ETSI TS 102 941 V2.2.1 (2022-11)

Intelligent Transport Systems (ITS);
Security;
Trust and Privacy Management;
Release 2

Reference
RTS/ITS-005102

Keywords
interoperability, ITS, management, 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

Contents

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.

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 specifies the trust and privacy management for Intelligent Transport Systems (ITS) communications. Based upon the security services defined in ETSI TS 102 731 [i.23] and the security architecture defined in ETSI TS 102 940 [5], it identifies the trust establishment and privacy management required to support security in an ITS environment and the relationships that exist between the entities themselves and the elements of the ITS reference architecture defined in ETSI EN 302 665 [i.25].

The present document identifies and specifies security services for the establishment and maintenance of identities and cryptographic keys in an Intelligent Transport Systems (ITS). Its purpose is to provide the functions upon which systems of trust and privacy can be built within an ITS.

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] Void.

[2] Void.

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

[4] Void.

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

[6] ISO/IEC 8824-1:2021: "Information technology -- Abstract Syntax Notation One (ASN.1): Specification of basic notation -- Part 1 Specification of basic notation".

[7] Recommendation ITU-T X.696 (02/2021): "Information technology - ASN.1 encoding rules: Specification of Octet Encoding Rules (OER)".

[8] Void.

[9] Void.

[10] Void.

[11] Void.

[12] Void.

[13] NIST FIPS PUB 198-1: "The Keyed-Hash Message Authentication Code (HMAC)".

[14] Void.

[15] IETF RFC 4862: "IPv6 Stateless Address Autoconfiguration".

[16] ETSI TS 103 836-6-1: "Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 6: Internet Integration; Sub-part 1: Transmission of IPv6 Packets over GeoNetworking Protocols; Release 2".

[17] Void.

[18] ETSI TS 103 836-4-1: "Intelligent Transportation 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".

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

[20] Void.

[21] IETF RFC 5280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

NOTE: Available from https://datatracker.ietf.org/doc/html/rfc5280.

[22] IETF RFC 5480: "Elliptic Curve Cryptography Subject Public Key Information".

NOTE: Available from https://www.rfc-editor.org/rfc/rfc5480.

[23] Void.

[24] IEEE 1609.2.1™-2022: "IEEE Standard for Wireless Access in Vehicular Environments (WAVE) - Certificate Management Interfaces for End Entities".

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] ISO/IEC 15408-2: "Information technology -- Security techniques -- Evaluation criteria for IT security; Part 2: Security functional components".

[i.2] ETSI TR 102 638: "Intelligent Transport Systems (ITS); Vehicular communication; Basic Set of Applications; Release 2".

[i.3] IETF RFC 4046: "Multicast Security (MSEC) Group Key Management Architecture".

[i.4] IETF RFC 4301: "Security Architecture for the Internet Protocol".

[i.5] IETF RFC 4302: "IP Authentication Header".

[i.6] IETF RFC 4303: "IP Encapsulating Security Payload (ESP)".

[i.7] IETF RFC 5246: "The Transport Layer Security (TLS) Protocol Version 1.2".

[i.8] IETF RFC 3547: "The Group Domain of Interpretation".

[i.9] IETF RFC 3830: "MIKEY: Multimedia Internet KEYing".

[i.10] IETF RFC 4535: "GSAKMP: Group Secure Association Key Management Protocol".

[i.11] IETF RFC 4306: "Internet Key Exchange (IKEv2) Protocol", December 2005.

[i.12] IETF RFC 4877: "Mobile IPv6 Operation with IKEv2 and the Revised IPsec Architecture".

[i.13] ETSI TS 102 723-8: "Intelligent Transport Systems (ITS); OSI cross-layer topics; Part 8: Interface between security entity and network and transport layer".

[i.14] CVRIA: "Connected Vehicle Reference Implementation Architecture".

NOTE: Available at http://www.iteris.com/cvria/.

[i.15] ISO 21210-2010: "Intelligent Transport Systems (ITS) -- Communications access for land mobiles (CALM) -- Ipv6 networking".

[i.16] IETF RFC 8446: "The Transport Layer Security (TLS) Protocol Version 1.3".

[i.17] ETSI TS 102 942: "Intelligent Transport Systems (ITS); Security; Access control; Release 2".

[i.18] ETSI TS 102 943: "Intelligent Transport Systems (ITS); Security; Confidentiality services; Release 2".

[i.19] ETSI TS 103 900: "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Specification of Cooperative Awareness Basic Service; Release 2".

[i.20] ETSI TS 103 831: "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Decentralized Environmental Notification Service; Release 2".

[i.21] ETSI TS 103 301: "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Facilities layer protocols and communication requirements for infrastructure services; Release 2".

[i.22] 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.23] ETSI TS 102 731: "Intelligent Transport Systems (ITS); Security; Security Services and Architecture; Release 2".

[i.24] Void.

[i.25] ETSI EN 302 665: "Intelligent Transport Systems (ITS); Communications Architecture".

[i.26] EU C-ITS Security Credential Management System (EU CCMS).

3 Definition of terms, symbols, abbreviations and notation

3.1 Terms

For the purposes of the present document, the terms given in ETSI TS 102 731 [i.23], ETSI TS 102 940 [5], ISO/IEC 15408-2 [i.1] and the following apply:

delta CTL: partial CTL that only contains CTL entries that have been updated since the issuance of the prior, base CTL

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI TS 103 097 [3], ETSI TS 102 940 [5], ETSI TS 103 836-4-1 [18] and the following apply:

AA	Authorization Authority
AES	Advanced Encryption Standard
ASN	Abstract Syntax Notation
AT	Authorization Ticket
CA	Certification Authority
CCH	Control CHannel
CCM	Counter with CBC-MAC
CCMS	Cooperative-ITS Certificate Management System
COER	Canonical Octet Encoding Rules
CPOC	C-ITS Point Of Contact
CRL	Certificate Revocation List
CTL	Certificate Trust List
CVRIA	Connected Vehicle Reference Implementation Architecture
DC	Distribution Centre
DEN	Decentralized Environmental Notification
DENM	Decentralized Environmental Notification Message
EA	Enrolment Authority
EC	Enrolment Credential
ECC	Elliptic Curve Cryptography
ECTL	European Certificate Trust List
EV	Electric Vehicle
FIPS	Federal Information Processing Standard
GET	command HTTP GET
GN/BTP	GeoNetworking/Basic Transport Protocol
GN6	GeoNetworking-IPv6
HMAC	keyed-Hash Message Authentication Code
HTTP	Hyper Text Transfer Protocol
IETF	Internet Engineering Task Force
IP	Internet Protocol
ITS-AID	ITS Application ID
ITU-T	International Telecommunication Union - Telecommunication standardization sector
KDF	Key Derivation Function
LTE	Long Term Evolution (4G)
MSB	Most Significant Bit
MSEC	Multicast SECurity
OBD	On-Board Diagnosis
PA	Policy Authority
PDU	Protocol Data Unit
PII	Personally Identifiable Information
POP	Proof Of Possession
PSID	Provider Service Identifier
RCA	Root Certification Authority
RFC	Request For Comment
SA	Security Association
SCH	Service CHannel
SLAAC	StateLess Address Auto Configuration
SM	Security Management
SSP	Service Specific Permissions
TCP	Transmission Control Protocol
TLM	Trust List Manager
TLS	Transport Layer Security
URL	Uniform Resource Locator
V2I	Vehicle-to-Infrastructure
WLAN	Wireless Local Area Network
XOR	eXclusive OR function

3.4 Notation

The requirements identified in the present document include:

a) mandatory requirements strictly to be followed in order to conform to the present document. Such requirements are indicated by clauses without any additional marking;

b) requirements strictly to be followed if applicable to the type of ITS Station concerned.

Such requirements are indicated by clauses marked by "[CONDITIONAL]"; and where relevant is marked by an identifier of the type of ITS-S for which the clauses are applicable as follows:

- [Itss_WithPrivacy] is used to denote requirements applicable to ITS-S for which pseudonymity has to be assured and re-identification by the AA is not allowed. This includes for instance personal user vehicle ITS-S or personal ITS-S Portable.
- [Itss_NoPrivacy] is used to denote requirements applicable to ITS-S for which pseudonymity does not have to be assured and are allowed to be re-identified by the AA. This may be for instance fixed or mobile RSUs or special vehicles.

4 ITS authority hierarchy

Trust and privacy management requires secure distribution and maintenance (including revocation when applicable) of trust relationships, which may be enabled by specific security parameters that include enrolment credentials that provide 3rd party certificates of proof of identity or other attributes such as pseudonym certificates. Public key certificates and Public Key Infrastructure (PKI) are used to establish and maintain trust between the ITS-S and other ITS-S and authorities.

ETSI TS 102 731 [i.23] specifies requirements on security management services and security management roles such as EAs and AAs. The ITS security architecture is defined in ETSI TS 102 940 [5] and covers both the secured Communication Architecture, the architecture of the ITS-S Communication security system and the Security Management System architecture.

The present document assumes the definition of the security management entities specified in ETSI TS 102 940 [5] and the top-level entities for the management of multiple Root CAs collaborating within a single Trust Model.

5 Privacy in ITS

ISO/IEC 15408-2 [i.1] identifies 4 key attributes that relate to privacy:

- anonymity;
- pseudonymity;
- unlinkability; and
- unobservability.

Anonymity alone is insufficient for protection of an ITS user's privacy and unsuitable as a solution for ITS, as one of the main requirements of ITS is that the ITS-S should be observable in order to provide improved safety. Consequently, pseudonymity and unlinkability offer the appropriate protection of the privacy of a sender of basic ITS safety messages (CAM and DENM). Pseudonymity ensures that an ITS-S may use a resource or service without disclosing its identity but can still be accountable for that use [i.1]. Unlinkability ensures that an ITS-S may make multiple uses of resources or services without others being able to link them together [i.1].

Pseudonymity shall be provided by using temporary identifiers in ITS safety messages, and never transmitting the station's canonical identifier in communications between ITS stations. Unlinkability can be achieved by limiting the amount of detailed immutable (or slowly changing) information carried in the ITS safety message, thus preventing the possible association of transmissions from the same vehicle over a long time period (such as two similar transmissions broadcast on different days).

ITS Privacy is provided in two dimensions:

i) privacy of ITS registration and authorization tickets provisioning:

   - ensured by permitting knowledge of the canonical identifier of an ITS-S to only a limited number of authorities (EAs);

   - provided by the separation of the duties and roles of PKI authorities into an entity verifying the canonical identifier known as the Enrolment Authority (EA) and an entity responsible for authorizing and managing services known as the Authorization Authority (AA);

ii) privacy of communications between ITS-Ss.

Separation of duties for enrolment (identification and authentication) and for authorization has been shown in ETSI TS 102 731 [i.23] as an essential component of privacy management and provides protection against attacks on a user's privacy. However, it is possible for the EA role to be delegated to the manufacturer and for the EA and AA roles to be assumed by a single authority.

When the same operational authority manages both the EA and AA, it shall guarantee privacy of requesting ITS-S i.e. providing all the technical and organizational measures to ensure that ITS identity information held by the EA is kept separately to avoid re-identification of pseudonym certificates (ATs).

When dedicated authorities are used only for certificates provisioning to ITS-S which do not have privacy requirements such as Road-Side Units, the EA and AA may not provide technical and operational separation.

6 Trust and privacy management

6.1 ITS-S Security Lifecycle

6.1.1 ITS-S Life-cycle management

The ITS-S Security Lifecycle includes the following stages (see Figure 1):

- initial ITS-S configuration during manufacture;
- enrolment;
- authorization;
- operation and maintenance;
- end of life.

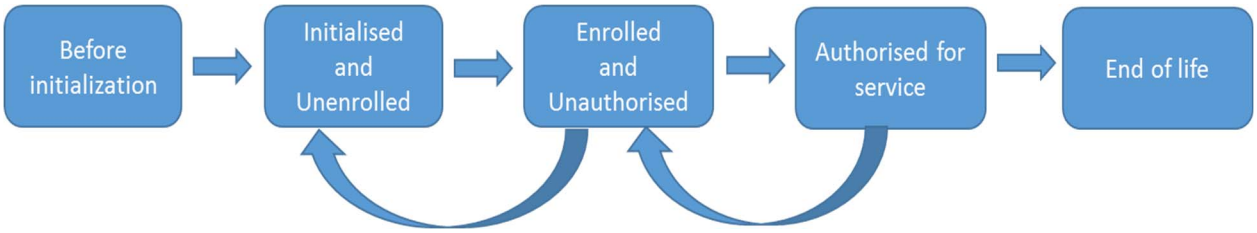


Figure 1: ITS Station Security Life Cycle

6.1.2 Manufacture

As part of the ITS-S manufacturing process, the following information elements associated with the identity of the station shall be established within the ITS-S itself and within the Enrolment Authority (EA):

- In the ITS-S, the following information elements shall be established using a physically secure process. The specification of this physically secure process is out of scope for the present document:
  - a canonical identifier which is globally unique (see note 1);
  - contact information for the EA and AA which will issue certificates for the ITS-S:
    - network address;
    - public key certificate;
  - the set of current known trusted AA certificates which the ITS-S may use to trust communications from other ITS-S;
  - when using the process specified in clause 6.2.3.2 for the initial enrolment: a public/private key pair for cryptographic purposes (canonical key pair); and
  - the trust anchor (Root CA) public key certificate and the DC network address;
  - in case of a multiple root CAs architecture as specified in ETSI TS 102 940 [5], the TLM public key certificate and the CPOC network address.

NOTE 1: The management of the canonical identifier and the means to guarantee uniqueness are not addressed in the present document.

- In the EA, the following three items of information shall be established, all associated with each other (see note 2):
  - the permanent canonical identifier of the ITS-S;
  - the profile information for the ITS-S that may contain an initial list of maximum appPermissions (ITS-AIDs with SSP), region restrictions and assurance level which may be modified over time;
  - when using the process specified in clause 6.2.3.2 for the initial enrolment: the public key from the key pair belonging to the ITS-S (canonical public key).

NOTE 2: The process for establishing this information within the ITS-S and the EA is beyond the scope of the present document.

NOTE 3: The EA certificate may contain `certIssuePermissions` with type `enrol` limiting the maximum permissions (ITS-AIDs with SSP) assigned to the ITS-S in the profile information. In this case, the Root CA (issuer of the EA certificate) contains at least these `certIssuePermissions` with type `enrol` in its certIssuePermissions.

6.1.3 Enrolment

6.1.3.0 General Considerations

There are two types of enrolment certificate that can be used to authenticate requests for authorization tickets:

- ETSI TS 102 941 enrolment credentials following the specification in the present document. The provisioning of this type is described in the present document.
- X.509 enrolment credentials following the X.509 format which is specified in IETF RFC 5280 [21] and IETF RFC 5480 [22]. The provisioning of this type is out-of-scope of the present document since mechanisms already exist. The present document will explicitly refer to X.509 enrolment credentials when this type is meant.

The following process applies to the provisioning of ETSI TS 102 941 enrolment credentials.

The ITS-S requests its enrolment certificate from the EA (see clause 6.2.3.2).

When an end entity applies for an enrolment certificate, it may indicate that it is entitled to the certificate *directly* or *indirectly*. Compare with section 4.1.4.2 of IEEE 1609.2.1 [24].

In the *indirect* initial enrolment case, the Enrolment Authority (EA) is given assurance that the end entity is entitled to the enrolment certificate by means outside the scope of the enrolment certificate request. For example, the enrolment request could happen in an environment that is trusted by the EA and the request could be transmitted over a secure connection.

In the *direct* initial enrolment case, before enrolment happens, the end entity generates a keypair known as the canonical keypair and is assigned (or generates) a globally unique identifier known as the canonical identity (see clause 6.1.2).

The state transitions for enrolment are shown in Figure 2.

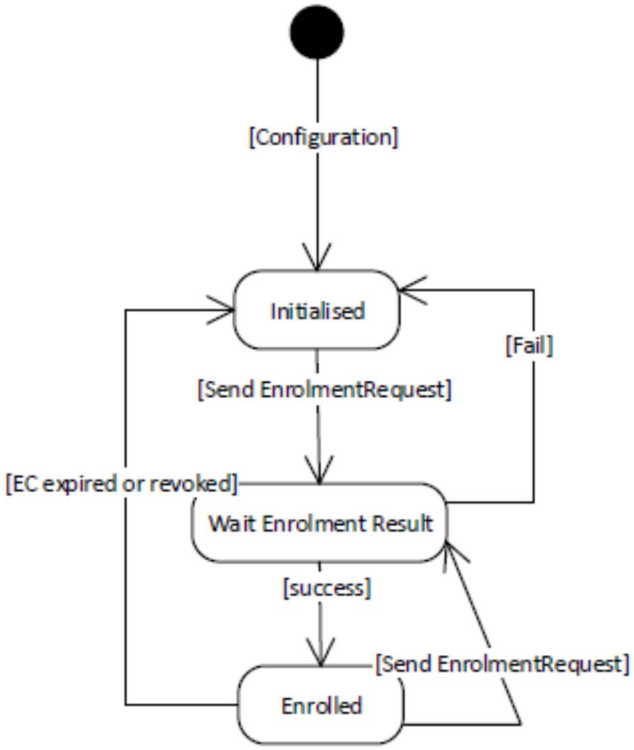


Figure 2: Simplified state machine for the enrolment process

After a successful enrolment process, the ITS-S shall possess an enrolment credential that shall be used in subsequent authorization requests.

For renewing the Enrolment Certificate at the EA, the ITS-S shall send an EnrolmentRequest signed by the previous valid enrolment credential issued by this EA.

6.1.3.1 Enrolment Credential Profile

6.1.3.1.0 Introduction

The profile for the ETSI enrolment credential is defined in ETSI TS 103 097 [3] along with the ETSI ITS security header and certificate format.

Since the format of the X.509 enrolment credential is not defined in ETSI TS 103 097 [3] but used for trust and privacy management in the present document, the profile for X.509 enrolment credentials is specified in the present document.

The X.509 enrolment credential shall apply the following conditions. Additional conditions may be required by the individual X.509 PKI in alignment with the Enrolment Authority.

6.1.3.1.1 Generic Requirements

The certificate shall follow the IETF PKIX profile as specified in IETF RFC 5280 [21]. When ECDSA keys are used, the encoding shall follow the specification in IETF RFC 5480 [22]. The cryptographic algorithms shall be aligned with ETSI TS 103 097 [3].

6.1.3.1.2 Version

The version shall be V3 (defined by the integer value 2).

6.1.3.1.3 Issuer

The identity of the issuer shall contain at least the following attributes:

- countryName;
- organizationName; and
- commonName.

Each attribute shall be limited to a single instance of the attribute. Additional attributes may be present.

The countryName attribute shall specify the country in which the issuer of the certificate is established.

The organizationName attribute shall contain the full registered name of the certificate issuing organization.

The commonName attribute value shall contain a name commonly used by the subject to represent itself. This name need not be an exact match of the fully registered organization name.

6.1.3.1.4 Subject

The subject field shall include at least the following attributes:

- countryName;
- organizationName; and
- commonName.

Only one instance of each of these attributes shall be present. Additional attributes may be present.

The countryName attribute shall specify the country in which the ITS-S is established.

The organizationName attribute shall contain the full registered name of the ITS-S.

The commonName attribute value shall contain a name commonly used by the subject to represent itself and may correspond to the canonical ID.

6.1.3.1.5 Authority key identifier extension

The authority key identifier extension shall be present, containing a key identifier for the issuing CA's public key.

6.1.3.1.6 Key usage extension

The key usage extension shall be present and shall contain the key usage settings specifying at least non-repudiation (bit 1) and digital signature (bit 0).

6.1.3.1.7 Certificate policies extension

This extension should not be marked critical. The certificate policies extension shall be present and shall contain the identifier of at least one certificate policy which reflects the practices and procedures undertaken by the CA.

6.1.3.1.8 CRL distribution points extension

If CRL is supported by the issuing CA, the CRL distribution point extension shall be present in certificates.

If the certificate does not include any access location of an OCSP responder, then the certificate shall include a CRL distribution point extension.

When present, the CRL distribution point extension shall include at least one reference to a publicly available CRL.

At least one of the present references shall use either http (http://) or ldap (ldap://) scheme.

The extension shall not be marked critical.

6.1.3.1.9 Authority Information Access extension

The Authority Information Access extension shall be present.

When OCSP is supported by the issuing CA, the Authority Information Access extension shall include an accessMethod OID, id-ad-ocsp, with an accessLocation value specifying at least one access location of an OCSP responder authoritative to provide certificate status information for the present certificate. In such case, at least one access location shall specify either the http (http://)] or https (https://) scheme. Such access location shall reference a publicly available OCSP responder, which accepts unsigned and unauthenticated status requests.

A reference to at least one OCSP responder shall be present if the certificate does not include any CRL distribution point extension.

6.1.4 Authorization

Having received the enrolment credentials (i.e. in state "Enrolled" as shown in Figure 2), the ITS-S is able to request its authorization ticket(s) from the AA (see clause 6.2.3.3).

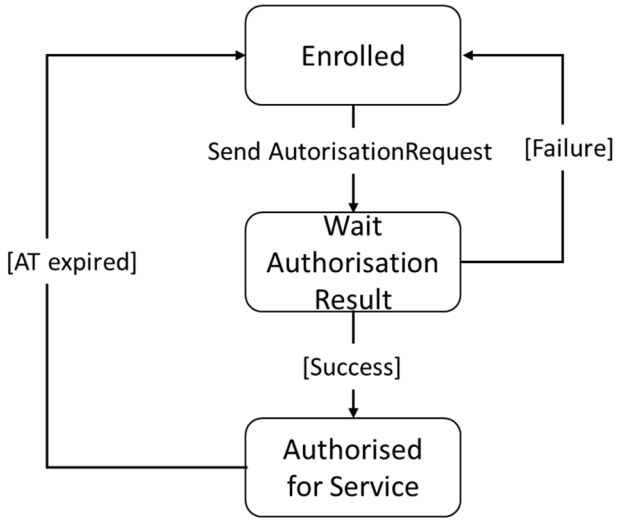


Figure 3: Simplified state machine for the authorization process

NOTE 1: This state machine only considers one instance of Authorization Request for one service (or class of services). Eventually, an ITS-S may perform several Authorization Requests to fill a pool of ATs stored in ITS-S memory (depending of the policy). The management of the pool of ATs within an ITS-S is out of the scope of the present document.

When in the state "Authorized for service" the ITS-S has a set of authorization tickets to allow signed transmission of messages to any other ITS-S that do not reveal the canonical identity nor the enrolment credential of the transmitting ITS-S.

NOTE 2: It is assumed that the ITS service requesting the use of a secure message transfer service only reveals PII in the payload if the release of that PII has been consented by the sending party.

NOTE 3: The ITS-S in state Authorized for Service may still have the possibility to obtain or update its pool of Authorization Tickets by sending Authorization requests (not representing on the Figure 3).

When the complete set of authorization tickets is exhausted, the ITS-S cannot sign transmission of messages to others ITS-S and is back to the state Enrolled.

NOTE 4: In this state diagram, it is assumed that revocation of authorization tickets is not possible as passive revocation is preferred (the ITS-S receives ATs of limited validity period and of limited allowed preloading period, renewing them frequently so that compromised ITS-S can be evicted from the ITS network by not reissuing them new ATs).

6.1.5 Maintenance

If an EA or AA is added to or removed from the system, the Root CA shall inform enrolled ITS-Ss of this change.

When multiple Root CAs are used in the same Trust Domain (as specified in ETSI TS 102 940 [5]), the trust relationship between the different PKIs may be managed by a Trusted Third Party (Trust List Manager). If a Root CA is added or removed from the system, the TLM should inform enrolled ITS-Ss of this change.

The process for updating the trust information lists such as the CTL and the CRL and for publishing these lists by the associated trust authority is specified in clause 6.3 and include different possible methods for updating the enrolled ITS-Ss:

- requesting CRL and CTL from the distribution centre associated to the root CA;
- sending a trust information list (CRL or CTL) across a wireless interface e.g. using a RSU able to transmit the CRL/CTL on ITS G5; or
- providing information to a trusted maintenance entity to enable it to update an individual ITS-S in a controlled environment.

6.1.6 End of life

In case of the device's end of life or following a compromise (revocation decided by its issuing EA), the ITS Station should be revoked and removed from operation in the ITS G5 communication network by means of a passive revocation mechanism, i.e. the EA shall reject the authorization of all the next Authorization Ticket requests for this specific ITS-S.

6.2 Public Key Infrastructure

6.2.0 General

6.2.0.1 Messages format

All the Security Management messages (SM_PDU) specified in the present document shall follow the message format shown in Figure 5.

Each SM-PDU message shall be encoded into an `EtsiTs103097Data-Encrypted, EtsiTs103097Data-Signed` or an `EtsiTs103097Data-SignedAndEncrypted` structure, depending on the specific message. This outermost structure shall contain an `EtsiTS102941Data` which in turn contains the content of the specific message.

Figure 4 shows an example of the use of above structures to provide enrolment/authorization requests and responses between an ITS-S and a Certification Authority. The same diagram applies for authorization validation requests and responses exchanged between Certification Authorities (EA and AA) as specified in clause 6.2.3.4.

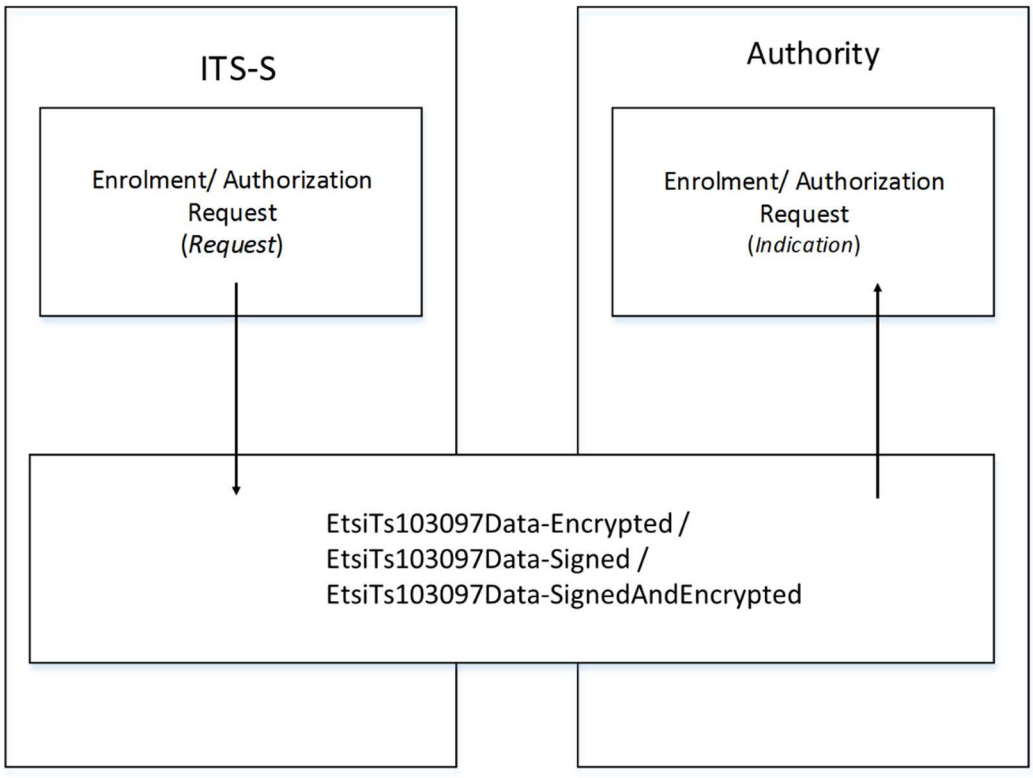


Figure 4: Illustration of using Security Management PDU structure

This outermost data structure `EtsiTs103097Data-Encrypted, EtsiTs103097Data-Signed` or `EtsiTs103097Data-SignedAndEncrypted` structure shall encapsulate an `EtsiTS102941Data` as shown in Figure 5. Specification of all containers and enclosed data structures are given in annex A.

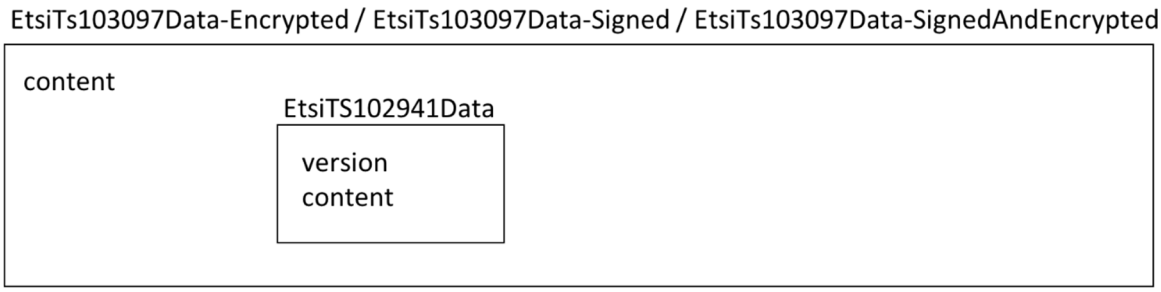


Figure 5: Generic Security Management PDU structure

Each of the SM_PDU is containing an `EtsiTS102941Data` as specified in clause A.2.1:

```
EtsiTS102941Data::= SEQUENCE {
  version Version (v1),
  content EtsiTS102941DataContent
  }
EtsiTS102941DataContent ::= CHOICE {
…}
```

In the present document, the `version` of `EtsiTS102941Data` structure shall be set to version v1 (integer value 1).

