificate message is generated;
* all other components of the component tbsdata.headerInfo not used and absent;
* the signer is declared as a digest, containing the hashedId8 of the “new” current valid RCA certificate;
* the signature over the tbsData computed using the private key corresponding to “new” RCA certificate.



Figure 24: Single Signed RCA Link certificate Message



Figure 25: Double Signed RCA Link certificate Message

#### **Editor Note:** **To be added to EtsiTs102941MessagesCA.asn**

## A.2.1 Security data structures

EtsiTs102941BaseTypes

{ itu-t(0) identified-organization(4) etsi(0) itsDomain(5) wg5(5) ts(102941) baseTypes(3) version~~2~~3(~~2~~3) }

DEFINITIONS AUTOMATIC TAGS ::=

BEGIN

IMPORTS

……………………

 CertificateId, SubjectAssurance, SequenceOfPsidSsp, SequenceOfPsidGroupPermissions,

 ValidityPeriod, GeographicRegion, HashedData

FROM

 IEEE1609dot2 {iso(1) identified-organization(3) ieee(111)
standards-association-numbered-series-standards(2) wave-stds(1609) dot2(2) base (1) schema (1) major-version-2(2)}

## A.2.2 Security Management messages for CA

EtsiTs102941MessagesCa

 { itu-t(0) identified-organization(4) etsi(0) itsDomain(5) wg5(5) ts(102941) messagesCa(0) version~~2~~3(~~2~~3)}

DEFINITIONS AUTOMATIC TAGS ::=

BEGIN

IMPORTS

EtsiTs103097Data-Signed,

--EtsiTs103097Data-Encrypted,

EtsiTs103097Data-SignedExternalPayload

--EtsiTs103097Data-SignedAndEncrypted

FROM EtsiTs103097Module

{ itu-t(0) identified-organization(4) etsi(0) itsDomain(5) wg5(5) ts(103097) securedMessageV1(0)}

ToBeSignedLinkCertificate, ToBeSignedLinkCertificateTlm, ToBeSignedLinkCertificateRca

FROM EtsiTs102941TypesLinkCertificate

 { itu-t(0) identified-organization(4) etsi(0) itsDomain(5) wg5(5) ts(102941) linkCertificate(9) version2(2)}

/\*\*\*\*\*\*\*\*\*\*\*\*

-- Messages

\*\*\*\*\*\*\*\*\*\*\*\*/

……………………

TlmLinkCertificateMessage ::= EtsiTs103097Data-Signed{

 EtsiTs102941Data (WITH COMPONENTS{

 ...,

 content (WITH COMPONENTS{

 linkCertificateTlm PRESENT

 })

 })

}

RcaSingleSignedLinkCertificateMessage ::= EtsiTs103097Data-Signed{

 EtsiTs102941Data (WITH COMPONENTS{

 ...,

 content (WITH COMPONENTS{

 singleSignedLinkCertificateRca PRESENT

 })

 })

}

RcaDoubleSignedLinkCertificateMessage ::= EtsiTs103097Data-Signed{

 EtsiTs102941Data (WITH COMPONENTS{

 ...,

 content (WITH COMPONENTS{

 doubleSignedlinkCertificateRca PRESENT

 })

 })

}

/\*\*\*\*\*\*\*\*\*\*\*\*

-- EtsiTs102941Data

\*\*\*\*\*\*\*\*\*\*\*\*/

……………………

EtsiTs102941DataContent ::= CHOICE {

 enrolmentRequest InnerEcRequestSignedForPop,

 enrolmentResponse InnerEcResponse,

 authorizationRequest InnerAtRequest,

 authorizationResponse InnerAtResponse,

 certificateRevocationList ToBeSignedCrl,

 certificateTrustListTlm ToBeSignedTlmCtl,

 certificateTrustListRca ToBeSignedRcaCtl,

 authorizationValidationRequest AuthorizationValidationRequest,

 authorizationValidationResponse AuthorizationValidationResponse,

 caCertificateRequest CaCertificateRequest,

 authorizationValidationRequest AuthorizationValidationRequest,

 authorizationValidationResponse AuthorizationValidationResponse,

 caCertificateRequest CaCertificateRequest,

 ...,

 linkCertificateTlm ToBeSignedLinkCertificateTlm,

 singleSignedLinkCertificateRca ToBeSignedLinkCertificateRca,

 doubleSignedlinkCertificateRca RcaSingleSignedLinkCertificateMessage

 }

NOTE: The EtsiTs102941DataContent is extended to add three additional options to support the messages defined in clause 6.4.

