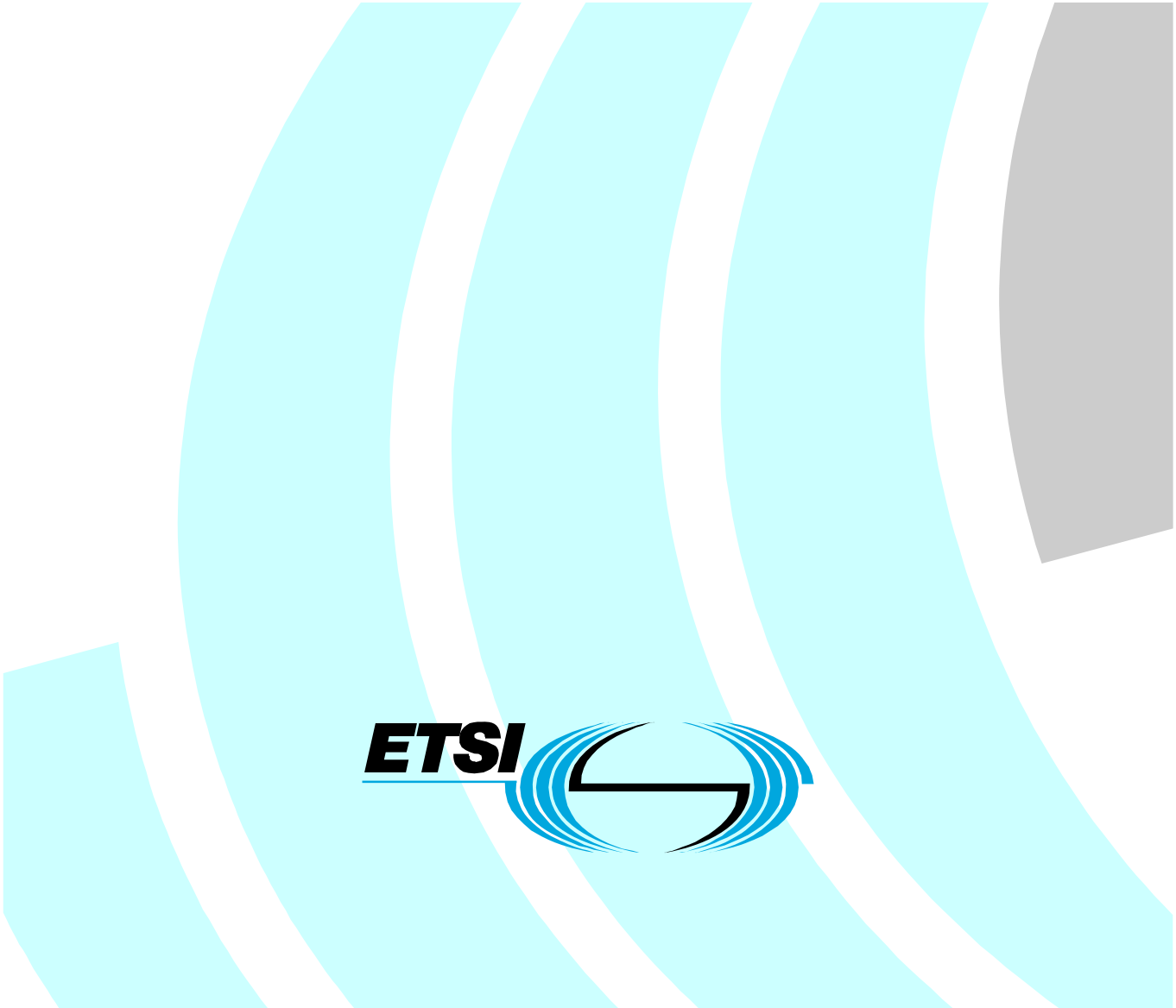
ETSI TS 102 731 V1.1.1 (2010-09)

Technical Specification

Intelligent Transport Systems (ITS);
Security;
Security Services and Architecture



Reference
DTS/ITS-0050001

Keywords
ITS, 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 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Contents

Intellectual Property Rights

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

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

Foreword

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

1 Scope

The present document specifies mechanisms at the stage 2 level defined by ETS 300 387 [i.2] for secure and privacy-preserving communication in ITS environments. It describes facilities for credential and identity management, privacy and anonymity, integrity protection, authentication and authorization.

The mechanisms are specified as stage 2 security services according to the 3 stage method described in ETS 300 387 [i.2], and identify the functional entities and the information flow between them. The stage 2 security services will be refined into a number of security protocols as part of the stage 3 specifications. There may be several security protocols able to fulfil the requirements of a security services.

The present document describes the stage 2 security architecture of the ETSI Intelligent Transport System (ITS). The stage 2 security architecture and security services shall be used as the basis for further developing the ITS security architecture by mapping the security services and its functional components to the ITS architecture [i.7]. This mapping is part of stage 3 specifications.

2 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 reference document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at http://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.

2.1 Normative references

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

Not applicable.

2.2 Informative references

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

[i.1] ETSI TR 102 893: "Intelligent Transport Systems (ITS); Security; Threat, Vulnerability and Risk Analysis (TVRA)".

[i.2] ETSI ETS 300 387: "Private Telecommunication Network (PTN); Method for the specification of basic and supplementary services".

[i.3] United Nations General Assembly resolution 217 A (III) 10 December 1948: "Universal Declaration of Human Rights".

[i.4] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

[i.5] COM 96/C 329/01: "European Union Council Resolution of 17 January 1995 on the Lawful Interception of Telecommunications".

[i.6] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[i.7] ETSI EN 302 665: "Intelligent Transport Systems (ITS); Communications Architecture".

[i.8] ITU-T Recommendation I.130: "Method for the characterization of telecommunication services supported by an ISDN and network capabilities of an ISDN".

[i.9] ISO/IEC 15408: "Information technology - Security techniques - Evaluation criteria for IT security".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

authorization authority: security management entity responsible for issuing, monitoring the use of and withdrawing authorization tickets

authorization ticket: data object that demonstrates that the valid holder is entitled to take specific actions

NOTE: In the present document, "authorization ticket" is reserved for data objects used in message exchanges between ITS Stations and does not refer to data objects used in message exchanges between an ITS Station and a security management entity.

canonical identity: identifier unique to a particular ITS-S that persists throughout the lifetime of the ITS-S and can be presented to an enrolment authority when the ITS-S requests enrolment credentials

enrolment authority: security management entity responsible for the life cycle management of enrolment credentials

enrolment credential: data object that is used in message exchanges between an ITS Station and a security management entity and demonstrates that the valid holder is entitled to apply for authorization tickets

enrolment domain: scope of authority of an enrolment authority; the conditions under which an enrolment authority's enrolment credentials are valid

EXAMPLE: A domain might be a country, a region within that country, multiple countries; or another grouping, such as all vehicles made by a particular OEM.

identity: See canonical identity.

official role vehicle: vehicle whose ITS-S is claiming privileges due to its having a particular role

EXAMPLE: Emergency response vehicles, public transit vehicles, or maintenance vehicles.

personal user vehicle: vehicle that is not an official role vehicle

pseudonym: alias identity within the context of the Pseudonymity service defined in ISO/IEC 15408 [i.9]

security management entity: entity within the ITS system that is responsible for issuing, supervising the use of and if necessary, withdrawing security material

NOTE: In the present document, the security management entities are enrolment authorities and authorization authorities.

security material: data objects such as authorization tickets, enrolment credentials, and keys, that are used by an ITS-S to ensure the correct operation of security services

security mechanism: process (or a device incorporating such a process) that can be used in a system to implement a security service that is provided by or within the system

security policy: set of rules and practices that specify or regulate how a system or organization provides security services to protect resources

security service: processing or communication capability that is provided by a system to give a specific kind of protection to resources where these resources may reside within the system or any other system

3.2 Abbreviations

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

BSA	Basic Set of Applications
CAM	Cooperative Awareness Message
DEN	Decentralized Environmental Notification
IAAA	Identification, Authentication, Authorization, Accountability
ITS	Intelligent Transport System
ITS-S	ITS Station
OEM	Original Equipment Manufacturer
O-UAT	Official role user Universal Authorization Ticket
P-BAT	Personal User Broadcast Authorization Ticket
PKI	Public Key Infrastructure
P-UAT	Personal User Unicast Authorization Ticket
SA	Security Association
SAID	SA identifier
TVRA	Threat, Vulnerability and Risk Analysis

4 Purpose of the Present Document

ETSI has developed a Threat, Vulnerability, Risk Analysis (TVRA) and a supportive database eTVRA with the aim of making better security standards. TVRA is directly related to the ITU-T Recommendation I.130 [i.8] 3 stage standards development method described in ETS 300 387 [i.2]. Figure 1 shows the mapping of TVRA to the 3 stages approach.

TVRA consist of seven steps, where step 1 provides security objectives, which aligns to stage 1 according to the 3 stages approach. TVRA step 2 provides security functional requirements, which aligns to stage 2, and TVRA step 7 provides detailed security requirements, which aligns to stage 3. TVRA steps 4, 5 and 6 provide proof that links the detailed security requirements to the security requirements and security objectives, documenting the argumentation for that the detailed security requirements or stage 3 specifications fulfil the security objectives and security requirements or the stage 1 and 2 specifications. TVRA steps 1, 2 and 7 results are fed directly into the relevant standards documents, while the results from TVRA steps 4, 5 and 6 are documented separately in a TVRA document (usually a TR).

The present document provides stage 2 descriptions of the security services and security architecture of the ETSI Intelligent Transport System (ITS). These are abstract in that they identify the main functional components and the information flow between them. These functional entities have in the present document been mapped to the stage 2 security architecture. The stage 2 architecture is a provisional architectural description that shall be refined in stage 3 into the ITS security architecture.

Stage 2 specifications are only intended as the basis for stage 3 specifications, and do not represent deployment and implementation details. Stage 3 specifications should be used for those purposes.

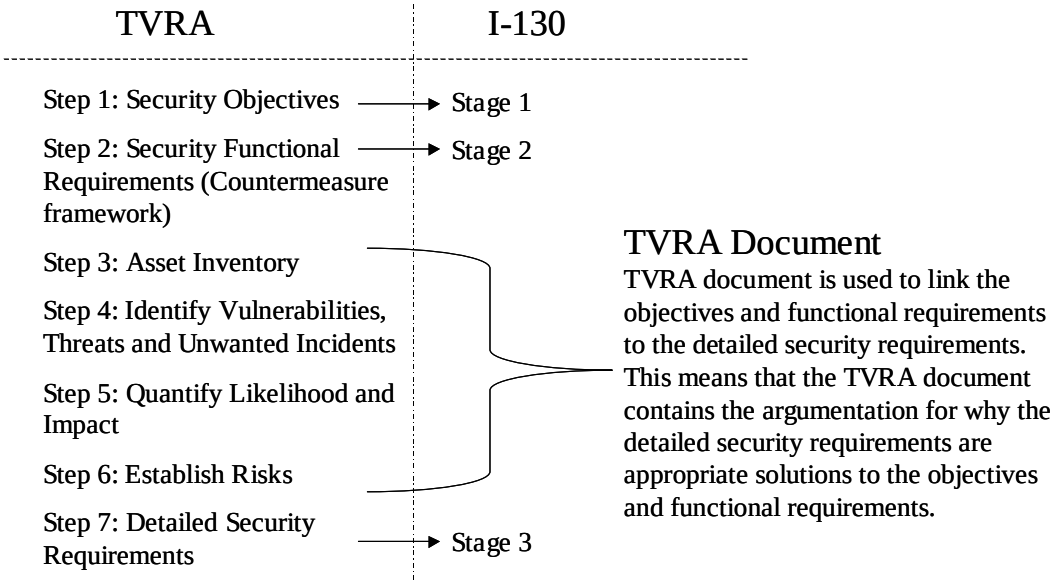


Figure 1: Mapping TVRA to the 3 stages approach as defined in ITU-T Recommendation I.130 [i.8]

5 Refinement of Countermeasures

The general ITS G5A security model is based upon the fundamental principles and assumptions described in TR 102 893 [i.1] and copied below:

1) An ITS-S communicates with the ITS infrastructure when such infrastructure is within 5,9 GHz radio range.

NOTE: The radio characteristics of V2V and V2I are identical and the present document does not identify means to distinguish between a station representing an infrastructure and a station representing another vehicle.

2) An ITS-S authenticates itself to the ITS infrastructure using an authoritative identifier which may be issued by a regulatory authority and is either:

- permanently embedded in the ITS-S hardware; or
- held in any other persistent and tamper-proof carrier.

3) Upon successful authentication, an ITS-S is given a pseudonym which it uses to identify itself in all communications with other ITS stations.

4) The quality and stability of any software installed on an ITS-S has been validated by the ITS authority before it is installed.

The countermeasures identified in the TR 102 893 [i.1] are implemented by a number of ITS security services which fall into two distinct categories:

1) changes to one or several component parts of the ITS architecture; and

2) the addition of new functionality (entities), including security services to single or several components or parts of the ITS architecture.

Table 1 summarizes the countermeasures and the security services required within an ITS-S to effect them. Security services identified in the table as "First Level" are those that are invoked directly by applications or other components or layers in the ITS Basic Set of Applications (BSA). Services identified as "Lower Level" are those that are invoked by other security services. Line items in table 1 which are "greyed" out are not defined in the present document as they do not lead to distinct security services but may be addressed by configuration of the ITS protocol stack or system.