Data structures in the present document are defined using Abstract Syntax Notation 1 (ASN.1) and shall be encoded using the Canonical Octet Encoding Rules (COER) as defined in Recommendation ITU-T X.696 [7].

The ASN.1 representation of Security Management PDUs shall be as specified in the annex A of the present document.

6.2.0.2 Signed and encrypted data structures

The present document assumes the definition of the data structures specified in ETSI TS 103 097 [3].

Especially the following ETSI TS 103 097 [3] data structures shall be used for encrypted/signed messages specified in the present document:

- `EtsiTs103097Data-Signed;`
- `EtsiTs103097Data-Encrypted;`
- `EtsiTs103097Data-SignedAndEncrypted;`
- `EtsiTs103097Data-SignedExternalPayload.`

All signed data structures contain a `headerinfo` which itself includes a PSID/ ITS-AID. This PSID/ITS-AID is mandatory and shall be used for certificate management with value as assigned in ETSI TS 102 965 [19].

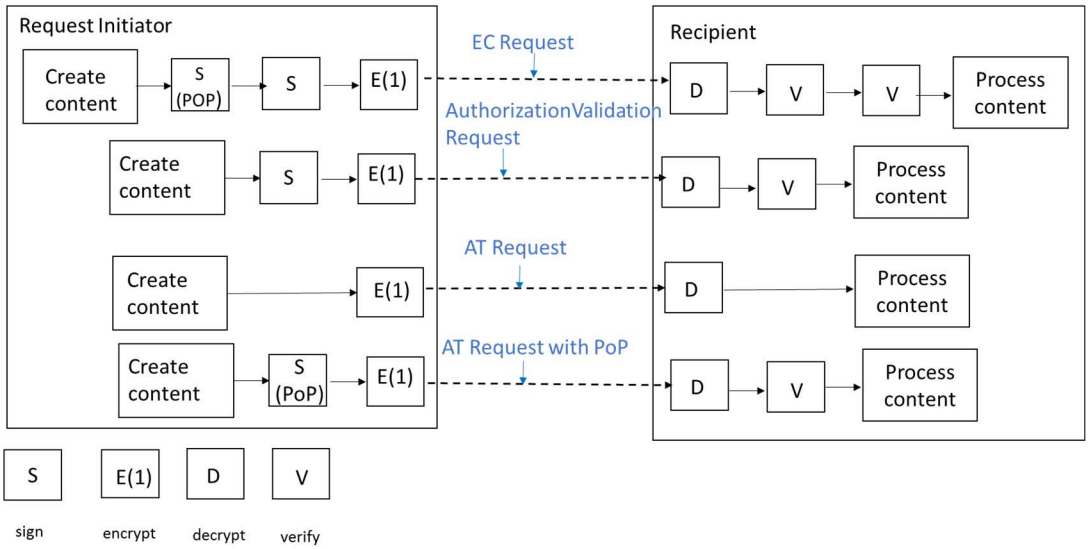
For all messages that are using the `EtsiTs103097Data-SignedAndEncrypted` structure as outermost message format, the `EtsiTs1030971Data-SignedAndEncrypted` structure shall be built using the security profile for signed and encrypted messages defined in ETSI TS 103 097 [3] and shall be composed of an `EtsiTs103097Data-Encrypted` structure containing an encrypted `EtsiTs103097Data-Signed` structure, containing a `EtsiTs102941` Data structure, containing a version and an `EtsiTs102941DataContent` structure corresponding to the specific message (see clauses 6.2.3.2 to 6.2.3.4).

For all request and responses messages used for the provisioning of EC or ATs to an ITS-S, the following generic request and responses messages are used as depicted in Figure 6 and Figure 7.

For each generation of a REQUEST message, the request initiator shall generate a new AES symmetric key k which is used to encrypt the inner message as shown in Figure 6.

The `EtsiTs103097Data-Encrypted` structure shall be used to encapsulate all this message data using encryption option 1: encryption is done using the recipient public encryption key corresponding to the recipient's certificate. The field recipients shall contain **one single** RecipientInfo of type certRecipInfo.

The request initiator shall store the encryption symmetric key (k) in memory until it receives and processes the corresponding RESPONSE message as this key is to be used to decrypt the response (session encryption key). See clause 7.3.

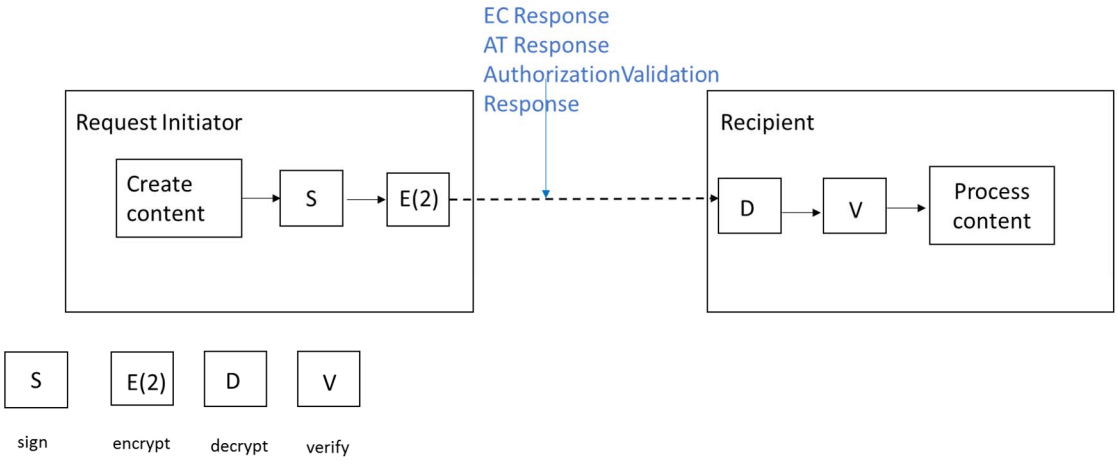


E(1): use EtsiTs103097Data-Encrypted with option 1 (using the recipient public encryption key corresponding to the recipient's certificate): the field recipients shall contain one single RecipientInfo of type certRecipInfo

NOTE: The AT Request depicted in Figure 6 uses different authentication mechanisms. See clause 6.2.3.3.1 for details.

Figure 6: Generic REQUEST message

For generating the RESPONSE message, the Recipient of the request shall use an outermost `EtsiTs103097Data-Encrypted` structure that encapsulates the response message as shown in Figure 7 using encryption option 2: the AES symmetric key used to encrypt the corresponding request is reused to encrypt the response, with the pskRecipInfo option in the RecipientInfo that indicates the use of a pre-shared symmetric key.



E(2): use EtsiTs103097Data-Encrypted with option 2. The key used to encrypt the corresponding request is reused to encrypt the response using one single RecipientInfo of type pskRecipInfo.

Figure 7: Generic RESPONSE message

An algorithm for encryption of a message from a sender to a receiver (Recipient) is given in annex E.

6.2.1 CA certificate request

The CACertificateRequest message defines a standalone certificate request, which shall be used to transport SubCA (i.e. EA or AA) certificate request to the RCA (across the interface at reference point S_9 or S_{10} as specified in ETSI TS 102 940 [5]).

For the initial application of a SubCA to the RCA, the SubCA needs to submit an application form containing organization identity and other registration information specified in the respective policy. The details of this application form and process are out of the scope of the present document.

The SubCA shall transfer the signed certificate request (`CACertificateRequest`) by an off-band mechanism to the RCA entity: for initial application of the subCA, the subCA shall use a separate communication channel with the RCA (electronic communication means) other than the channel used for transmitting the application form and documents to the RCA. The application form should include the digital fingerprint of the `CACertificateRequest` in printable format. For rekeying, an application form is not needed because the RCA has a trust relation after the initial request.

NOTE 1: The digital fingerprint of the CACertificateRequest is computed using an ETSI TS 103 097 [3] approved hash algorithm.

For the initial application of a Sub CA to the RCA for issuance of its certificate, the SubCA shall generate its key pairs and the `CACertificateRequest` shall be signed with the private key corresponding to the verification public key provided by the Sub-CA for certification, to prove possession of the private key.

After approval of the application form and associated documents supplied by the SubCA and validation of the integrity and authenticity of the certificate request transmitted by the SubCA, the RCA shall generate the certificate of the SubCA, which is provided as a response to the `CACertificateRequest:` the certificate issued by the RCA to the SubCA shall follow the requirements of CA certificate as defined in ETSI TS 103 097 [3].

For the subsequent applications of the SubCA for requesting new certificate to the RCA, the SubCA shall generate its new key pairs. Then the CA certificate request shall be signed with the new private key corresponding to the verification public key (inner signature) and the whole request shall be signed with the current valid private key (outer signature) to ensure the integrity and authenticity of the request. If the current private key has reached its end of validity period or is revoked, the SubCA shall restart the initial certificate application process.

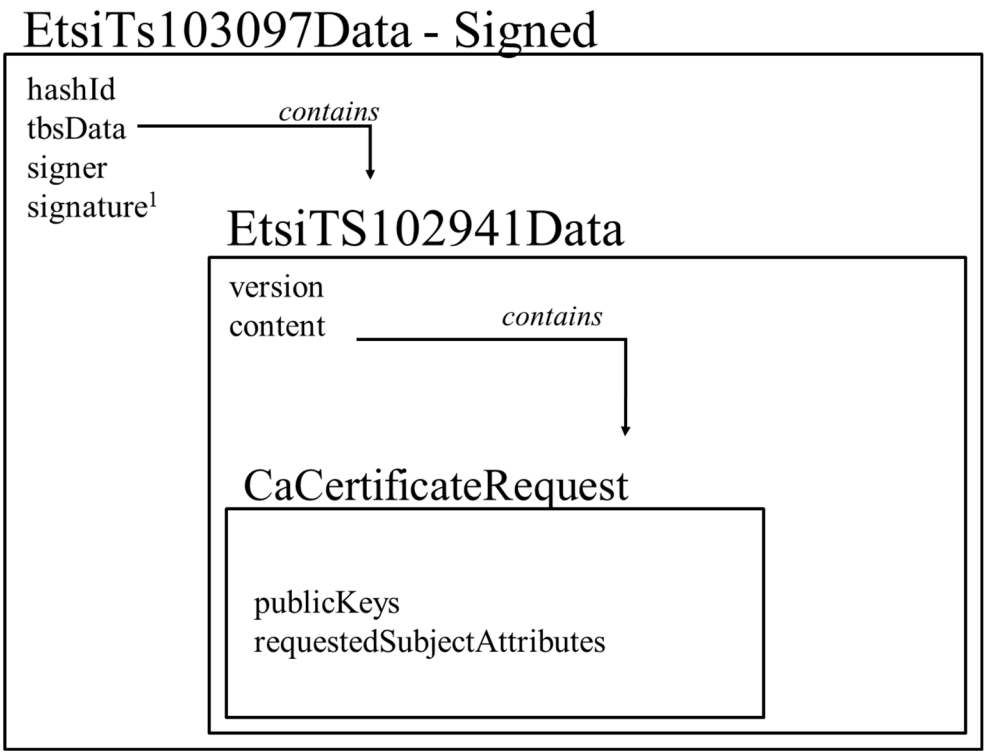
The content of the `CACertificateRequest` message shall be as described in Figure 8.

The specification of the `CACertificateRequest` message using ASN.1 [6], [7] shall be as specified in clause A.2.6.

For the initial application to the RCA, an EA or AA shall follow this process to create a `CaCertificateRequestMessage`:

- An ECC private key is randomly generated, the corresponding public key (`verificationKey`) is provided to be included in the `CaCertificateRequest`.
- An ECC encryption private key is randomly generated, the corresponding public key (`encryptionKey`) is provided to be included in the `CACertificateRequest`.
- An `EtsiTs102941Data` structure is built, containing:
  - `version` is set to v1 (integer value set to 1);
  - a `CaCertificateRequest` is built with:
    - publicKeys shall contain verification_key and encryption_key;
    - requestedSubjectAttributes shall contain the requested certificates attributes as specified in ETSI TS 103 097 [3], clause 7.2.4.
- An `EtsiTs103097Data-Signed` structure is built, containing: hashId, tbsData, signer and signature:
  - the `hashId` shall indicate the hash algorithm to be used as specified in ETSI TS 103 097 [3];

- in `tbsData`:
  - the `payload` shall contain the previous `EtsiTs102941Data` structure;
  - in the `headerInfo`:
    - the `psid` shall be set to "secured certificate request" as assigned in ETSI TS 102 965 [19];
    - the `generationTime` shall be present;
    - all other components of the component `tbsdata.headerInfo` not used and absent;
- the `signer` is set to 'self';
- the `signature` over the `tbsData` computed using the private key corresponding to the new `verificationKey` to be certified (i.e. the request is self-signed).



NOTE: [1] Signature computed using the private key corresponding to the verification public key to be certified.

Figure 8: CA Certificate Request message for initial creation

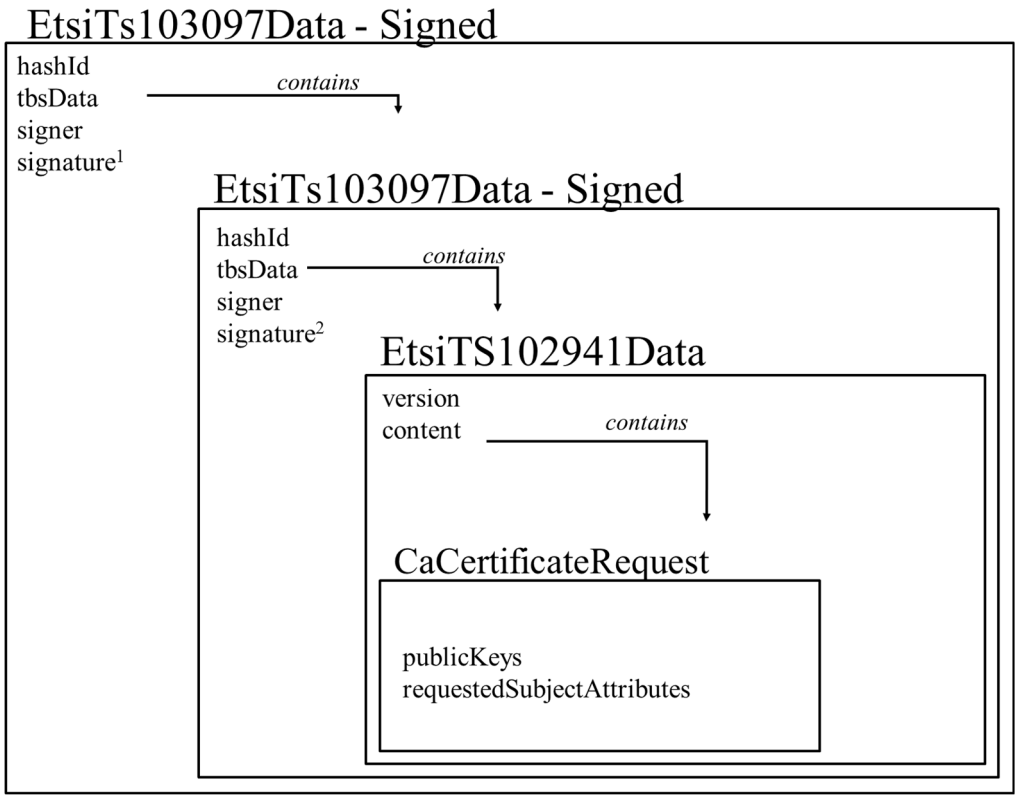
For the re-keying application to the RCA, an EA or AA shall follow this process to create a `CaCertificateRekeyingMessage:`

- An `EtsiTs103097Data-Signed` structure is built, containing: `hashId`, `tbsData, signer` and `signature`:
  - the `hashId` shall indicate the hash algorithm to be used as specified in ETSI TS 103 097 [3];
  - in the `tbsData`:
    - the `payload` shall contain the previous `CaCertificateRequestMessage` structure;
    - in the `headerInfo`:
      - the `psid` shall be set "secured certificate request" as assigned in ETSI TS 102 965 [19];
      - the `generationTime` shall be present;

- all other components of the component `tbsdata.headerInfo` not used and absent;

- the `signer` declared as a `digest`, containing the hashedId8 of the EA or AA certificate;

- the `signature` over `tbsData` computed using the currently valid private key corresponding to the AA or EA certificate (outer signature).



NOTE: [1] Signature computed using the currently valid private key corresponding to the AA or EA certificate.
[2] Signature computed using the private key corresponding to the verification public key to be certified.

Figure 9: CA certificate Request message for certificate re-keying

NOTE 2: If the SubCA certificate contains an encryption public key, a proof of possession for this private key may be provided by the requesting SubCA. The method for establishing this proof of possession between the SubCA and the RCA is beyond the scope of the present document.

6.2.2 Enrolment/Authorization assumption and requirements

The present document assumes the ITS security reference model that is described in ETSI TS 102 940 [5].

For obtaining security credentials from the PKI, the ITS station has to set up a communication with the Certificate Authority (EA or AA). The ITS station may use different communication types for the provisioning of certificates, such as for instance:

- An ITS G5 communication via a roadside station.
- A WLAN consumer network using IEEE 802.11 [i.22] protocol (via a public or private hotspot or a home network).
- A Cellular network link (3G, 4G or LTE).
- A wired or wireless connection at EV Charging station.
- Using the Vehicle On-Board Diagnostic (OBD) port and a diagnostic system at the Service Garage or inspection workshop.

Figure 10 and Figure 11 present two possible options for ITS-S communication with the PKI, in order to support the security management services as specified in ETSI TS 102 940 [5] and shown in clause 4 above.

This functional model extends the ITS Communication security model specified in ETSI TS 102 940 [5] with the different communication paths. It introduces functional entities as defined in Table 1 and specifies the communication paths needed to support the ITS-S communication via a cellular network (Figure 10) or via an ITS G5 access network to the ITS infrastructure (Figure 11).

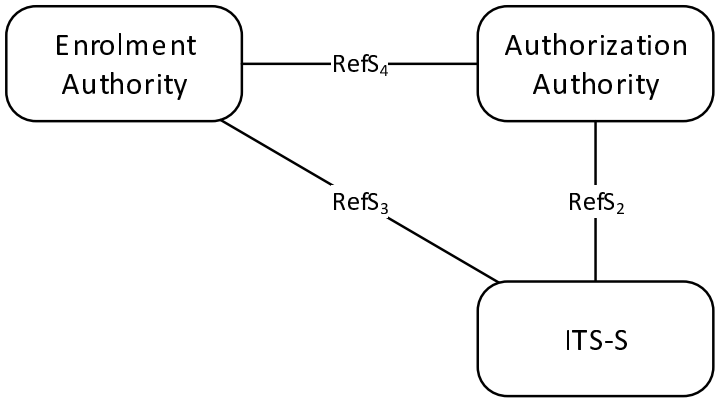


Figure 10: Communication with PKI using a cellular network connection

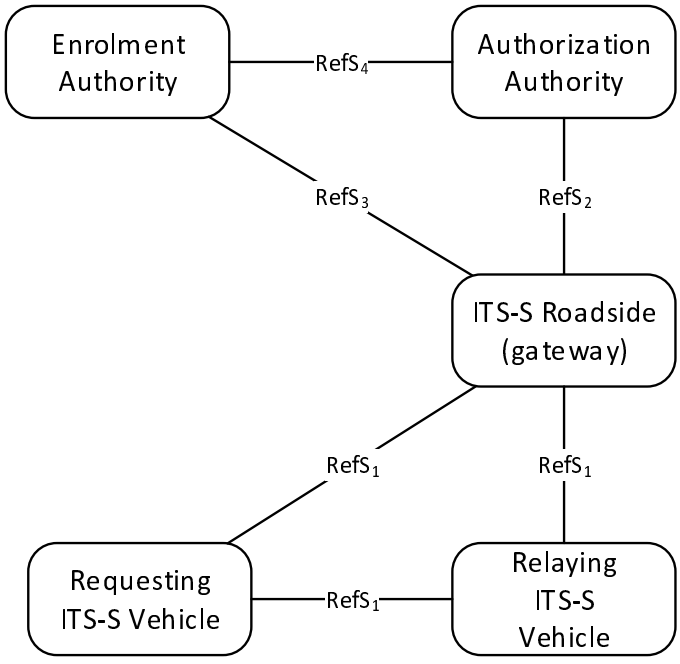


Figure 11: Communication with PKI using a V2I connection

In Figure 11, the model specified in ETSI TS 102 940 [5] is refined by considering one ITS-S sending the certificate request message, one roadside ITS-S for relaying the message via the infrastructure network to the recipient Certificate Authority and the receiving Certificate Authority (EA or AA). The certificate request message shall be sent in one-hop or multi-hops using the GeoNetworking protocol specified in ETSI EN 302 636-4-1 [18].

Table 1: Functional element roles

Functional element	Role
Enrolment Authority	See definition of functional elements, as specified in ETSI TS 102 940 [5]
Authorization Authority	
Requesting ITS-S	
Relaying ITS-S	
ITS-S Roadside Gateway	Receives broadcast messages from mobile ITS-S and relays certificate requests and responses to/from the Receiving Certificate Authority within the PKI

The model depicted in Figure 11 assumes that a mobile ITS-S has the capabilities to transmit security management messages such as defined in clauses 6.2.3.2, 6.2.3.3 and 6.2.3.4 through the ITS G5 communication interface (Reference Point S_1). For that scenario, a communication bandwidth should be made available to the requesting ITS-S on an allocated G5 channel for security management purpose (e.g. CCH, SCH1 or SCH2).

The present document specifies messages format for certificate provisioning that is agnostic to the underlying communication path and communication media.

The term message refers to the Security Management PDUs which are processed by the Security Management Functional entity specified in ETSI TS 102 940 [5], clause 5. There is no application payload in these messages provided by the ITS Applications layer. The generation and processing of Security Management Messages in the ITS-S should be executed in a trusted software platform environment.

Several communication profiles are possible as described in annex C.

For all the communication profiles which are using IP protocol, HTTP/1.1 over TCP/IP shall be used in end-to-end communication paths, over the reference points S_2 and S_3. (directly or after forwarding via reference points S_1). No supplementary cryptographic layer such as TLS is required.

The term message refers to the Security Management PDUs which are processed by the Security Management Functional entity specified in ETSI TS 102 940 [5], clause 5. There is no application payload in these messages provided by the ITS Applications layer. The generation and processing of Security Management Messages in the ITS-S shall be executed in a trusted software platform environment.

NOTE 1: The present document does not specify the interface between Security Entity and the ITS-S communication layers and does not specify the interface between the Security Entity and the Facilities layer, i.e. mechanism for transferring Security Management PDUs via the SF-SAP. It does not specify the way the communication profile parameters are provided to the ITS-S communication stacks.

If an ITS station needs to provide pseudonym change management for privacy protection (e.g. vehicle ITS-S or personal ITS-S Portable), the following requirements shall be satisfied:

- [Itss_WithPrivacy] if the requesting ITS-S uses an Ipv6 communication link to request a CCMS service, the ITS-S shall support temporary pseudonyms instead of permanent identifiers such as defined in ETSI TS 102 731 [i.23] and further specified in ETSI TS 102 940 [5] and shall use automatically configured Ipv6 address using Stateless Address Autoconfiguration (SLAAC) as specified in IETF RFC 4862 [15].

- [Itss_WithPrivacy] upon notification of an ID Change, the ITS-S Ipv6 layer shall modify the MAC address of each virtual interface which implies a change in the Ipv6 addresses associated to the virtual interfaces.

- [Itss_WithPrivacy] in case the ITS-S communication profile used is based on Ipv6 over GeoNetworking (GN6), the ITS-S shall provide support for pseudonym change as specified in ETSI TS 103 636-6-1 [16], clause 11. This function enables change of the GN_Addr and the change of MAC address implies creation of a new temporary Ipv6 address for the ITS-S originating the connection with the CCMS service. For security protection of Ipv6 over GeoNetworking traffic, the ITS-S should protect integrity & authenticity of packets by signature as presented in ETSI EN 103 636-6-1 [16], clause G.1.

- [Itss_WithPrivacy] the ITS-S security entity shall perform an ID change (as specified in ETSI TS 102 940 [5]) each time before sending an AT request to the Authorization Authority (i.e. change the used Ipv6 address, MAC address, etc.) if no previous Authorization request is waiting for the response. Otherwise the ITS-S shall block ID Change until it receives the corresponding response from the AA or after a maximum time limit.

NOTE 2: The security entity uses the ID Change service in order to force ITS-S' IPv6 address change. To this end, it is not mandatory to change the AT prior to use the ID Change service. When no AT change occurs, the HashedId8 passed with the ID_Change should contain a random value (SN-IDCHANGE-EVENT as specified in ETSI TS 102 723-8 [i.13]).

6.2.3 Message Sequences

6.2.3.1 Introduction

The overall ITS-S initialization sequence to achieve ITS secured message transfer on ITS G5 is given in Figure 12. The messages are specified in details in clauses 6.2.3.2, 6.2.3.3 and 6.2.3.4.

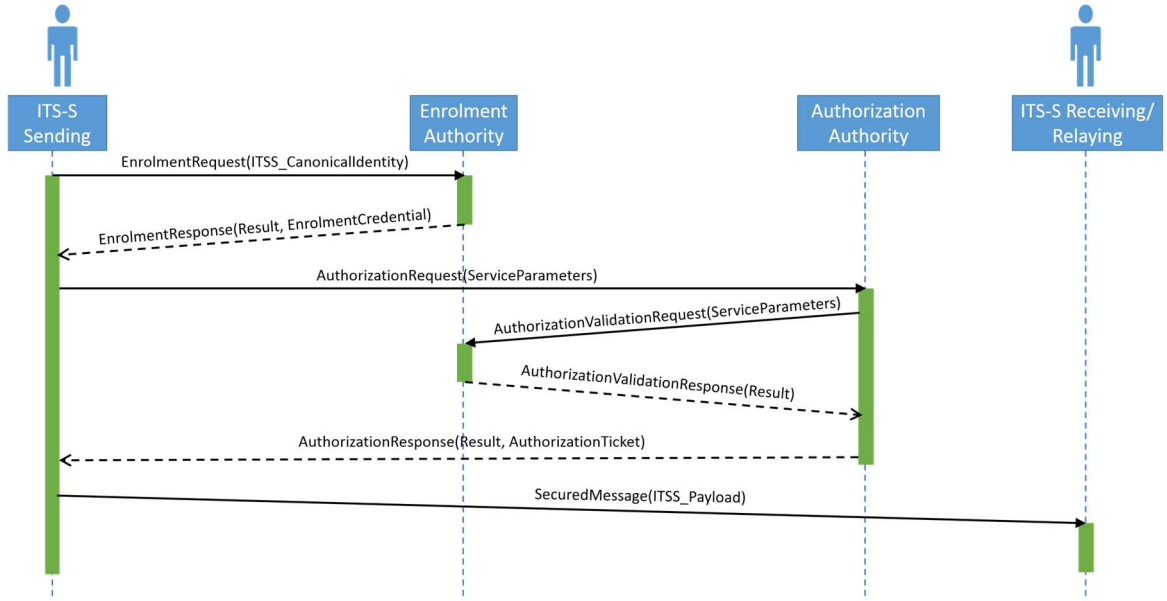


Figure 12: Sequence to achieve signed message transfer between ITS-Ss

Instead of the depicted workflow for the Authorization Ticket provisioning, a second variant, called Butterfly key provisioning, exists which can be used as an alternative. An implementation shall support one of the two options. Since this only applies to the AT provisioning process, the interoperability between vehicles is ensured.

6.2.3.2 Enrolment Management

6.2.3.2.0 Overview

The Enrolment Request message shall be sent by an ITS-S to the Enrolment Authority (EA) across the interface at reference point S_3 (see Figure 8 in ETSI TS 102 940 [5]) to request an enrolment certificate to be used in a subsequent authorization request. Figure 13 shows an example of a message sequence for a successful or unsuccessful enrolment request.