#### **Editor Note: To be added to EtsiTs102941MessagesItss.asn**

## A.2.3 Security Management messages for ITS-S\_WithPrivacy

EtsiTs102941MessagesItss

 { itu-t(0) identified-organization(4) etsi(0) itsDomain(5) wg5(5) ts(102941) messagesItss(1) version~~2~~3(~~2~~3)}

DEFINITIONS AUTOMATIC TAGS ::=

BEGIN

IMPORTS

……………………

ToBeSignedLinkCertificate, ToBeSignedLinkCertificateTlm

FROM EtsiTs102941TypesLinkCertificate

 { itu-t(0) identified-organization(4) etsi(0) itsDomain(5) wg5(5) ts(102941) linkCertificate(9) version2(2)}

……………………

/\*\*\*\*\*\*\*\*\*\*\*\*

-- Messages

\*\*\*\*\*\*\*\*\*\*\*\*/

……………………

TlmLinkCertificateMessage ::= EtsiTs103097Data-Signed{

 EtsiTs102941Data (WITH COMPONENTS{

 ...,

 content (WITH COMPONENTS{

 linkCertificateTlm PRESENT

 })

 })

}

/\*\*\*\*\*\*\*\*\*\*\*\*

-- EtsiTs102941Data

\*\*\*\*\*\*\*\*\*\*\*\*/

……………………

EtsiTs102941DataContent ::= CHOICE {

 enrolmentRequest InnerEcRequestSignedForPop,

 enrolmentResponse InnerEcResponse,

 authorizationRequest InnerAtRequest,

 authorizationResponse InnerAtResponse,

 certificateRevocationList ToBeSignedCrl,

 certificateTrustListTlm ToBeSignedTlmCtl,

 certificateTrustListRca ToBeSignedRcaCtl,

 authorizationValidationRequest NULL,

 authorizationValidationResponse NULL,

 caCertificateRequest NULL,

 ...,

 linkCertificateTlm ToBeSignedLinkCertificateTlm,

 singleSignedLinkCertificateRca NULL,

 doubleSignedlinkCertificateRca NULL

 }

NOTE: The EtsiTs102941DataContent is extended to add the additional option to support the TLM Link Certificate message defined in clause 6.4. Other additional choices are NULL.

#### **Editor Note: To be added to EtsiTs102941MessagesItss\_OptionalPrivacy.asn**

## A.2.4 Security Management messages for ITSS\_NoPrivacy

EtsiTs102941MessagesItss-OptionalPrivacy

 { itu-t(0) identified-organization(4) etsi(0) itsDomain(5) wg5(5) ts(102941) messagesItssOp(2) version~~2~~3(~~2~~3)}

DEFINITIONS AUTOMATIC TAGS ::=

BEGIN

IMPORTS

……………………

ToBeSignedLinkCertificate, ToBeSignedLinkCertificateTlm

FROM EtsiTs102941TypesLinkCertificate

 { itu-t(0) identified-organization(4) etsi(0) itsDomain(5) wg5(5) ts(102941) linkCertificate(9) version2(2)}

……………………

/\*\*\*\*\*\*\*\*\*\*\*\*

-- Messages

\*\*\*\*\*\*\*\*\*\*\*\*/

……………………

TlmLinkCertificateMessage ::= EtsiTs103097Data-Signed{

 EtsiTs102941Data (WITH COMPONENTS{

 ...,

 content (WITH COMPONENTS{

 linkCertificateTlm PRESENT

 })

 })