Table 1: Countermeasures and related security services

Countermeasure	Security Services		
	First Level	Lower Level	Data Accessed
Reduce frequency of repeated messages (note 2)			
Include pseudonym in all V2V messages	Pseudonym Validation		
Require an ITS-S to be authorized by an ITS authority before its messages are accepted by the ITS system	Obtain Enrolment Credentials		Security Parameters (Authentication Keys)
Limit message traffic to V2I/I2V where possible	Obtain Enrolment Credentials		Security Parameters (Authentication Keys)
		Authorization	Policy Database, Security Parameters (Authorization Ticket)
		Establish Security Association	Security Parameters (Pseudonym, Encryption Keys)
	Send Secured Message	Encrypt Outgoing Message	Security Parameters (Pseudonym, Encryption Key)
		Authenticate Outgoing Message	Security Parameters (Pseudonym, Authentication Key)
	Receive Secured Message	Decrypt Incoming Message	Security Parameters (Encryption Key)
		Validate Authentication on Incoming Message	Security Parameters (Pseudonym, Authentication Key)
	Update Security Association	Remove Security Association	Security Parameters (Pseudonym, Encryption Key)
		Establish Security Association	Security Parameters (Pseudonym, Encryption Key)
	Remove Enrolment Credentials	Authorization	Policy Database, Security Parameters (Authorization Ticket)
		Remove Security Association	Security Parameters (Pseudonym, Encryption Key)
Implement frequency agility within the 5,9 GHz band (note 2)			
Alternative communications path for security management purposes (note 2)			

Countermeasure	Security Services		
	First Level	Lower Level	Data Accessed
Implement plausibility validation on incoming information	Validate Data Plausibility	Validate Dynamic Parameters	LDM
		Validate Timestamp	
		Validate Sequence Number	
Include a non cryptographic checksum of the message in each message sent (note 1)	Insert Check Value	Calculate Check Value	
	Validate Check Value	Calculate Check Value	
Use broadcast time (Universal Coordinated Time - UTC - or GPS) to timestamp all messages		Timestamp Message	
		Validate Timestamp	
Include a sequence number in each new message		Insert Sequence Number	
		Validate Sequence Number	
Software authenticity and integrity are certified before it is installed (note 2)			
Include an authoritative identity in each message and authenticate it	Validate pseudonym		Security Parameters (Authentication Keys)
Encrypt the transmission of personal and private data	Send Encrypted Data	Encrypt Outgoing Message	Security Parameters (Encryption Keys)
	Process Received Encrypted Data	Decrypt Incoming Message	Security Parameters (Encryption Keys)
Use hardware-based identity and protection of software on an ITS-S (note 2)			
Add an audit log to ITS stations to store the type and content of each message sent to and from an ITS-S	Update Audit Log	Record Incoming ITS Messages	Audit Logs
		Record Outgoing ITS Messages	Audit Logs
Digitally sign each message using a Kerberos/PKI-like token	Sign Outgoing Message	Generate Signature	Security Parameters (Certificate, Keys)
		Authorization	Policy database, Security Parameters (Authorization Ticket)
	Verify Incoming Signed Message	Verify Signature	Security Parameters (Certificate, Keys)
		Authorization	Policy database, Security Parameters (Certificate Status Information)
Use a pseudonym that cannot be linked to the true identity of either the user or the user's vehicle	Obtain Enrolment Credentials	Identification (authoritative identity provider)	Security Parameters (Pseudonym, Encryption Key)
	remove Enrolment Credentials	Identification (authoritative identity provider)	Security Parameters (Pseudonym, Encryption Key)
Allow remote activation and deactivation of ITS-S	ITS-S Remote Management Report Misbehaving ITS-S	Authorization	Policy Database
		Deactivate ITS Transmission	Security Parameters (Authorization Ticket)
		Activate ITS Transmission	Security Parameters (Authorization Ticket)
		Report Misbehaviour	Security Parameters (Authorization Ticket)

NOTE 1: The use of checksums and Cyclic Redundancy Checks is only effective at the ITS protocol layers below the Application and Network layers where a check value can easily be recalculated and inserted in a false or manipulated message.

NOTE 2: Items which are "greyed" out are not defined in the present document but may be addressed in other parts of the ETSI ITS standardisation programme.

For the sake of convenience, the security services identified in table 1 have been grouped according to the security service they provide from the Confidentiality Integrity Availability model in … and by function, as shown in table 3.

Table 2: Identified security service mapped to CIA paradigm

	Confidentiality	Integrity	Availability
Include source address in all V2V messages			X
Require an ITS-S to be authorized by an ITS authority before its messages are accepted by the ITS system		X	
Limit message traffic to V2I/I2V where possible			X
Implement plausibility validation on incoming information		X	X
Include a non cryptographic checksum of the message in each message sent		X	
Use broadcast time (Universal Coordinated Time - UTC - or GPS) to timestamp all messages			X
Include a sequence number in each new message			X
Include an authoritative identity in each message and authenticate it			X
Encrypt the transmission of personal and private data	X		
Add an audit log to ITS stations to store the type and content of each message sent to and from an ITS-S		X	
Digitally sign each message using a Kerberos/PKI-like token		X	X
Use a pseudonym that cannot be linked to the true identity of either the user or the user's vehicle	X		
Allow remote activation and deactivation of ITS-S			X

The bulk of the availability measures can be further broken down into classifications of Identification, Authentication and Authorisation.

Table 3: ITS security service grouping

Security Service Group	Security Service at Tx	Security service at Rx
Enrolment	Obtain Enrolment Credentials	
		Remove Enrolment Credentials
	Update Enrolment Credentials	
Authorisation	Add authorisation credential to single message	
	Obtain Authorization Ticket	
		Validate authorisation credential of received message
	Update Authorization Ticket	
Security Association management	Establish Security Association	Establish Security Association
	Remove Security Association	Remove Security Association
	Update Security Association	Update Security Association
Authentication services	Authenticate ITS user	Authenticate ITS user
	Authenticate ITS network	Authenticate ITS network
Confidentiality services	Encrypt single outgoing message	
		Decrypt single incoming message
	Send secured message	
		Receive secured message
Integrity services	Insert check value	
		Validate check value
	Calculate check value	

Security Service Group	Security Service at Tx	Security service at Rx
Replay Protection services	Timestamp message	
		Validate timestamp
	Insert sequence number	
		Validate sequence number
	Insert challenge	
		Use received challenge
	Validate use of challenge	
Accountability services		Record incoming message
	Record outgoing message	
Plausibility validation		Validate data plausibility
		Validate dynamic parameters
		Validate timestamp
		Validate sequence number
Remote management	Activate ITS transmission	
	Deactivate ITS transmission	
Report Misbehaving ITS-S	Report Misbehaviour	Report Misbehaviour

The result of providing the security services identified in table 3 is to enable strong assurance of identity and authority in ITS with the ability to protect privacy of the ITS-S user. The basic security services identified in table 3 may be combined to provide necessary security functions for ITS communications. Especially for V2V adhoc network security, security mechanisms shall be provided to ensure both authenticity and integrity of the data transmitted in messages. These security mechanisms may include message signature capabilities, applied on single message or on multiple messages (to optimize network efficiency and reduce the added security payload e.g. on CAM broadcast or geo-casting messages).

6 ITS Communications Security Architecture

6.1 Overview

The general ITS security architecture upon which the security services in the present document are based is shown in figure 2.

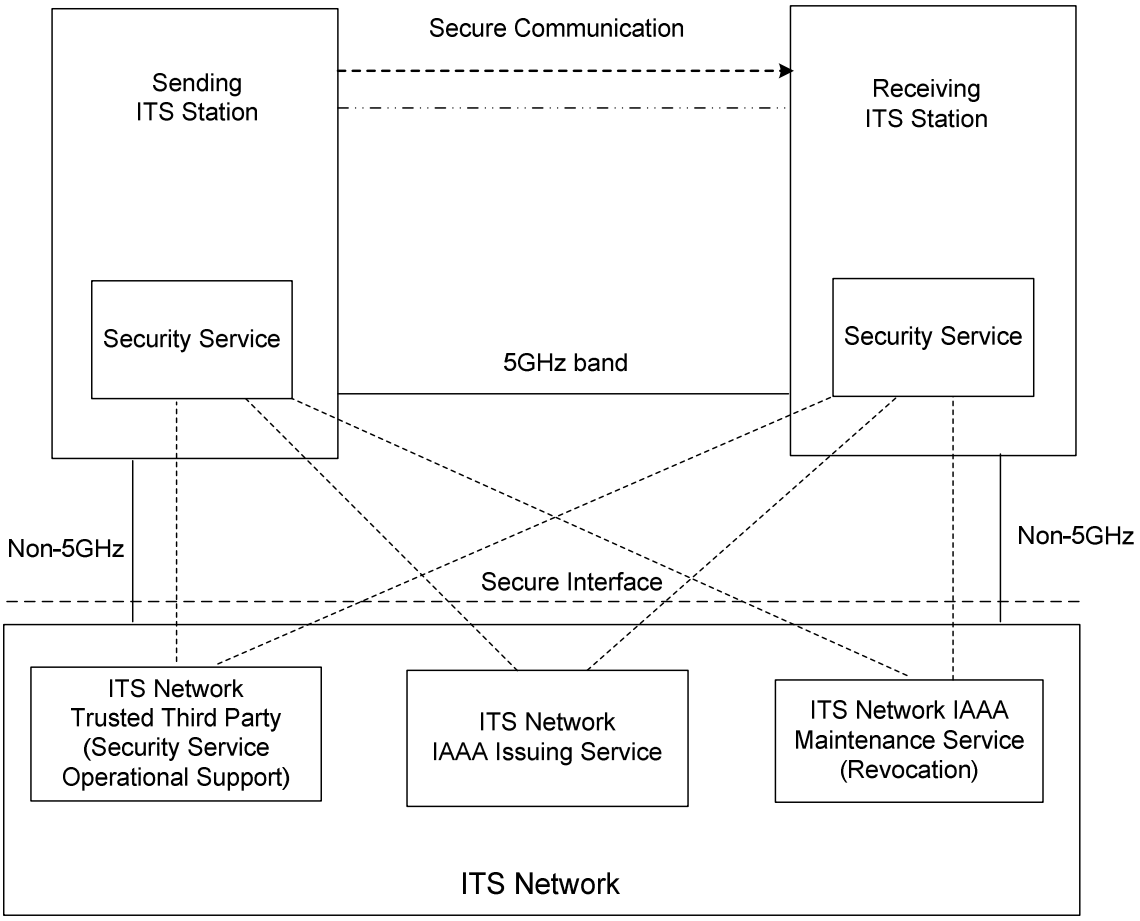


Figure Legend
Physical connection: ———
Security association: -------
Indirect security association: – · – –
Logical communication: - - →
Interface: – – – -

NOTE: The scope of the security architecture is that defined for the BSA using the 5,9 GHz radio allocation in Europe. However the services are defined in the main body of this document without specific use of 5,9 GHz radio links.

Figure 2: Schematic overview of ITS security architecture

NOTE 1: Security associations are logical relationships between 2 entities that may be associated with a communications link but SAs are not communications links.

NOTE 2: Security associations may take a number of forms but in each case they identify the nature of the security service (confidentiality, integrity, authentication or authorisation), the required algorithm and key. Security associations may be established for single transactions (and thus their establishment may form part of the transaction itself) or for session based associations (in such instances the association is generally established independently of the individual transactions that are to be secured).

6.2 ITS Authoritative Hierarchy

6.2.1 Overview

Security management roles are taken by:

- manufacturers:
  - provide ITS authoritative identities on behalf of the regional ITS authority;
- enrolment authorities:
  - validate an ITS-S as a whole; and
- authorization authorities:
  - authorize an ITS-S to use a particular application, service, or privilege.

6.2.2 Manufacturer

The following description applies to the manufacture of both ITS-S (Roadside) and ITS-S (Vehicle).

During the manufacturing process an ITS-S shall receive a globally unique canonical identity in the form of an octet string. It shall persist for the operational lifetime of the ITS-S.

NOTE: The unique identity may be in the form of a serial number.

A newly manufactured ITS-S shall be able to check the validity of and establish an encrypted, authenticated communication session with at least one valid enrolment authority.

A newly manufactured ITS-S shall be able to check the validity of and establish an encrypted, authenticated communication session with one or more valid authorization authorities.

A newly manufactured ITS-S shall be able to add trusted enrolment authorities and authorization authorities.

6.2.3 Enrolment Authority

The following description applies to the relationship between an enrolment authority and both an ITS-S (Roadside) and an ITS-S (Vehicle).

NOTE 1: An enrolment authority validates that an ITS-S can be trusted to function correctly.

NOTE 2: An enrolment authority issues enrolment credentials to the ITS-S which identifies the enrolment authority and contain a pseudonym (temporary identity) for the ITS-S. These credentials are valid within the enrolment authority's enrolment domain.

An enrolment authority shall be able to determine the canonical identity of an ITS-S from its enrolment credentials if the security of the ITS-S has been determined to be compromised. An enrolment authority may be prevented from determining the canonical identity of an ITS-S from its enrolment credentials if the ITS-S has not been determined to be compromised.

The ITS-S shall present its identity to the enrolment authority on enrolment.

NOTE 3: The enrolment authority may require additional attributes from the enrolling ITS-S in order to determine if enrolment is allowed but this is not described in the present document.