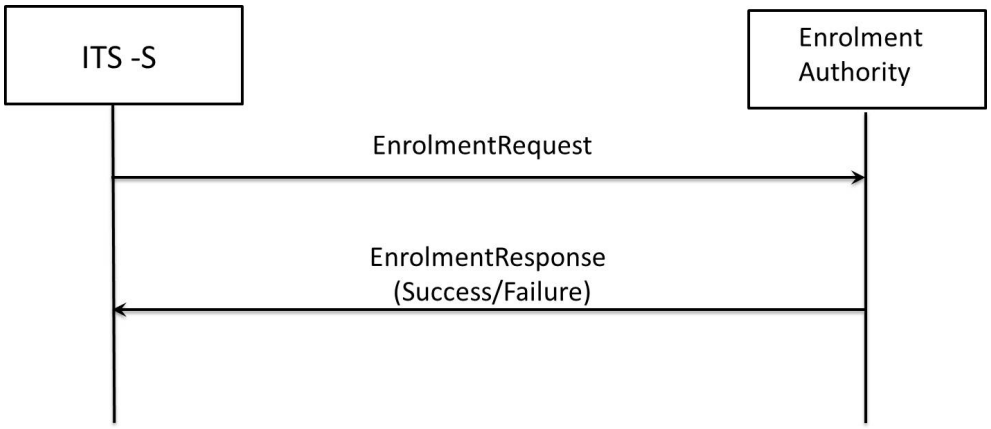


Figure 13: Message sequence for enrolment request and response

6.2.3.2.1 Enrolment request

The following functional requirements are defined on the state machine of Figure 2 (sender ITS-S for the enrolment process):

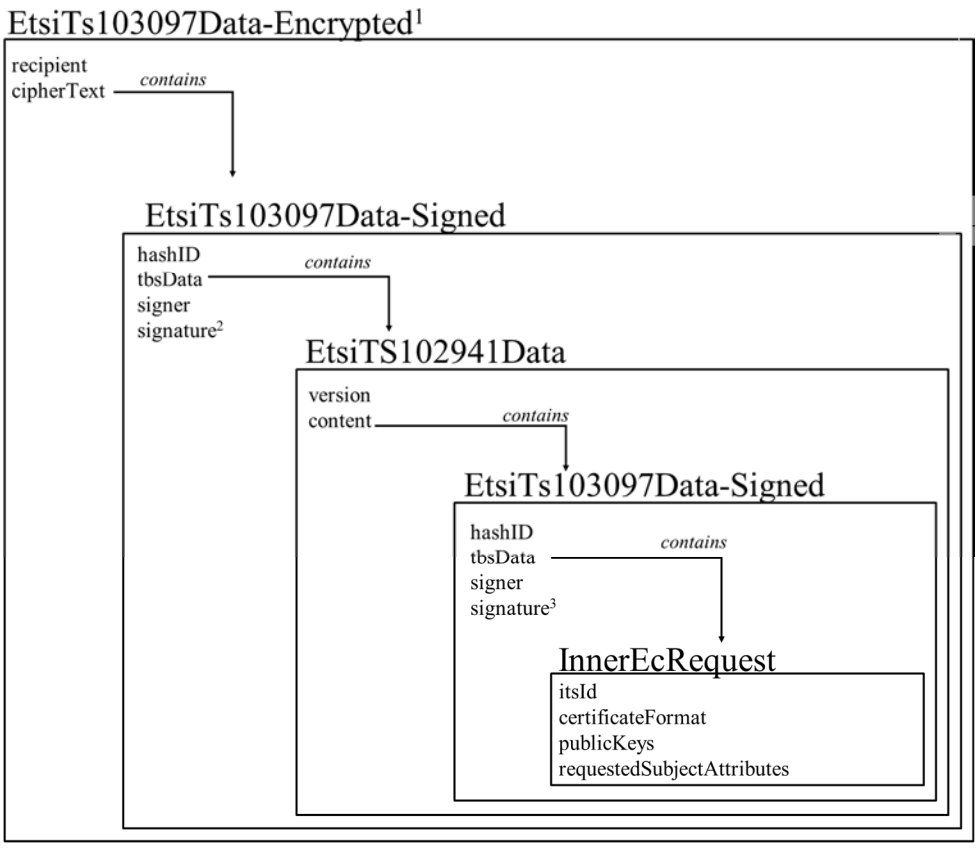
- The EnrolmentRequest message shall be encrypted using a ETSI TS 103 097 [3] approved encryption algorithm and the public key provided by the enrolment authority.
- For each enrolment request, the ITS-S shall generate a new verification key pair corresponding to an approved signature algorithm as specified in ETSI TS 103 097 [3].
- The contents of the EnrolmentRequest message shall be as described in Figure 14. The specification of the ITS-S EnrolmentRequest message using ASN.1 [6], [7] shall be as specified in clause A.2.

To create an enrolment request, an ITS-S shall follow this process:

- An ECC private key is randomly generated, the corresponding public key (verificationKey) is provided to be included in the EC.
- An `InnerECRequest` structure is built, containing:
  - the identifier of the requesting ITS-S (`itsId`): this identifier shall be set to the canonical identifier of the ITS-S for the initial enrolment with the recipient EA. For a re-enrolment of the ITS-S, the requesting ITS-S shall use the identifier of its current valid Enrolment Credential (EC identifier) which is computed as the HashedID8 of the Enrolment Credential (as specified in ETSI TS 103 097 [3]);
  - the `certificateFormat` which specifies the version used for the certificate format specification. In the present document, the certificate format shall be set to `ts103097v131` (integer value 1);
  - the `verificationKey` for the EC;
  - the desired attributes (`requestedSubjectAttributes`);
  - the `requestedSubjectAttributes` shall not contain a `certIssuePermissions` field and the fields `validityPeriod` and `region` are optional because the EA already knows the ITS-S and can set duration and region restrictions on its own.
- For the proof of possession of the verification key pair, an `EtsiTs103097Data-Signed` structure (InnerECRequestSignedForPOP) is built containing: `hashId, tbsData`, `signer` and `signature`:
  - the `hashId` shall indicate the hash algorithm to be used as specified in ETSI TS 103 097 [3];
  - in the `tbsData`:
    - the `payload` shall contain the previous `InnerEcRequest` structure;

  - in the `headerInfo`:
    - the `psid` shall be set to "secured certificate request" as assigned in ETSI TS 102 965 [19];
    - the `generationTime` shall be present;
    - all other component of the component `tbsdata.headerInfo` not used and absent;
- the `signer` is set to 'self';
- the `signature` over the `tbsData` computed using the private key corresponding to the new `verificationKey` to be certified (i.e. the request is self-signed) to prove possession of the generated verification key pair.

- An `EtsiTs102941Data` structure is built with:
  - `version` is set to v1 (integer value set to 1);
  - the `content` is set to the previous signed data structure (InnerECRequestSignedForPOP).
- An `EtsiTs1030971Data-Signed` structure is built containing: `hashId, tbsData, signer` and `signature`:
  - the `hashId` shall indicate the hash algorithm to be used as specified in ETSI TS 103 097 [3];
  - in the `tbsData`:
    - the `payload` field shall contain the previous `EtsiTs102941Data` structure;
    - in the `headerInfo`:
      - the `psid` shall be set to "secured certificate request" as assigned in ETSI TS 102 965 [19];
      - the `generationTime` shall be present;
      - all other components of the component `tbsData.headerInfo` not used and absent;
  - the `signer` declared as `self` when the itsId is set to canonical identifier in the initial request or declared as `digest`, containing the HashedId8 of the EC when the itsId is set to the EC identifier in a successive re-keying request. In the latter case, the digest of the `SignerIdentifier` shall match with the digest in the itsId;
  - the `signature` computed using the canonical private key if the `itsId` is set to canonical identifier or the current valid EC private key corresponding to the verification public key.
- An `EtsiTs103097Data-Encrypted` structure is built with:
  - the component `recipients` containing one instance of `RecipientInfo` of choice `certRecipInfo`, containing:
    - the hashedId8 of the EA certificate in `recipientId`; and
    - the encrypted data encryption key in `encKey`; the public key to use for encryption is the `encryptionKey` found in the EAcertificate referenced in `recipientId`;
  - the component `ciphertext` containing the encrypted representation of the `EtsiTs1030971Data-Signed` structure.



NOTE: [1] Encryption is done with ECIES using the public encryption key of the EA.
[2] In the outer signed data structure, the signature is computed using either the canonical private key if the itsId is set to the canonical identifier or the current valid private key corresponding to the EC's verification public key if the itsId is set to the EC identifier.
[3] In the inner signed data structure (`InnerECRequestSignedForPOP`), the signature is computed on InnerECRequest with the private key corresponding to the new `verificationKey` to prove possession of the generated verification key pair.

Figure 14: EnrolmentRequest message

6.2.3.2.2 Enrolment response

The `EnrolmentResponse` message shall be sent by the EA to the ITS-S across the interface at reference point S_3 in response to a received `EnrolmentRequest` message.

The `EnrolmentResponse` message shall be encrypted using an ETSI TS 103 097 [3] approved algorithm and the encryption shall be done with the same AES key as the one used by the ITS-S requestor for the encryption of the `EnrolmentRequest` message.

The contents of the `EnrolmentResponse` message shall be as described in Figure 15. The specification of the ITS-S `EnrolmentResponse` message using ASN.1 [6], [7] shall be as specified in clause A.2.

To read an `EnrolmentResponse` message, the ITS-S shall receive an `EtsiTs103097Data-Encrypted` structure, containing an `EtsiTs103097Data-Signed` structure, containing an `EtsiTs102941Data`, containing an `InnerECResponse` structure.

The outermost structure is an `EtsiTs103097Data-Encrypted` structure containing:

- 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 to encrypt the `EnrolmentRequest` message to which the response is built;
- the component `ciphertext`, once decrypted, contains an `EtsiTs103097Data-Signed` structure.

If the ITS-S has been able to decrypt the content, this expected `EtsiTs103097Data-Signed` structure shall contain `hashId`, `tbsData`, `signer` and `signature`:

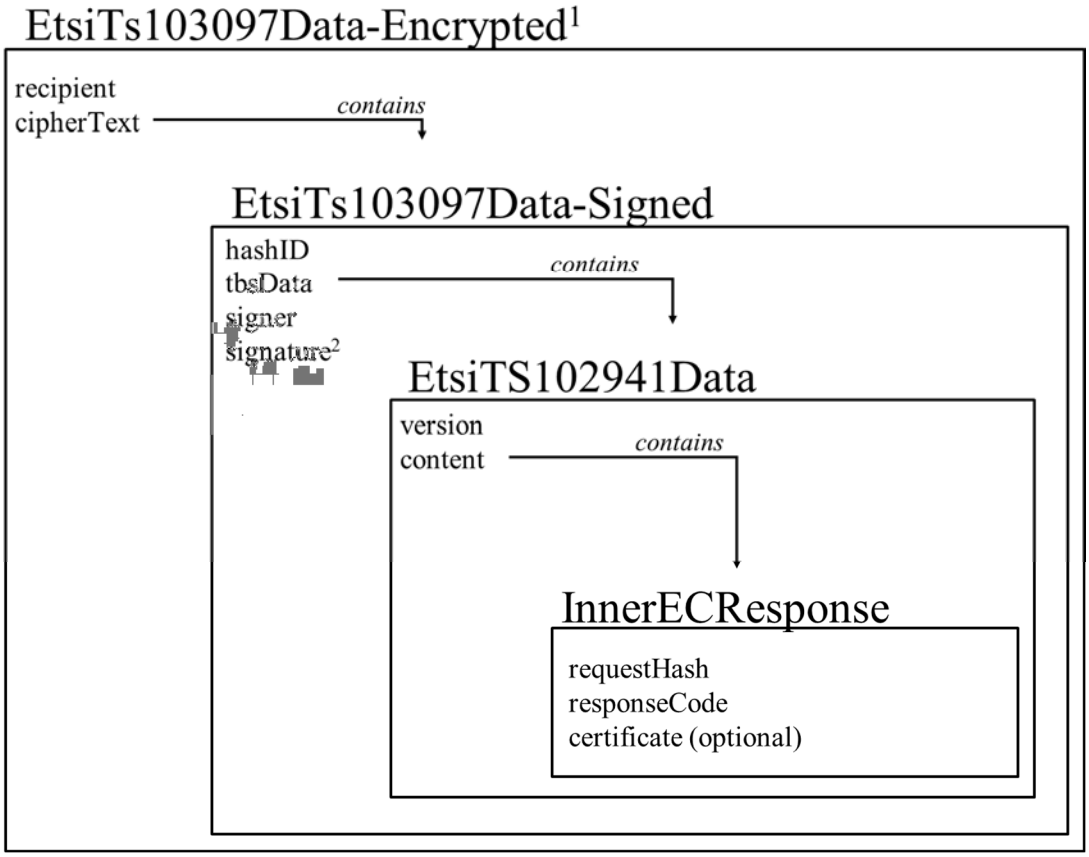
- the `hashId` shall indicate the hash algorithm to be used as specified in ETSI TS 103 097 [3];
- in the `tbsData`:
  - the `payload` shall contain the `EtsiTS102941Data` structure;
  - in the `headerInfo`:
    - the `psid` shall be set to "secured certificate request" as assigned in ETSI TS 102 965 [19];
    - the `generationTime` shall be present;
    - all other components of the component `tbsData.headerInfo` not used and absent;
- the `signer` declared as a `digest`, containing the HashedId8 of the EA certificate;
- the `signature` over `tbsData` computed using the EA private key corresponding to its publicVerificationKey found in the referenced EA certificate.

The `EtsiTS102941Data` shall contain:

- the `version` set to v1 (integer value set to 1);
- the `content` set to `InnerECResponse`.

The `InnerECResponse` shall contain:

- the `requestHash` is the left-most 16 octets of the SHA256 digest of the topmost `EtsiTs103097Data-Encrypted` structure received in the request;
- a `responseCode` indicating the result of the request;
- if `responseCode` is 0, indicating a positive response, then a certificate is returned;
- if `responseCode` is different than 0, indicating a negative response, then no certificate will be returned.



NOTE: [1] Encryption is done with the AES key used in ECIES for the encryption of the ECrequest.
[2] Signature computed using the private key corresponding to the EA certificate's verification public key.

Figure 15: EnrolmentResponse message

6.2.3.3 Authorization Management

6.2.3.3.0 Overview

The Authorization Request message shall be sent by an ITS-S to the Authorization Authority (AA) across the interface at reference point S_2 (see clause 6.2.2) to request an authorization ticket to be used in subsequent ITS communications. Figure 16 shows an example of a message sequence for a successful or unsuccessful authorization request.

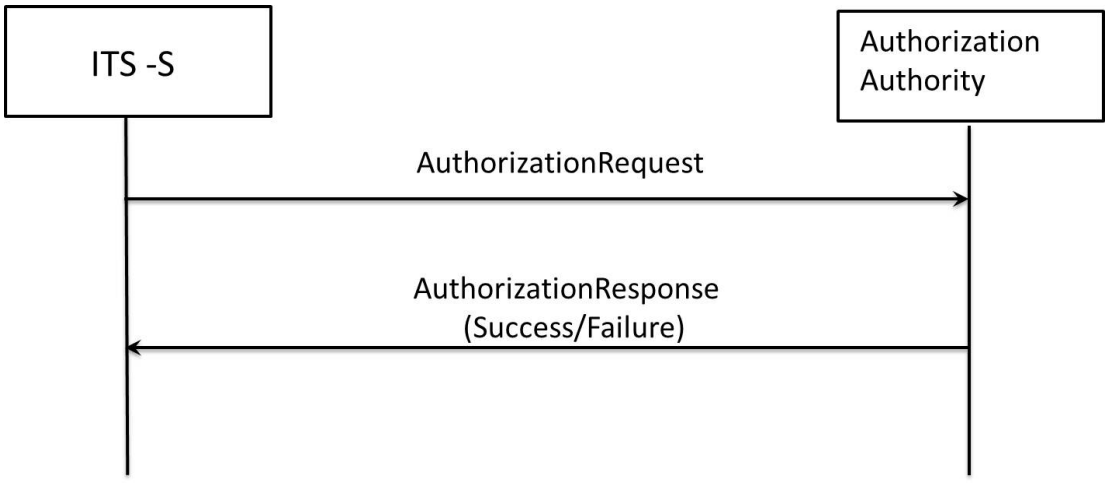


Figure 16: Message sequence for authorization request and response

All messages supporting the authorization process will satisfy the following security and privacy requirements:

- integrity, data origin authenticity, and confidentiality shall be ensured;
- authorization and access control: only registered and authenticated ITS stations shall get Authorization Tickets that enable them to access to cooperative ITS services.

For ITS-S that need privacy protection such as ITS-S vehicles or personal devices, the following requirements apply:

- pseudonymity of the ITS-S requester towards external attackers and against the Authorization Authority should be ensured;
- unlinkability of the ITS-S requesting Authorization Tickets: several successive requests should not be linked to the same ITS-S requester or linked between them.

6.2.3.3.1 Authorization request

The following functional requirements are defined on the state machine of Figure 3 (sender ITS-S for the authorization process):

- The AuthorizationRequest message shall be encrypted using an ETSI TS 103 097 [3] approved encryption algorithm and the public key provided by the Authorization Authority.
- For each authorization request, the ITS-S shall generate a new verification key pair corresponding to an approved signature algorithm as specified in ETSI TS 103 097 [3].
- The contents of the Authorization Request message shall be as described in Figure 17.
- The complete nested data structure of the Authorization Request message is specified in Figure 17. The specification of the content of the ITS-S Authorization Request message using ASN.1 [6], [7] shall be as specified in clause A.2.

To create an authorization request, the ITS-S shall follow this process:

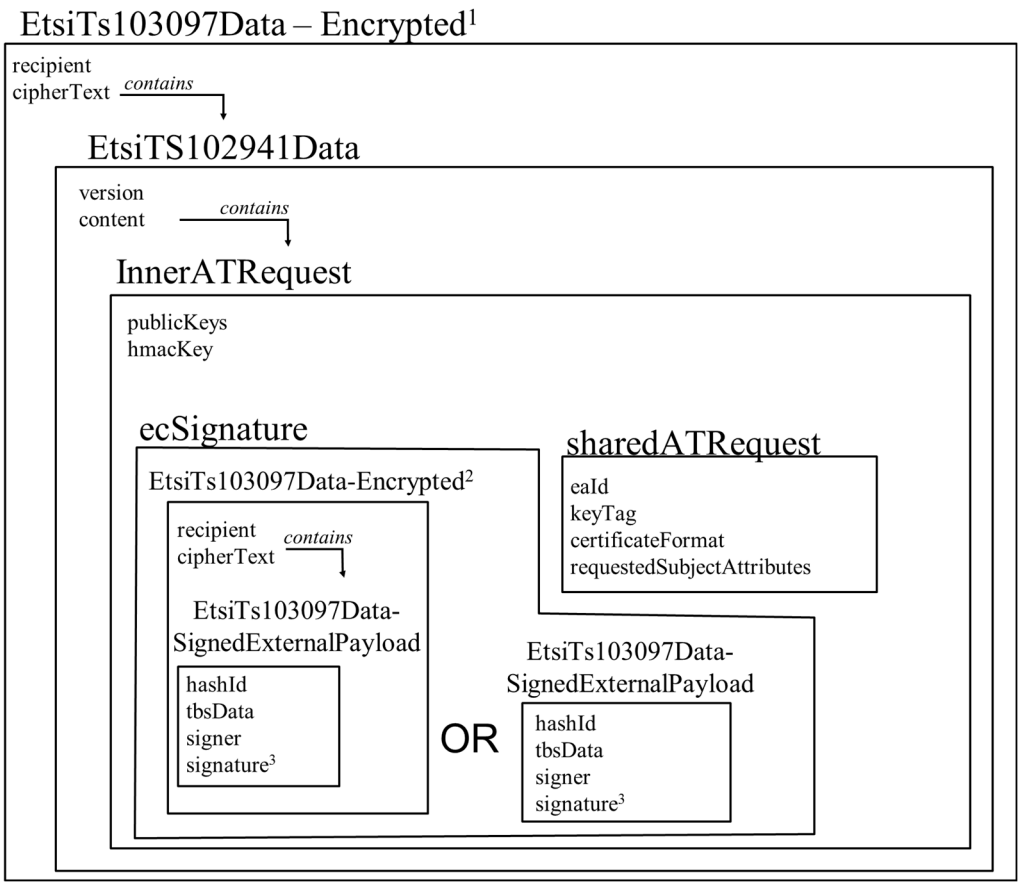
- An ECC private key is randomly generated, the corresponding public key (`verificationKey`) is provided to be included in the AT.
- Optionally, an ECC encryption private key is randomly generated, the corresponding public key (`encryptionKey`) is provided to be included in the AT.
- A random 32 octets long secret key (hmac-key) is generated.
- A tag using the HMAC-SHA256 function is computed using the previously generated hmac-key, on the concatenation of the serialization of `verificationKey` and `encryptionKey` elements (`encryptionKey` is optional); this tag is truncated to the leftmost 128 bits and named `keyTag` (see FIPS PUB 198-1 [13]). By including the tag in the `SharedATRequest` structure the integrity as well as the non-repudiation of the `verificationKey` and `encryptionKey` elements is ensured. The use of an HMAC function ensures that the tag can only be verified by the instances that are in possession of the hmac-key. By this means the AA can verify that the HMAC value of the public keys match the given `keyTag` and the EA is not able to draw conclusions on the keys requested by the ITS-S.
- A `SharedATRequest` structure is built with:
  - the `eaId` identifying the EA certificate of the EA that can be contacted for validation;
  - the calculated `keyTag`;
  - the `certificateFormat` which specifies the version used for the certificate format specification. In the present document, the certificate format shall be set to `ts103097v131` (integer value 1);
  - the desired attributes (`requestedSubjecAttributes`).

- An `EtsiTs103097Data-SignedExternalPayload` structure is built containing: `hashId`, `tbsData`, `signer` and `signature`:
  - the `hashId` shall indicate the hash algorithm to be used as specified in ETSI TS 103 097 [3];
  - in the `tbsData`:
    - the `payload` shall contain an `extDataHash` with the hash of `SharedATRequest`;
    - in the `headerInfo`:
      - the `psid` shall be se to "secured certificate request" as assigned in ETSI TS 102 965 [19];
      - the `generationTime` shall be present;
      - all other components of the component `tbsdata.headerInfo` not used and absent;
  - the `signer` declared as a `digest` referencing the hashedId8 of the EC certificate;
  - the `signature` over `tbsData` computed using the private key corresponding to the EC's verification public key.
- [Itss_WithPrivacy] An `EtsiTs103097Data-Encrypted` structure (`encryptedEcSignature`) is built with:
  - the component `recipients` with one instance of `RecipientInfo` of choice `certRecipInfo`, containing:
    - the HashedId8 of the EA certificate in `recipientId`; and
    - the encrypted data encryption key in `encKey`; the public key to use for encryption is the `encryptionKey` found in the EA certificate referenced in `recipientId`;
  - the component `ciphertext` containing the encrypted representation of the `EtsiTs103097Data-SignedExternalPayload` structure;
  - [Itss_NoPrivacy] For special purpose ITS-Ss which do not require privacy and are allowed to be re-identified by the AA, the message structure shall omit the encryption of the signer information and signature by omitting the pervious step.
- An `InnerATRequest` structure is built, containing:
  - the publicKeys: a verificationKey requested for certification and an optional encryptionKey to be placed in the same certificate;
  - the generated `hmac-key`;
  - the `SharedATRequest` structure;
  - [Itss_WithPrivacy] the encrypted detached signature containing the `EtsiTs103097Data-Encrypted` structure (`encryptedEcSignature`);
  - [Itss_NoPrivacy] the not encrypted detached signature containing the `EtsiTs103097Data-SignedExternalPayload`.
- An `EtsiTs102941Data` structure is built with:
  - the `version` set to v1 (integer value set to 1);
  - the `content` set to the previous `InnerATRequest` structure.

The POP signature is optional. That is why there is two types of messages for the authorization request provided in the ASN.1 module present in clause A.2: AuthorizationRequestMessage and AuthorizationRequestMessageWithPop. The use of this signature is recommended since it is an important security mechanism to ensure the trustworthiness of the ITS-S. It ensures that the requesting ITS-S is in possession of the corresponding private key. If present, this `EtsiTs103097Data-Signed` contains a signature providing a proof of possession of the ITS-S verification key that is provided to the AA for certification. This component is an `EtsiTs103097Data-Signed` structure containing (see Figure 18) the `hashId`, the `tbsData`, the `signer` and `signature`:

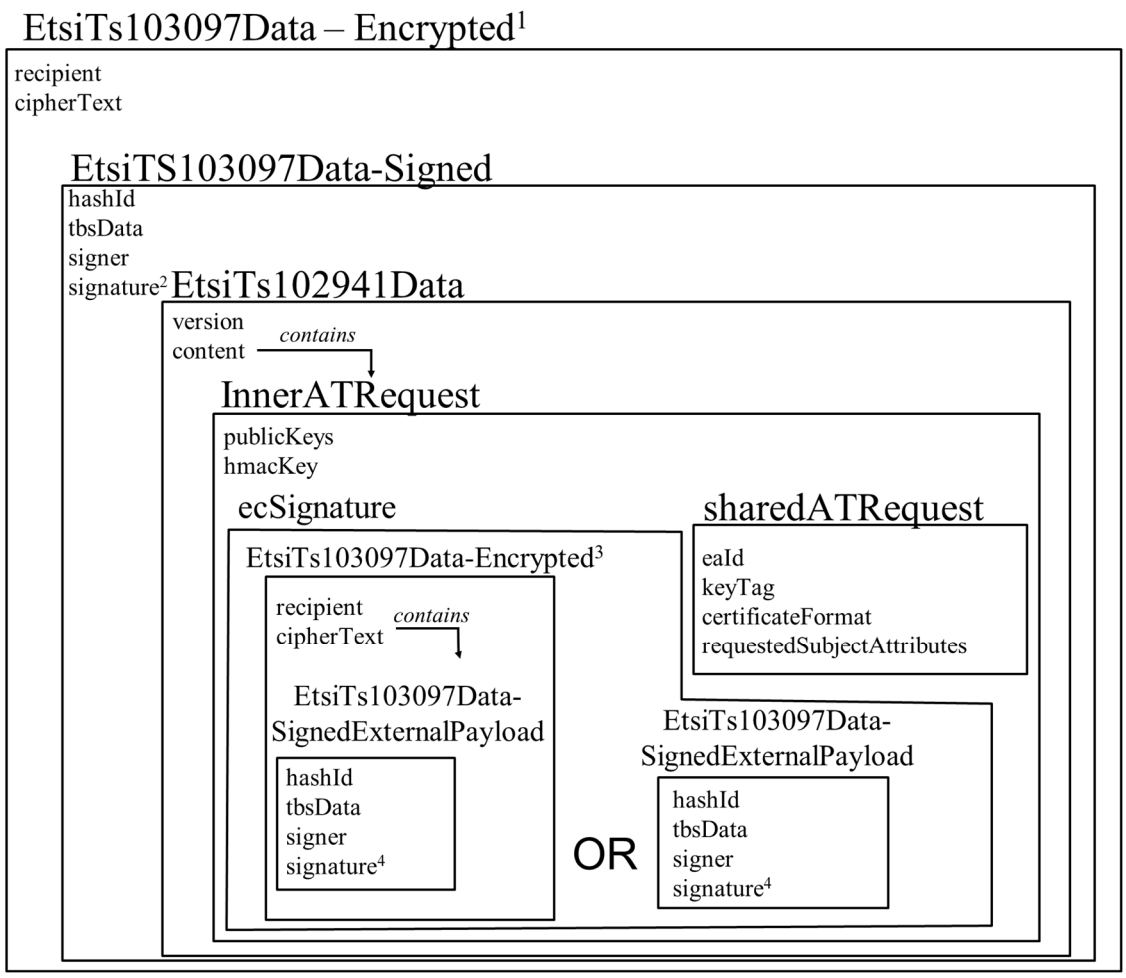
- The `hashId` shall indicate the hash algorithm to be used as specified in ETSI TS 103 097 [3].
- In the `tbsData`:
  - the `payload` shall contain the previous `EtsiTs102941Data` structure;
  - in the `headerinfo`:
    - the `psid` shall be set to "secured certificate request" as assigned in ETSI TS 102 965 [19];
    - the `generationTime` in the `headerInfo` shall be present;
    - all other components of the component `tbsdata.headerInfo` not used and absent.
- The `signer` declared as self.
- The `signature` over `tbsData` computed using the private key corresponding to the verification public key `verificationKey` to be certified and provided in the ATRequest.
- An `EtsiTs103097Data-Encrypted` structure is built with:
  - the component `recipients` containing one instance of `RecipientInfo` of choice `certRecipInfo`, containing:
    - the hashedId8 of the AA certificate in `recipientId`; and
    - the encrypted data encryption key in `encKey`, the public key to use for encryption is the `encryptionKey` found in the AA certificate referenced in `recipientId`;
  - the component `ciphertext` containing the encrypted representation of the previous `EtsiTs103097Data-Signed` structure if the POP signature is present otherwise the `EtsiTs103097Data` unsecured envelope containing the `EtsiTs102941Data` structure.

The `requestedSubjecAttributes` shall not contain a `certIssuePermissions` attribute, but shall contain an `appPermissions` attribute.