}

/\*\*\*\*\*\*\*\*\*\*\*\*

-- EtsiTs102941Data

\*\*\*\*\*\*\*\*\*\*\*\*/

……………………

EtsiTs102941DataContent ::= CHOICE {

 enrolmentRequest InnerEcRequestSignedForPop,

 enrolmentResponse InnerEcResponse,

 authorizationRequest InnerAtRequest,

 authorizationResponse InnerAtResponse,

 certificateRevocationList ToBeSignedCrl,

 certificateTrustListTlm ToBeSignedTlmCtl,

 certificateTrustListRca ToBeSignedRcaCtl,

 authorizationValidationRequest NULL,

 authorizationValidationResponse NULL,

 caCertificateRequest NULL,

 ...,

 linkCertificateTlm ToBeSignedLinkCertificateTlm,

 singleSignedLinkCertificateRca NULL,

 doubleSignedlinkCertificateRca NULL

 }

NOTE: The EtsiTs102941DataContent is extended to add the additional option to support the TLM Link Certificate message defined in clause 6.4. Other additional choices are NULL.

## A.2.8 Link certificate message data types

EtsiTs102941TypesLinkCertificate

 { itu-t(0) identified-organization(4) etsi(0) itsDomain(5) wg5(5) ts(102941) linkCertificate(9) version2(2)}

DEFINITIONS AUTOMATIC TAGS ::=

BEGIN

IMPORTS

Time32, HashedData

FROM EtsiTs102941BaseTypes

{itu-t(0) identified-organization(4) etsi(0) itsDomain(5) wg5(5) ts(102941) baseTypes(3) version2(2)}

;

/\*\*\*\*\*\*\*\*\*\*\*\*

-- Link certificate messages

\*\*\*\*\*\*\*\*\*\*\*\*/

ToBeSignedLinkCertificate ::= SEQUENCE {

expiryTime Time32,

 certificateHash HashedData,

 ...

}

## B.2 CTL SSPs definition

……………………

Table B.2: CTL service-specific permissions

| Bit position | Permission | Bit Value |
| --- | --- | --- |
| 0 (80h) | The certificate can be used to sign CTL containing the TLM entries.The certificate can be used to sign TLM Link certificates messages. | 0: certificate not allowed to sign 1: certificate allowed to sign |
| 1 (40h) | The certificate can be used to sign CTL containing the Root CA entries | 0: certificate not allowed to sign 1: certificate allowed to sign |
| 2 (20h) | The certificate can be used to sign CTL containing the EA entries.The certificate can be used to sign root CA link certificates messages. | 0: certificate not allowed to sign 1: certificate allowed to sign |
| 3 (10h) | The certificate can be used to sign CTL containing the AA entries.The certificate can be used to sign root CA link certificates messages. | 0: certificate not allowed to sign 1: certificate allowed to sign  |
| 4 (08h) | The certificate can be used to sign CTL containing the DC entries | 0: certificate not allowed to sign 1: certificate allowed to sign  |
| 5 to 7  | unused |  |

To sign a RCA link certificate message, a Root CA certificate shall contain CTL Service ITS-AID (0x02 70 / decimal 624) with one of the associated SSPs bits at position 2 (20h) or position 3 (10h) set to 1. The receiver shall enforce an OR condition on these two bits position 2-3 to accept RCA link cert messages.

|  |
| --- |
| **CHANGE REQUEST** |
|  | ETSI TS 102 941 | **Version** | 1.3.1 | **CR** | 4 | **rev** | - |  |
|  |
| **CR Title** | The AuthorizationValidationResponse message is encrypted by EA using the symmetric key provided by AA in the AuthorizationValidationRequest message. |
|  |  |
| **Original Source** | ITS WG 5 |
|  |  |
| **Work Item Ref** | RTS/ITS-00552 | **Submission date** | 01/07/2020 |
| **Approving TB**  | ITS | **Approval date** | 03.07.2020 |
| **Category:** | **D** | **Release** | 1 |  |
|  | Use **one** of the following categories:**F** (correction)**A** (correction in an earlier release)**B** (addition of feature) **C** (functional modification of feature)**D** (editorial modification) |  |
|  |  |
| **Reason for change** | In the Authorization Validation Response, in the structure EtsiTs103097Data-Encrypted, there is an error. The response shall be encrypted with a key generated by the AA (not the by the ITS-S). |
|  |  |
| **Consequence if not approved** | EA generate the encrypted Authorization Validation Response with a wrong, undefined key and the AA cannot decrypt the message. |
|  |  |
| **Summary of change** | To enable the EA to generate the correct encrypted AuthorizationValidationResponse message, we need to replace ‘key generated by ’ITS-S’ by ‘key generated by AA’ in the text. |
|  |  |
| **Clauses affected** | 6.2.3.4.2 |
|  |  |
| **Linked Change Requests** |  |  |
|  |  |  |
|  |  |
| **Other comments** |  |
|  |  |