Communications between an ITS-S and an Enrolment Authority shall be encrypted with an Enrolment Authority Key, which is made available to the ITS-S by mechanisms not specified in the present document.

The ITS-S may authenticate to the Enrolment Authority explicitly using an ITS-S key or implicitly by connecting to the Enrolment Authority over a trusted connection that is used only for enrolment.

Enrolment credentials shall contain the following items of information:

- the temporary identity of the ITS-S;
- an identifier of the enrolment authority;
- cryptographic material or a reference to cryptographic material allowing the credential holder to demonstrate ownership of the credentials.

In addition, enrolment credentials may contain any or all of the following items of information:

- Attributes of the ITS-S or references to those attributes. If included, these attributes shall be protected in such a way that they are only available to recipients with a legitimate need to know them.
- Additional information not specific to an ITS-S such as an issue or expiry date.

The enrolment and authorization system shall support the use of a hierarchy of enrolment authorities, with lower-layer authorities enrolling vehicles and higher-layer authorities authorizing lower-level authorities.

An ITS-S may enrol with multiple enrolment authorities covering multiple enrolment domains.

An enrolment authority may require an enrolled ITS-S to re-enrol periodically. During this re-enrolment process the ITS-S shall present evidence that it has not been compromised. If it cannot present such evidence it shall be considered compromised.

6.2.4 Authorization Authority

The following description applies to the relationship between an ITS authorization authority and both an ITS-S (Roadside) and an ITS-S (Vehicle).

An ITS-S that has enrolled with an enrolment authority may apply to an authorization authority for specific permissions within the enrolment authority's domain and the authorization authority's authorization context. These privileges are denoted by means of authorization tickets. When it requests authorization tickets, an ITS-S shall present its enrolment credentials to the authorization authority. When it requests permissions to access a specific ITS capability, an ITS-S shall present a valid authorization ticket to the ITS-S providing that capability.

Each authorization ticket specifies a particular authorization context which comprises a set of permissions.

EXAMPLE: An authorization ticket might grant permission to an ITS-S to broadcast messages from a particular message set. Alternatively, it might grant permission to claim certain privileges.

The authorization context shall be specified either by explicitly encoding the permissions granted or by including a reference to a known policy that specifies the context.

NOTE: An authorization authority will normally be responsible for a specific set of contexts which may be specified by one or more of the following:

- application (for example, CAM and DEN messages for personal user vehicles, emergency service vehicles or tolling);
- time period;
- geographic region (nation, state, locality); or
- any other encodable means.

The authorization system shall support the use of a hierarchy of authorization authorities, with lower-layer authorities authorizing vehicles and higher-layer authorities authorizing lower-level authorities.

EXAMPLE 1: Official role vehicles may use the following three layer structure:

a) ITS global (National) authorization authority,

b) ITS regional authorization authority; and

c) ITS local authorization authority.

EXAMPLE 2: Personal user vehicles may have a single national authorization authority for CAM and DEN messages to reduce bandwidth associated with authorization data.

An authorization authority shall accept credentials from one or more enrolment authorities. When an ITS-S applies to that authorization authority for a set of authorization tickets, it shall present and demonstrate ownership of enrolment credentials from one or more of its enrolment authorities. If the authorization authority does not accept credentials from any of the enrolment authorities in the application, it shall reject the application.

Communications between an ITS-S and an authorization authority shall be encrypted with an authorization authority Key, which is made available to the ITS-S by mechanisms not specified in the present document.

Before issuing authorization tickets, an authorization authority may apply a policy to the presented enrolment credentials. For example, it may require that enrolment credentials were issued within a certain period of time.

An authorization authority shall only issue an authorization ticket to an ITS-S that is valid within the combined enrolment domains of all the enrolment credentials presented to it by the ITS-S.

An authorization authority shall be able to determine the enrolment credentials of an ITS-S from its set of authorization tickets if the security of the ITS-S has been determined to be compromised. An authorization authority may be prevented from determining the enrolment credentials of an ITS-S from its set of authorization tickets if the ITS-S has not been determined to be compromised.

Authorization tickets shall contain the following items of information, by value or reference:

- the authorization context;
- an identifier of the authorization authority;
- cryptographic material allowing the ticket holder to demonstrate ownership of the ticket.

Authorization tickets may contain additional information as necessary to support the use of the authorization context. The signature generated by the ticket authorisation may be viewed as the authorisation code.

6.2.5 Trust Assumptions

6.2.5.1 Trust Assumptions in normal operation

The security of an ITS system relies on the following trust assumptions.

- The enrolment authorities and authorization authorities are not compromised.

NOTE: This is an assumption because this document does not define mechanisms for use should one of these authorities become compromised.

- The enrolment authorities are able to determine whether or not an ITS-S is in a compromised state.
- The security of an ITS-S cannot be compromised in such a way that neither the authorizing authorities nor the enrolment authorities are able to determine that the compromise has occurred.
- The authorization authorities are able to determine whether or not an ITS-S or its operator is entitled to the privileges it is requesting.
- The canonical identity of an ITS-S is globally unique.
- An ITS-S is able to establish a secure (authenticated and confidential) channel to a enrolment authority when necessary.
- An ITS is able to determine that it is communicating with a valid enrolment authority.
- An ITS-S is able to establish an authenticated and confidential channel to an authorization authority when necessary.
- An ITS is able to determine that it is communicating with a valid authorization authority.

6.2.5.2 Compromised ITS-S

If an enrolment authority determines that an ITS-S has been compromised or is informed by an authorization authority that the ITS-S is compromised, the enrolment authority shall inform other enrolment authorities of this fact using the canonical identity to identify the ITS-S.

If an enrolment authority determines that a re-enrolling ITS-S has been compromised (either through its failure to present evidence of non-compromise or because the enrolment authority has been informed that the ITS-S is compromised), it shall not issue the ITS-S with new enrolment credentials while the ITS-S remains in a known compromised state.

If an authorization authority determines that an ITS-S has been compromised, it shall inform the enrolment authority associated with the enrolment credentials presented by the ITS-S.

If an enrolment authority determines that an ITS-S has been compromised or is informed that the ITS-S is compromised, it shall immediately make that information available to authorization authorities.

If an ITS-S is known by an authorization authority to be compromised, that authorization authority shall not grant the ITS-S any further tickets until the ITS-S has been determined to be no longer compromised.

If an ITS-S is known by an authorization authority to be compromised, that authorization authority may distribute information to any or all other ITS-Ss in the system instructing them to ignore messages authorized by the compromised ITS-S's authorization tickets.

An authorization authority may request any trusted ITS-S to report any observed use of authorization tickets from a compromised ITS-S back to the authorization authority. This request shall be authenticated by the authorization authority. The authorization authority may send a cancellation notice to revoke this request. This notice shall be authenticated by the authorization authority. Any ITS-S that receives a request to report such use of authorization tickets and has not received a cancellation notice shall report any observed use of authorization tickets by the compromised ITS-S at the earliest practical opportunity.

6.2.5.3 Compromised Authorities

The present document does not specify procedures within an ITS-S for detecting or managing compromised enrolment or authorization authorities.

6.3 ITS Security Parameter Management

6.3.1 Identities and Identifiers in ITS

The ITS should ensure consistency with Article 12 of the Universal Declaration of Human Rights [i.3] which states that "*No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks*". This article is embodied in the EC directives on privacy (2002/58/EC [i.4]) and on data protection (EU Directive 95/46/EC [i.6]) with exceptions consistent with the provisions for lawful interception given in COM 96/C329/01 [i.5].

Although an ITS user is generally considered to be an application or functional agent that represents a human, there are links between a vehicle and its driver that can be either directly derived or indirectly deduced. Consequently, identifiers used for communication in ITS shall not be directly related to the real identity of either the ITS-S (Vehicle) or its driver except where this is a requirement for operation of a specific ITS application.

6.3.1.1 Authorization and privacy with authorization tickets

6.3.1.1.1 Personal user vehicles

An ITS-S shall present a valid authorization ticket to another ITS-S in order to establish that it is authorized to use or access a particular application. There are two classes of authorization ticket for ITS users on a personal user vehicle. These preserve anonymity in two different ways:

- Personal User Unicast Authorization Ticket (P-UAT):
  - shall only be sent over encrypted channels to end-points that are known to be authorized.
- Personal User Broadcast Authorization Ticket (P-BAT):
  - may be sent over non-encrypted channels or to end-points that are not known to be authorized at the time of sending.

A P-UAT may contain any information required to consume or provide the service authorized by the P-UAT, including information about the user's identity if necessary.

A P-BAT shall:

- preserve the privacy of the P-BAT holder in accordance with the legal framework that applies in the area of operation;
- limit the time that a P-BAT is associated with a particular ITS-S; and
- be traceable even after it has expired (for audit purposes).

6.3.1.1.2 Official role vehicles and infrastructure

In addition to personal user vehicles, the system will contain ITS users who are not acting in a personal user vehicle role. Two examples of these are vehicles that are acting in a public service or incident response capacity and infrastructure ITS users. (Vehicles that are acting in a public service capacity may be claiming heightened privileges above those claimed by personal user vehicles, such as the ability to ask other vehicles to give way or to request traffic signal phase changes.)

NOTE: Official role vehicles may choose to suppress the requirements for privacy when operating in that role. When operating in other modes privacy requirements may be the same as those for personal user vehicles.

ITS official role users use only one kind of authorization ticket:

- Official role user Universal Authorization Ticket (O-UAT):
  - shall contain details of the authorization context; and
  - may contain a long-lived identifier for the official role user depending on the requirements of the authorization context.

6.3.1.2 Authorization tickets and cryptography for personal user vehicles and official role users

Authorization tickets can be used directly to authorize a message or to establish a Security Association (see clause 6.4). They can also use symmetric or asymmetric cryptography. which is denoted below by including (A) or (S) after the ticket type. The full set of authorization tickets is therefore:

- P-UAT(A): Personal user unicast tickets supporting authorization via asymmetric cryptography.
- P-UAT(S): Personal user unicast tickets supporting authorization via symmetric cryptography.

- P-BAT(A): Personal user broadcast tickets supporting authorization via asymmetric cryptography.
- P-BAT(S): Personal user broadcast tickets supporting authorization via symmetric cryptography.

NOTE: These tickets will be used to locate other ITS Users with whom the sender can establish a Security Association (see clause 6.4.4), rather than directly to provide authorization to messages.

- O-UAT(A): Official Role User tickets supporting authorization via symmetric cryptography.
- O-UAT(S): Official Role User tickets supporting authorization via asymmetric cryptography.

The specific symmetric and asymmetric algorithms to be used are out of the scope of the present document.

6.4 ITS Message Communication Models

6.4.1 Overview

There are three different application messaging models that can be used to enable secure communications between one ITS-S and another:

- individual public messages;
- individual private messages; and
- security associations.

6.4.2 Individual public messages

In the individual public message communication model, an ITS-S sends a broadcast message that is not targeted at a recipient with whom the ITS-S already has an established Security Association (SA). The message requires authorization, authentication, and integrity. If the message originates from an ITS-S playing a personal user vehicle role it requires privacy; if it originates from an ITS-S of a different type it may not require privacy. The message does not require confidentiality.

6.4.3 Individual private messages

In the individual private message communication model, an ITS-S sends a message to a specific recipient. The ITS-S does not have an established security association with the recipient. Messages require authorization, authentication, integrity, privacy and confidentiality. This application communication model can be looked on as establishing a once-off SA with the recipient. Its advantage over the use of an SA is that it does not require an SA establishment phase, so for exchanges with small numbers of messages it may be more efficient than establishing an SA proper.

6.4.4 Security Associations

A Security Association (SA) is a long-term relationship established between two or more ITS-Ss to enable them to exchange messages securely. The SA defines the set of cryptographic algorithms, keys, and other private and public parameters that are used to provide confidentiality, authentication and integrity in one direction over one point-to-point connection. A security association may be duplicated across all authorized receivers in a multicast group and each sender may have multiple security associations.

At the time the SA is established, the ITS-Ss authorize and authenticate to each other using the appropriate authentication tickets and establish the cryptographic material that is associated with that SA. The ongoing correct use of the cryptographic material in the SA provides a level of assurance that the sending ITS-S is still correctly authorized and authenticated.

The parties in an SA may choose from time to time to re-negotiate the SA. Re-negotiation requires that the parties reauthorize and re-authenticate to each other using the appropriate tickets.

NOTE: Credential sets may be in the form of authentication or authorisation tickets that are exchanged between parties. The choice of ticket is established by the context.

The parties to an SA shall establish an SA identifier (SAID) which shall be used to allow recipients to identify the SA applied to a particular message. If the SAID is sent in clear text, it shall be changed from time to time. The SAID may be used across multiple communications sessions.

7 ITS Security Services

7.1 Enrolment Credentials

The Enrolment Credentials services consist of:

- Obtain Enrolment Credentials;
- Update Enrolment Credentials; and
- Remove Enrolment Credentials.

7.1.1 Obtain Enrolment Credentials

The Obtain Enrolment Credentials is used by an ITS-S to enrol with an enrolment authority.

7.1.1.1 Functional model

7.1.1.1.1 Functional model description

The functional model of the "Obtain Enrolment Credentials" security service comprises the following functional entities:

- In the ITS-S:
  - Invoke Enrolment.
  - Enrolment Request.
  - Process Authentication.
- In the ITS infrastructure:
  - Enrol Station.
  - Authenticate Station.