NOTE: [1] Encryption is done with ECIES using the public encryption key of the AA.
[2] Encryption is done with ECIES using the public encryption key of the EA.
[3] Signature computed using currently valid private key corresponding to the EC's verification public key.

Figure 17: AuthorizationRequest message



NOTE: [1] Encryption is done with ECIES using the public encryption key of the AA.
[2] Signature computed using the private key corresponding to the verification public key to be certified.
[3] Encryption is done with ECIES using the public encryption key of the EA.
[4] Signature computed using currently valid EC private key corresponding to the verification public key.

Figure 18: AuthorizationRequestMessageWithPop

When receiving an `AuthorizationRequest` or an `AuthorizationRequestMessageWithPop` message, the AA shall make the following verifications before preparing and sending the corresponding `AuthorizationResponse` (see Figure 12):

- AA shall decrypt the `AuthorizationRequest` using the encryption private key corresponding to the recipient certificate (`certRecipInfo` specified in the message `Recipients` field).
- AA shall verify the inner signature (if the POP is present).
- AA shall verify the HMAC-SHA256 value on the concatenation of the serialization of `publicKeys` using the received `hmacKey` to check the request authenticity.
- If the result is equal to the `keyTag` in the received request, the AA shall request to the EA identified by its certificate digest (`eaId`) the authorization validation for the requested AT. If result is not equal, the AA shall return an `AuthorizationResponse` with negative response code (different than 0).
- After receiving a positive `AuthorizationValidationResponse` from the EA, the AA shall be authorized to issue the requested AT. Otherwise it shall return a negative response code in the `AuthorizationResponse.`

6.2.3.3.2 Authorization response

The `AuthorizationResponse` message shall be sent by the AA to the ITS-S across the interface at reference point S_2 in response to a received `AuthorizationRequest` message.

The `AuthorizationResponse` message shall be encrypted using an ETSI TS 103 097 [3] approved algorithm and the encryption shall be done with the same AES key as the one used by the ITS-S requestor for the encryption of the `AuthorizationRequest` message.

The complete nested data structure of the `AuthorizationResponse` message is specified in Figure 19. The specification of the ITS-S `AuthorizationResponse` message using ASN.1 [6], [7] shall be as specified in clause A.2.

To read an authorization response, the ITS-S shall receive an `EtsiTs103097Data-Encrypted` structure, containing an `EtsiTs103097Data-Signed` structure, containing an `EtsiTs102941Data` structure, containing an `authorizationResponse` structure:

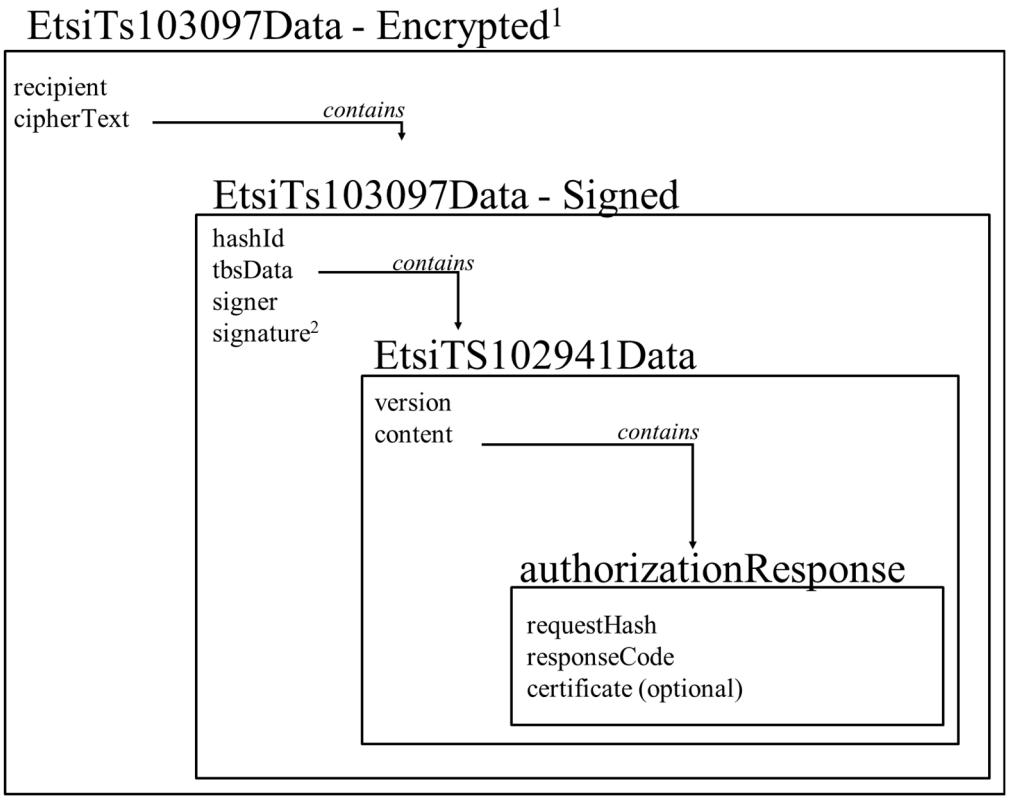
- The outermost structure is an `EtsiTs103097Data-Encrypted` structure with:
  - the component `recipients` containing one instance of `RecipientInfo` of choice `pskRecipInfo`, which contains the HashedId8 of the `SymmetricEncryptionKey` structure containing the symmetric key used by the ITS-S to encrypt the `AuthorizationRequest` message to which the response is built;
  - the component `ciphertext`, once decrypted, contains an `EtsiTs103097Data-Signed` structure.

If the ITS-S has been able to decrypt the content, this expected `EtsiTs103097Data-Signed` structure shall contain `hashId, tbsData`, `signer` and `signature`:

- The `hashId` shall indicate the hash algorithm to be used as specified in ETSI TS 103 097 [3]:
  - in the `tbsData`:
    - the `payload` shall contain an `EtsiTs102941Data` structure;
    - in the `headerInfo`:
      - the `psid` shall be se to "secured certificate request" as assigned in ETSI TS 102 965 [19];
      - the `generationTime` shall be present;
      - all other components of the component `tbsdata.headerInfo` not used and absent;
  - the `signer` as a `digest` referencing the hashedId8 of AA certificate;
  - the signature over `tbsData` computed using the AA private key corresponding to its public verification key found in the AA certificate.

The `authorizationResponse` shall contain:

- The `requestHash` is the left-most 16 octets of the SHA256 digest of the `COER` representation of the topmost `EtsiTs103097Data-Encrypted` structure of the received request (see Figure 17 and Figure 18);
- A `responseCode` indicating the result of the request.
- If `responseCode` is 0, indicating a positive response, then a certificate is returned.
- If `responseCode` is different than 0, indicating a negative response, then no certificate will be returned.



NOTE: [1] Encryption is done with the AES key used for the encryption of the ATRequest.
[2] Signature computed using the verification private key associated with the AA certificate.

Figure 19: AuthorizationResponse message

6.2.3.4 Authorization Validation protocol

6.2.3.4.0 Overview

The `AuthorizationValidation` Request message shall be sent by the Authorization Authority (AA) to the Enrolment Authority (EA) across the interface at reference point S_4 (see Figure 8 in ETSI TS 102 940 [5]) to request the validation of the Authorization Ticket (AT) request receiving from an ITS-S.

Figure 20 shows an example of a message sequence for a successful or unsuccessful AT validation request.

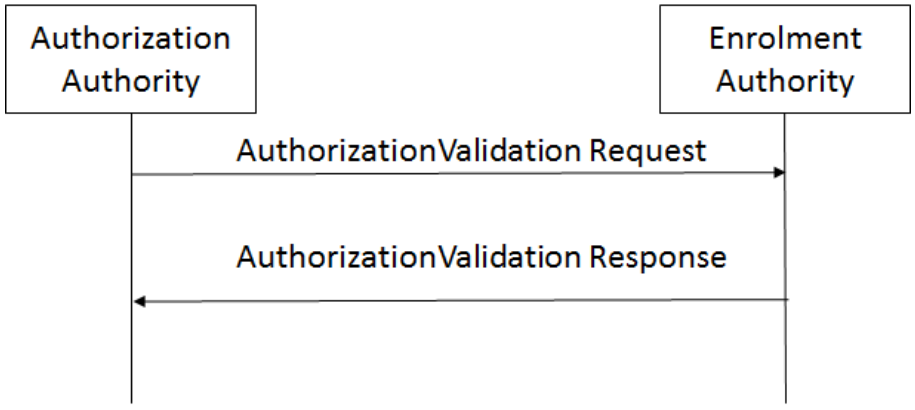


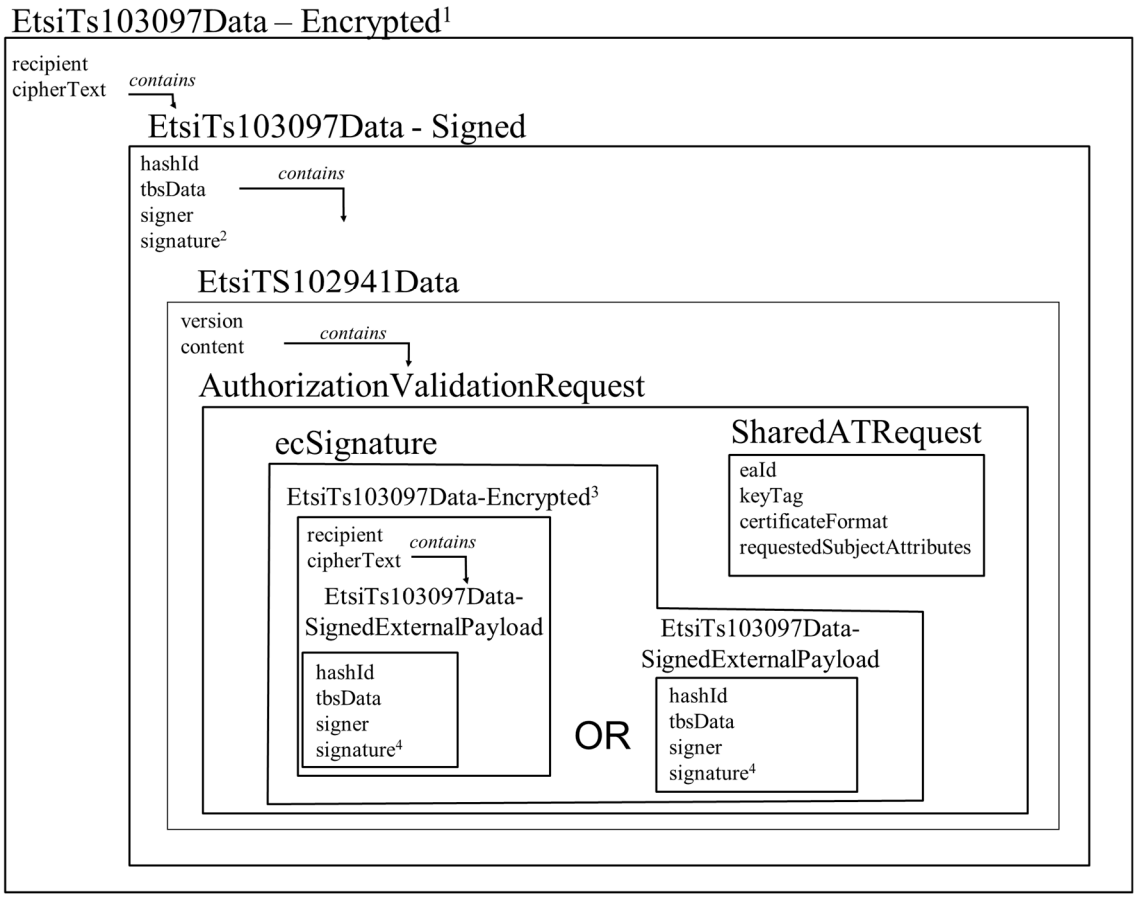
Figure 20: Message sequence for an authorization validation request

6.2.3.4.1 Authorization validation request

The following functional requirements are defined on the communication flow of Figure 20.

The `AuthorizationValidationRequest` message shall be encrypted using a ETSI TS 103 097 [3] approved encryption algorithm and the public key provided by the enrolment authority.

The contents of the `AuthorizationValidationRequest` message shall be as described in Figure 21.



NOTE: [1] Encryption is done with ECIES using the public encryption key of the EA.
[2] Signature computed using the private key corresponding to the AA certificate's verification public key.
[3] Encryption is done with ECIES using the public encryption key of the EA.
[4] Signature computed using current valid EC verification private key.

Figure 21: AuthorizationValidationRequest message

The specification of the ITS-S `AuthorizationValidationRequest` message using ASN.1 [6], [7] shall be as specified in clause A.2.

To create an `AuthorizationValidationRequest` , the AA shall follow this process:

- An `AuthorizationValidationRequest` structure is built with:
  - in the component `sharedAtRequest`, the `sharedAtRequest` component from the `InnerAtRequest` received in the `AuthorizationRequestMessage` or `AuthorizationRequestMessageWithPop`;
  - in the component `ecSignature`, the `ecSignature` component from the `InnerAtRequest` received in the `AuthorizationRequestMessage` or `AuthorizationRequestMessageWithPop`.

- An `EtsiTs102941Data` structure is built with:
  - the version set to v1 (integer value set to 1);
  - the content set to the previous data structure (`AuthorizationValidationRequest`).
- An `EtsiTs103097Data-Encrypted` with:
  - the component `recipients` with one instance of `RecipientInfo` of choice `certRecipInfo`, containing:
    - the hashedId8 of the EA certificate in `recipientId`; and
    - the encrypted data encryption key in `encKey`; the public key to use for encryption is the `encryptionKey` found in the EA certificate referenced in `recipientId`;
  - the component `ciphertext` containing the encrypted representation of the `EtsiTs103097Data-Signed` structure.
- An `EtsiTs103097Data-Signed` structure is built containing `hashId, tbsData, signer` and `signature:`
  - the `hashId` shall indicate the hash algorithm to be used as specified in ETSI TS 103 097 [3];
  - in the `tbsData`:
    - the `payload` shall contain the previous `EtsiTs102941Data` structure;
    - in the `headerInfo`:
      - the `psid` shall be set to "secured certificate request" as assigned in ETSI TS 102 965 [19];
      - the `generationTime` shall be present;
      - all other components of the component `tbsdata.headerInfo` not used and absent;
    - the `signer` declared as a `digest` referencing the hashedId8 of the AA certificate;
    - the `signature` over `tbsData` computed using the AA private key corresponding to its public verification key found in the AA certificate.

6.2.3.4.2 Authorization validation response

The `AuthorizationValidationResponse` message shall be sent by the EA to the AA across the interface at reference point S_4 in response to a received `AuthorizationValidationRequest` message.

The following functional requirements are defined on the communication flow of Figure 20.

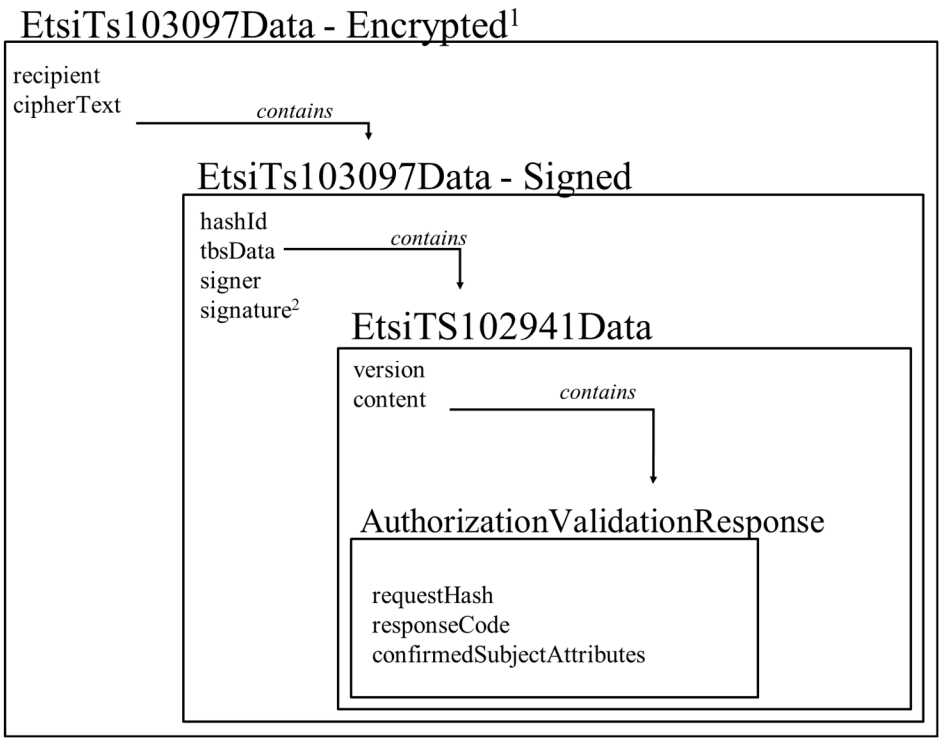
The `AuthorizationValidationResponse` message shall be encrypted using an ETSI TS 103 097 [3] approved algorithm and the response encryption key provided in the `AuthorizationValidationRequest` message.

The complete nested data structure of the `AuthorizationValidationResponse` message is specified in Figure 22. The specification of the ITS-S AuthorizationValidationRequest message using ASN.1 [6], [7] shall be as specified in clause A.2.

To read an authorization validation response, the AA shall receive an `EtsiTs103097Data-Encrypted` structure, containing an `EtsiTs103097Data-Signed` structure, containing an `EtsiTs102941Data` structure, containing an `AuthorizationValidationResponse` structure.

To create an AuthorizationValidationResponse message, an EA shall follow this process:

- An AuthorizationValidationResponse structure is built, containing:
  - the requestHash is the left-most 16 octets of the SHA256 digest of the topmost EtsiTs103097Data-Encrypted structure received in the AuthorizationValidationRequest;
  - a responseCode the response code applying to the request, based on EA internal verification results;
  - if responseCode is 0, in the field confirmedSubjectAttributes, the attributes the EA wishes to confirm, except for certIssuePermissions which is not allowed to be present;
  - if responseCode is different than 0, no component confirmedSubjectAttributes.
- An EtsiTs102941Data structure is built with:
  - the version set to v1 (integer value set to 1);
  - the content set to the previous data structure (AuthorizationValidationResponse).
- An EtsiTs103097Data-Encrypted with:
  - 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 to encrypt the AuthorizationValidationRequest message to which the response is built;
  - the component ciphertext containing the encrypted representation of the EtsiTs103097Data-Signed.
- An EtsiTs103097Data-Signed structure is built containing hashId, tbsData, signer and signature:
  - the hashId shall indicate the hash algorithm to be used as specified in ETSI TS 103 097 [3];
  - in the tbsData:
    - the payload shall contain the previous EtsiTs102941Data structure;
    - in the headerInfo:
      - the psid shall be set to "secured certificate request" as assigned in ETSI TS 102 965 [19];
      - the generationTime shall be present;
      - all other components of the component tbsdata.headerInfo not used and absent;
  - the signer declared as a digest referencing the hashedId8 of the EA certificate;
  - the signature over tbsData computed using the EA private key corresponding to its public verification key found in the referenced EA certificate.



NOTE: [1] Encryption is done with the AES key used for the encryption of the AuthorizationValidationRequest.
[2] Signature computed using the private key corresponding to the EA certificate's verification public key.

Figure 22: AuthorizationValidationResponse

A successful response shall contain a subject assurance, a start date and an end date, which shall be in the produced AT certificate. The subject assurance is defined in ETSI TS 103 097 [3].

6.2.3.5 Authorization Management with Butterfly Keys

6.2.3.5.0 Introduction

The authorization management with butterfly keys is another option for AT provisioning which can be used as an alternative to the scheme described in clauses 6.2.3.3 and 6.2.3.4.

The butterfly key scheme is based on the solution described in IEEE 1609.2.1 [24].

6.2.3.5.1 Overview

When provisioning large number of Authorization Tickets for vehicles that require pseudonymity, the butterfly key mechanism provides advantages to make the process more efficient for both the ITS-Station (ITS-S) and the PKI. The ITS-S only has to issue a single request and the PKI will expand this request and issue multiple ATs that can be downloaded asynchronously.

The `ButterflyKeyRequestMessage` or `X509SignedButterflyAuthorizationRequest` shall be sent by an ITS-S to the Enrolment Authority (EA) across the interface at reference point S_3 (see clause 6.2.2) to request a batch of authorization ticket to be used in subsequent ITS communications. The EA shall respond with a `ButterflyAuthorizationResponseMessage` that contains information on when the batch of Authorization Tickets can be downloaded.

The EA then performs the butterfly key expansion and sends multiple `ButterflyCertRequestMessages` to the Authorization Authority (AA) across the interface at reference point S_4. The AA issues the Authorization Tickets (ATs) and responds with a `ButterflyCertResponseMessage`.

NOTE: The EA may provide out-of-band means for the ITS-S to specify its preferences for which AA or AAs should be used as well as additional parameters, e.g. the version used for the certificate format specification.

The ITS-S sends a `ButterflyAtDownloadRequestMessage` to the EA across the interface at reference point S_3 to request the download of its AT batch. The EA responds with a collection of `AcaEeCertResponsePrivateSpdu` containing the ATs that it received from the AA in the previous step.

Figure 23 shows an example of a message sequence for a successful butterfly authorization request.

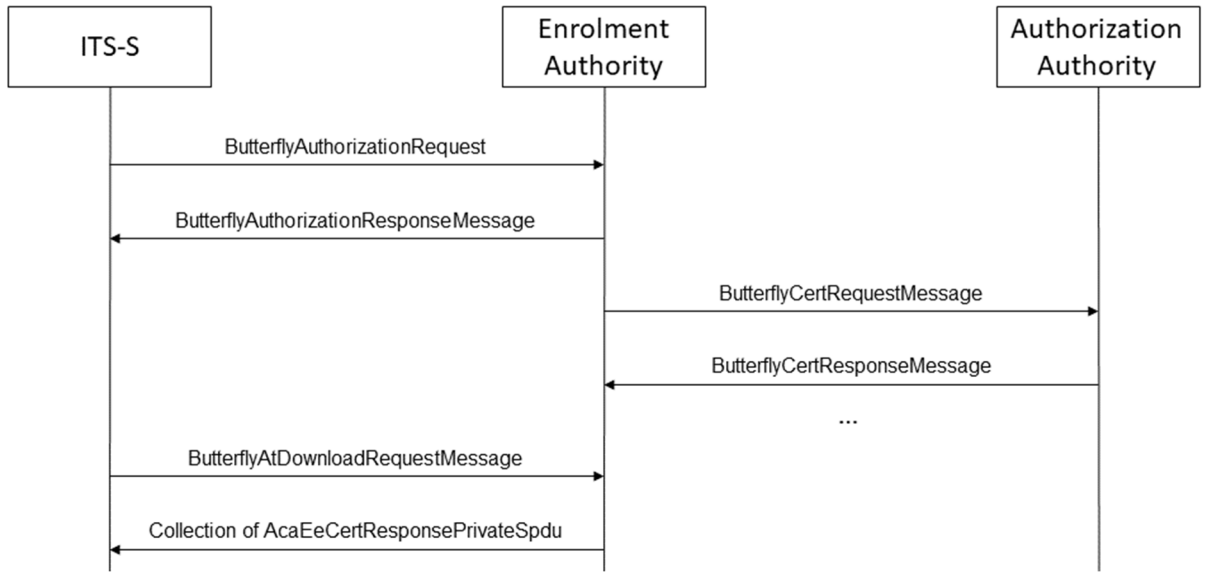


Figure 23: Message sequence for butterfly authorization request and response

All messages supporting the authorization process will satisfy the following security and privacy requirements:

- integrity, data origin authenticity, and confidentiality shall be ensured;
- authorization and access control: only registered and authenticated ITS stations shall get Authorization Tickets that enable them to access to cooperative ITS services.

For ITS-S that need privacy protection such as ITS-S vehicles or personal devices, the following requirements apply:

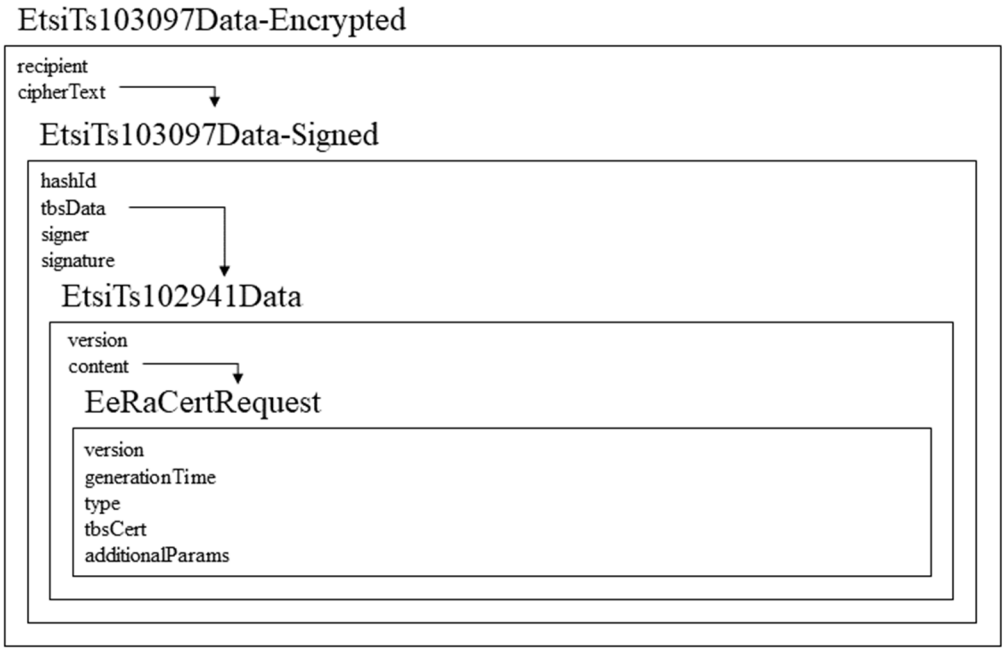
- pseudonymity of the ITS-S requester towards external attackers and towards the Authorization Authority should be ensured;
- unlinkability of the ITS-S requesting Authorization Tickets: the issued ATs from the butterfly authorization request should not be linked to the same ITS-S requester or linked between them.

6.2.3.5.2 Butterfly Authorization request

The following functional requirements are defined on the state machine of Figure 3 (sender ITS-S for the authorization process):

- The `ButterflyAuthorizationRequest` message and `X509SignedButterflyAuthorizationRequest` message shall be encrypted using an ETSI TS 103 097 [3] approved encryption algorithm and the public key from the certificate of the Enrolment Authority. The EA certificate may be injected during manufacture or can be obtained from the CTL.
- For each butterfly authorization request, the ITS-S shall generate a new caterpillar key pair, used for the expansion to individual verification key pairs, corresponding to an approved signature algorithm as specified in ETSI TS 103 097 [3].
- The contents of the `ButterflyAuthorizationRequest` message shall be as described in Figure 24.

- The complete nested data structure of the `ButterflyAuthorizationRequest` message is specified in Figure 24. The specification of the content of this message using ASN.1 [6], [7] shall be as specified in clause A.2.



NOTE: Encryption is done with ECIES using the public encryption key of the EA. The signature is computed using currently valid private key corresponding to the EC's verification public key.

Figure 24: ButterflyAuthorizationRequest message

To create a butterfly authorization request, the ITS-S shall follow this process:

- An ECC private key is randomly generated, the corresponding public key (`verifyKeyIndicator`) is to be used as caterpillar key for the butterfly key expansion.
- A `ToBeSignedCertificate` structure is built with:
  - the `id` being set to none;
  - the `cracaId` being set to '000000'H;
  - the `crlSeries` being set to 0;
  - the `validityPeriod` shall specify the validity of the first AT batch;
  - the `geographicRegion` can be optionally included;
  - the `appPermissions` containing the requested permissions for the Authorization Tickets;
  - the `verifyKeyIndicator` shall contain the generated caterpillar key.

NOTE 1: The butterfly authorization request does not support the provisioning of ATs with encryption keys.