##### 6.2.3.4.2 Authorization validation response

…………..

the component recipients containing one instance of RecipientInfo of choice pskRecipInfo, which contains the HashedId8 of the SymmetricEncryptionKey structure containing the symmetric key used by the ~~ITS-S~~ AA to encrypt the AuthorizationValidationRequest message to which the response is built;”

|  |
| --- |
| **CHANGE REQUEST** |
|  | ETSI TS 102 941 | **Version** | 1.3.1 | **CR** | *5* | **rev** | - |  |
|  |
| **CR Title** | Move newly defined TS103097 data types from TS 102 941 to TS 103 097 |
|  |  |
| **Original Source** | ITS WG5 |
|  |  |
| **Work Item Ref** | RTS/ITS-00559 | **Submission date** | 01.07.2020 |
| **Approving TB**  | ITS | **Approval date** | 03.07.2020 |
| **Category:** | **F** | **Release** | 1 |  |
|  | Use **one** of the following categories:**F** (correction)**A** (correction in an earlier release)**B** (addition of feature) **C** (functional modification of feature)**D** (editorial modification) |  |
|  |  |
| **Reason for change** | In the revision of TS 102 941 to its V1.3.1 three data types were defined that in reality belong to TS 103 097 and should be moved  |
|  |  |
| **Consequence if not approved** | Unclean design of ASN.1 code. Possible duplication of ASN.1 Types in future. |
|  |  |
| **Summary of change** | Delete the following data types from TS 102 941 V1.3.1.: EtsiTs103097Data-Unsecured, EtsiTs103097Data-Encrypted-Unicast, EtsiTs103097Data-SignedAndEncrypted-Unicast |
|  |  |
| **Clauses affected** | A.2.1 |
|  |  |
| **Linked Change Requests** | TS 103 097 V1.3.1. CR8 |  |
|  |  |  |
|  |  |
| **Other comments** |  |
|  |  |

A.2.1 Security data structures

***Delete the following data structures from the module EtsiTs102941BaseTypes:***

~~EtsiTs103097Data-Unsecured {ToBeSentDataContent} ::= EtsiTs103097Data (WITH COMPONENTS {...,~~

 ~~content (WITH COMPONENTS {~~

 ~~unsecuredData (CONTAINING ToBeSentDataContent)~~

 ~~})~~

~~})~~

~~EtsiTs103097Data-Encrypted-Unicast {ToBeEncryptedDataContent} ::= EtsiTs103097Data-Encrypted { EtsiTs103097Data-Unsecured{ToBeEncryptedDataContent}} (WITH COMPONENTS {...,~~

 ~~content (WITH COMPONENTS {~~

 ~~encryptedData (WITH COMPONENTS {...,~~

 ~~recipients (SIZE(1))~~

 ~~})~~

 ~~})~~

~~})~~

~~EtsiTs103097Data-SignedAndEncrypted-Unicast {ToBesignedAndEncryptedDataContent} ::= EtsiTs103097Data-Encrypted {EtsiTs103097Data-Signed {ToBesignedAndEncryptedDataContent}} (WITH COMPONENTS {...,~~

 ~~content (WITH COMPONENTS {~~

 ~~encryptedData (WITH COMPONENTS {...,~~

 ~~recipients (SIZE(1))~~

 ~~})~~

 ~~})~~

~~})~~

***Add the following imports statement to the module EtsiTs102941BaseTypes:***

IMPORTS

EtsiTs103097Data-Unsecured, EtsiTs103097Data-Encrypted-Unicast, EtsiTs103097Data-SignedAndEncrypted-Unicast FROM