The following relationships exist between the functional entities:

ra: between Invoke Enrolment and Enrolment Request;

rb: between Enrolment Request and Enrol Station;

rc: between Enrol Station and Authenticate Station;

rd: between Authenticate Station and Process Authentication.

The functional entities and the relationships between them are shown in figure 3.

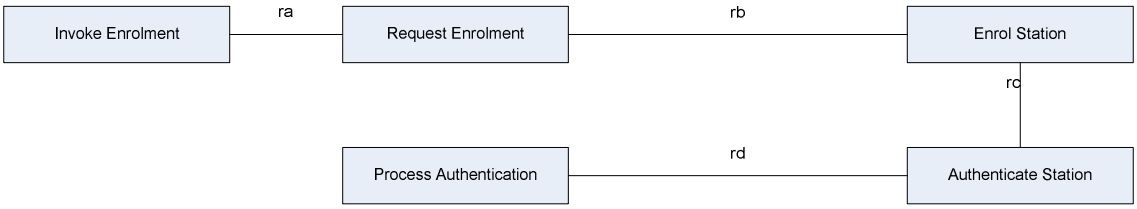


Figure 3: Functional model for the Obtain Enrolment Credentials security service

7.1.1.1.2 Description of functional entities

7.1.1.1.2.1 Invoke Enrolment

The *Invoke Enrolment* functional entity detects the need for the ITS-S to enrol with the ITS infrastructure and initiates the enrolment procedure.

7.1.1.1.2.2 Enrolment Request

The *Enrolment Request* functional entity delivers a Enrolment Request to the ITS infrastructure, receives the associated response and stores the received secure communication parameters within the ITS-S.

7.1.1.1.2.3 Enrol Station

The *Enrol Station* functional entity receives a request for registration from an ITS-S, initiates the authentication of the user and if successful, delivers a positive response containing the parameters necessary for ongoing secure communication to the ITS-S.

7.1.1.1.2.4 Authenticate Station

The *Authenticate Station* functional entity validates the identification information provided by *Enrol Station* functional entity.

7.1.1.1.2.5 Process Authentication

The *Process Authentication* functional entity provides the response to the challenge from the *Authenticate Station* functional entity.

7.1.1.2 Information flows

7.1.1.2.1 Definition of information flows

7.1.1.2.1.1 Marking convention

In the tables identifying the contents of individual information flow in the present documents, the letter "M" in either the "Request" or "Confirm" column indicates that the associated information element is mandatory . The letter "O" indicates that the information element is optional.

7.1.1.2.1.2 Enrol

Enrol is a confirmed information flow across relationship *ra* from *Invoke Enrolment* to *Enrolment Request* which is used to initiate the user registration process. It contains the service elements specified in table 4.

Table 4: Contents of the Enrol information flow

Service elements	Allowed values	Request	Confirm
Canonical identity	Character string: Permanent identifier	M	
ITS-S Key	Public or symmetric key identifier	M	
Enrolment result	- Accepted - Rejected		M
List of enrolment credentials	Temporary identities		O (note 1)
Cause of rejection	- Canonical identity unknown - User not permitted to enrol - User authentication failed		O (note 2)
NOTE 1: This service element shall be included if the enrolment result is "Accepted". NOTE 2: This service element shall be included if the enrolment result is "Rejected".			

7.1.1.2.1.3 Enrolment Request

Enrolment Request is a confirmed information flow across relationship *rb* from *Enrolment Request* to *Enrol Station* which is used to request that the ITS user is enrolled by the infrastructure. It contains the service elements specified in table 5.

Table 5: Contents of the Enrolment Request information element

Service elements	Allowed values	Request	Confirm
Canonical identity	Character string: Permanent identifier	M	M
ITS-S Key	Public or symmetric key identifier	M	
Network identifier	Character string		M
Network challenge	Randomly generated character string (note 1)	M	
Registration result	- Accepted - Rejected		M
List of enrolment credentials	Temporary identities (note 2)		O (note 3)
Cause of rejection	- Canonical identity unknown - User not permitted to enrol - User authentication failed		O (note 4)
NOTE 1: Encrypted using the Enrolment Authority Key and cryptographically signed using the ITS-S key. NOTE 2: Encrypted using the ITS-S key and cryptographically signed using the Enrolment Authority Key. NOTE 3: This service element shall be included if the registration result is "Accepted". NOTE 4: This service element shall be included if the registration result is "Rejected".			

7.1.1.2.1.4 Authentication Request

Authentication Request is a confirmed information flow across relationship *rc* from *Enrol Station* to *Authenticate Station* which is used to request that the ITS user's identity is validated. It contains the service elements specified in table 6.

Table 6: Contents of the Authentication Request information flow

Service elements	Allowed values	Request	Confirm
Canonical identity	Character string: Permanent identifier	M	M
Network identifier	Character string	M	M
Network challenge	Randomly generated character string (note 1)	M	
Authentication result	- Passed - Failed		M
Cause of failure	- User authentication disabled - User authentication failed		O (note 2)
NOTE 1: Encrypted using the Enrolment Authority Key and cryptographically signed using the ITS-S key. NOTE 2: This service element shall be included if the authentication result is "Failed".			

7.1.1.2.1.5 Enrolment Challenge

Enrolment Challenge is a confirmed information flow across relationship *rd* from *Authenticate Station* to *Process Authentication* to exchange and validate authentication challenges. It contains the service elements specified in table 7.

Table 7: Contents of the Enrolment Challenge information flow

Service elements	Allowed values	Request	Confirm
Canonical identity	Character string: Permanent identifier		M
Network identifier	Character string	M	M
Network challenge response	Result of cryptographically processing the received network challenge (note 1)	M	
Vehicle challenge	Randomly generated character string (note 1)	M	
Vehicle challenge response	Result of cryptographically processing the received vehicle challenge (note 1)		M
Registration result	- Successful - Failed		M
Cause of failure	- Canonical identity unknown - User not permitted to enrol - User authentication failed		O (note 3)
NOTE 1: Encrypted using the Enrolment Authority Key and cryptographically signed using the ITS-S key. NOTE 2: Encrypted using the ITS-S key and cryptographically signed using the Enrolment Authority Key. NOTE 3: This service element shall be included if the authentication result is "Failed".			

7.1.1.2.1.6 Examples of information flow sequences

A stage 3 standard for the Obtain Enrolment Credentials security service shall provide procedures in support of the information flow sequences specified in clause 7.1.1.2.1.6.1. In addition, signalling procedures shall be provided to cover other sequences arising from, for example, error situations and interactions with other security services.

7.1.1.2.1.6.1 Obtain Enrolment Credentials

Figure 4 shows the information flow for an ITS-S (Vehicle) arriving and successfully enrolling in a new infrastructure enrolment area.

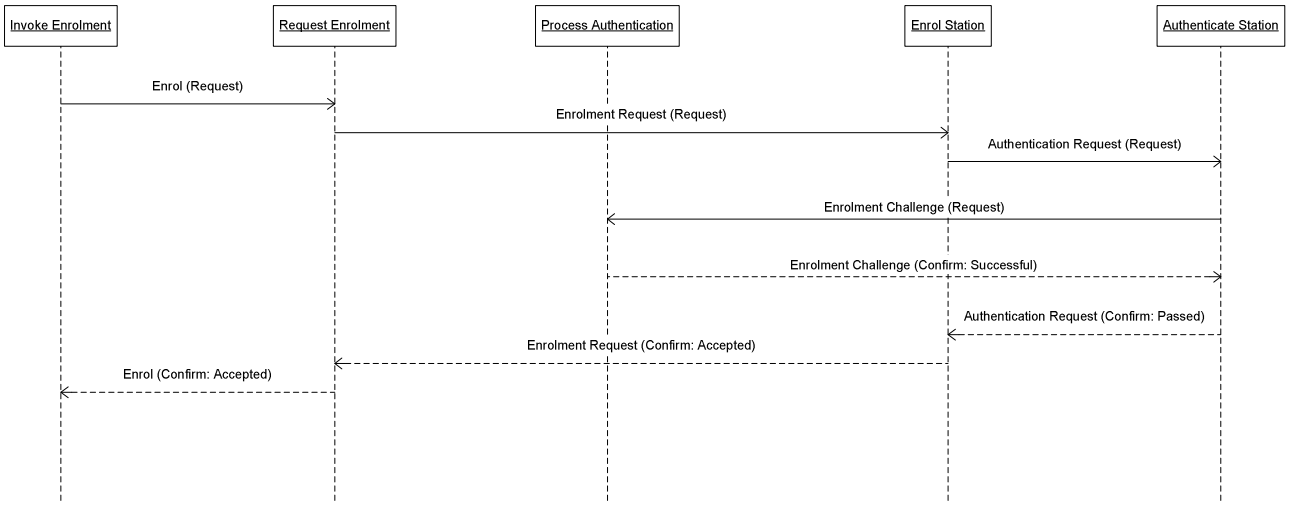


Figure 4: Successful acquisition of enrolment credentials

Figure 5 shows an example information flow for an ITS-S (Vehicle) arriving and unsuccessfully attempting to enrol in a new infrastructure enrolment area.

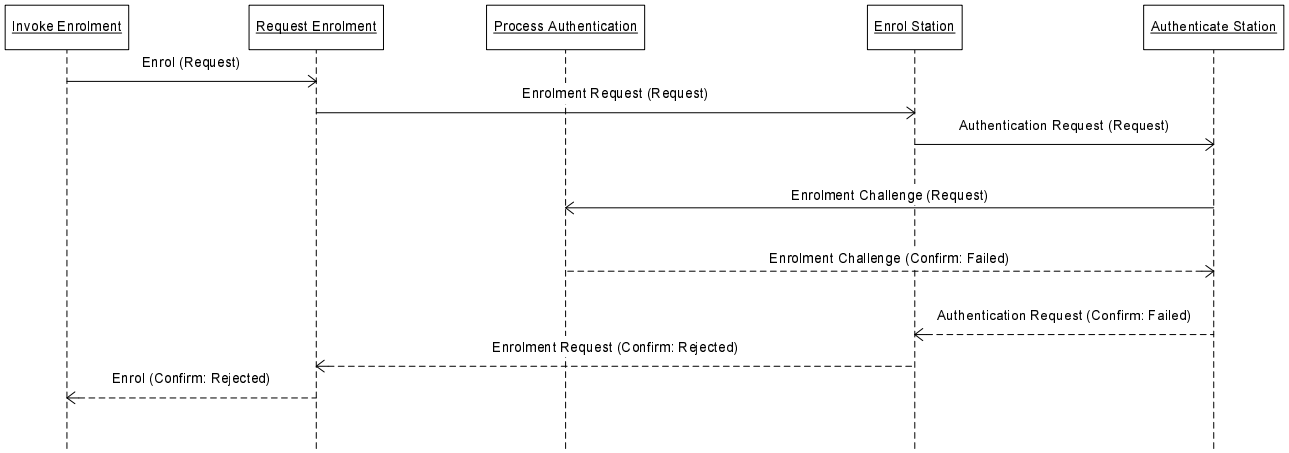


Figure 5: Unsuccessful acquisition of enrolment credentials

7.1.2 Update Enrolment Credentials

7.1.2.1 Functional model

7.1.2.1.1 Functional model description

Upon request from an ITS-S the Update Enrolment Credentials security service is able to update its enrolment credentials.

The functional model of the "Update Enrolment Credentials" security service comprises the following functional entities:

- In The ITS-S:
  - Update Enrolment Credentials.
- In the ITS infrastructure:
  - Request enrolment credentials.
  - Issue Enrolment Credentials.

The following relationships exist between the functional entities:

pa: between *Update Enrolment Credentials* and *Request Enrolment Credentials*;

pb: between *Request Enrolment Credentials* and *Issue Enrolment Credentials*;

pc: between *Issue Enrolment Credentials* and *Update Enrolment Credentials.*

The functional entities and the relationships between them are shown in figure 6.

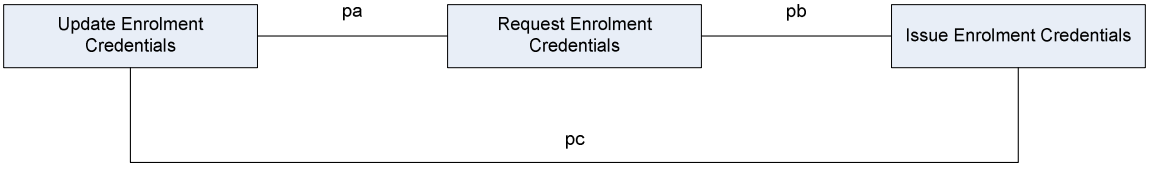


Figure 6: Functional model for the Update Enrolment Credentials security service

7.1.2.1.2 Description of functional entities

7.1.2.1.2.1 Update Enrolment Credentials

The *Update Enrolment Credentials* functional entity detects the need to update the list of enrolment credentials used to communicate over G5A and sends an update request to the ITS infrastructure on behalf of the ITS-S.

7.1.2.1.2.2 Request Enrolment Credentials

The *Request Enrolment Credentials* functional entity receives the update request and creates a set of accountable enrolment credentials which are linked to the true identity of the requesting ITS-S.

NOTE: Enrolment Credentials need to be accountable and to ensure privacy on behalf of the enrolment credentials holder. The linkage between a enrolment credentials and the enrolment credentials holder is stored in a manner that makes it accessible only to authorities.