- An `EeRaCertRequest` structure, as defined in IEEE 1609.2.1 [24], section 7.3.30, is built with:
  - the `version` being set to 2;
  - the `generationTime` being set to the generation time of this structure;
  - the `certificateType` being set to `explicit`;
  - the `tbsCert` shall contain the `ToBeSignedCertificate` structure that was generated previously;

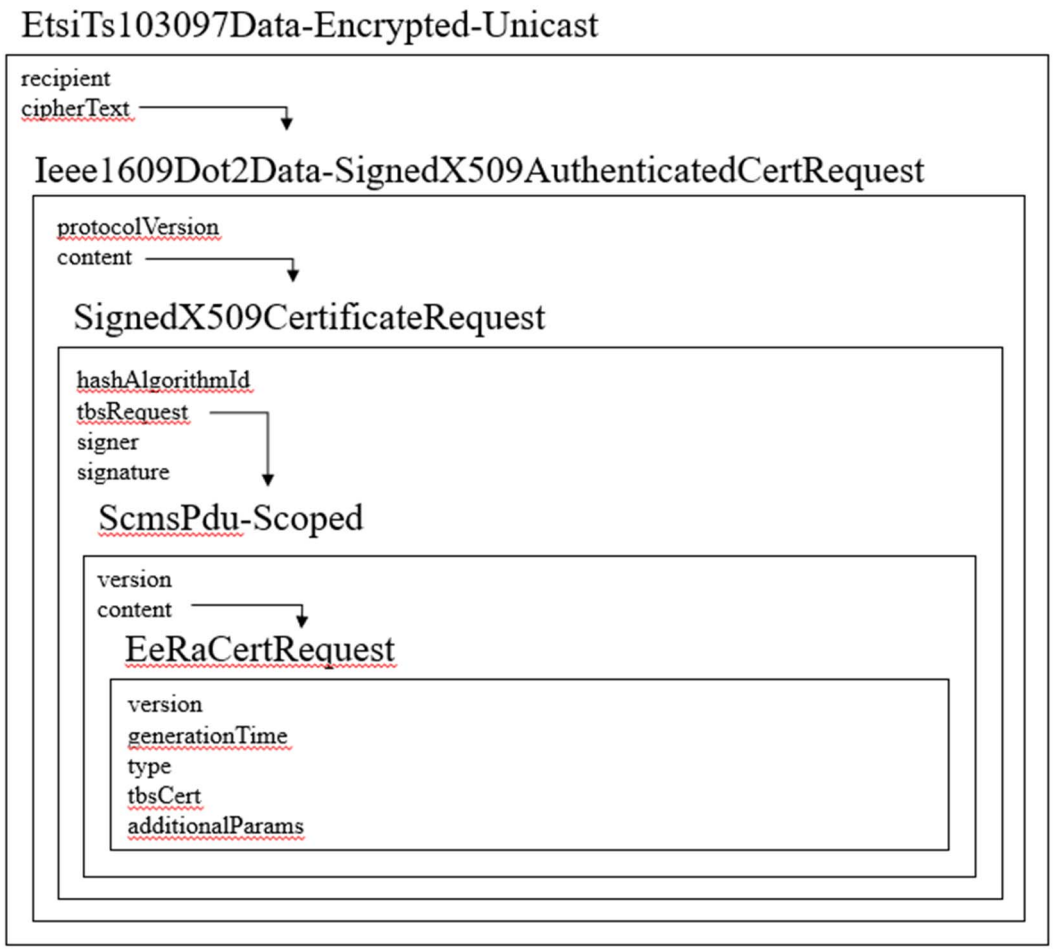
- the `additionalParams` structure shall contain either of the following:
  - the `original` option with the `ButterflyParamsOriginal` containing a `signingExpansion` containing a freshly generated 16 Byte string to be used as a key for the expansion function for signing , an `encryptionKey` containing the caterpillar public key for encryption, and an `encryptionExpansion` containing a freshly generated 16 Byte string to be used as a key for the expansion function for encryption;
  - the `unified` option with the `ButterflyExpansion` containing a freshly generated 16 Byte string that shall be used as key for the butterfly expansion.

- An `EtsiTs102941Data` structure is built with:
  - the version set to v1 (integer value set to 1);
  - the content set to the previous data structure (`EeRaCertRequest`).
- An EtsiTs103097Data-Signed structure is built containing: hashId, tbsData, signer and signature:
  - the `hashId` shall indicate the hash algorithm to be used as specified in ETSI TS 103 097 [3];
  - in the `tbsData`:
    - the `payload` shall contain the `EeRaCertRequest` structure;
    - in the `headerInfo`:
      - the `psid` shall be set to "secured certificate request" as assigned in ETSI TS 102 965 [19];
      - the `generationTime` shall be present;
      - all other components of the component `tbsdata.headerInfo` not used and absent;
    - the `signer` declared as a `digest` referencing the hashedId8 of the EC certificate;
    - the `signature` over `tbsData` computed using the private key corresponding to the EC's verification public key.
- An `EtsiTs103097Data-Encrypted` structure is built with:
  - the component `recipients` containing one instance of `RecipientInfo` of choice `certRecipInfo`, containing:
    - the hashedId8 of the EA certificate in `recipientId`; and
    - the encrypted data encryption key in `encKey`, the public key to use for encryption is the `encryptionKey` found in the EA certificate referenced in `recipientId`;
    - the component `ciphertext` containing the encrypted representation of the previous `EtsiTs103097Data-Signed` structure.

NOTE 2: The EA may provide out-of-band means for the ITS-S to specify its preferences for which AA or AAs should be used as well as additional parameters, e.g. the version used for the certificate format specification.

The contents of the `X509SignedButterflyAuthorizationRequest` message is illustrated in Figure 25.

The complete nested data structure of the `X509SignedButterflyAuthorizationRequest` message is specified in Figure 25. The specification of the content of this message using ASN.1 [6], [7] shall be as specified in clause A.2.



NOTE: Encryption is done with ECIES using the public encryption key of the EA. The signature is computed using currently valid private key corresponding to the X.509 EC's verification public key.

Figure 25: X509SignedButterflyAuthorizationRequestMessage

All contents of the EeRaCertRequest shall be built as described above for the ButterflyAuthorizationRequestMessage.

A `ScmsPdu-Scoped` structure is built with:

- The version set to v2 (integer value set to 2).
- The content set to a `EeRaInterfacePdu` which contains the previous data structure (`EeRaCertRequest`).
- A `SignedX509CertificateRequest` structure, as defined in IEEE 1609.2.1 [24], section 7.3.43, is built containing: `hashAlgorithmId`, `tbsRequest`, signer, and signature:
  - the `hashAlgorithmId` shall indicate the hash algorithm to be used as specified in ETSI TS 103 097 [3];
  - the `tbsRequest` shall contain the previous structure (`ScmsPdu-Scoped`);
  - the `signer` declared as a `SignerSingleX509Cert` containing the X.509 EC; X.509 certificates are encoded with the ASN.1 Distinguished Encoding Rules and cannot be "directly" imported into these structures.

- The `signature` over `tbsData` computed using the private key corresponding to the X.509 EC's verification public key. The signature is generated on the hash of this structure, obtained per the rules specified for hashing data objects in ETSI TS 103 097 [3], with the parameter Data Input equal to the C-OER encoding of tbsRequest, and the parameter Signer Identifier Input equal to the signer's certificate, i.e. the X.509 certificate contained in the OCTET STRING indicated by the first X509Certificate in signer.

An `Ieee1609Dot2Data-SignedX509AuthenticatedCertRequest` structure is built containing protocolVersion and content:

- The `version` set to v2 (integer value set to 2).
- The `content` set to a `signedX509CertificateRequest` which contains the previous data structure (`SignedX509CertificateRequest`).

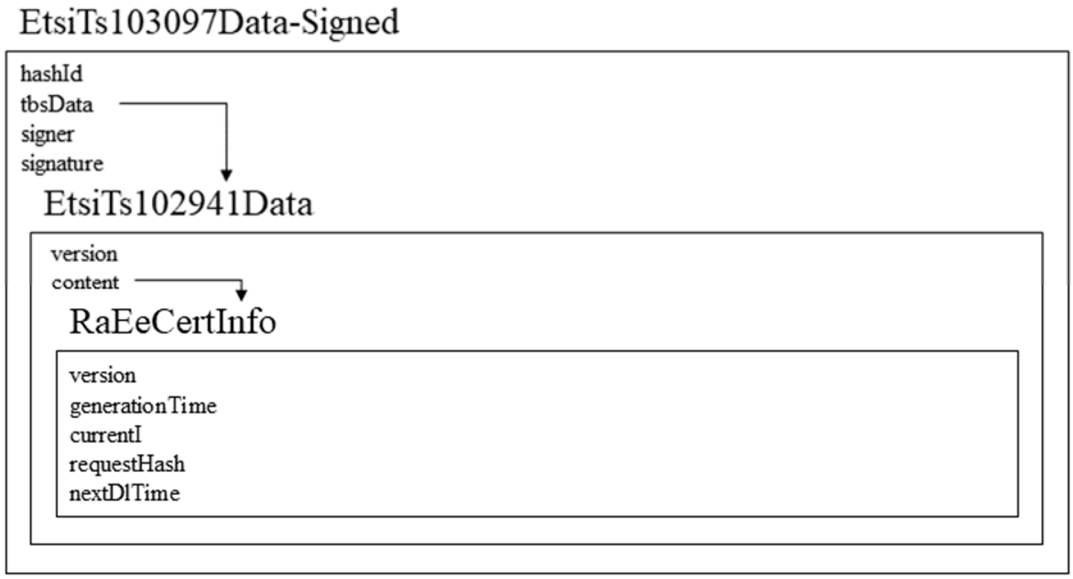
An `EtsiTs103097Data-Encrypted-Unicast` structure is built with:

- the component `recipients` containing one instance of `RecipientInfo` of choice `certRecipInfo`, containing:
  - the hashedId8 of the EA certificate in `recipientId`; and
  - the encrypted data encryption key in `encKey`, the public key to use for encryption is the `encryptionKey` found in the EA certificate referenced in `recipientId`;
  - the component `ciphertext` containing the encrypted representation of the previous `Ieee1609Dot2Data-SignedX509AuthenticatedCertRequest` structure.

NOTE 3: The EA may provide out-of-band means for the ITS-S to specify its preferences for which AA or AAs should be used as well as additional parameters, e.g. the version used for the certificate format specification.

6.2.3.5.3 Butterfly authorization response

The complete nested data structure of the `ButterflyAuthorizationResponse` message is specified in Figure 26. The specification of the ITS-S `ButterflyAuthorizationResponse` message using ASN.1 [6], [7] shall be as specified in clause A.2.



NOTE: The signature is computed using the verification private key associated with the EA certificate.

Figure 26: ButterflyAuthorizationResponse message

To read a butterfly authorization response, the ITS-S shall receive an `EtsiTs103097Data-Signed` structure, containing an `EtsiTs102941Data` structure, containing a `butterflyAuthorizationResponse` structure.

The outermost structure is an `EtsiTs103097Data-Signed` structure that shall contain `hashId, tbsData, signer` and `signature`:

- the `hashId` shall indicate the hash algorithm to be used as specified in ETSI TS 103 097 [3]:
  - in the `tbsData`:
    - the `payload` shall contain an `EtsiTs102941Data` structure;
    - in the `headerInfo`:
      - the `psid` shall be set to "secured certificate request" as assigned in ETSI TS 102 965 [19];
      - the `generationTime` shall be present;
      - all other components of the component `tbsdata.headerInfo` not used and absent;
  - the `signer` as a `digest` referencing the hashedId8 of EA certificate;
  - the signature over `tbsData` computed using the EA private key corresponding to its public verification key found in the EA certificate.

The `butterflyAuthorizationResponse` shall contain:

- the `version` shall be set to 2;
- the `generationTime` shall contain the generation time of this data structure;
- the `currentI` shall contain the i-value that is associated with the current batch of Authorization Tickets (ATs);
- the `requestHash` is the left-most 16 octets of the SHA256 digest of the `COER` representation of the topmost `EtsiTs103097Data-Encrypted` structure of the received request (see Figure 17 and Figure 18);
- the `nextDlTime` shall contain the time after which the ITS-S should try to download the AT batch;
- the `acpcTreeId` shall be absent.

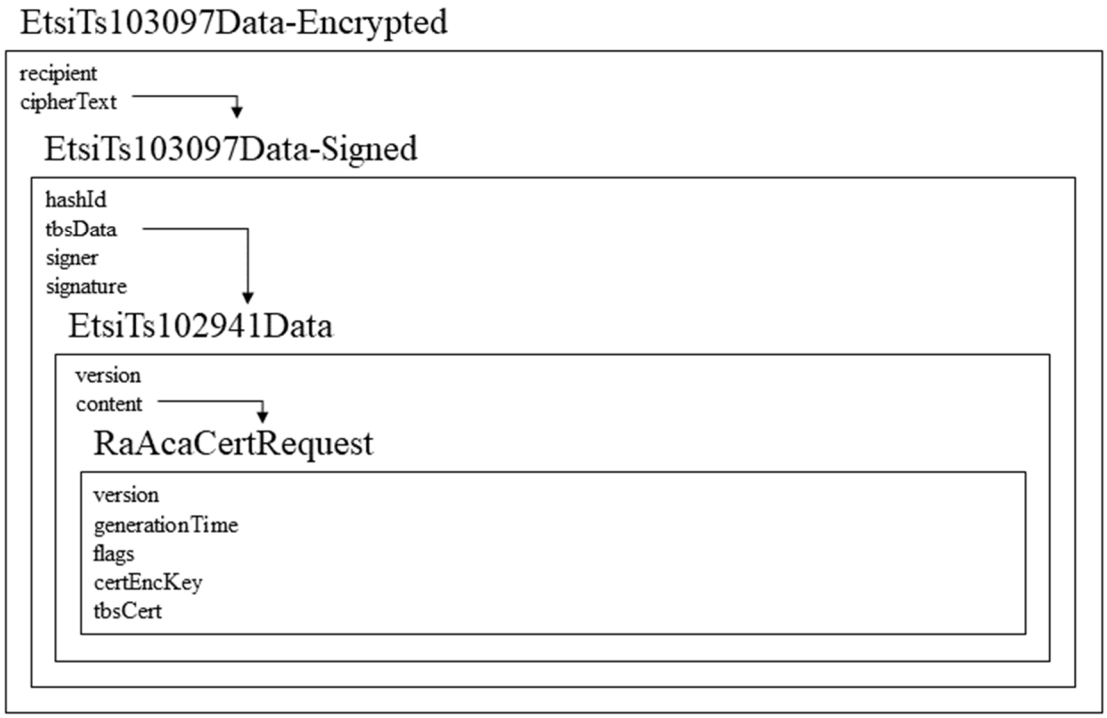
6.2.3.5.4 Butterfly certificate request

The following functional requirements are defined on the communication flow of Figure 23.

The butterfly expansion, for both the verification and, if applicable, the certificate encryption key, shall be done according to IEEE 1609.2.1 [24]. The EA may provide additional privacy to end entities by "shuffling" together individual certificate requests from many different end entities, creating confusion at the AA as to which certificates belong to which end entities.

The `ButterflyCertRequest` message shall be encrypted using an ETSI TS 103 097 [3] approved algorithm and the encryption shall be done with the public key provided by the Authorization Authority (AA).

The complete nested data structure of the `ButterflyCertRequest` message is specified in Figure 27. The specification of the `ButterflyCertRequest` message using ASN.1 [6], [7] shall be as specified in clause A.2.



NOTE: Encryption is done with ECIES using the public encryption key of the AA. The signature is computed using the verification private key associated with the EA certificate.

Figure 27: ButterflyCertRequest message

To create a `ButterflyCertRequest`, the Enrolment Authority (EA) shall follow this process:

- A `RaAcaCertRequest` structure is built with:
  - The `version` shall be set to 2.
  - The `generationTime` shall correspond to the generation time of this structure.
  - The `flags` shall be unset for all options (no butterflyExplicit, no useCubk).
  - The `linkageInfo` shall be absent.
  - The `certEncKey` corresponding to the cocoon key that shall be derived by the EA:
    - For the `original` option: using the caterpillar key provided as `encryptionKey` and expansion parameter;
    - for the `unified` option: using the caterpillar key provided as `verifyKeyIndicator` and expansion parameter.
  - The `tbsCert` structure corresponding to the information provided to the EA by the ITS-S with the ButterflyAuthorizationRequest except for the `verifyKeyIndicator` being expanded to the cocoon key by the EA.
- An `EtsiTs102941Data` structure is built with:
  - the `version` set to v1 (integer value set to 1);
  - the `content` set to the previous data structure (`RaAcaCertRequest`).
- An `EtsiTs103097Data-Signed` structure is built containing: hashId, tbsData, signer and signature:
  - the `hashId` shall indicate the hash algorithm to be used as specified in ETSI TS 103 097 [3];

- in the `tbsData`:
  - the `payload` shall contain the `RaAcaCertRequest` structure;
  - in the `headerInfo`:
    - the `psid` shall be se to "secured certificate request" as assigned in ETSI TS 102 965 [19];
    - the `generationTime` shall be present;
    - all other components of the component `tbsdata.headerInfo` not used and absent;
  - the `signer` declared as a `digest` referencing the hashedId8 of the EA certificate;
  - the `signature` over `tbsData` computed using the private key corresponding to the EA's verification public key.

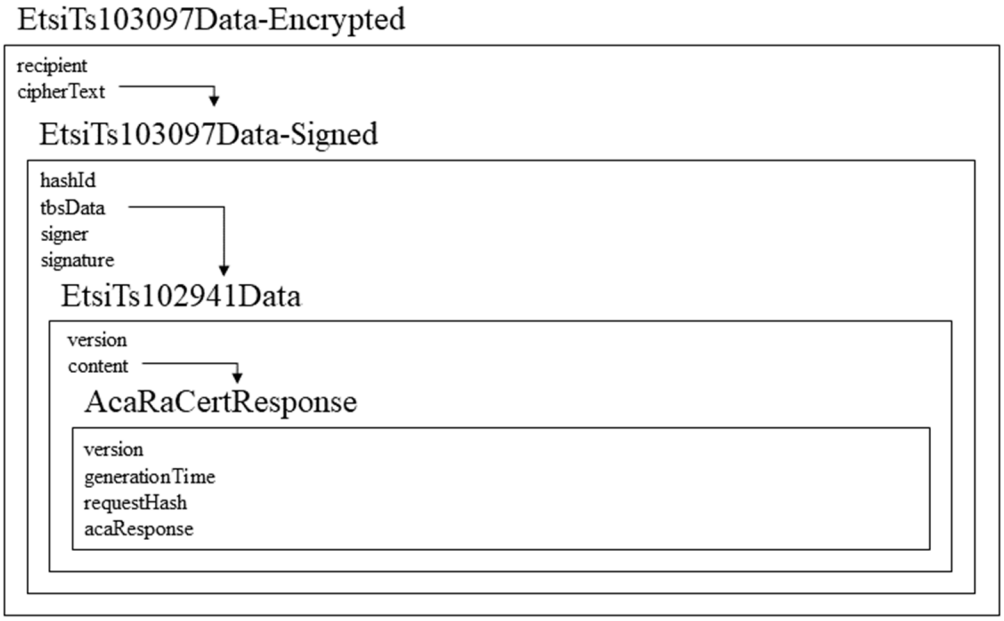
- An `EtsiTs103097Data-Encrypted` structure is built with:
  - the component `recipients` containing one instance of `RecipientInfo` of choice `certRecipInfo`, containing:
  - the hashedId8 of the AA certificate in `recipientId`; and
  - the encrypted data encryption key in `encKey`, the public key to use for encryption is the `encryptionKey` found in the AA certificate referenced in `recipientId`;
  - the component `ciphertext` containing the encrypted representation of the previous `EtsiTs103097Data-Signed` structure.

6.2.3.5.5 Butterfly certificate response

The following functional requirements are defined on the communication flow of Figure 23.

The `ButterflyCertResponse` message shall be encrypted using an ETSI TS 103 097 [3] approved algorithm and the encryption shall be done with the same AES key as the one used by the EA requestor for the encryption of the `ButterflyCertRequest` message.

The complete nested data structure of the `ButterflyCertResponse` message is specified in Figure 28. The specification of the ITS-S `ButterflyCertResponse` message using ASN.1 [6], [7] shall be as specified in clause A.2.



NOTE: Encryption is done with the AES key used for the encryption of the Butterfly Authorization Request. The signature is computed using the verification private key associated with the AA certificate.

Figure 28: ButterflyCertResponse message

To read a butterfly certificate response, the EA shall receive an `EtsiTs103097Data-Encrypted` structure, containing an `EtsiTs103097Data-Signed` structure, containing an `EtsiTs102941Data` structure, containing a `butterflyCertResponse` structure:

- The outermost structure is an `EtsiTs103097Data-Encrypted` structure with:
  - 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 EA to encrypt the `ButterflyCertRequest` message to which the response is built;
  - the component `ciphertext`, once decrypted, contains an `EtsiTs103097Data-Signed` structure.

If the EA has been able to decrypt the content, this expected `EtsiTs103097Data-Signed` structure shall contain `hashId, tbsData`, `signer` and `signature`:

- The `hashId` shall indicate the hash algorithm to be used as specified in ETSI TS 103 097 [3]:
  - in the `tbsData`:
    - the `payload` shall contain an `EtsiTs102941Data` structure;
    - in the `headerInfo`:
      - the `psid` shall be se to "secured certificate request" as assigned in ETSI TS 102 965 [19];
      - the `generationTime` shall be present;
      - all other components of the component `tbsdata.headerInfo` not used and absent;
  - the `signer` as a `digest` referencing the hashedId8 of AA certificate;
  - the signature over `tbsData` computed using the AA private key corresponding to its public verification key found in the AA certificate.

The `butterflyCertificateResponse` shall contain:

- The `version` shall be set to 2;
- The `generationTime` shall contain the generation time of this data structure;
- The `requestHash` is the left-most 16 octets of the SHA256 digest of the `COER` representation of the topmost `EtsiTs103097Data-Encrypted` structure of the received request (see Figure 17 and Figure 18);
- The `acaResponse` shall contain encrypted Authorization Ticket (AT) in the `private` field. The encoding is specified in section 7.3.4 of IEEE 1609.2.1 [24].

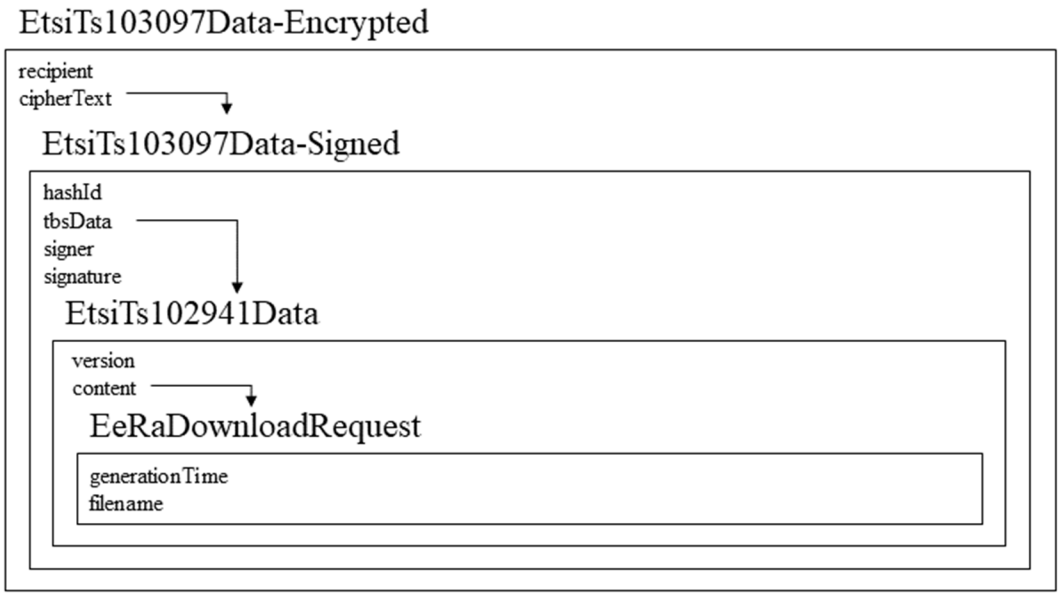
6.2.3.5.6 Butterfly AT download request

The following functional requirements are defined on the state machine of Figure 3 (sender ITS-S for the authorization process):

NOTE: The AT download request does not contain confidential information and thus it may also be issued by other means, e.g. using a REST API.

The AT download request shall be authorized though, e.g. using an internal blocklist at the EA or an OAuth token, to ensure that the ITS-S has not been revoked:

- If the ButterflyAtDownloadRequest message shall be encrypted, it shall use an ETSI TS 103 097 [3] approved encryption algorithm and the public key provided by the Authorization Authority.
- The contents of the Butterfly AT Download Request message shall be as described in Figure 29.
- The complete nested data structure of the Butterfly AT Download Request message is specified in Figure 29. The specification of the content of the Butterfly AT Download Request message using ASN.1 [6], [7] shall be as specified in clause A.2.



NOTE: Encryption is done with ECIES using the public encryption key of the EA. The signature is computed using currently valid private key corresponding to the EC's verification public key.

Figure 29: ButterflyAtDownloadRequest message

To create a butterfly AT download request, the ITS-S shall follow this process:

- An `EeRaDownloadRequest` structure is built with:
  - The `generationTime` being set to the generation time of this structure,
  - The `filename` being set in the format *h*-*i*.zip:
    - *h* is the 16-byte ASCII hex representation of the HashedId8 of the submitted butterfly authorization request message, as returned in the requestHash field of `butterflyAuthorizationResponse` structure.
    - *i* is the i-value.
- An `EtsiTs102941Data` structure is built with:
  - the version set to v1 (integer value set to 1);
  - the content set to the previous data structure (`EeRaDownloadRequest`).
- An EtsiTs103097Data-Signed structure is built containing: hashId, tbsData, signer and signature:
  - the `hashId` shall indicate the hash algorithm to be used as specified in ETSI TS 103 097 [3];
  - in the `tbsData`:
    - the `payload` shall contain the `EeRaDownloadRequest` structure;
    - in the `headerInfo`:
      - the `psid` shall be se to "secured certificate request" as assigned in ETSI TS 102 965 [19];
      - the `generationTime` shall be present;
      - all other components of the component `tbsdata.headerInfo` not used and absent;
  - the `signer` declared as a `digest` referencing the hashedId8 of the EC certificate;
  - the `signature` over `tbsData` computed using the private key corresponding to the EC's verification public key.
- An `EtsiTs103097Data-Encrypted` structure is built with:
  - the component `recipients` containing one instance of `RecipientInfo` of choice `certRecipInfo`, containing:
  - the hashedId8 of the EA certificate in `recipientId`; and
  - the encrypted data encryption key in `encKey`, the public key to use for encryption is the `encryptionKey` found in the EA certificate referenced in `recipientId`;
  - the component `ciphertext` containing the encrypted representation of the previous `EtsiTs103097Data-Signed` structure.

6.2.3.5.7 Butterfly AT download response

The butterfly AT download response corresponds to a ZIP file, as requested with the ButterflyAtDownloadRequest message. The EA generates this ZIP file by collecting all AcaEeCertResponsePrivateSpdu that is received as acaResponse with the ButterflyCertResponse message from the AA.

The data format within the ZIP file shall correspond to the specification in IEEE 1609.2.1 [24], except that in each AcaEeCertResponsePrivateSpdu containing an individual certificate, the `psid` shall be set to "secured certificate request" ITS-AID as assigned in ETSI TS 102 965 [19] and the AA certificate shall contain Secured Certificate Request SSP application permission for signing Authorization Response (Auth Resp is set to value "1" as specified in clause B.5. The contents of the .info file in the zip file shall be encoded as ButterflyAuthorizationResponseMessage.

6.3 Generation, distribution and use of Trust information lists

6.3.1 Generation and distribution of CTL by TLM

The Trust List Manager (TLM) is a superior entity in the C-ITS trust model. It is responsible for approving or rejecting the insertion of a Root CA certificate in the Certificate Trust List (CTL) in accordance with the Policy Authority (PA) as specified in ETSI TS 102 940 [5].

NOTE: In the planned deployment of C-ITS in Europe, the CTL issued by the TLM is called ECTL (European Certificate Trust List).

The TLM shall update and publish the Certificate Trust List (CTL) using the Full CTL format specified in clause 6.3.4. Especially, the update and distribution of CTL information to all C-ITS entities is needed to support the following use cases:

- add a new Root CA;
- update trust information of a Root CA, i.e. renewing the Root CA certificate, removing expired Root CA certificate;
- delete a Root CA certificate (e.g. revoked);
- update the TLM certificate after a renewal process (creation of new key and generation of TLM certificates);
- update the CPOC access point (URL) to enable secure distribution of TLM contact details.

The CTL issued by the TLM shall be signed using the TLM verification key and time-stamped using a time-stamp counter (ctlSequence) which is specified as a monotonically increasing counter, with increased value of 1 and maximum value 255. The list is valid when received and shall contain a validity end (nextUpdate).

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

- TLM certificate and link certificate (optional);
- Root CA certificates and link certificates (optional);
- CPOC access point.

For each update of the CTL, the TLM shall also generate the Delta CTL list using the formats specified in clause 6.3.4. The sequence number of the Full CTL (ctlSequence) shall be identical to the sequence number of the Delta CTL.

The full and delta CTL should be published via the C-ITS Point Of Contact (CPOC).

6.3.2 Generation and distribution of CTL by RCA

The Root CA is the root of trust for the PKI hierarchy. The RCA is responsible of managing and providing trust information about all its subordinate authorities (EAs, AAs), e.g. CA certificates and access points (URL) as specified in ETSI TS 102 940 [5].