EtsiTs103097Module

{itu-t(0) identified-organization(4) etsi(0) itsDomain(5) wg5(5) secHeaders(103097) core(1) version2(2)}

# Corrections for ETSI EN 302 637-2 (V1.4.1)

|  |
| --- |
| **Overview of Change Requests** |
| <Change Requesrt> | <Date> | <Title> |
| CR 302 637-2#001 | 12-07-19 | Description of LanePosition in the CAM standard |
| CR 302 637-2#002 | 17-01-20 | Description of closedLanes in the CAM standard (B.43) |
| CR 302 637-2#003 | 05-08-20 | Harmonize the use of vehicle dimensions between ETSI Documents |
|  |  |  |

|  |
| --- |
| **CHANGE REQUEST** |
|  | ETSI EN 302 637-2 | **Version** | 1.4.1 | **CR** | 1 | **rev** | - |  |
|  |
| **CR Title** | Description of LanePosition in the CAM standard |
|  |  |
| **Original Source** | ITS WG1 |
|  |  |
| **Work Item Ref** | REN/ITS-0010089 | **Submission date** | 22/03/2019 |
| **Approving TB**  | TC ITS | **Approval date** | 08/04/2019 |
| **Category:** | **F** | **Release** | 1 |  |
|  | Use **one** of the following categories:**F** (correction)**A** (correction in an earlier release)**B** (addition of feature) **C** (functional modification of feature)**D** (editorial modification) |  |
|  |  |
| **Reason for change** | The description of LanePosition is not in line with the description of LanePosition in CDD. The CAM standard defines counting lanes from outside to inside and the CDD defines counting from inside to outside. It is unclear which definition of LanePosition prevails. |
|  |  |
| **Consequence if not approved** | It is unclear how to interpret the information provided on the lane the vehicle is in. This could lead to wrong interpretations and wrong advice to drivers. |
|  |  |
| **Summary of change** | The CAM standard should not re-define what is already defined elsewhere. Hence delete the last part of the first sentence in B.24The DE lanePosition of the *referencePosition* of a vehicle, ~~counted from the~~~~outside border of the road, in the direction of the traffic flow.~~ |
|  |  |
| **Clauses affected** | B.24 |
|  |  |
| **Linked Change Requests** | CR 102 894-2 - #0001 Correction of ASN.1 definition for Data Element [LanePosition ]. |  |
|  |  |  |
|  |  |
| **Other comments** | See similar CR for the DENM standard. |
|  |  |

### B.24 lanePosition

|  |  |
| --- | --- |
| Description | The DE lanePosition of the *referencePosition* of a vehicle.This DE shall be present if the data is available at the originating ITS-S (see note). |
| Data setting and presentation requirements | The DE shall be presented as specified in ETSI TS 102 894-2 [2] *LanePosition.* |
| NOTE: Additional information is needed to unambiguously identify the lane position and to allow the correlation to a map. |

|  |
| --- |
| **CHANGE REQUEST** |
|  | ETSI EN 302 637-2 | **Version** | 1.4.1 | **CR** | 2 | **rev** | - |  |
|  |
| **CR Title** | Description of closedLanes in the CAM standard (B.43) |
|  |  |
| **Original Source** | ITS WG1 |
|  |  |
| **Work Item Ref** | REN/ITS-0010089 | **Submission date** | 20/11/2019 |
| **Approving TB**  | TC ITS | **Approval date** | 17/01/2020 |
| **Category:** | **F** | **Release** | 1 |  |
|  | Use **one** of the following categories:**F** (correction)**A** (correction in an earlier release)**B** (addition of feature) **C** (functional modification of feature)**D** (editorial modification) |  |
|  |  |
| **Reason for change** | The description of closedLines is not in line with the description of ClosedLines (A.106 and A.23) in CDD. |
|  |  |
| **Consequence if not approved** | It is unclear how to interpret the information provided on the closed lanes. This could lead to wrong interpretations and wrong advice to drivers. |
|  |  |
| **Summary of change** | The CAM standard should not re-define what is already defined elsewhere. Hence delete the part of the B.43 as it is already defined in CDD in A.106 and A.23 |
|  |  |
| **Clauses affected** | B.43 |
|  |  |
| **Linked Change Requests** | CR 102 894-2 - #0001 Correction of ASN.1 definition for Data Element [LanePosition ]. |
|  | CR 302 637-2 - #0001 Description of LanePosition in the CAM standard. |
|  |  |
| **Other comments** | See similar CR for the LanePosition DE. |
|  |  |