7.1.2.1.2.3 Issue Enrolment Credentials

The *Issue Enrolment Credentials* functional entity packages the enrolment credentials into a randomised list, encrypts and signs the list and sends it to the requesting ITS-S.

7.1.2.2 Information flows

7.1.2.2.1 Definition of information flows

7.1.2.2.1.1 Update Enrolment Credentials

Update Enrolment Credentials is a confirmed information flow across relationship *pa* from *Update Enrolment Credentials* to *Request Enrolment Credentials* which is used to initiate the update enrolment credentials process. It contains the service elements specified in table 8.

Table 8: Contents of the Update Enrolment Credentials information flow

Service elements	Allowed values	Request	Confirm
Canonical identity	Character string: Permanent identifier	M	
ITS-S Key	Public or symmetric key	M	
Update request result	- Accepted - Rejected		M
List of enrolment credentials	Temporary identities (note 3)		O (note 1)
Cause of rejection	- Canonical identity unknown - User not permitted to request enrolment credentials - Failed to create enrolment credentials		O (note 2)
NOTE 1: This service element shall be included if the request result is "Accepted". NOTE 2: This service element shall be included if the request result is "Rejected". NOTE 3: Encrypted using the ITS-S key and cryptographically signed using the Enrolment Authority Key.			

7.1.2.2.1.2 Create Enrolment Credentials

Create Enrolment Credentials is a confirmed information flow across relationship *pb* from *Request Enrolment Credentials* to *Issue Enrolment Credentials* which is used to create and validate that enrolment credentials have been created and successfully linked to the real identity of the requesting ITS-S. It contains the service elements specified in table 9.

Table 9: Contents of the Create Enrolment Credentials information flow

Service elements	Allowed values	Request	Confirm
Canonical identity	Character string: Permanent identifier	M	
Request result	- Success - Failure		M
Linked enrolment credentials	Associations between real identity and temporary identities		O (note 1)
Cause of failure	- Failed to create enrolment credentials - Link enrolment credentials to identity failed		O (note 2)
NOTE 1: This service element shall be included if the request result is "Success". NOTE 2: This service element shall be included if the request result is "Failure".			

7.1.2.2.2 Examples of information flow sequences

A stage 3 standard for the Update Enrolment Credentials security service shall provide procedures in support of the information flow sequences specified in clause 7.1.2.2.2.1. In addition, signalling procedures shall be provided to cover other sequences arising from, for example, error situations and interactions with other security services.

7.1.2.2.2.1 ITS Update Enrolment Credentials

Figure 7 shows the information flow for an ITS-S (Vehicle) successfully updating the list of enrolment credentials used to communicate over G5A.

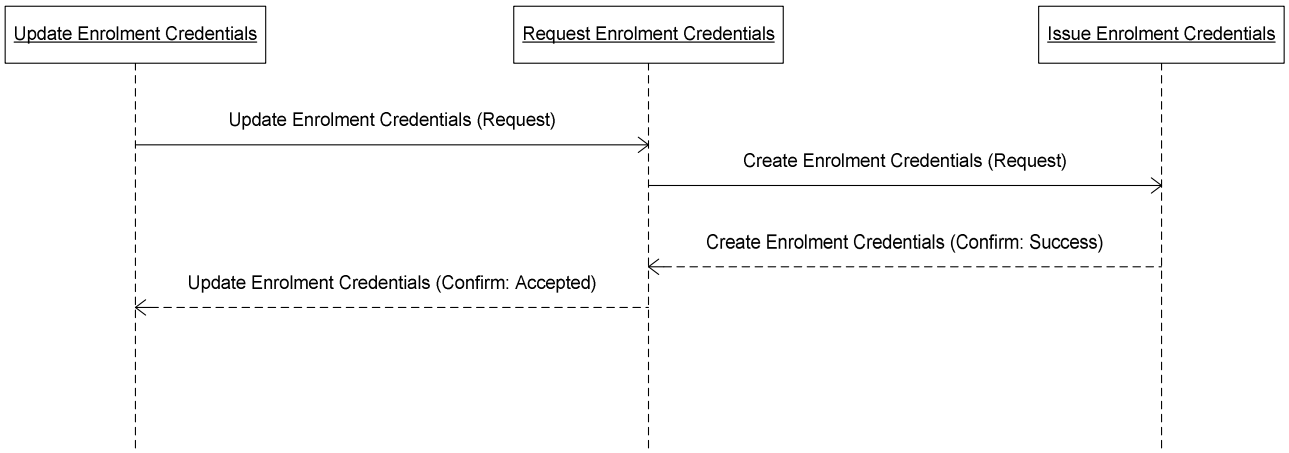


Figure 7: Successful update of enrolment credentials

Figure 8 shows an example information flow for an ITS-S (Vehicle) unsuccessfully attempting to update the list of enrolment credentials used to communicate over G5A.

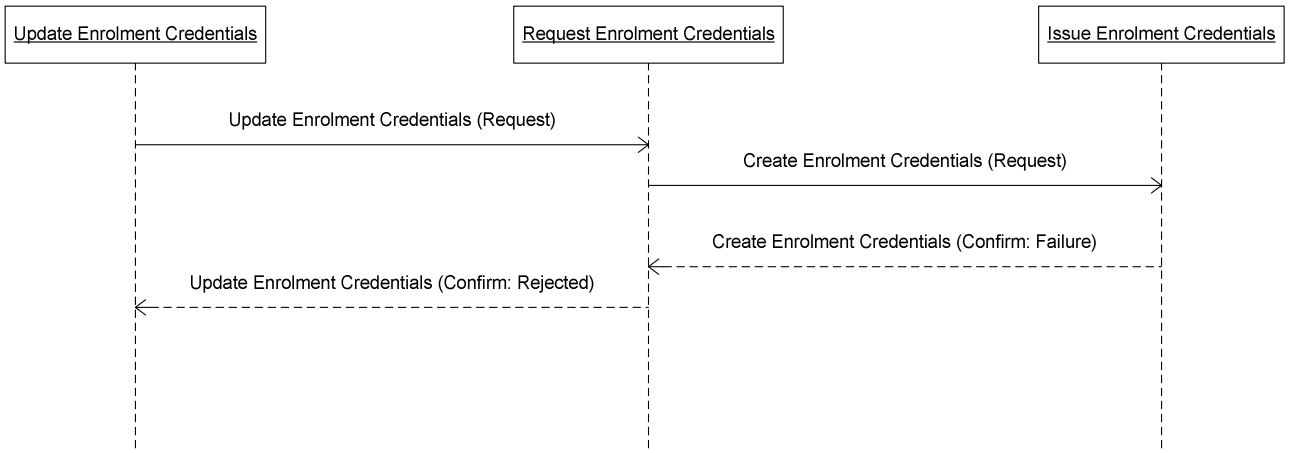


Figure 8: Unsuccessful update of enrolment credentials

7.1.3 Remove Enrolment Credentials

The Remove Enrolment Credentials security service provides the ITS network with the capability of removing the enrolment of a previously enrolled ITS-S thus nullifying any information currently in use by the ITS-S for communication with other ITS stations.

For the removal to be effective, the enrolment authority and authorization authority shall on a regular basis exchange enrolment credential and authorization status information. It is particularly important for the enrolment authority to keep the authorization authority updated at all times to ensure an accurate publishing of authorization status updates.

7.1.3.1 Functional model

7.1.3.1.1 Functional model description

The functional model of the "Remove Enrolment Credentials" security service comprises the following functional entities:

- In The ITS-S:
  - Remove enrolment credentials.
- In the ITS infrastructure:
  - Invoke enrolment credentials removal.
  - Revoke enrolment credentials.
  - Distribute enrolment revocation information.

The following relationships exist between the functional entities:

va: between *Invoke Enrolment Credentials Removal* and *Revoke Enrolment Credentials*;

vb: between *Revoke Enrolment Credentials* and *Distribute enrolment revocation information*;

vc: between *Distribute enrolment revocation information* and *Remove enrolment credentials.*

The functional entities and the relationships between them are shown in figure 9.

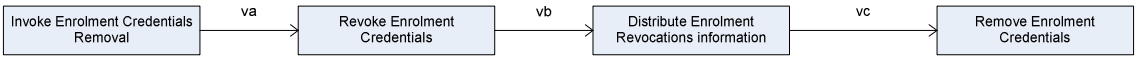


Figure 9: Functional model for the Update Enrolment Credentials security service

7.1.3.1.2 Description of functional entities

7.1.3.1.2.1 Invoke enrolment credentials removal

The *Invoke Enrolment Credentials Removal* functional entity detects the need to update the list of enrolment credentials used to communicate over G5A and sends an update request to the ITS infrastructure on behalf of the ITS-S.

7.1.3.1.2.2 Revoke enrolment credentials

The *Revoke Enrolment Credentials* functional entity receives the invoke enrolment credential request and initiate the enrolment credential removal procedure, which if successful, removes the particular enrolment credentials from the ITS network enrolment credentials repository and distribute the revocation information across the ITS infrastructure, including Authorization authorities.

7.1.3.1.2.3 Distribute enrolment revocation information

The *Distribute Enrolment Revocation Information* functional entity publishes the enrolment revocation information across the ITS infrastructure and sends a push message to the ITS-S telling it to remove its enrolment credentials.

7.1.3.1.2.4 Remove enrolment credentials

The *Remove Enrolment Credentials* functional entity receives a request to remove enrolment credentials and removes the current enrolment credentials and any information linked to or using the credentials locally on the ITS-S.

7.1.3.2 Information flows

7.1.3.2.1 Definition of information flows

7.1.3.2.1.1 Invoke Credentials Removal

Invoke Credentials Removal is a confirmed information flow across relationship *va* from *Invoke Enrolment Credentials Removal* to *Revoke Enrolment Credentials* which is used to initiate the enrolment credentials removal process. It contains the service elements specified in table 10.

Table 10: Contents of the Invoke Credentials Removal information flow

Service elements	Allowed values	Request	Confirm
Enrolment credential	Temporary identity previously allocated by the ITS infrastructure (note 2)	M	
Enrolment credential removal request	Removal request field (note 2)		
Removal request result	Accepted Rejected		M
Cause of rejection	- Enrolment credential unknown - Removal failed - Distribution failed		O (note 1)
NOTE 1: This service element shall be included if the request result is "Rejected". NOTE 2: Cryptographically signed using the Enrolment Authority key.			

7.1.3.2.1.2 Revoke Credentials

Revoke Credentials is a confirmed information flow across relationship *vb* from *Invoke Enrolment Credentials Removal* to *Revoke Enrolment Credentials* which is used to initiate the enrolment credentials removal process. It contains the service elements specified in table 11.

Table 11: Contents of the Revoke Credentials information flow

Service elements	Allowed values	Request	Confirm
Enrolment credential	Temporary identity previously allocated by the ITS infrastructure (note 2)	M	
Enrolment credential revocation result	Successful Failed		M
Cause of rejection	- Enrolment credential unknown - Revocation failed - Distribution failed		O (note 1)
NOTE 1: This service element shall be included if the request result is "Failed". NOTE 2: Cryptographically signed using the Enrolment Authority key.			

7.1.3.2.1.3 Distribute Revocation

Distribute Revocation is a confirmed information flow across relationship *vc* from *Distribute Enrolment Revocation-Information* to *Remove Enrolment Credentials* which is used to distribute the revocation information across the ITS network and in particular to Authorization authorities and other enrolment authorities. It contains the service elements specified in table 12.

Table 12: Contents of the Distribute Revocation information flow

Service elements	Allowed values	Request	Confirm
Enrolment credential	Temporary identity previously allocated by the ITS infrastructure (note 2)	M	
Credential Removal result	Successful Failed		M
Cause of rejection	- Distribution failed		O (note 1)
NOTE 1: This service element shall be included if the request result is "Failed". NOTE 2: Cryptographically signed using the Enrolment Authority key.			

7.1.3.2.2 Examples of information flow sequences

A stage 3 standard for the Update Enrolment Credentials security service shall provide procedures in support of the information flow sequences specified in clause 7.1.3.2.2.1. In addition, signalling procedures shall be provided to cover other sequences arising from, for example, error situations and interactions with other security services.

7.1.3.2.2.1 Remove Enrolment Credentials

Figure 10 shows the information flow for an ITS-S (Vehicle) successfully updating the list of enrolment credentials used to communicate over G5A.

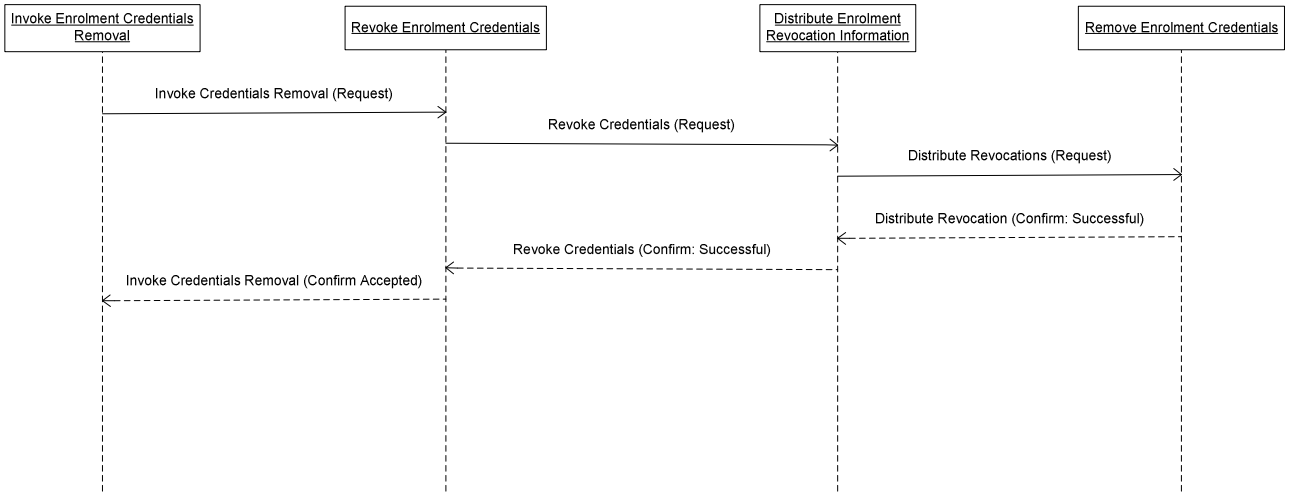


Figure 10: Successful removal of enrolment credentials

Figure 11 shows an example information flow for an ITS-S (Vehicle) unsuccessfully attempting to update the list of enrolment credentials used to communicate over G5A.