The RCA shall update and publish the Certificate Trust List (CTL) using the Full CTL format specified in clause 6.3.4. Especially, the update and distribution of CTL information to all C-ITS entities is needed to support the following use cases:

- add a new trusted EA or AA;

- update EA certificates (renewing the EA certificate, removing expired EA certificate) and access points (URL);
- update AA certificates (renewing the AA certificate, removing expired AA certificate) and access points (URL);
- update DC access point to enable secure distribution of RCA contact details.

The CTL issued by the RCA shall be signed using the private key corresponding to the RCA certificate's verification public key and time-stamped using a time-stamp counter (ctlSequence) which is specified as a monotonically increasing counter, with increased value of 1 and maximum value 255. The list is valid when received and shall contain a validity end (nextUpdate).

The CTL issued by a RCA may contain the following information:

- EA certificates and access points;
- AA certificates and access point;
- DC access point.

The CTL issued by a RCA shall not contain the following information: the TLM certificate and associated linked certificate (optional) and the Root CAs certificates.

For each update of the CTL, the RCA shall also generate the Delta CTL list using the formats specified in clause 6.3.4. The sequence number of the Full CTL (ctlSequence) shall be identical to the sequence number of the Delta CTL.

The full and delta CTL should be published via the Distribution Centre (DC) associated to the RCA.

6.3.3 Generation and distribution of CRL by RCA

A Certificate Revocation List (CRL) is issued and signed by the RCA verification key. It contains the CA certificates identifiers (HashedID8) that are no longer worthy of being trusted. It is accessible through a defined DC associated to the RCA.

NOTE 1: The CRL may contain the revoked certificate of the Root CA.

NOTE 2: A certificate when revoked is revoked permanently and cannot be reinstated.

The CRL issued by a Root CA shall not contain RCA certificates identifiers of other RCAs.

The RCA shall update the CRL by adding the identifiers of the revoked CA certificates and removing the identifiers of the expired ones.

The generated CRL CA shall be signed and time-stamped (thisUpdate) and shall use the CRL data structure as specified in clause A.2.7.

The RCA shall publish and distribute the updated CRL CA via a Distribution Centre (DC).

6.3.4 Specification of Full CTL and Delta CTL

The CTL messages are split in two different message types depending of the issuer category: the TlmCertificateTrustListMessage shall be issued by a TLM entity and an RcaCertificateTrustListMessage shall be issued by a Root CA.

The `signer` in the `SignedData` shall contain the certificate of the CTL issuer.

The CTL data structure as specified in clause A.2.7 takes into account the need for transmitting the Full CTL list over any kind of medium (providing that message fragmentation is supported) and the possible transmission of a small size format for transmission over ITS G5 (Delta CTL).

A `ToBeSignedTlmCtl` or `ToBeSignedRcaCtl` shall be of type `FullCtl` or `DeltaCtl`. Both types use the same common format `CtlFormat`.

The type `CtlFormat` shall have the following components:

- version indicates the version of the CTL Format. For this version of the Technical Specification the version is set to 1;
- nextUpdate indicates the time when a next update of the CTL is expected, and consequently the time after which the CTL is to be considered expired;
- isFullCtl is a flag indicating if the list is a full or delta list;
- ctlSequence indicated the sequence number of the list and is monotonically increased with steps of one unit, and clipped around 255;
- ctlCommands contains the CTL commands add or delete, add is of type CtlEntry, and indicates that the entry shall be trusted; delete is of type CtlDelete, and indicates explicitly that an entry that was previously trusted is not trustable anymore and shall be removed.

A `ToBeSignedCtl` of type `FullCtl` shall have `isFullCtl` set to `TRUE` and shall contain only `ctlCommands` of type `CtlEntry,` generating the full list of trustable entries.

A `ToBeSignedCtl` of type `DeltaCtl` shall have `isFullCtl` set to `FALSE,` and shall contain `ctlCommands` of type `CtlEntry` to indicate trust in new or updated entries, and `ctlCommands` of type `CtlDelete` to indicate that it has been removed from the trust domain, and that such entries shall be considered deleted from the full List. A `ToBeSignedCtl` of type `DeltaCtl` shall always be generated with respect to the previous full list, i.e. the full list with ctlSequence with one unit less than the current.

Note that a full list and a delta list may exist in parallel, e.g. a full list of `ctlSequence` 5 may coexist with a delta list of `CtlSequence` 5, generated with respect to the Full List of `CtlSequence` of 4.

A `CtlEntry` shall provide either a `rca`, `ea`, `aa`, `dc` or `tlm` entry of type respectively `RootCaEntry`, `EaEntry`, `AaEntry`, `DcEntry`, `TlmEntry`.

A `CtlDelete` shall provide either the `cert` to delete a `CtlEntry` entry corresponding to a certificate (i.e. `rca`, `ea`, `aa`, `tlm`) using its HashedId8 or the `dc` to delete a `CtlEntry` entry corresponding to a distribution centre using its URL.

`RootCAEntry` shall contain a Root CA certificate and optionally a link certificate.

`EaEntry` shall contain an EA certificate, the URL for the connection by the AA, and optionally the URL for the connection by the ITS-Station. If the EA only supports butterfly authorization requests, the URL for connection by the AA shall be set to an empty string.

`AaEntry` shall contain an AA certificate, and optionally the URL for the connection by the ITS-Station. The URL for connection by the EA to allow butterfly key requests shall be distributed using out-of-band-measures.

`TlmEntry` shall contain the TLM Certificate which is a self-signed certificate, optionally the TLM link certificate and the CPOC URL for the connection by the all the entities of C-ITS trust domain.

`DcEntry` shall contain the URL of the Distribution Centre and a list of certificate digests (HashedId8).

The CTL issued by a RCA shall contain one or multiple DCEntry with elements as follows:

- URL of Distribution Centre concerned;
- the RCA(s) certificate digests that publish via the Distribution Centre. This list of certificate digests may not be exhaustive.

A CTL issued by a RCA shall have at least one DC entry where its certificate is contained in the list of certificate digests.

6.3.5 Transmission of CTL and CRL

Different methods for updating the enrolled ITS-Ss may be used as specified in clause 6.1.5. Communication profiles for transmitting the CTL or CRL CA to enrolled ITSs are specified in annex D.

The communication requirements for requesting the ECTL, Delta ECTL, TLM certificates and TLM link certificate messages to the CPOC are specified in Annex E.

For broadcasting a CTL issued by TLM over ITS-G5, an ITS-S shall re-transmit the received TlmCertificateTrustListMessage defined in clause A.2 without modifications. The CTL transmitted issued by the TLM shall contain a DeltaCtl (the value of CtlFormat shall be set to DeltaCtl). The communication profile for CTL broadcast communication is specified in clause D.3.

For broadcasting a CTL issued by RCA over ITS-G5, an ITS-S shall re-transmit the received RcaCertificateTrustListMessage defined in clause A.2 without modifications. The CTL transmitted issued by a RCA shall contain a DeltaCtl (the value of CtlFormat shall be set to DeltaCtl). The communication profile for CTL broadcast communication is specified in clause D.3.

For broadcasting a CRL over ITS-G5, an ITS-S shall re-transmit the received CertificateRevocationListMessage defined in annex A without modifications.

The communication profile for CRL broadcast communication is specified in clause D.3.

6.3.6 CTL and CRL use by ITS-Ss

Upon the reception of the CTL or the CRL, the ITS-S verifies that it is signed by the associated RCA.

The ITS-S uses the CTL to update its trust information list in terms of trust anchors. This information allows to build a candidate certificate chain only based on declared `issuer` component as specified in ETSI TS 103 097 [3].

The ITS-S extracts the list of revoked CA certificates from the CRL and utilizes this information while performing the validation of the certification path.

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 (IETF RFC 5280 [21]), 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 [5], clause 7.1. 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 [21], 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 [5], clause 7.1.

NOTE 3: The Annex I of CPOC protocol [21] 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 ETSI 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 30. 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:

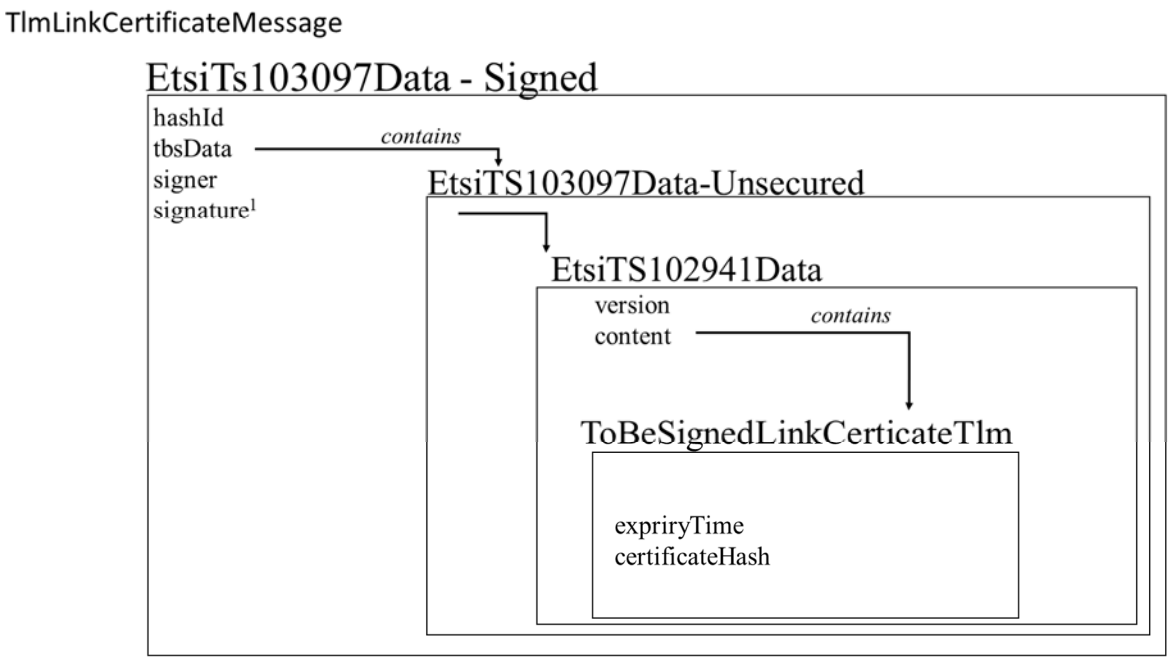
- An `EtsiTs102941Data` structure is built, containing:
  - `version` is set to v1 (integer value set to 1);
  - a `linkCertificateTlm` of type `ToBeSignedLinkCertificateTlm` is built with:
    - `expiryTime` is the time at which the link certificate message expires. It shall be equal to the end of the 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 [21], 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 ETSI TS 103 097 [3], clause A.2.2.

- 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.



NOTE: [1] Signature computed using the currently valid private key corresponding to "old" TLM certificate.

Figure 30: Message TlmLinkCertificateMessage

6.4.2.2 Generation of Link Certificate Message by a Root CA

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 ETSI 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 31) 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 31 and the content of the `RcaDoubleSignedLinkCertificateMessage` is depicted in Figure 32. 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 [21], 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 ETSI TS 103 097 [3], clause A.2.2.

- An `EtsiTs103097Data-Signed` structure of type `RcaSingleSignedLinkCertificateMessage` is built (see Figure 31), 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 32), 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];

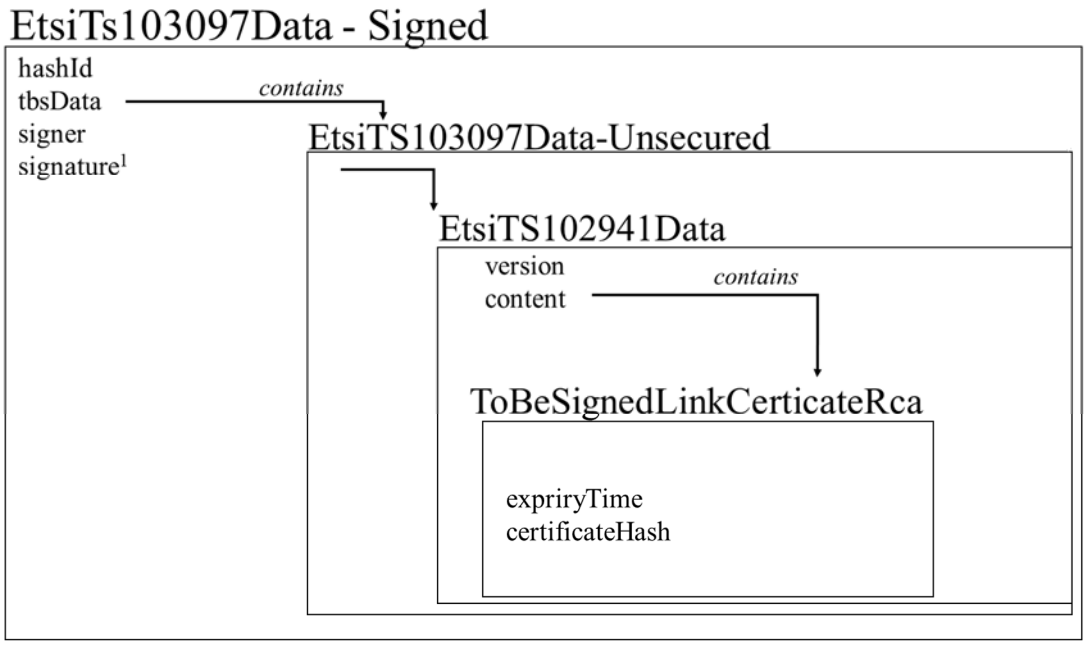
            - the `generationTime` shall be present and set to the time at which the link certificate message is generated;

            - 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.

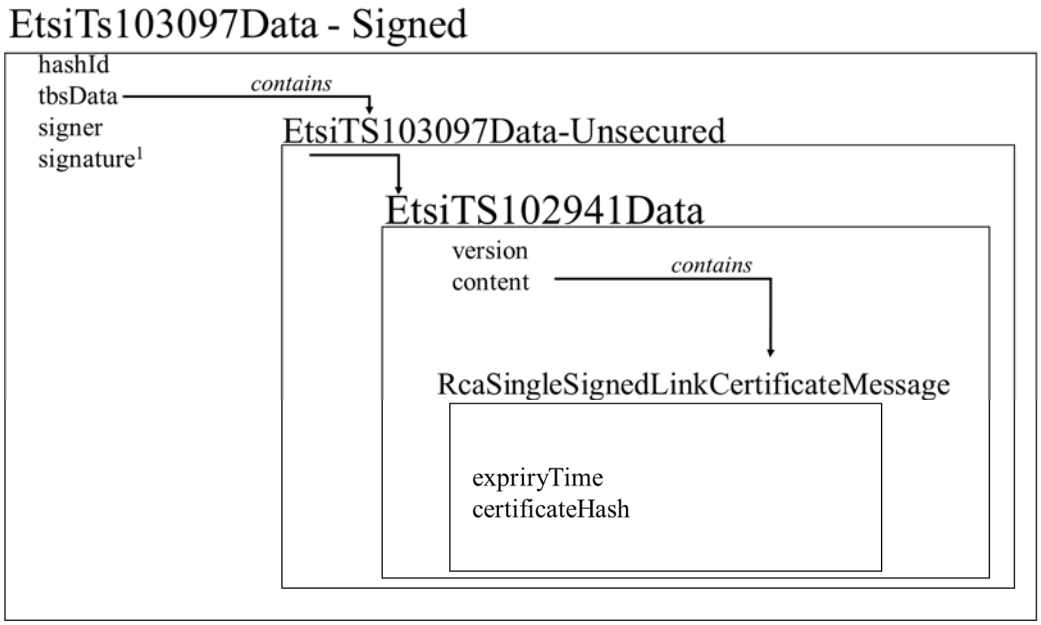
RcaSingleSignedLinkCertificateMessage



NOTE: [1] Signature computed using the currently valid private key corresponding to "old" RCA certificate.

Figure 31: Single Signed RCA Link certificate Message

RcaDoubleSignedLinkCertificateMessage



NOTE: [1] Signature computed using the private key corresponding to "new" certificate.

Figure 32: Double Signed RCA Link certificate Message

7 Security association and key management between ITS Stations

7.0 Introduction

A detailed set of use case examples for ITS applications is presented in ETSI TR 102 638 [i.2]. In addition, ETSI TS 102 940 [5] categorizes the application communication (addressing) patterns used as:

- Broadcast;
- Multicast;
- Unicast.

In contrast to the strictly safety-related broadcast applications (CAM and DENM), multicast and unicast applications are assumed to be offered by several providers and, possibly, to be commercially sensitive. Therefore, the requirements depend heavily on the specific application and the respective business model.

With the exception of broadcast applications, all other multicast and unicast communications can use either asymmetric or symmetric key systems to provide for Security Association (SA) lifecycle and the related key management (registration, key establishment, updates and removal).

Unicast and multicast applications shall use link layer encryption and regular changes of the ITS MAC addresses to protect the privacy of the ITS-S (and its user) as well as all higher layer information from radio channel eavesdropping. Further details can be found in ETSI TS 102 942 [i.17] and ETSI TS 102 943 [i.18].

7.1 Broadcast SAs

Broadcast applications such as CA basic service, DEN basic service or Infrastructure messages service specified in [i.19], [i.20] and [i.21] require authentication, authorization and integrity but not confidentiality. Senders of CAM and DENM shall obtain this service by signing with an authorization ticket using the mechanisms specified in ETSI TS 103 097 [3], clauses 7.1 (Security profile for CAMs), 7.2 (Security profile for DENMs) or 7.3 (Generic profile for other broadcast messages) respectively.

To enable broadcast message signature verification, a receiving ITS-S or a relaying ITS-S shall have the capabilities to construct the certificate chain from the certificate of the Sending ITS-S up to a trust anchor. A trust anchor is either a trusted root certificate or any other CA certificate that is known to be trustworthy from the receiving or relaying ITS-S.

A receiving or relaying ITS-S shall have the capabilities to cryptographically verify the constructed certificate chain.

A receiving or relaying ITS-S shall have the capabilities to cryptographically verify the signature of the broadcasted message.

7.2 Multicast SAs

Multicast applications such as public transport information and Point of Interest notification services require secure group communications with message authentication, authorization and encryption depending on that group's particular security policy.

The following specifications assume that the ITS-S is using an IP-based multicast communication.

An ITS-S may join a multicast group using an authorization ticket (see clause 6.2.3.3) followed, possibly, by further registration steps.

The key management for multicast applications can be controlled by the multicast service provider or a separate security manager. Such key management may be application-specific or it may use a standard multicast key management system such as the IETF Multicast Security (MSEC) Group Key Management Architecture [i.3], [i.8], [i.9] and [i.10].

For other use cases using communications that are not IP-based, ETSI TS 103 097 [3] provides data structures that may be used to establish SA in a multicast group.

For key establishment, the multicast group leader should generate a fresh symmetric key k, use it to encrypt the first multicast message (with AES-CCM), then encrypt k for each recipient with the corresponding recipient key.

The structure `EtsiTs103097Data-Encrypted` can be used to encapsulate all this data in the following way:

- The field `recipients` shall contain one or more `RecipientInfo`s, one for each key used to encrypt the symmetric key k.
- Each `RecipientInfo` shall be of type `certRecipInfo` or `signedDataRecipInfo`:
  - `certRecipInfo` shall be used if the symmetric key k is encrypted with a public encryption key present in a certificate.
  - `signedDataRecipInfo` shall be used if the symmetric key k is encrypted with an encryption key present in a previously received `SignedData` structure.
- The field `ciphertext` shall contain the encrypted message.

After each recipient in the multicast group receives the encrypted data structure, it shall decrypt the key k and the encrypted multicast message. This key may be reused to encrypt further confidential multicast messages, with the `pskRecipInfo` option in the `RecipientInfo` that indicates the use of a pre-shared symmetric key. However, the AES-CCM nonce shall be chosen randomly and shall never be reused with the same key.

If the multicast group already has a pre-shared key obtained through another key establishment protocol, the group can use this key with the structure `EtsiTs103097Data-Encrypted` and the `pskRecipInfo` option in the `RecipientInfo`.

The structure EtsiTs103097Data-SignedAndEncrypted can be used if authentication is also required in the key establishment step and/or the multicast group communication.

NOTE: The detailed requirements and the protocols for secure group communications with message authentication, authorization and encryption will be later specified in ETSI TS 102 943 [i.18].

7.3 Unicast SAs

Unicast applications such as automatic access control, parking management and media downloading services require secure unicast communications with message authentication, authorization and encryption.

The following specifications assume that the ITS-S is using an IP-based unicast communication.

An ITS-S may join such services using its authorization ticket followed, possibly, by further registration protocol steps.

Unicast key management may be application-specific or it may use a standard key management systems such as network layer security using Ipsec as defined by the IETF RFC 4301 [i.4], IETF RFC 4877 [i.12], IETF RFC 4306 [i.11], IETF RFC 4302 [i.5] and IETF RFC 4303 [i.6]. Also, security in the transport layer can be provided using methods such as the IETF Transport Layer Security (TLS) [i.7],[i.16]. An ITS-S should support TLS 1.2 [i.7] or TLS 1.3 [i.16] and the allowed and mandatory cipher-suites to protect data transmission over the Transport layer (TCP protocol).

NOTE 1: The rules on allowed and mandatory cipher-suites and on allowed and mandatory extensions as specified in TLS 1.2 and TLS 1.3 are out of the scope of the present document.

For other use cases such as the Trust and Privacy management services specified in the present document, other unicast solutions using the ETSI ITS security standards for ITS G5 communications shall be considered (ETSI TS 103 097 [3]).

For non-IP unicast SA, it is possible to proceed in the same way as multicast SA to establish a shared key. The SA initiator should generate a fresh symmetric key k, use it to encrypt the first confidential message, then encrypt k for the recipient with the corresponding recipient key. The structure `EtsiTs103097Data-Encrypted` shall be used to encapsulate all this data in the following way:

- The field `recipients` shall contain one `RecipientInfo` of type `certRecipInfo` or `signedDataRecipInfo` depending on which recipient key is used.
- The field `ciphertext` shall contain the encrypted message.

After the recipient receives the encrypted data structure, it shall decrypt the key k and the encrypted message. This key may be reused to encrypt further confidential messages, with the `pskRecipInfo` option in the `RecipientInfo` that indicates the use of a pre-shared symmetric key. However, the AES-CCM nonce shall be chosen randomly and shall never be reused with the same key.

If the units involved in a unicast communication already have a pre-shared key obtained through another key establishment protocol, the units can use this key with the structure `EtsiTs103097Data-Encrypted` and the `pskRecipInfo` option in the `RecipientInfo`.

The structure `EtsiTs103097Data-SignedAndEncrypted` can be used if authentication is also required in the key establishment step and/or the unicast communication.

NOTE 2: The detailed requirements and the protocols for Secure unicast communications with message authentication, authorization and encryption will be later specified in ETSI TS 102 943 [i.18].

Annex A (normative): ITS security management messages specified in ASN.1

A.1 ITS trust and privacy messages specified in ASN.1

The ASN.1 [6] modules in this annex specify data types for ITS trust and privacy services together with useful ASN.1 value notations. Security Management Messages specified in the present document shall comply with the structures specified here but the definitive encoding of messages in an implementation of the present document is specified in clause 6.2.0.

A.2 Security management messages structures

A.2.1 Security data structures

The ASN.1 module `EtsiTs102941BaseTypes` is identified by the Object Identifier {itu-t(0) identified-organization(4) etsi(0) itsDomain(5) wg5(5) ts(102941) baseTypes(3) version3(3)}. The module can be downloaded as a file as indicated in Table A.1. The associated SHA-256 cryptographic hash digest of the referenced file offers a means to verify the integrity of that file.

Table A.1: `EtsiTs102941BaseTypes` ASN.1 module information

Module name	EtsiTs102941BaseTypes
OID	`{itu-t(0) identified-organization(4) etsi(0) itsDomain(5) wg5(5) ts(102941) baseTypes(3) major-version-3(3) minor-version-1(1)}`
Link	https://forge.etsi.org/rep/ITS/asn1/pki_ts102941/blob/v2.2.1/EtsiTs102941BaseTypes.asn
SHA-256 hash	c6504fad4202a12fbbb2ea7c0da7f5c5a7e6cf720a46aabbf71dcd91c0f942b4

A.2.2 Security Management messages for CA

The ASN.1 module `EtsiTs102941MessagesCa` is identified by the Object Identifier {itu-t(0) identified-organization(4) etsi(0) itsDomain(5) wg5(5) ts(102941) messagesCa(0) version3(3)}. The module can be downloaded as a file as indicated in Table A.2. The associated SHA-256 cryptographic hash digest of the referenced file offers a means to verify the integrity of that file.

Table A.2: `EtsiTs102941MessagesCa` ASN.1 module information

Module name	EtsiTs102941MessagesCa
OID	`{ itu-t(0) identified-organization(4) etsi(0) itsDomain(5) wg5(5) ts(102941) messagesCa(0) major-version-3(3) minor-version-2(3)}`
Link	https://forge.etsi.org/rep/ITS/asn1/pki_ts102941/-/blob/v2.2.1/EtsiTs102941MessagesCa.asn
SHA-256 hash	b3292ebe38e937b9fb7d54efc67d97170ce6e2121abd6b1409cdb5c2e16514cc

NOTE: The EtsiTs102941DataContent is extended to add three additional options to support the messages defined in clause 6.2.0.1.

A.2.3 Security Management messages for ITS-S_WithPrivacy

The ASN.1 module `EtsiTs102941MessagesItss` is identified by the Object Identifier {itu-t(0) identified-organization(4) etsi(0) itsDomain(5) wg5(5) ts(102941) messagesItsss (1) version3(3)}. The module can be downloaded as a file as indicated in Table A.3. The associated SHA-256 cryptographic hash digest of the referenced file offers a means to verify the integrity of that file.

Table A.3: `EtsiTs102941MessagesItss` ASN.1 module information

Module name	EtsiTs102941MessagesItss
OID	`{ itu-t(0) identified-organization(4) etsi(0) itsDomain(5) wg5(5) ts(102941) messagesItss(1) major-version-3(3) minor-version-2(3)}`
Link	https://forge.etsi.org/rep/ITS/asn1/pki_ts102941/-/blob/v2.2.1/EtsiTs102941MessagesItss.asn
SHA-256 hash	555947e42bfb74aede98a2d170bb3dfdf518ad13379ed43132350b8bb319a0ce

NOTE: The EtsiTs102941DataContent is extended to add the additional option to support the TLM Link Certificate message defined in clause 6.2.0.1. Other additional choices are NULL.

A.2.4 Security Management messages for ITSS_NoPrivacy

The ASN.1 module `EtsiTs102941MessagesItss-OptionalPrivacy` is identified by the Object Identifier {itu-t(0) identified-organization(4) etsi(0) itsDomain(5) wg5(5) ts(102941) messagesItsss (1) version3(3)}. The module can be downloaded as a file as indicated in Table A.4. The associated SHA-256 cryptographic hash digest of the referenced file offers a means to verify the integrity of that file.

Table A.4: `EtsiTs102941MessagesItss-OptionalPrivacy` ASN.1 module information

Module name	EtsiTs102941MessagesItss-OptionalPrivacy
OID	`itu-t(0) identified-organization(4) etsi(0) itsDomain(5) wg5(5) ts(102941) messagesItssOp(2) major-version-3(3) minor-version-3(3)`
Link	https://forge.etsi.org/rep/ITS/asn1/pki_ts102941/-/blob/v2.2.1/EtsiTs102941MessagesItss-OptionalPrivacy.asn
SHA-256 hash	5b3694ee8374edb1319c8f026b3e90ece64ad7fb398bc35adf8494255daadac0

NOTE: The EtsiTs102941DataContent is extended to add the additional option to support the TLM Link Certificate message defined in clause 6.2.0.1. Other additional choices are NULL.

A.2.5 Enrolment and authorization data types

A.2.5.1 Enrolment

The ASN.1 module `EtsiTs102941TypesEnrolment` is identified by the Object Identifier {itu-t(0) identified-organization(4) etsi(0) itsDomain(5) wg5(5) ts(102941) enrolment(4) version3(3)}. The module can be downloaded as a file as indicated in Table A.5. The associated SHA-256 cryptographic hash digest of the referenced file offers a means to verify the integrity of that file.

Table A.5: `EtsiTs102941TypesEnrolment` ASN.1 module information

Module name	EtsiTs102941TypesEnrolment
OID	`itu-t(0) identified-organization(4) etsi(0) itsDomain(5) wg5(5) ts(102941) enrolment(4) major-version-3(3) minor-version-1(1)`
Link	https://forge.etsi.org/rep/ITS/asn1/pki_ts102941/-/blob/v2.2.1/EtsiTs102941TypesEnrolment.asn
SHA-256 hash	c712d158c49525b5e6102a4679bdea7aea641df25709292bffb221cf899bf545

A.2.5.2 Authorization

The ASN.1 module `EtsiTs102941TypesAuthorization` is identified by the Object Identifier {itu-t(0) identified-organization(4) etsi(0) itsDomain(5) wg5(5) ts(102941) authorization(5) version3(3)}. The module can be downloaded as a file as indicated in Table A.6. The associated SHA-256 cryptographic hash digest of the referenced file offers a means to verify the integrity of that file.