### B.43

It provides information about the opening/closure status of the lanes ahead. ~~Lanes are counted from the outside boarder of the road. If a lane is closed to traffic, the corresponding bit shall be set to 1.~~

|  |
| --- |
| **CHANGE REQUEST** |
|  | ETSI EN 302 637-2 | **Version** | 1.4.1 | **CR** | *3* | **rev** | - |  |
|  |
| **CR Title** | Harmonize the use of vehicle dimensions between ETSI Documents |
|  |  |
| **Original Source** | ITS WG1 |
|  |  |
| **Work Item Ref** | REN/ITS-0010089 | **Submission date** | 02.06.2020 |
| **Approving TB**  | ITS | **Approval date** | 05.08.2020 |
| **Category:** | **F** | **Release** | 1 |  |
|  | Use **one** of the following categories:**F** (correction)**A** (correction in an earlier release)**B** (addition of feature) **C** (functional modification of feature)**D** (editorial modification) |  |
|  |  |
| **Reason for change** | There is an inconsistency between the EN 302 637-2 (CA Service), the TS 102 894-2 (CDD) and the EN 302 890-2 (PoTi). Whereas the CA-Service and the CDD state that the vehicle width DF (Clause B.36 in CA-Service; Clause A.95 in CDD) shall include the width of the vehicle ITS-S with side mirrors included, the PoTi EN (Clause 6.2.2) states that side mirrors are excluded. It is proposed to follow the interpretation of the PoTi EN as the detection of side mirrors is difficult for perception sensors from other vehicles. However, the vehicle width information could be used in data association algorithms. A vehicle following the vehicle ITS-S disseminating the e.g., CAM with this information is likely not to perceive the width including the side mirrors. |
|  |  |
| **Consequence if not approved** | Non-hamonized use of the vehicleWidth DE between different ITS-S due to contradicting specifications |
|  |  |
| **Summary of change** | Change wording in Clause B.36 of EN 302 637-2 to “Vehicle width of the vehicle ITS-S that originates the CAM, excluding side mirrors and possible similar extensions.” |
|  |  |
| **Clauses affected** | B.36  |
|  |  |
| **Linked Change Requests** | See below |  |
|  |  |  |
|  |  |
| **Other comments** |  |
|  |  |

# B.36 vehicleWidth

**Change to:**

|  |  |
| --- | --- |
| Description | ~~Vehicle width, measured of the vehicle ITS-S that originates the CAM, including side mirrors.~~Vehicle width of the vehicle ITS-S that originates the CAM, excluding side mirrors and possible similar extensions.” |
| Data setting and presentation requirements | The DE shall be presented as specified inETSI TS 102 894-2 [2] *VehicleWidth.* |

# Corrections for ETSI EN 302 637-3 (V1.3.1)

|  |
| --- |
| **Overview of Change Requests** |
| <Change Requesrt> | <Date> | <Title> |
| CR 302 637-2#001 | 12-07-19 | Description of LanePosition in the DENM standard |
| CR 302 637-2#002 | 12-07-19 | Type of ServiceSpecificPermissions in the DENM standard |
|  |  |  |
|  |  |  |