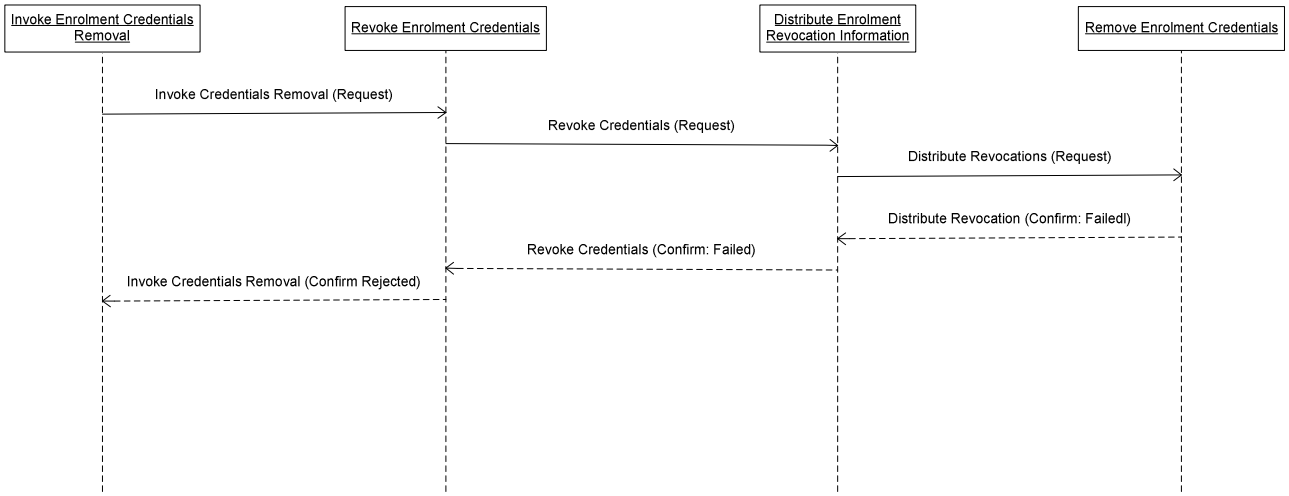


Figure 11: Unsuccessful removal of enrolment credentials

7.2 Authorization Tickets

The Authorization Tickets services consist of:

- Obtain Authorization Tickets.
- Update Authorization Tickets.
- Publish Authorization Status.
- Update Local Authorization Status Repository.

7.2.1 Functional model

7.2.1.1 Functional model description

The functional model for the Authorization Tickets security service comprises the following functional entities:

- In The ITS-S:
  - ITS Station Agent.
  - Station Authorization Manager.
- In the ITS infrastructure:
  - A-Ticket Distributor.
  - Enrolment Credentials Verifier.
  - ITS Network Agen.
  - ITS Authorization Status Manager.

The following relationships exist between the functional entities:

ua: between *ITS Station Agent* and *Station Authorization Manager*;

ub: between *Station Authorization Manager* and *A-Ticket Distributor*;

uc: between *A-Ticket Distributor* and *Enrolment Credentials Verifier*;

ud: between *Station Authorization Manager* and *ITS Authorization Status Manager*;

ue: between *ITS Authorization Status Manager* and *ITS Network Agent*;

uf; between *ITS Authorization Status Manager* and *Enrolment Credentials Verifier*.

The functional entities and the relationships between them are shown in figure 12.

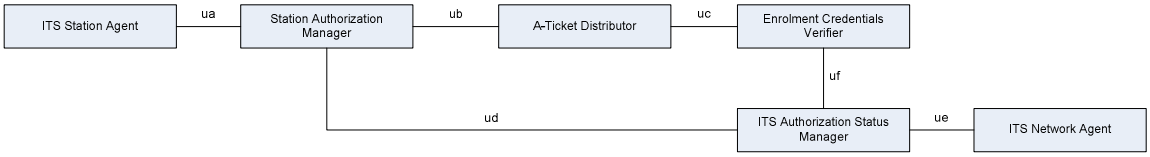


Figure 12: Functional model for the Authorization Tickets security services

7.2.1.2 Description of functional entities

7.2.1.2.1 ITS Station Agent

The *ITS Station Agent* functional entity detects the need for the ITS-S to obtain authorization tickets from the ITS infrastructure and initiates the A-tickets request procedure.

The *ITS Station Agent* functional entity receives the list of authorization status updates from the Station Authorization Manager functional entity, processes the list and updates the local authorization status repository accordingly.

The *ITS Station Agent* functional entity detects the need to update the authorization status repository for the ITS-S and initiates the repository update procedure.

NOTE: The repository is local to the ITS-S.

7.2.1.2.1.1 Station Authorization Manager

The *Station Authorization Manager* functional entity delivers an A-Ticket Request to the ITS infrastructure, receives the associated response and stores the received set of A-Tickets within the ITS-S.

The *Station Authorization Manager* functional entity receives the list of authorization status updates and forwards it to the ITS Station Agent.

The *Station Authorization Manager* functional entity delivers an update repository request to the ITS infrastructure, receives the associated response and uses this information to update its local authorization status repository.

7.2.1.2.2 A-Ticket Distributor

The *A- Ticket Distributor* functional entity receives a request for A-Tickets from an ITS-S, initiates the A-tickets issuance process and, if successful, delivers a positive response containing the set of A-Tickets for future privacy protected communication to other ITS stations.

7.2.1.2.3 Enrolment Credentials Verifier

The *Enrolment Credentials Verifier* functional entity validates the credential information provided by *A-Ticket Distributor* functional entity.

7.2.1.2.4 ITS Network Agent

The *ITS Network Agent* functional entity detects the need to update authorization status either due to a time determined update schema or due to updates to status of one or more ITS-S and initiates the update authorization status procedure. Note that the update is targeting the local authorization status repository of ITS-S.

7.2.1.2.5 ITS Authorization Status Manager

The *ITS Authorization Status Manager* functional entity receives the update authorization status request, initiates the update process and if successful, sends a list of authorization status updates to ITS-Ss within range.

7.2.2 Obtain Authorization Tickets service

The Obtain Authorization Tickets service is used by an ITS-S to request and download authorization tickets from one or more authorization authorities.

The functional model of the "Obtain Authorization Tickets" security service is specified in clause 7.2.1. The functional entities involved and the relationships between them are shown in figure 12.

7.2.2.1 Information flows

7.2.2.1.1 Definition of information flows

7.2.2.1.1.1 Get Authorization

Get Authorization is a confirmed information flow across relationship *ua* from *ITS Station Agent* to *Request A-Tickets* which is used to initiate the issue authorization ticket process. It contains the service elements specified in table 13.

Table 13: Contents of the Get Authorization information flow

Service elements	Allowed values	Request	Confirm
Enrolment Credentials	Temporary identity previously allocated by the ITS infrastructure	M	
A-Tickets Request result	- Accepted - Rejected		M
List of A-tickets	Temporary authorization parameters		O (note 1)
Cause of rejection	- Enrolment credentials unknown - A-Tickets request disabled - Authorization request failed		O (note 2)
NOTE 1: This service element shall be included if the request result is "Accepted". NOTE 2: This service element shall be included if the request result is "Rejected".			

7.2.2.1.1.2 Request Authorization

Request Authorization is a confirmed information flow across relationship *ub* from *Station Authorization Manager* to *A-Ticket Distributor* which is used to request and obtain necessary authorization tickets from the infrastructure. It contains the service elements specified in table 14.

Table 14: Contents of the Request Authorization information element

Service elements	Allowed values	Request	Confirm
Enrolment Credentials	Temporary identity previously allocated by the ITS infrastructure (note 3)	M	
A-Tickets Request	List of ITS applications for which authorization is requested (note 3)	M	
ITS-S Key	Public or symmetric key	M	
A-Tickets Request result	Accepted Rejected		M
List of A-tickets	Temporary authorization parameters		O (note 1)
Cause of rejection	- Enrolment credentials unknown - A-Tickets request disabled - No permission to use ITS application - Authorization request failed		O (note 2)
NOTE 1: This service element shall be included if the request result is "Accepted". NOTE 2: This service element shall be included if the request result is "Rejected". NOTE 3: Encrypted using the Authorization Authority Key and cryptographically signed using the ITS-S key.			

7.2.2.1.1.3 Verify Credentials

Verify Credentials is a confirmed information flow across relationship *rc* from *A-Ticket Distributor* to *Enrolment Credentials Verifier* which is used to check the correctness and validity of the enclosed ITS user's temporary identity. It contains the service elements specified in table 15.

Table 15: Contents of the Verify Credentials information flow

Service elements	Allowed values	Request	Confirm
Enrolment Credentials	Temporary identity previously allocated by the ITS infrastructure	M	
Verify Credentials result	- Success - Failure		M
Cause of rejection	- Enrolment credentials unknown - Enrolment credentials withdrawn - Marked as misbehaving ITS-S		O (note)
NOTE: This service element shall be included if the credential verification result is "Failed".			

7.2.2.1.1.4 Examples of information flow sequences

A stage 3 standard for the Obtain Authorization Tickets security service shall provide procedures in support of the information flow sequences specified in clause 7.2.2.1.1.4.1. In addition, signalling procedures shall be provided to cover other sequences arising from, for example, error situations and interactions with other security services.

7.2.2.1.1.4.1 Obtain Authorization Tickets

Figure 13 shows the information flow for an ITS-S (Vehicle) successfully requesting authorization tickets to use for future privacy protected communication with other ITS-S.

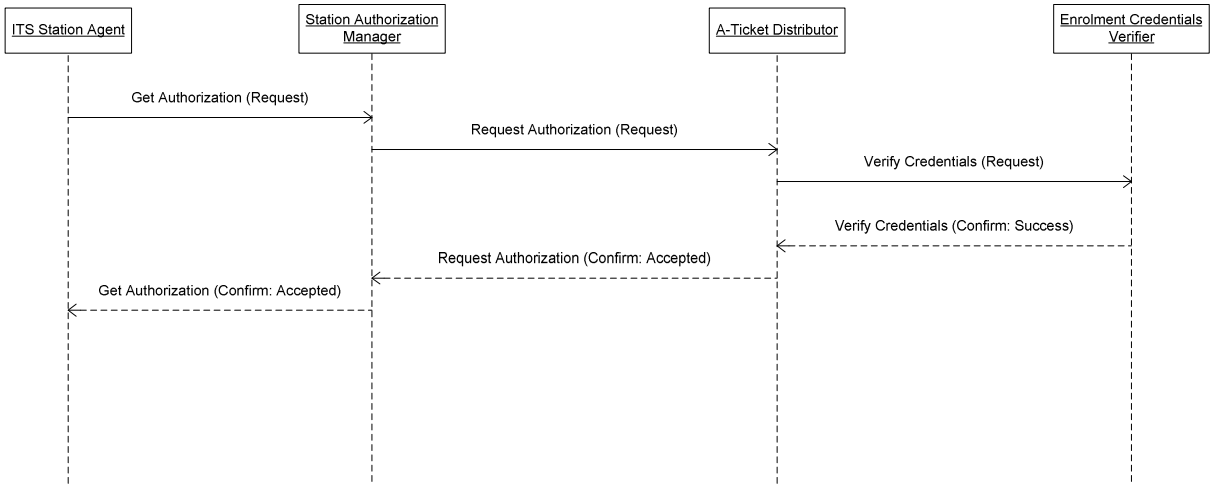


Figure 13: Successful authorization tickets request

Figure 14 shows an example information flow for an ITS-S (Vehicle) unsuccessfully attempting to request authorization tickets to use for future privacy protected communication with other ITS-S.