Table A.6: `EtsiTs102941TypesAuthorization` ASN.1 module information

Module name	EtsiTs102941TypesAuthorization
OID	`itu-t(0) identified-organization(4) etsi(0) itsDomain(5) wg5(5) ts(102941) authorization(5) major-version-3(3) minor-version-3(3)`
Link	https://forge.etsi.org/rep/ITS/asn1/pki_ts102941/-/blob/v2.2.1/EtsiTs102941TypesAuthorization.asn
SHA-256 hash	d915b7b5fb312437083f379edc60a0045205399983c8af025f5222f82a215381

A.2.5.3 AuthorizationValidation

The ASN.1 module `EtsiTs102941TypesAuthorizationValidation` is identified by the Object Identifier {itu-t(0) identified-organization(4) etsi(0) itsDomain(5) wg5(5) ts(102941) authorization(5) version3(3)}. The module can be downloaded as a file as indicated in Table A.7. The associated SHA-256 cryptographic hash digest of the referenced file offers a means to verify the integrity of that file.

Table A.7: `EtsiTs102941TypesAuthorizationValidation` ASN.1 module information

Module name	EtsiTs102941TypesAuthorizationValidation
OID	`itu-t(0) identified-organization(4) etsi(0) itsDomain(5) wg5(5) ts(102941) authValidation(7) major-version-3(3) minor-version-1(1)`
Link	https://forge.etsi.org/rep/ITS/asn1/pki_ts102941/-/blob/v2.2.1/EtsiTs102941TypesAuthorizationValidation.asn
SHA-256 hash	af36e281886b495f846a99d0b6656f07cda53972cc3c868026cb7c5226f8a7db

A.2.6 Offline message structures

The ASN.1 module `EtsiTs102941TypesCaManagement` is identified by the Object Identifier {itu-t(0) identified-organization(4) etsi(0) itsDomain(5) wg5(5) ts(102941) authorization(5) version3(3)}. The module can be downloaded as a file as indicated in Table A.8. The associated SHA-256 cryptographic hash digest of the referenced file offers a means to verify the integrity of that file.

Table A.8: `EtsiTs102941TypesCaManagement` ASN.1 module information

Module name	EtsiTs102941TypesCaManagement
OID	`itu-t(0) identified-organization(4) etsi(0) itsDomain(5) wg5(5) ts(102941) caManagement (8) major-version-3(3) minor-version-1(1)`
Link	https://forge.etsi.org/rep/ITS/asn1/pki_ts102941/-/blob/v2.2.1/EtsiTs102941TypesCaManagement.asn
SHA-256 hash	b20903849161b9c4784906833f35f0bc340c6cb8bc1d3e248e2cb965324e59ab

A.2.7 Trust lists data types

The ASN.1 module `EtsiTs102941TrustLists` is identified by the Object Identifier {itu-t(0) identified-organization(4) etsi(0) itsDomain(5) wg5(5) ts(102941) trustLists(6)version3(3)}. The module can be downloaded as a file as indicated in Table A.9. The associated SHA-256 cryptographic hash digest of the referenced file offers a means to verify the integrity of that file.

Table A.9: `EtsiTs102941TrustLists` ASN.1 module information

Module name	EtsiTs102941TrustLists
OID	`itu-t(0) identified-organization(4) etsi(0) itsDomain(5) wg5(5) ts(102941) trustLists(6) major-version-3(3) minor-version-1(1)`
Link	https://forge.etsi.org/rep/ITS/asn1/pki_ts102941/-/blob/v2.2.1/EtsiTs102941TrustLists.asn
SHA-256 hash	e0686b9c7c46205f236730aa7096f8adae56a773b4b0bee6c302904cd5a92505

A.2.8 Link certificate message data types

The ASN.1 module `EtsiTs102941TypesLinkCertificate` is identified by the Object Identifier {itu-t(0) identified-organization(4) etsi(0) itsDomain(5) wg5(5) ts(102941) linkCertificate(9) version3(3)}. The module can be downloaded as a file as indicated in Table A.10. The associated SHA-256 cryptographic hash digest of the referenced file offers a means to verify the integrity of that file.

Table A.10: `EtsiTs102941TypesLinkCertificate` ASN.1 module information

Module name	EtsiTs102941TypesLinkCertificate
OID	`itu-t(0) identified-organization(4) etsi(0) itsDomain(5) wg5(5) ts(102941) linkCertificate(9) major-version-3(3) minor-version-1(1)`
Link	https://forge.etsi.org/rep/ITS/asn1/pki_ts102941/-/blob/v2.2.1/EtsiTs102941TypesLinkCertificate.asn
SHA-256 hash	abbc7b9eafd9b7ede703f3c2e8d25d1996a3e81b43054515c13a47afbbb5b18d

A.3 Imported messages structures

A number of ASN.1 modules from IEEE 1609.2.1 [24] are essential for the operation of the core ASN.1 modules defined in clause A.2 of the present document.

Table A.11: `Ieee1609Dot2Crl` ASN.1 module information

Module name	Ieee1609Dot2Crl
OID	`iso(1) identified-organization(3) ieee(111) standards-association-numbered-series-standards(2) wave-stds(1609) dot2(2) crl(3) major-version-3(3) minor-version-2(2)`
Link	https://forge.etsi.org/rep/ITS/asn1/ieee1609.2/-/blob/2022-published/Ieee1609Dot2Crl.asn
SHA-256 hash	5b1f5612a151b8da4356797d217802a4e4eccd9f9fcd529bd257944c51b40ed5

Table A.12: `Ieee1609Dot2CrlBaseTypes` ASN.1 module information

Module name	Ieee1609Dot2CrlBaseTypes
OID	`iso(1) identified-organization(3) ieee(111) standards-association-numbered-series-standards(2) wave-stds(1609) dot2(2) crl(3) base-types(2) major-version-3(3) minor-version-2(2)`
Link	https://forge.etsi.org/rep/ITS/asn1/ieee1609.2/-/blob/2022-published/Ieee1609Dot2CrlBaseTypes.asn
SHA-256 hash	ffaa6d4aeb1135cdf8b77b368f912607b5a64192d538a83779d04d0e013b23f2

Table A.13: `Ieee1609Dot2Dot1AcaEeInterface` ASN.1 module information

Module name	Ieee1609Dot2Dot1AcaEeInterface
OID	`iso(1) identified-organization(3) ieee(111) standards-association-numbered-series-standards(2) wave-stds(1609) dot2(2) extension-standards(255) dot1(1) interfaces(1) aca-ee(1) major-version-2(2) minor-version-3(3)`
Link	https://forge.etsi.org/rep/ITS/asn1/ieee1609.2.1/-/blob/2022-published/Ieee1609Dot2Dot1AcaEeInterface.asn
SHA-256 hash	3e9e325e3b39ff2fe1e0eb328bd741170520d01d779fdec8d1c4bde60edf0a6e

Table A.14: `Ieee1609Dot2Dot1AcaLaInterface` ASN.1 module information

Module name	Ieee1609Dot2Dot1AcaLaInterface
OID	`iso(1) identified-organization(3) ieee(111) standards-association-numbered-series-standards(2) wave-stds(1609) dot2(2) extension-standards(255) dot1(1) interfaces(1) aca-la(2) major-version-2(2) minor-version-1(1)`
Link	https://forge.etsi.org/rep/ITS/asn1/ieee1609.2.1/-/blob/2022-published/Ieee1609Dot2Dot1AcaLaInterface.asn
SHA-256 hash	e26b8eba57105fb0165db47157780702422985c5c86e2c635ca0804e030b99e4

Table A.15: `Ieee1609Dot2Dot1AcaMaInterface` ASN.1 module information

Module name	Ieee1609Dot2Dot1AcaMaInterface
OID	`iso(1) identified-organization(3) ieee(111) standards-association-numbered-series-standards(2) wave-stds(1609) dot2(2) extension-standards(255) dot1(1) interfaces(1) aca-ma(3) major-version-2(2) minor-version-1(1)`
Link	https://forge.etsi.org/rep/ITS/asn1/ieee1609.2.1/-/blob/2022-published/Ieee1609Dot2Dot1AcaLaInterface.asn
SHA-256 hash	e26b8eba57105fb0165db47157780702422985c5c86e2c635ca0804e030b99e4

Table A.16: `Ieee1609Dot2Dot1AcaRaInterface` ASN.1 module information

Module name	Ieee1609Dot2Dot1AcaRaInterface
OID	`iso(1) identified-organization(3) ieee(111) standards-association-numbered-series-standards(2) wave-stds(1609) dot2(2) extension-standards(255) dot1(1) interfaces(1) aca-ra(4) major-version-3(3) minor-version-1(1)`
Link	https://forge.etsi.org/rep/ITS/asn1/ieee1609.2.1/-/blob/2022-published/Ieee1609Dot2Dot1AcaRaInterface.asn
SHA-256 hash	ba6d088314e84aba616b60f1f66213ddac59871aa6b4dd4c0e67c28b03364ad0

Table A.17: `Ieee1609Dot2Dot1Acpc` ASN.1 module information

Module name	Ieee1609Dot2Dot1Acpc
OID	`iso(1) identified-organization(3) ieee(111) standards-association-numbered-series-standards(2) wave-stds(1609) dot2(2) extension-standards(255) dot1(1) interfaces(1) acpc(18) major-version-3(3) minor-version-1(1)`
Link	https://forge.etsi.org/rep/ITS/asn1/ieee1609.2.1/-/blob/2022-published/Ieee1609Dot2Dot1Acpc.asn
SHA-256 hash	274eac6a838365f27c4b2e57c9fc3fe631d01f8a102ba78f23b1aade4ee774e8

Table A.18: `Ieee1609Dot2Dot1CamRaInterface` ASN.1 module information

Module name	Ieee1609Dot2Dot1CamRaInterface
OID	`iso(1) identified-organization(3) ieee(111) standards-association-numbered-series-standards(2) wave-stds(1609) dot2(2) extension-standards(255) dot1(1) interfaces(1) cam-ra(19) major-version-2(2) minor-version-2(2)`
Link	https://forge.etsi.org/rep/ITS/asn1/ieee1609.2.1/-/blob/2022-published/Ieee1609Dot2Dot1CamRaInterface.asn
SHA-256 hash	1ad2d323bc1df046e2754a818daedbb27c4403084f7bf93f4192e5118d9898c8

Table A.19: `Ieee1609Dot2Dot1CertManagement` ASN.1 module information

Module name	Ieee1609Dot2Dot1CertManagement
OID	`iso(1) identified-organization(3) ieee(111) standards-association-numbered-series-standards(2) wave-stds(1609) dot2(2) extension-standards(255) dot1(1) interfaces(1) cert-management(7) major-version-3(3) minor-version-1(1)`
Link	https://forge.etsi.org/rep/ITS/asn1/ieee1609.2.1/-/blob/2022-published/Ieee1609Dot2Dot1CertManagement.asn
SHA-256 hash	2ae224980487e9b76e02884aacd724316a4290d165d0f55e593d542b44ec28f1

Table A.20: `Ieee1609Dot2Dot1EcaEeInterface` ASN.1 module information

Module name	Ieee1609Dot2Dot1EcaEeInterface
OID	`iso(1) identified-organization(3) ieee(111) standards-association-numbered-series-standards(2) wave-stds(1609) dot2(2) extension-standards(255) dot1(1) interfaces(1) eca-ee(9) major-version-3(3) minor-version-1(1)`
Link	https://forge.etsi.org/rep/ITS/asn1/ieee1609.2.1/-/blob/2022-published/Ieee1609Dot2Dot1EcaEeInterface.asn
SHA-256 hash	5a808bb3209241cd55cbbeee257629076cc0574d507dfba90a4a69a4dc081cbf

Table A.21: `Ieee1609Dot2Dot1EeMaInterface` ASN.1 module information

Module name	Ieee1609Dot2Dot1EeMaInterface
OID	`iso(1) identified-organization(3) ieee(111) standards-association-numbered-series-standards(2) wave-stds(1609) dot2(2) extension-standards(255) dot1(1) interfaces(1) ee-ma(10) major-version-2(2) minor-version-1(1)`
Link	https://forge.etsi.org/rep/ITS/asn1/ieee1609.2.1/-/blob/2022-published/Ieee1609Dot2Dot1EeMaInterface.asn
SHA-256 hash	0e31e548070ca9af2a73fa607fffd52cfdbbb77f3d5e64abf9ab0aabf2450580

Table A.22: `Ieee1609Dot2Dot1EeRaInterface` ASN.1 module information

Module name	Ieee1609Dot2Dot1EeRaInterface
OID	`iso(1) identified-organization(3) ieee(111) standards-association-numbered-series-standards(2) wave-stds(1609) dot2(2) extension-standards(255) dot1(1) interfaces(1) ee-ra(11) major-version-3(3) minor-version-1(1)`
Link	https://forge.etsi.org/rep/ITS/asn1/ieee1609.2.1/-/blob/2022-published/Ieee1609Dot2Dot1EeRaInterface.asn
SHA-256 hash	5f96c040dfc9282aa11089a7961dc542bb58fc9f03b05c198c4b086c4a90c2fa

Table A.23: `Ieee1609Dot2Dot1LaMaInterface` ASN.1 module information

Module name	Ieee1609Dot2Dot1LaMaInterface
OID	`iso(1) identified-organization(3) ieee(111) standards-association-numbered-series-standards(2) wave-stds(1609) dot2(2) extension-standards(255) dot1(1) interfaces(1) la-ma(12) major-version-2(2) minor-version-1(1)`
Link	https://forge.etsi.org/rep/ITS/asn1/ieee1609.2.1/-/blob/2022-published/Ieee1609Dot2Dot1LaMaInterface.asn
SHA-256 hash	003c19ce857aff7350835094ff532b51a07e758bd375c67139845096faa7b96b

Table A.24: `Ieee1609Dot2Dot1LaRaInterface` ASN.1 module information

Module name	Ieee1609Dot2Dot1LaRaInterface
OID	`iso(1) identified-organization(3) ieee(111) standards-association-numbered-series-standards(2) wave-stds(1609) dot2(2) extension-standards(255) dot1(1) interfaces(1) la-ra(13) major-version-2(2) minor-version-1(1)`
Link	https://forge.etsi.org/rep/ITS/asn1/ieee1609.2.1/-/blob/2022-published/Ieee1609Dot2Dot1LaRaInterface.asn
SHA-256 hash	c3e599663f5e770785fb532ad886191dd82b06a63568caf7e91c59d5f7a65420

Table A.25: `Ieee1609Dot2Dot1MaRaInterface` ASN.1 module information

Module name	Ieee1609Dot2Dot1MaRaInterface
OID	`iso(1) identified-organization(3) ieee(111) standards-association-numbered-series-standards(2) wave-stds(1609) dot2(2) extension-standards(255) dot1(1) interfaces(1) ma-ra(14) major-version-2(2) minor-version-1(1)`
Link	https://forge.etsi.org/rep/ITS/asn1/ieee1609.2.1/-/blob/2022-published/Ieee1609Dot2Dot1MaRaInterface.asn
SHA-256 hash	61321da9ee2967d9f151c1d0cd2de554b5970f9d9502fd2caa5814aa9f4ddbfc

Table A.26: `Ieee1609Dot2Dot1Protocol` ASN.1 module information

Module name	Ieee1609Dot2Dot1Protocol
OID	`iso(1) identified-organization(3) ieee(111) standards-association-numbered-series-standards(2) wave-stds(1609) dot2(2) extension-standards(255) dot1(1) interfaces(1) protocol(17) major-version-3(3) minor-version-1(1)`
Link	https://forge.etsi.org/rep/ITS/asn1/ieee1609.2.1/-/blob/2022-published/Ieee1609Dot2Dot1Protocol.asn
SHA-256 hash	b98b1c982b17776a38dc3cf2150cfd1c080c072be2dac35950ce386cf51045ed

Table A.27: `EtsiTs103097ExtensionModule` ASN.1 module information

Module name	EtsiTs103097ExtensionModule
OID	`itu-t(0) identified-organization(4) etsi(0) itsDomain(5) wg5(5) secHeaders(103097) extension(2) major-version-1(1) minor-version-1(1)`
Link	https://forge.etsi.org/rep/ITS/asn1/sec_ts103097/blob/v2.1.1/EtsiTs103097ExtensionModule.asn
SHA-256 hash	a6d68f030f66ff77cac43f2ca4d40245805b09b3b123cf960ebb29ace9817c0a

Table A.28: `EtsiTs103097Module` ASN.1 module information

Module name	EtsiTs103097Module
OID	`itu-t(0) identified-organization(4) etsi(0) itsDomain(5) wg5(5) secHeaders(103097) core(1) major-version-3(3) minor-version-1(1)`
Link	https://forge.etsi.org/rep/ITS/asn1/sec_ts103097/blob/v2.1.1/EtsiTs103097Module.asn
SHA-256 hash	ef6d97bd97a8cfb080f25e9652a7b861dd2cd17e2586ed55729d631b5e909308

Table A.29: `Ieee1609Dot2` ASN.1 module information

Module name	Ieee1609Dot2
OID	`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) minor-version-6(6)`
Link	https://forge.etsi.org/rep/ITS/asn1/ieee1609.2/blob/2022-published/Ieee1609Dot2.asn
SHA-256 hash	990de68dc76dfe235c999c5f5de973b989167b61b7cc29e000e81c38a28ce609

Table A.30: `Ieee1609Dot2BaseTypes` ASN.1 module information

Module name	Ieee1609Dot2BaseTypes
OID	`iso(1) identified-organization(3) ieee(111) standards-association-numbered-series-standards(2) wave-stds(1609) dot2(2) base(1) base-types(2) major-version-2(2) minor-version-4(4)`
Link	https://forge.etsi.org/rep/ITS/asn1/ieee1609.2/blob/2022-published/Ieee1609Dot2BaseTypes.asn
SHA-256 hash	cc0fe455d56e33692907325e8c927db8fd1d7d927ce03a2c43f4580098bb7191

Annex B (normative): Service Specific Permissions (SSP) definition

B.1 Overview

Service permissions are indicated by a pair of identifiers within a certificate, the ITS-AID and the SSP. The ITS-Application Identifier (ITS-AID) as given in ETSI TS 102 965 [19] indicates the overall type of permission(s) being granted.

The Service Specific Permissions (SSP) is a field that indicates specific sets of permissions within the overall permissions indicated by the ITS-AID. The originating ITS-S shall provide SSP information in its certificate for all generated signed messages.

The SSP information for Security Management messages is constructed in a common way, containing 1 or more octets depending of the actual service. 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 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, SSP contains information as defined in the present document.

2 to 255: Reserved for future usage.

B.2 CTL SSP definition

The interpretation of the CTL SSP octet scheme is defined as depicted in Figure B.1.

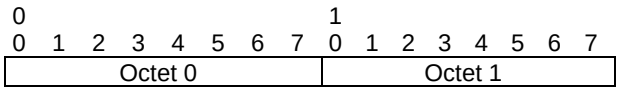


Figure B.1: The CTL SSP schema

The SSP for the CTL service shall be of 2 octets length, corresponding to the scheme defined in Table B.1.

Table B.1: Octet Scheme for CTL SSP

Octet #	Description
0	SSP version control
1	Service-specific parameters

The service specific parameter bits shall be as defined in Table B.2.

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	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	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	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	

According to clauses 6.3.1 and 6.3.2 of the present document, only combinations of SSP defined in the Table B.3 shall be allowed.

Table B.3: Allowed combinations of CTL SSP

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

B.3 CRL SSP definition

The interpretation of the CRL SSP octet scheme is defined as depicted in Figure B.2.

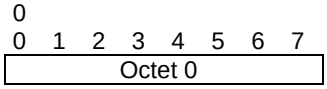


Figure B.2: The CRL SSP schema

The SSP for the CTL service shall be of 1 octet length, containing the SSP version control only.

B.4 Certificate request messages SSP definition

The interpretation of the Certificate Request SSP octet scheme is defined as depicted in Figure B.3.

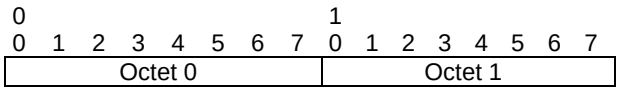


Figure B.3: The Security Management SSP schema

The SSP for the Security Management service shall be of 2 octets length, corresponding to the scheme defined in Table B.4.

Table B.4: Octet Scheme for Security Management SSP

Octet #	Description
0	SSP version control
1	Service-specific parameters

The service specific parameter shall be as defined in Table B.5.

Table B.5: Security Management service-specific permissions

Bit position	Permission	Bit Value
0 (80h)	The certificate can be used to sign the Enrolment Request messages	0: certificate not allowed to sign 1: certificate allowed to sign
1 (40h)	The certificate can be used to sign the Authorization Request messages	0: certificate not allowed to sign 1: certificate allowed to sign
2 (20h)	The certificate can be used to sign the AuthorizationValidation Request messages	0: certificate not allowed to sign 1: certificate allowed to sign
3 (10h)	The certificate can be used to sign the Authorization Response messages	0: certificate not allowed to sign 1: certificate allowed to sign
4 (08h)	The certificate can be used to sign the Authorization Validation Response messages	0: certificate not allowed to sign 1: certificate allowed to sign
5 (04h)	The certificate can be used to sign the Enrolment Response messages	0: certificate not allowed to sign 1: certificate allowed to sign
6 (02h)	The certificate can be used to sign the CA Certificate Request messages	0: certificate not allowed to sign 1: certificate allowed to sign
7 (01h)	Unused	

B.5 Security Management certificate permissions

The overall allowance of certificate permissions for Security Management purpose is defined in Table B.6.

Table B.6: SM_PDU certificate permissions

ITS Entity	Certificate	CTL SSP					CRL	Secured Certificate Request SSP						
		TLM entry (bit 0)	RootCA entry (bit 1)	EA entry (bit 2)	AA entry (bit 3)	DC entry (bit 4)		Enr Req (bit 0)	Auth Req (bit 1)	Auth Valid Req (bit 2)	Auth Resp (bit 3)	Auth Valid Resp (bit 4)	Enr Resp (bit 5)	CA Cert Req (bit 6)
TLM	TLM	A	A	-	-	A	-	-	-	-	-	-	-	-
RootCA	Root	-	-	A	A	A	A	I	I	I	I	I	I	I
EA	EA	-	-	-	-	-	-	I	I	-	-	A	A	A
AA	AA	-	-	-	-	-	-	-	-	A	A	-	-	A
ITS-S	EC	-	-	-	-	-	-	A	A	-	-	-	-	-
	AT	-	-	-	-	-	-	-	-	-	-	-	-	-

A Certificate may contain correspondent application permission.
I Certificate may contain correspondent certificate issuing permission.
- Certificate shall not contain correspondent permission.

All issuing permissions, described in Table B.6, shall be included in the `certIssuePermissions` field of the certificate with EndEntityType containing 'app', permitting to include these permissions into the `appPermissions` field of subordinated certificates.

Annex C (informative): Communication profiles for security credential provisioning services (EC request, AT request)

C.0 General

All the messages exchanged are sent as HTTP POST requests. HTTP/1.1 is used.

Parameters for the POST requests and responses are described in the tables below containing the corresponding messages descriptions.

NOTE: Additional authorization information, such as OAuth access tokens, may be added to requests that are signed with a X.509 enrolment credential if the certificate does not contain authorization information. When ETSI certificates are used, authorization is performed based on the certificate request message SSP in the ETSI certificate defined in clause B.4.

Table C.1: Enrolment Credential Request

POST http://<ea_access_point>
Inputs:
• Content-type: application/x-its-request
• Content: binary encoded EnrolmentRequestMessage object
Outputs:
• Content-type: application/x-its-response
• Content: binary encoded EnrolmentResponseMessage object

Table C.2: Request Authorization Ticket (AT)

POST http://<aa_access_point>
Inputs:
• Content-type: application/x-its-request
• Content: binary encoded AuthorizationRequestMessage object
Outputs:
• Content-type: application/x-its-response
• Content: binary encoded AuthorizationResponseMessage object

Table C.3: Request Authorization Ticket (AT) with PoP

POST http://<aa_access_point>
Inputs:
• Content-type: application/x-its-request
• Content: binary encoded AuthorizationRequestMessageWithPop object
Outputs:
• Content-type: application/x-its-response
• Content: binary encoded AuthorizationResponseMessage object

Table C.4: Validate Authorization Ticket (AT) request

POST http://<ea_access_point>
Inputs:
• Content-type: application/x-its-request
• Content: binary encoded AuthorizationValidationRequestMessage object
Outputs:
• Content-type: application/x-its-response
• Content: binary encoded AuthorizationValidationResponseMessage object

C.1 Communication profiles description

This annex follows the CVRIA approach ([i.14]) for the specification of the layered sets of communications protocols that are required to support communications between the ITS-S and other ITS stations and PKI authorities.

Figure C.1, Figure C.2, Figure C.3 and Figure C.4 specify the communication protocols of the requesting ITS-S for different communication media (cellular networks or ITS G5 access network).

Figure C.1 specifies the communication protocols that should be used between the ITS-S and the PKI authorities when a cellular network connection is used. It shows the mapping to ITS-S Communication layers such as specified in ETSI EN 302 665 [i.25]. This figure specifies the reference points S_2 and S_3 in the model of Figure 10.

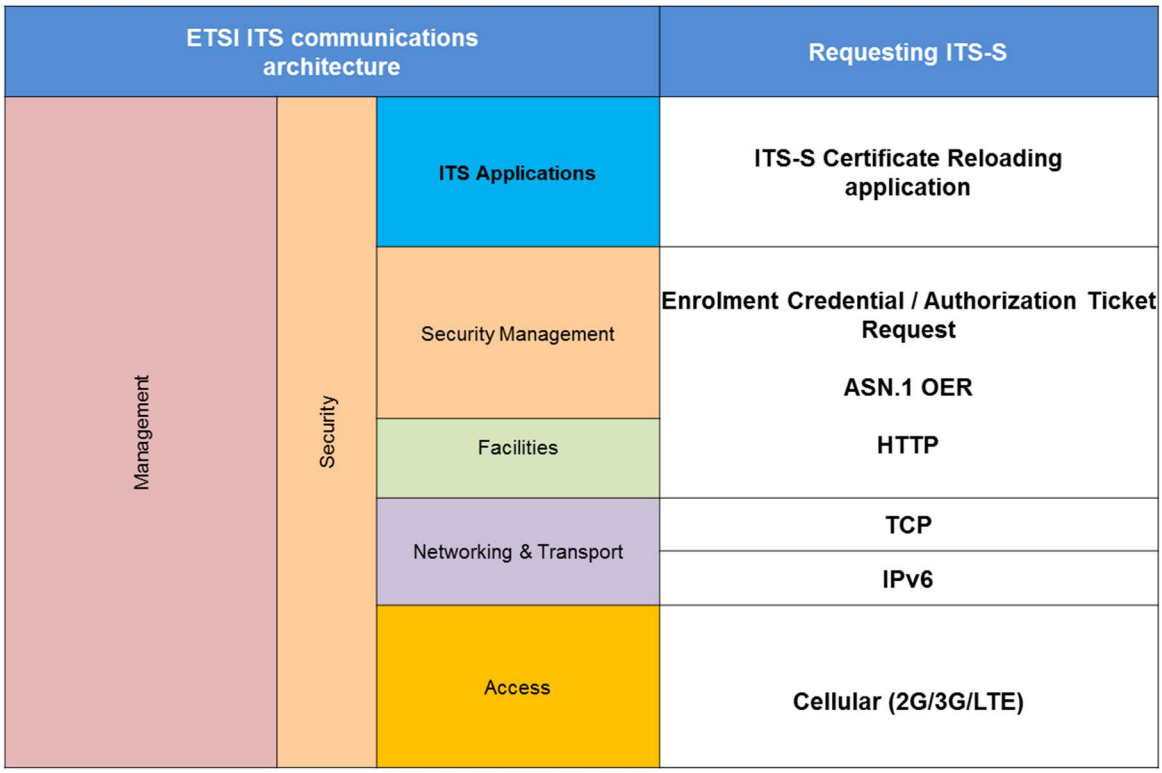


Figure C.1: Communication protocols between Requesting ITS-S and PKI authorities using cellular networks

Figure C.2, Figure C.3 and Figure C.4 depict the possible communication stacks of the requesting ITS-S when communication is based on ITS G5 media. These figures specify alternative communication profiles available on ITS G5 and the required security services that should be applied for message authentication. These figures specify the reference points S_1 between the requesting ITS-S and the Relaying ITS-S or the ITS-S Roadside Gateway shown in Figure 11.