|  |
| --- |
| **CHANGE REQUEST** |
|  | ETSI EN 302 637-3 | **Version** | 1.3.1 | **CR** | 1 | **rev** | - |  |
|  |
| **CR Title** | Description of LanePosition in the DENM standard |
|  |  |
| **Original Source** | ITS WG1 |
|  |  |
| **Work Item Ref** | REN/ITS-0010090 | **Submission date** | 22/03/2019 |
| **Approving TB**  | TC ITS | **Approval date** | 08/04/2019 |
| **Category:** | **F** | **Release** | 1 |  |
|  | Use **one** of the following categories:**F** (correction)**A** (correction in an earlier release)**B** (addition of feature) **C** (functional modification of feature)**D** (editorial modification) |  |
|  |  |
| **Reason for change** | The description of LanePosition is not in line with the description of LanePosition in CDD. The DENM standard defines counting lanes from outside to inside and the CDD defines counting from inside to outside. It is unclear which definition of LanePosition prevails. |
|  |  |
| **Consequence if not approved** | It is unclear how to interpret the information related to the lane of the event. This could lead to wrong interpretations and wrong advice to drivers. |
|  |  |
| **Summary of change** | Delete the last part of the first sentence in B.24The lane position of the event position in the road ~~counted from the outside~~~~boarder of the road.~~ |
|  |  |
| **Clauses affected** | B.24 |
|  |  |
| **Linked Change Requests** | CR 102 894-2 - #0001 Correction of ASN.1 definition for Data Element [LanePosition ]. |  |
|  |  |  |
|  |  |
| **Other comments** | See similar CR for the CAM standard. |
|  |  |

### B.24 lanePosition

|  |  |
| --- | --- |
| Description | The lane position of the event position in the road.This DE in included in the *alacarte* container.If this data is provided, the originating ITS-S is required to determine the lane position with a predefined confidence level as defined by the ITS applications (e.g. 95 %). |
| Data setting and presentation requirements | This DE is OPTIONAL. It shall be present when this information is required by the ITS application. This DE shall be presented as specified in ETSI TS 102 894-2 [5] *LanePosition*. |

|  |
| --- |
| **CHANGE REQUEST** |
|  | ETSI EN 302 637-3 | **Version** | 1.3.1 | **CR** | 2 | **rev** | - |  |
|  |
| **CR Title** | Type of ServiceSpecificPermissions in the DENM standard |
|  |  |
| **Original Source** | ITS WG5 |
|  |  |
| **Work Item Ref** | REN/ITS-0010090 | **Submission date** | 22/03/2019 |
| **Approving TB**  | ITS | **Approval date** | 08/04/2019 |
| **Category:** | **F** | **Release** | 1 |  |
|  | Use **one** of the following categories:**F** (correction)**A** (correction in an earlier release)**B** (addition of feature) **C** (functional modification of feature)**D** (editorial modification) |  |
|  |  |
| **Reason for change** | There are two options for specifying SSPs in TS 103 097. The DENM standard does not state which one to use. |
|  |  |
| **Consequence if not approved** | If it is not clarified which one option be used, this could cause interoperability problems if sending and receiving implementations use different options. The permissions could potentially not be decoded and hence DENMs cannot be validated from a security/permissions point of view. |
|  |  |
| **Summary of change** | 1. Add the following sentence to 6.2.2.2:

*DENMs shall be signed using private keys associated to Authorization Tickets that contain SSPs of type BitmapSsp as specified in ETSI TS 103 097 (V1.3.1) [9].*1. Move reference [i.17] to the normative references as reference [9]
 |
|  |  |
| **Clauses affected** | 2.1 and 6.2.2.2 |
|  |  |
| **Linked Change Requests** |  |  |
|  |  |  |
|  |  |
| **Other comments** | The same change has already been done in the CAM standard clause 6.2.2.2 during the ENAP comment resolution. |
|  |  |

### 6.2.2.2 Service Specific Permissions (SSP)

The octet scheme allows the SSP format to accommodate current and future versions of the present document. The octet scheme for DENM SSP is constructed out of four octets as illustrated in Figure 4.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 |  |  |  |  |  |  |  | 1 |  |  |  |  |  |  |  | 2 |  |  |  |  |  |  |  | 3 |  |  |  |  |  |  |  |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| Octet 0 | Octet 1 | Octet 2 | Octet 3 |

Figure 4: Format for the Octets

EXAMPLE of bit order: The decimal value 199 shall be represented as shown in Figure 5.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 1 | 1 | 0 | 0 | 0 | 1 | 1 | 1 |

Figure 5: Example of octet presentation

For each octet, the most significant bit (MSB) shall be the leftmost bit. The transmission order shall always be the MSB first. The first octet (octet 0 in Figure 4) shall control the SSP version and be interpreted in the following way:

 0: No version, length 1 octet; the value shall only be used for testing purposes.