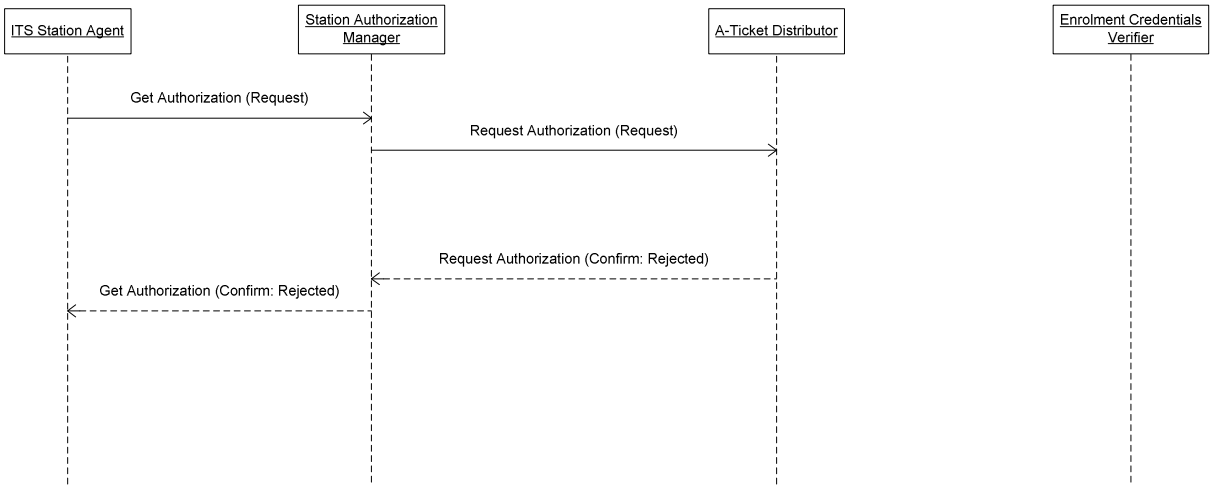


Figure 14: Unsuccessful authorization ticket request

7.2.3 Update Authorization Tickets

7.2.3.1 Functional model

7.2.3.1.1 Functional model description

Authorization tickets are restricted in number and time and shall be updated regularly. The update interval is ITS application dependent and not specified in this document. The Update Authorization Tickets security service handles all kinds of A-tickets update.

The functional model of the "Update Authorization Tickets" security service is specified in clause 7.2.1. The functional entities involved and the relationships between them are shown in figure 12.

7.2.3.2 Information flows

7.2.3.2.1 Definition of information flows

7.2.3.2.1.1 Update Authorization

Update Authorization is a confirmed information flow across relationship *ua* from *ITS Station Agent* to *Station Authorization Manager* which is used to initiate the issue authorization ticket process. It contains the service elements specified in table 16.

Table 16: Contents of the Update Authorization information flow

Service elements	Allowed values	Request	Confirm
Enrolment Credentials	Temporary identity previously allocated by the ITS infrastructure	M	
A-Tickets Update Request Result	- Accepted - Rejected		M
ITS-S Key	Public or symmetric key	M	
List of updated A-tickets	Temporary authorization parameters		O (note 1)
Cause of rejection	- Enrolment credentials unknown - A-Tickets update disabled - Authorization update failed		O (note 2)
NOTE 1: This service element shall be included if the request result is "Accepted". NOTE 2: This service element shall be included if the request result is "Rejected".			

7.2.3.2.1.2 Update A-Tickets

Update A-Tickets is a confirmed information flow across relationship *ub* from *Update A-Tickets* to *A-Ticket Distributor* which is used to request and obtain necessary authorization tickets from the infrastructure. It contains the service elements specified in table 17.

Table 17: Contents of the Update A-Tickets information element

Service elements	Allowed values	Request	Confirm
Enrolment Credentials	Temporary identity previously allocated by the ITS infrastructure (note 3)	M	
A-Tickets Update Request	List of ITS applications for which authorization is requested (note 3)	M	
A-Tickets Update Result	- Accepted - Rejected		M
List of updated A-tickets	Temporary authorization parameters		O (note 1)
Cause of rejection	- Enrolment credentials unknown - A-Tickets update disabled - No permission to use ITS application - Authorization update failed		O (note 2)
NOTE 1: This service element shall be included if the update request result is "Accepted". NOTE 2: This service element shall be included if the update request result is "Rejected". NOTE 3: Encrypted using the Authorization Authority Key and cryptographically signed using the ITS-S key.			

7.2.3.2.1.3 Verify Credentials

Verify Credentials is a confirmed information flow across relationship *uc* from *A-Ticket Distributor* to *Enrolment Credentials Verifier* which is used to check the correctness and validity of the enclosed ITS user's temporary identity. It contains the service elements specified in table 15.

7.2.3.2.1.4 Examples of information flow sequences

A stage 3 standard for the Update Authorization Tickets security service shall provide procedures in support of the information flow sequences specified in clause 7.2.3.2.1.4.1. In addition, signalling procedures shall be provided to cover other sequences arising from, for example, error situations and interactions with other security services.

7.2.3.2.1.4.1 Update Authorization Tickets

Figure 15 show the information flow for an ITS-S (Vehicle) successfully updating the list of authorization tickets for the ITS-S or for a particular ITS application.

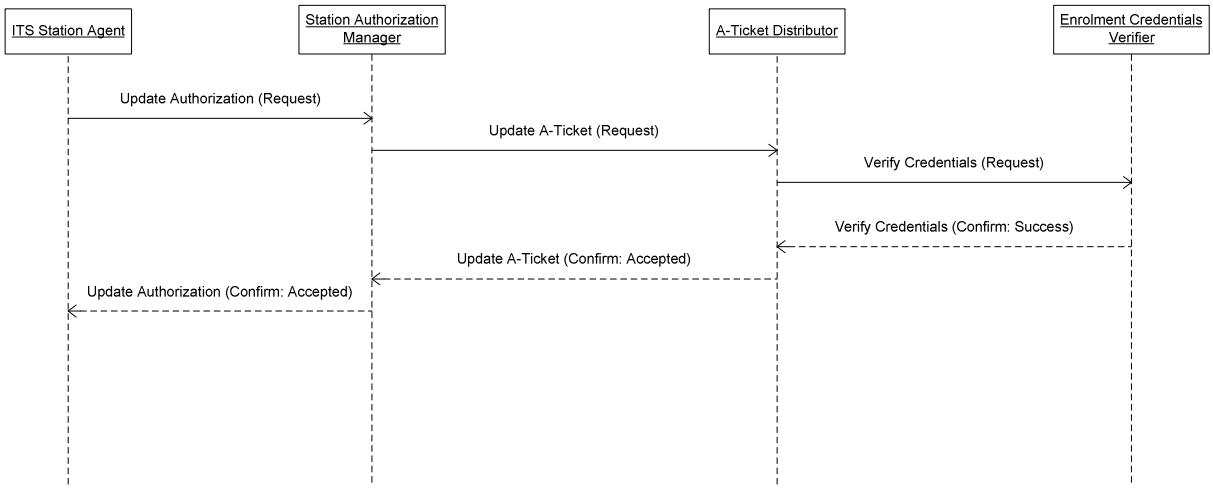


Figure 15: Successful update of authorization tickets

Figure 16 show an example information flow for an ITS-S (Vehicle) unsuccessfully attempting to update the list of authorization tickets for the ITS-S or for a particular ITS application.

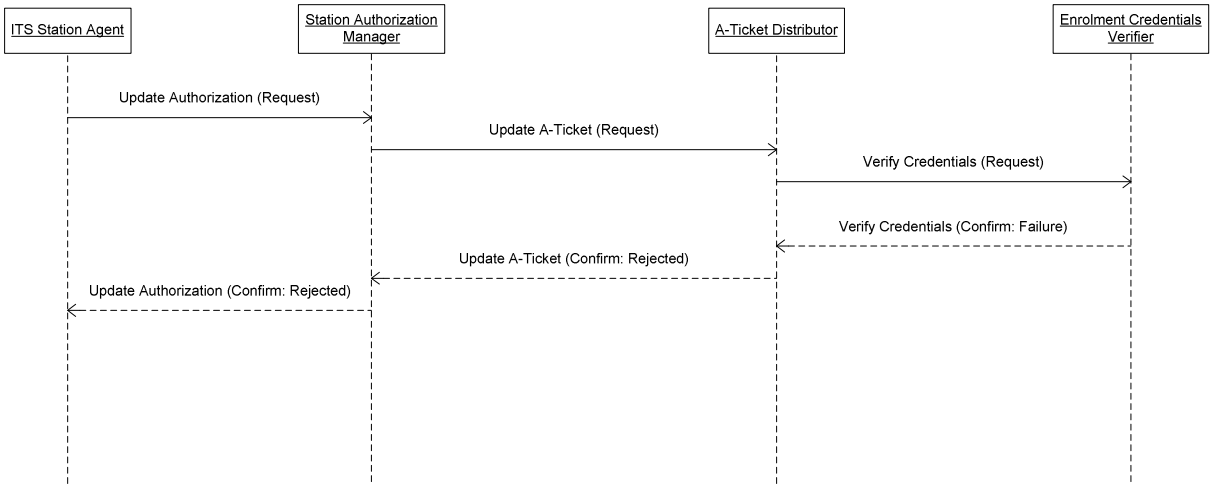


Figure 16: Unsuccessful update of authorization tickets

7.2.4 Publish Authorization Status

The Publish Authorization Status security service sends authorization status information from the ITS infrastructure either on request from an ITS-S or when determined by any authoritative entity in the ITS network to be necessary. Authorization status is used to mark particular ITS-S as misbehaving or otherwise not trustworthy or accountable in terms of either temporary disabling authorizations or removing authorizations altogether for a particular ITS-S.

The functional model of the "Publish Authorization Status" security service is specified in clause 7.2.2. The functional entities involved and the relationships between them are shown in figure 12.

7.2.4.1 Information flows

7.2.4.1.1 Definition of information flows

7.2.4.1.1.1 Broadcast Authorization Status

Broadcast Authorization Status is a confirmed information flow across relationship *ue* from *ITS Network Agent* to *ITS Authorization Status Manager* which is used to initiate the authorization status update process. It contains the service elements specified in table 18.

Table 18: Contents of the Broadcast Authorization Status information flow

Service elements	Allowed values	Request	Confirm
Authoritative Credentials	Trustworthy and Assured Identity of the Authority requesting the authorization status update	M	
Broadcast Authorization Status Request	- Accepted - Rejected		M
Authorization Status Update Information	List of authorization status updates		O (note 1)
Cause of rejection	- Authoritative credentials unknown - Status update disabled - Status update failed		O (note 2)
NOTE 1: This service element shall be included if the update request result is "Accepted". NOTE 2: This service element shall be included if the update request result is "Rejected".			

7.2.4.1.1.2 Authorization Status

Authorization Status is a confirmed information flow across relationship *ud* from *ITS Authorization Status Manager* to *Station Authorization Manager* which is used for the ITS network to push status updates to ITS stations. It contains the service elements specified in table 19.

Table 19: Contents of the Authorization Status information flow

Service elements	Allowed values	Request	Confirm
Authoritative Credentials	Trustworthy and Assured Identity of the Authority requesting the authorization status update	M	
Broadcast Authorization Status Request	- Accepted - Rejected		M
Authorization Status Update Information	List of authorization status updates (note 3)		O (note 1)
Cause of rejection	- Authoritative credentials unknown - Status update disabled - Status update failed		O (note 2)
NOTE 1: This service element shall be included if the update push result is "Accepted". NOTE 2: This service element shall be included if the update push result is "Rejected". NOTE 3: Cryptographically signed using the Authoritative key.			

7.2.4.1.1.3 Authorization Status Update

Authorization Status Update is a confirmed information flow across relationship *ua* from *Station Authorization Manager* to *ITS Station Agent* which is used for the ITS-S to receive and process update information pushed from the ITS network. It contains the service elements specified in table 19.

Table 20: Contents of the Authorization Status Update information flow

Service elements	Allowed values	Request	Confirm
Authorization Status Update Information	List of authorization status updates		O (note 1)
Authorization Status Update Result	- Accepted - Rejected		M
Cause of rejection	- Status update disabled - Status update failed		O (note 2)
NOTE 1: This service element shall be included if the update request result is "Accepted". NOTE 2: This service element shall be included if the update request result is "Rejected".			

7.2.4.1.1.4 Examples of information flow sequences

A stage 3 standard for the Publish Authorization Status security service shall provide procedures in support of the information flow sequences specified in clause 7.2.4.1.1.4.1. In addition, signalling procedures shall be provided to cover other sequences arising from, for example, error situations and interactions with other security services.

7.2.4.1.1.4.1 Publish Authorization Status

Figure 17 shows the information flow for a successful network-initiated authorization status update.

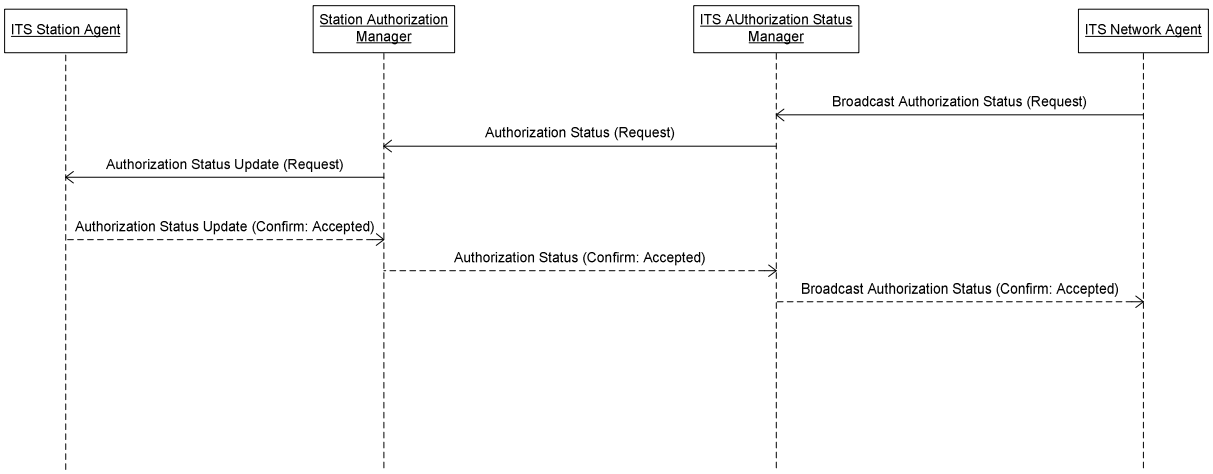


Figure 17: Successful publication of authorization status

Figure 18 shows an example information flow for an unsuccessful network-initiated authorization status update.