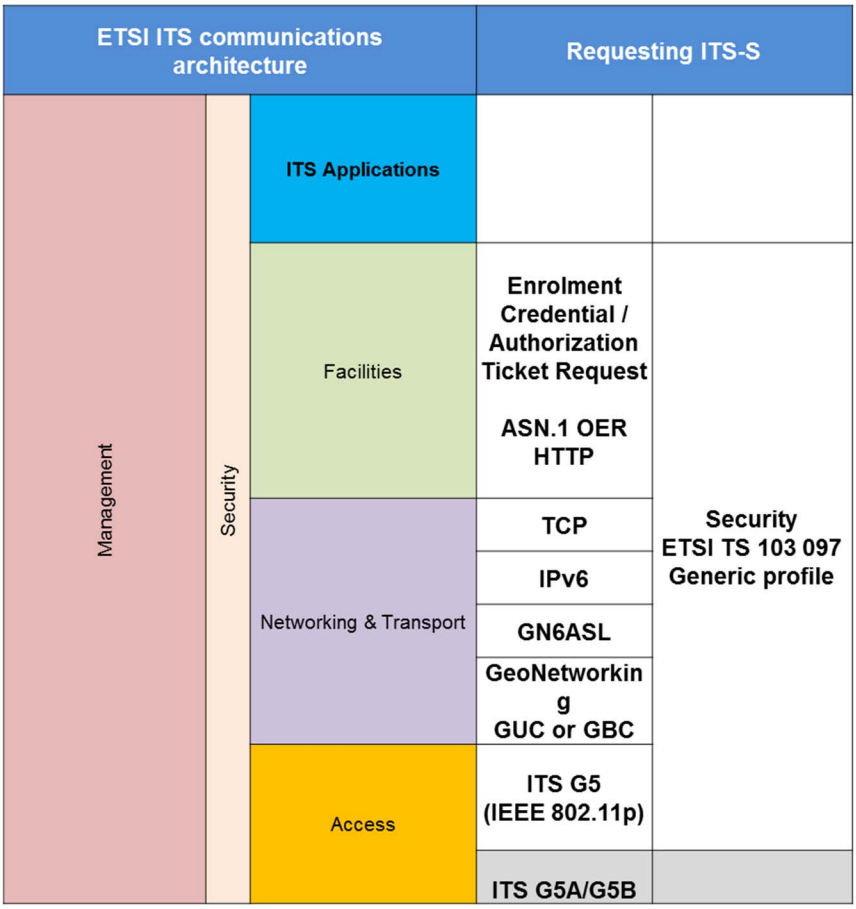


Figure C.2: Communication protocols of the Requesting ITS-S Vehicle and ITS-S Roadside Gateway using Ipv6 over GeoNetworking

NOTE 1: With respect to Figure C.2, the protocol layers include GN6ASL as specified in ETSI TS 103 636-6-1 [16] and the Ipv6 (and mobility extensions as defined in [i.15]).

NOTE 2: Security management services may use any service channel (SCH) available in the ITS G5A, except the CCH channel reserved for safety messages or other supplementary ITS channels when available (G5B, G5D).

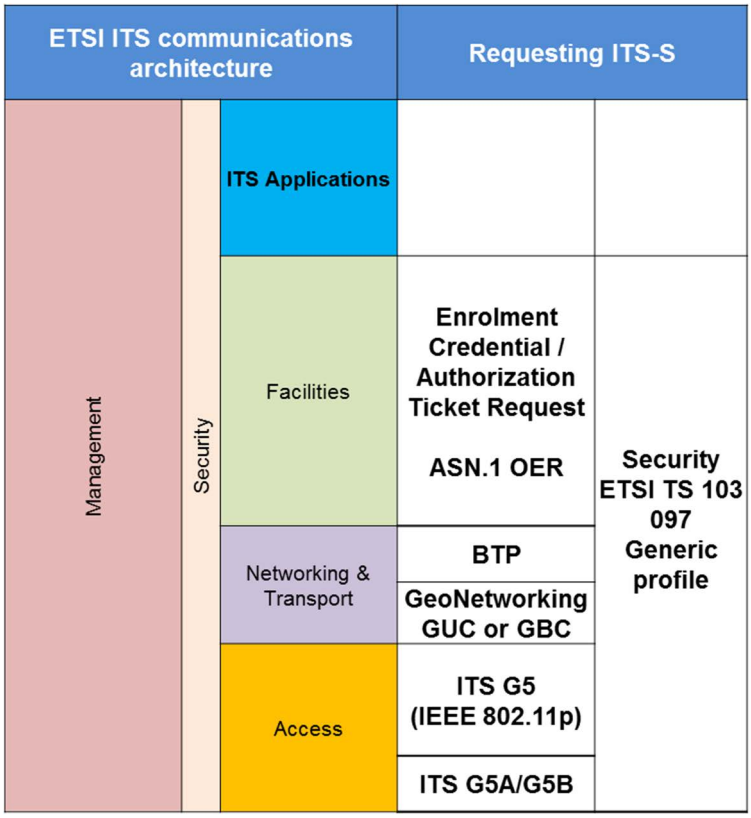


Figure C.3: Communication protocols between Requesting ITS-S Vehicle and ITS-S Roadside Gateway using GN/BTP protocol

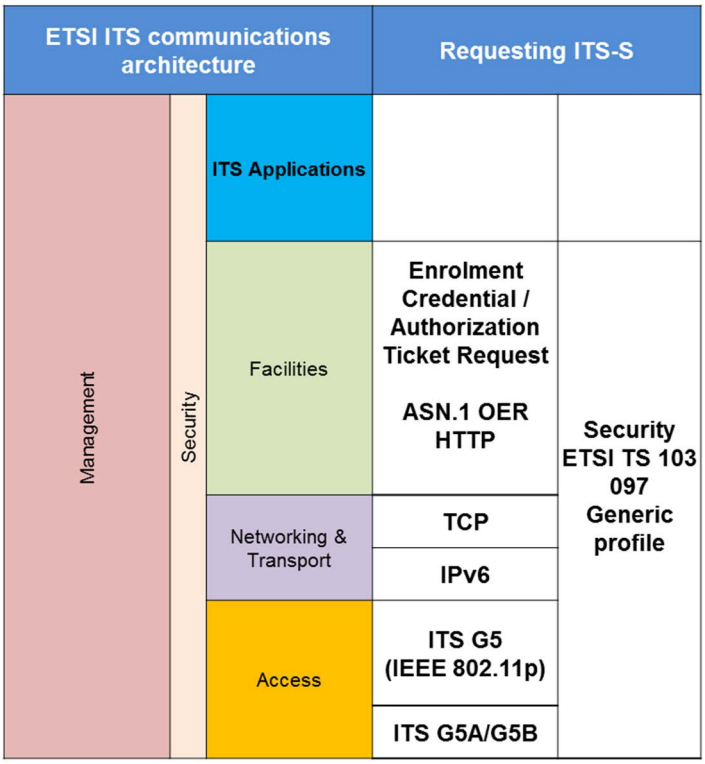


Figure C.4: Communication protocols of the Requesting ITS-S Vehicle and ITS-S Roadside Gateway using Ipv6 over G5

Figure C.5 specifies the communication path and the communication protocols used between the requesting ITS-S and the PKI when V2I communication is based on Ipv6 over GeoNetworking, for sending a service request to the CCMS, for instance requesting a EC (or AT) certificate to the EA (or AA).

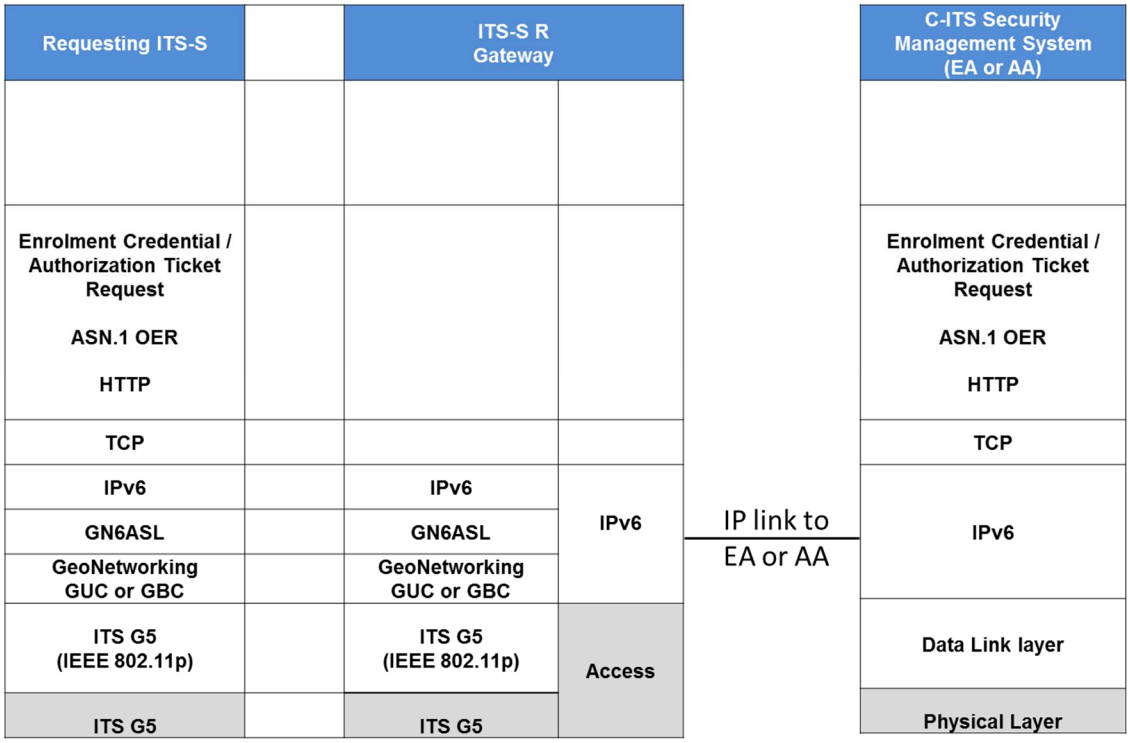


Figure C.5: Communication path between requesting ITS-S and PKI authorities

Annex D (normative): Communication profiles for CTL and CRL

D.1 CTL request and response protocol

In order to obtain the CTL from a Distribution Centre, an ITS-S may contact the DC using an HTTP GET as specified in Table D.1 using the Certificate Identifier of its Root CA (HashedID8) or the Certificate Identifier of a trusted Root CA included in the ECTL.

Table D.1: Get CTL

GET http://dc_access_point/getctl/HashedId8/ctlSequence The abs_path part of the HTTP request is built by taking the DC access point (from the CTL or from an ad-hoc configuration), appending "/getctl/" and the uppercase hexadecimal representation of HashedId8, then appending the /ctlSequence if necessary. Where the last part /ctlSequence may be missing. If /ctlSequence is specified, the DC shall provide the deltaCTL of sequence ctlSequence issued by the entity identified by HashedId8. If /ctlSequence is ABSENT, the DC shall provide the latest fullCTL issued by the entity identified by HashedId8. Inputs: • No inputs Outputs: • Content-type: application/x-its-ctl • Content: binary encoded CTL object issued by the entity identified by HashedId8

The format of CTL is described in clause A.2.7.

D.2 CRL request and response protocol

In order to obtain the CRL from a Distribution Centre, an ITS-S may contact the DC using an HTTP GET as specified in Table D.2 using the Certificate Identifier of its Root CA (HashedID8) or the Certificate Identifier of a trusted Root CA included in the ECTL.

Table D.2: Get CRL

GET http://dc_access_point/getcrl/HashedId8 The abs_path part of the HTTP request is built by taking the DC access point (from the CTL or from an ad-hoc configuration), appending "/getcrl/", and the uppercase hexadecimal representation of HashedId8. Inputs: • No inputs Outputs: • Content-type: application/x-its-crl • Content: binary encoded CRL object issued by the entity identified byHashedId8

The format of CRL is described in clause A.2.7.

D.3 Broadcast communication of CTL/CRL

This clause specifies the communication profile which may be used for transmitting the trust information list such as the CRL or CTL on ITS G5.

To provide a CTL/ CRL broadcasting service over G5, the RSU shall provide a proxy application which periodically transmits updated trust list information issued by the Distribution Centre. The Trust List message shall be sent in one-hop (SHB packets) using the GeoNetworking protocol specified in ETSI TS 103 636-4-1 [18].

The size of CRL/CTL messages to be transmitted should be small, using the CRL/ DeltaCTL format structures as specified in clause A.2.3. No data segmentation/reassembling is provided in the lower or upper protocol layers depicted in Figure D.1.

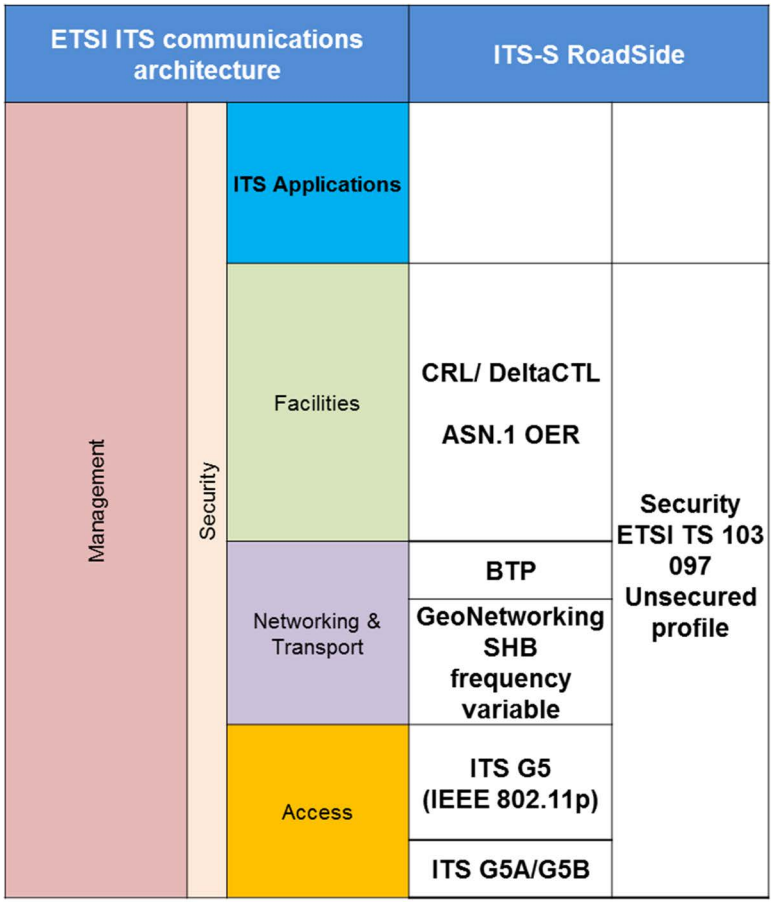


Figure D.1: Communication protocols for CRL/CTL transmission using GN/BTP protocol over G5

Annex E (normative): Communication profiles for TLM Certificates, TLM Link Certificate Messages, ECTLs and delta ECTLs access

E.1 CPOC HOST URL Definition

In order to provide a machine-readable interface, the distribution of TLM certificates, TLM Link certificate messages, ECTLs and delta ECTLs shall be done via a defined HOST URL of the CPOC distribution centre.

NOTE 1: In the EU C-ITS Security Credential Management System (EU CCMS), the CPOC HOST URL is currently set to cpoc.jrc.ec.europa.eu [i.26].

Naming scheme and interpretation of TLM name

The TLM certificate profile specified in ETSI TS 103 097 [3], clause 7.2.5 requires that the CertificateId component of the `ToBeSignedCertificate` contains the TLM unique name of type string (`UTF8String(SIZE(0..255))`).

In the EU CCMS a mandatory naming scheme for TLM name in the `CertificateID` component is specified as well as a naming scheme and names meaning for Root CAs ([i.26]).

NOTE 2: In the EU CCMS, the naming scheme for TLM certificates is specified as follows allowing to be able to reflect different possible levels of its operating environment:

- the `CertificateID` in TLM Certificates consists of the pre-fix "`EU-TLM`" and an optional <`TLM-ENVIRONMENT`> component, combined with a separator ("_"): `EU-TLM_<TLM-ENVIRONMENT>;`
- the `<TLM-ENVIRONMENT>` post-fix is an optional component which is set by the TLM to create TLM certificates which are used to sign specific ECTLs for specific RCA certificate environments (in this case the same optional `<RCA_ENVIRONMENT>` field is set in the RCA CertificateID component of the `ToBeSignedCertificate`). If the post-fix is ABSENT, the regular operational TLM entity used to sign the ECTL.

The following clauses assume that the name for the "default TLM" (i.e. the regular operational TLM entity used for the operation of deployed C-ITS services) is specified and hence the ECTL issued by these TLM certificates is called "`default ECTL`".

E.2 Request of TLM certificate

```
GET http(s)://<HOST>/[<subpath>]/gettlmcertificate/[<HashedId8>]
```

The absolute path in the GET request shall be set to `<HOST>/[<subpath>]` where the <HOST> is the URL of the CPOC Distribution Centre and [<subpath>] may optionally contain a defined value in order to enable the CPOC to provide different sets of TLM Certificates and ECTLs using this specific access point:

- Inputs:
  - `<HOST>`: The fixed hostname as described in clause E.1.
  - `<subpath>:` Optional as described above.
  - `<HashedId8>`: Optional: The HashedId8 of the requested TLM certificate. If omitted, the latest valid TLM certificate will be returned.
- Outputs:
  - Content-type: application/octet-stream.

- Content: The requested TLM certificate, COER-encoded of type `EtsiTs103097Certificate`.

If the `<subpath>` is omitted, the CPOC shall either return:

- the TLM Certificate used to sign ECTLs for RCA certificates where no specific RCA environment is set; or

NOTE: What is currently provided as such "default ECTL" in the EU CCMS is subject to decision of the CPA which instructs the CPOC accordingly.

- no file at all.

E.3 Request of TLM link certificate message

```
GET http(s)://<HOST>/[<subpath>]/gettlmlinkcertificate/[<HashedId8>]
```

- Inputs:
  - `<HOST>`: The fixed hostname as described in clause E.1.
  - `<subpath>:` Optional as described in clause E.2.
  - `<HashedId8>`: Optional: The HashedId8 of the TLM certificate to which the TLM link certificate message links to. If omitted, the link certificate message linking to the latest issued and valid TLM certificate ("current valid TLM Certificate") will be returned.
- Return value:
  - Content-type: application/octet-stream.
  - Content: The requested TLM link certificate message (as specified in clause 6.4).

If the `<subpath>` is omitted, the CPOC shall either return:

- the TLM link certificate message establishing the link to the specified TLM Certificate (through its certificate digest `HashedId8`)used to sign ECTLs for RCA certificates where no specific RCA environment is set; or

NOTE: What is currently provided as such "default ECTL" in the EU CCMS is subject to decision of the CPA which instructs the CPOC accordingly.

- no file at all.

E.4 Request of full ECTL

```
GET http(s)://<HOST>/[<subpath>]/getectl/HashedId8
```

- Inputs:
  - `<HOST>`: The fixed hostname as described in clause E.1.
  - `<subpath>:` Optional as described in clause E.2.
  - `<HashedId8>`: The HashedId8 of the signing TLM certificate which shall return the last ECTL signed by that TLM certificate.
- Outputs:
  - Content-type: application/octet-stream.
  - Content: The requested full ECTL, COER-encoded of type `TlmCertificateTrustListMessage`.

Even if the TLM has already re-keyed its TLM Certificate, the TLM shall continue to provide the last ECTL signed with the specific (old) TLM Certificate through the above GET command.

If the <subpath> is omitted, the CPOC shall either return:

- the full ECTL containing RCA certificates where no specific RCA environment is set; or

NOTE: What is currently provided as such "default ECTL" in the EU CCMS is subject to decision of the CPA which instructs the CPOC accordingly.

- no file at all.

E.5 Request of delta ECTL

```
GET http(s)://<HOST>/[<subpath>]/getdeltaectl/<HashedId8>/[<EctlSequenceNumber>]
```

- Inputs:.
  - <HOST>: The fixed hostname as described in clause E.1.
  - <subpath>: Optional as described in clause E.2.
  - <HashedId8>: The HashedId8 of the signing TLM certificate.
  - <EctlSequenceNumber>: Optional: The sequence number of the requested delta ECTL. If omitted, the latest delta ECTL will be returned.
- Outputs:
  - Content-type: application/octet-stream.
  - Content: The requested delta ECTL, COER-encoded of type TlmCertificateTrustListMessage.

The EctlSequenceNumber of range [0...255] in (delta) ECTLs is reset to 0 with every new signing TLM certificate (i.e. with each TLM re-key and the first signing of a new ECTL making use of the new re-keyed TLM certificate). This is done in order to reduce the chance of overruns of EctlSequenceNumber during the lifetime of each used TLM certificate. In case the TLM has to sign more than 255 (delta) ECTLs during the validity period of a TLM certificate, the TLM shall re-key its TLM certificate before it reaches 255.

If the <subpath> is omitted, the CPOC shall either return:

- the delta ECTL containing RCA certificates where no specific RCA environment is set; or

NOTE: What is currently provided as such "default ECTL" in the EU CCMS is subject to decision of the CPA which instructs the CPOC accordingly.

- no file at all.

Annex F (informative): Encryption of a message from a sender to a receiver

This annex describes cryptographic operations to be implemented to encrypt a message using mechanisms compliant with the present document. Message encryption is used for example to encrypt EC requests or AT requests.

The message is encrypted with a freshly generated symmetric key (AES-CCM key). Then, this symmetric key is encrypted with the public key of the receiver (using ECIES) and transmitted alongside the encrypted message.

Detailed description

Parameters

- Key Derivation Function (KDF). Here: KDF(S) = SHA256(S || counter).
- Symmetric encryption algorithm for ECIES. Here a XOR function is used ($E(m, k) = m \oplus k$, $E^{-1}(c, k) = c \oplus k$). This should not be confused with AES-CCM which is used for message encryption.
- Message Authentication Code (MAC). Here: MAC (m, km) = HMAC (m, km).
- Elliptic curve parameters (p: curve prime, G: base point, q: base point order, O point at infinity).
- ||: concatenation.

Encryption

Input

m: Message of the sender.

Kr: Encryption public key of the receiver.

Output

C: Encryption of the message m with AES-CCM concatenated with CCM authentication tag.

V: ECIES ephemeral public key.

c: encryption of the AES-CCM key used to encrypt m.

t: ECIES authentication tag.

Algorithm

1) The sender encrypts the message with AES-CCM:
   a) Sender generates a random AES key A (16 octets).
   b) Sender chooses a random nonce n, 12 octets.
   c) Sender encrypts the message m with AES-CCM mode using the key A and the nonce n. The output is the value C that consists of the encrypted message followed by the encrypted authentication value.
2) The sender encrypts the key A with ECIES:
   a) Sender generates an ephemeral private key r in [1, q-1], and the associated public key V=r.G, 33 octets if compressed.
   b) Sender derives a shared secret S from receiver encryption public key Kr:
      S = Px, where Px is the x-coordinate of the point P = r.Kr = (Px, Py). (verify that P != O, if not, back to previous step).
   c) Sender then derives a set of keys ke and km with derivation algorithm: (ke || km)=KDF(S), ke is 16 octets long, km is 32 octets long.

d) Sender encrypts the AES key: c=E(A, ke), c is 16 octets long.

e) Sender produces a tag on the encrypted message: t=MAC(c, km), t is 16 octets long.

3) Sender transmits to the receiver a message containing:

- The identifier for the recipient's certificate (cert_id), 8 octets.
- The encrypted message C.
- The encryption parameters (algorithm identifier aes_128_ccm, nonce n), 13 octets.
- The ephemeral public key (V).
- The encrypted key (c) with the associated tag (t).

Decryption

Input

kr: Private key of the receiver.

n: Nonce used for AES-CCM.

C: Output of the AES-CCM encryption: encrypted message || CCM tag.

V: ECIES ephemeral public key.

c: encryption of the AES-CCM key used to encrypt m.

t: ECIES authentication tag.

Output

m: Message of the sender or *failed* if any of the checks fails.

Algorithm

1) ECIES decryption to get the AES-CCM key A:

a) Receiver derives a shared secret S=Px, with (Px, Py)=kr.V or outputs *failed* if s.V = O.

b) Receiver derives the keys (ke || km)=KDF(S).

c) Receiver checks that the tag t=MAC(c, km), if not, receiver outputs *failed*.

d) Receiver decrypts the key $A = E^{-1}(c, ke) = c \oplus ke$.

2) AES-CCM decryption and verification of the message:

a) Receiver decrypts the encrypted message part of C using AES-CCM with the key A.

b) Receiver checks the validity of the authentication tag computed on the plaintext, if it is not valid, receiver outputs *failed*.

NOTE: It is important that the nonce of CCM should be carefully chosen to never be used more than once for a given key.
To avoid timing attacks, the output of decryption should be given after performing all the computations even if it outputs failed.

Annex G (informative): Bibliography

- ETSI TS 103 898: "Intelligent Transport Systems (ITS); Communications Architecture; Release 2".
- 26th International Conference on Computer Communication and Networks (ICCCN), July 2017: "Securing PKI Requests for C-ITS Systems", JP. Monteuuis, Badis Hammi, Eduardo Sallés, Houda Labiod, Rémi Blancher, Erwan Abalea, Brigitte Lonc.
- ISE Project (SystemX): "PKI system requirements specification, v1.1", (PUBLIC); March 2015.
- ISE Project (SystemX): "PKI architecture and technical specifications, v1.1", (PUBLIC), July 2015.
- SCOOP@F technical specifications Release 2: Deliverable 2.4.4.6: "PKI architecture and technical specifications", May 2016.

NOTE: Available at http://www.scoop.developpement-durable.gouv.fr/en/technical-specifications-a22.html.

Annex H (informative): Change request history

NOTE: Copies of CRs that have been implemented in the present document are available from: https://docbox.etsi.org/ITS/Open/Implemented%20CRs/TS%20102%20941/

Date	Version	Information about changes
June 2012	1.1.1	First version of the TS
April 2018	1.2.1	Revised to add new roles in Security architecture and align to ETSI TS 103 097 ASN.1 format
January 2019	1.2.2	Revised to add corrections and clarifications provided for the ETSI ITS CMS6 - Security Plugtests™

The following changes were incorporated to V1.4.1 of the present document

Date	Output Version	Information about changes
February 2019	1.4.1	Ready for publication
June 2020	1.4.1	Revised to add following CRs: • CR #0001 (Allowing of DC entries in the ECTL), • CR #0002 (Add definitions of CTL and CRL update fields), • CR #0003 (Add a specification of Link Certificates as ETSI TS 102 941 messages for RCAs and TLM), • CR #0004 (typo error in AuthorizationValidationResponse clause).
July 2020	1.4.1	Completed the EtsiTs102941TypesLinkCertificate module in A.2.8. The following CRs are implemented: • CR TS 102 941#0005: Move newly defined TS103097 data types from ETSI TS 102 941 to ETSI TS 103 097. All the CRs are available at the following link: https://docbox.etsi.org/ITS/Open/CRs.
October 2020	1.4.1	The following CRs are integrated: • CR TS 102 941#0006: Replace RCA link certificate by successorTo to provide linkage information in the RootCaEntry entry of the ECTL. Replace TLM link certificate by successorTo to provide linkage information in the TlmEntry entry of the ECTL. • CR TS 102 941#0007: Specify the CPOC distribution protocol for TLM certificates, TLM link certificates, ECTL and DeltaECTL. • CR TS 102 941#0008: Align the figure D.1 of Annex D.3 with the corresponding figure in ETSI TS 103 601 V1.1.1 (CPS_003) and add a reference to the protocol specification in ETSI TS 103 601. All the CRs are available at the following link: https://docbox.etsi.org/ITS/Open/CRs.
November 2020	1.4.1	Replace modules' ASN.1 code by the corresponding reference to the ETSI forge in clause A.2

The following CRs have been incorporated in the present document.

CR	Date	Class	Output Version	File	Short description	Status
201	30-6-20	A	V2.1.1	CR201	Enables an ITS-S to support TLS V1.2 or TLS 1.3 to establish a unicast security association between the 2 peer entities when they use an IP communication link	WG5 approved
202	30-6-20	B	V2.1.1	CR202	Adding butterfly key option for AT provisioning	WG5 approved
203	30-6-20	B	V2.1.1	CR203	Adding indirect initial enrolment	WG5 approved
204	30-6-20	C	V2.1.1	CR204	Not limiting of security permission to EndEntityType 'app'	WG5 approved
205	13-10-20	B	V2.1.1	CR205	Adding X.509 Enrolment Credentials	WG5 approved
NOTE: Changes to the ASN.1 annex from the CRs above all have been merged in Forge.						
206	17-11-20	C	V2.1.1	CR206	Clarification of authorization requirement for Butterfly AT Download	WG5 approved
207	28-6-22	F	2.2.1	CR207	Clarify AID to be used for Butterfly AT Download	WG5 approved

History

Document history		
V1.1.1	June 2012	Publication
V1.2.1	May 2018	Publication
V1.3.1	February 2019	Publication
V1.4.1	January 2021	Publication
V2.1.1	October 2021	Publication
V2.2.1	November 2022	Publication