 1: First version, length 4 octets.

 2 to 255: Reserved for Future Usage.

The SSP has a maximum length as specified in ETSI TS 103 097 [i.17]. The first octet shall reflect the version of the present document. As future versions of the present document are published, the first octet shall be accordingly incremented. The second to fourth octet (octet 1 to octet 3 in Figure 4) is based on the *causeCode* types described in the clause 7.1.4.

Length of SSP is the length of the Octet String. Table 8 presents the octet scheme for DENM SSPs.

When the ITS Application Identifier (ITS-AID) is set for the DEN basic service, the permissions shall be as defined in Table 9.

DENMs shall be signed using private keys associated to Authorization Tickets that contain SSPs of type BitmapSsp as specified in ETSI TS 103 097 (V1.3.1) [9].

Table 8: Octet Scheme for DENM SSPs

|  |  |
| --- | --- |
| Octet # | Description |
| 0 | SSP version control |
| 1 to 3 | Service-specific parameter |
| 4 to 30 | Reserved for Future Usage |

………………..

### 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.

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

[1] SAE J2735 (2009-11-19): "Dedicated Short Range Communications (DSRC) Message Set Dictionary".

…………………..

[9] ETSI TS 103 097 (V1.3.1): "Intelligent Transport Systems (ITS); Security; Security header and certificate formats".

### 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] ETSI TR 102 638 (V1.1.1): "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Definitions".

……………….

 [i.17] Void.

[i.18] ETSI TR 102 965 (V1.1.1): "Intelligent Transport Systems (ITS); Application object identifier (ITS-AID); Registration list".

# Corrections for ETSI TS 103 301 (V1.3.1)

|  |
| --- |
| **Overview of Change Requests** |
| <Change Requesrt> | <Date> | <Title> |
| CR 103 301#001 | 3-07-20 | Correct the SSP version control for the GPC service |
|  |  |  |
|  |  |  |
|  |  |  |

|  |
| --- |
| **CHANGE REQUEST** |
|  | ETSI TS 103 301 | **Version** | 1.3.1 | **CR** | *1* | **rev** | - |  |
|  |
| **CR Title** | Correct the SSP version control for the GPC service |
|  |  |
| **Original Source** | ITS WG1 |
|  |  |
| **Work Item Ref** | RTS/ITS-00181 | **Submission date** | 19.05.2020 |
| **Approving TB**  | ITS | **Approval date** | 03.07.2020 |
| **Category:** | **F** | **Release** | 1 |  |
|  | Use **one** of the following categories:**F** (correction)**A** (correction in an earlier release)**B** (addition of feature) **C** (functional modification of feature)**D** (editorial modification) |  |
|  |  |
| **Reason for change** | The SSP version control for the GPC service is set to value0.This is not possible as the value 0 is reserved for testing only and the value for SSP version control should start at value 1 in a published TS.  |
|  |  |
| **Consequence if not approved** | in a real deployment an ITS-S which receives RTCMEM messages with version 0 in the signing certificate migh drop the received messages. |
|  |  |
| **Summary of change** | Change value of SSP version control to 1 in table 25. |
|  |  |
| **Clauses affected** | 9.4.3.2 |
|  |  |
| **Linked Change Requests** | - |  |
|  |  |  |
|  |  |
| **Other comments** |  |
|  |  |

#### 9.4.3.2 GPC service communication requirements for short range access technologies

……………………

Table : Octet Scheme for GPC service SSPs

|  |  |  |
| --- | --- | --- |
| Octet # | Description | Value |
| 0 | SSP version control | ~~0~~1 |

History

|  |
| --- |
| **Document history** |
| <Version> | <Date> | <Milestone> |
| 0.0.1 | 03-04-19 | First draft |
| 0.0.2 | 20-01-20 | Second Draft |
| 0.0.3 | 06-08-20 | Third draft |
|  |  |  |

*Latest changes made on 2020-08-06*