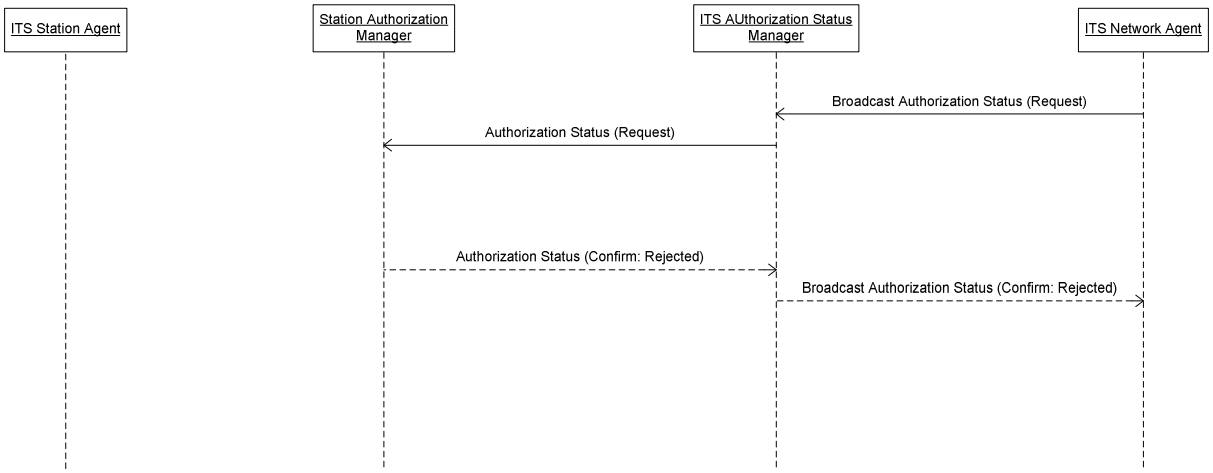


Figure 18: Unsuccessful publication of authorization status

7.2.5 Update Local Authorization Status Repository

In cases where the ITS-S does not have access to the ITS infrastructure, it uses a local authorization status repository to check authorization information presented to it by other ITS-S. This local repository is updated on a regular basis when the ITS-S gains access to the ITS infrastructure.

The functional model of the "Update Local Authorization Status Repository" security service is specified in clause 7.2.2. The functional entities involved and the relationships between them are shown in figure 12.

7.2.5.1 Information flows

7.2.5.1.1 Definition of information flows

7.2.5.1.1.1 Update Status Repository

Update Status Repository is a confirmed information flow across relationship *ua* from *ITS Station Agent* to *Station Authorization Manager* which is used to initiate the update local repository process. It contains the service elements specified in table 21.

Table 21: Contents of the Update Status Repository information flow

Service elements	Allowed values	Request	Confirm
Enrolment Credentials	Temporary identity previously allocated by the ITS infrastructure	M	
Repository Update Request	- Accepted - Rejected		M
Authorization Status Update Information	List of authorization status updates		O (note 1)
Cause of rejection	- Enrolment credentials unknown - Repository update disabled - Repository update failed		O (note 2)
NOTE 1: This service element shall be included if the update request result is "Accepted". NOTE 2: This service element shall be included if the update request result is "Rejected".			

7.2.5.1.1.2 Update Repository

Update Repository is a confirmed information flow across relationship *ud* from *Station Authorization Manager* to *ITS Authorization Status Manager* which is used to request necessary authorization status information update from the ITS infrastructure. It contains the service elements specified in table 22.

Table 22: Contents of the Update Repository information element

Service elements	Allowed values	Request	Confirm
Enrolment Credentials	Temporary identity previously allocated by the ITS infrastructure (note 3)	M	
Repository Update Request	- Accepted - Rejected		M
Authorization Status Update Information	List of authorization status updates		O (note 1)
Cause of rejection	- Enrolment credentials unknown - Repository update disabled - Repository update failed		O (note 2)
NOTE 1: This service element shall be included if the update request result is "Accepted". NOTE 2: This service element shall be included if the update request result is "Rejected". NOTE 3: Encrypted using the Authorization Authority Key and cryptographically signed using the ITS-S key.			

7.2.5.1.1.3 Verify Credentials

Verify Credentials is a confirmed information flow across relationship *uf* from *ITS Authorization Status Manager* to *Enrolment Credentials Verifier* which is used to check the correctness and validity of the relevant ITS user's temporary identity. It contains the service elements specified in table 15.

7.2.5.1.1.4 Examples of information flow sequences

A stage 3 standard for the Update Local Authorization Status Repository security service shall provide procedures in support of the information flow sequences specified in clause 7.2.5.1.1.4.1. In addition, signalling procedures shall be provided to cover other sequences arising from, for example, error situations and interactions with other security services.

7.2.5.1.1.4.1 Update Local Authorization Status Repository

Figure 19 shows the information flow for an ITS-S successfully updating its local authorization status repository.

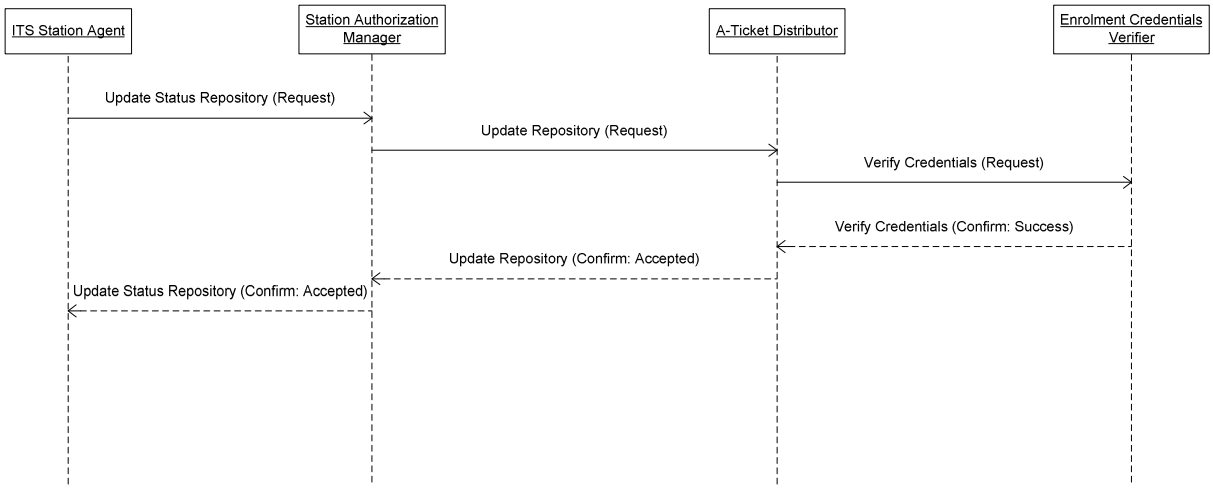


Figure 19: Successful update of local authorization status repository

Figure 20 shows an example information flow for an ITS-S unsuccessfully attempting to update its local authorization status repository.

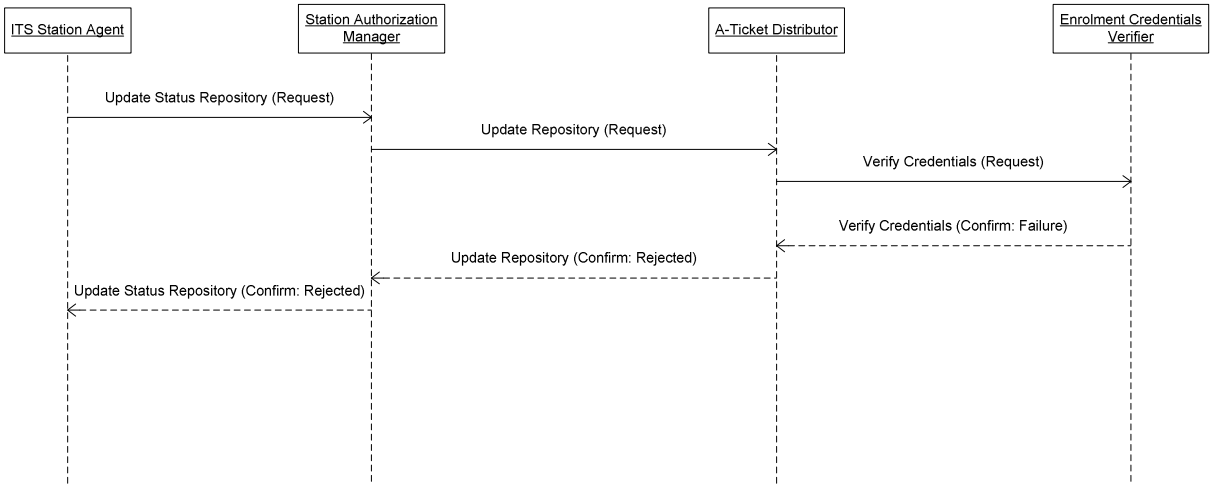


Figure 20: Unsuccessful update of local authorization status repository

7.3 Security Associations

7.3.1 Model

The use of a Security Association (SA) involves the following services:

- Establish Security Association:
  - allows two ITS-Ss to establish a one-way SA so that one ITS-S may send securely to the other. In order to allow two ITS-Ss to establish a bi-directional secure communication this service shall be used twice;
- Update Security Association:
  - allows two ITS-Ss that already share an SA to update any of the parameters of that SA;

- Send Secured Message over SA:
  - allows two ITS-Ss who have established an SA to send and receive a message securely using that SA;
- Remove Security Association:
  - allows two ITS-Ss to terminate an established SA.

7.3.1.1 Functional model

7.3.1.1.1 Functional model description

The functional model for the Security Associations group of security services comprises the following functional entities:

- In the Initiator:
  - Security Association Initiator Agent.
  - Initiator's Security Association Management.
- In the Responder:
  - Security Association Responder Agent.
  - Responder's Security Association Management.

The following relationships exist between the functional entities:

ra: between the *Security Association Initiator Agent* and the *Initiator's Security Association Management*;

rb: between the *Initiator's Security Association Management* and the *Responder's Security Association Management*;

rc: between the *Responder's Security Association Management* and the *Security Association Responder Agent.*

The functional entities and the relationships between them are shown in figure 21.

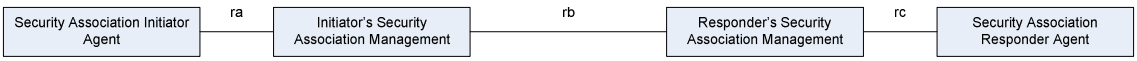


Figure 21: Functional model for the Establish Security Association security service

7.3.1.1.2 Description of functional entities

7.3.1.1.2.1 Security Association Initiator Agent

The *Security Association Initiator Agent* functional entity determines the need for the Initiator to establish or update an SA with the Responder and initiates the establishment or update procedure.

7.3.1.1.2.2 Initiator's Security Association Management

The *Initiator's Security Association Management* functional entity establishes a dialogue with the Responder in order to:

- exchange keys and other cryptographic material;
- establish the authenticity of the Responder and the scope of its authorization;
- assert the authenticity of the Initiator and the scope of its authorization.

The *Initiator's Security Association Management* functional entity stores the SA keys and parameters.

7.3.1.1.2.3 Security Association Responder Agent

The *Security Association Responder Agent* functional entity responds to the request from the Initiator to establish or update an SA between the Initiator and the Responder.

7.3.1.1.2.4 Responder's Security Association Manager

The *Responder's Security Association Manager* functional entity communicates with the *Initiator's Security Association Manager* FE to establish the keys and identifier for a new or updated SA.

The *Responder's Security Association Manager* functional entity stores the SA keys and parameters.

7.3.2 Establish Security Association

A Security Association is established between two parties, the Initiator and the Responder, each of which is an ITS-S of any type.

The functional model of the "Establish Security Association" security service is specified in clause 7.3.1.1. The functional entities and the relationships between them are shown in figure 21.

7.3.2.1 Information flows

7.3.2.1.1 Definition of information flows

7.3.2.1.1.1 Initiate SA

Initiate SA is a confirmed information flow across relationship *ra* from *Security Association Initiator Agent* to *initiator's Security Association Management.* It contains the service elements specified in table 23.

Table 23: Contents of the Initiate SA information flow

Service elements	Allowed values	Request	Confirm
Initiator's identifier	Enrolment Credentials	M	
Responder's identifier	Responder Authorization Credentials	M	
Result	- Success - Failure		M
Security Association	Set of Security Association Parameters		O (note 1)
Cause of rejection	- No parameters in common with Responder - Administrative reasons		O (note 2)
NOTE 1: This service element shall be included if the registration result is "Accepted". NOTE 2: This service element shall be included if the registration result is "Rejected".			

7.3.2.1.1.2 Initiate SA Received

Initiate SA Received is a confirmed information flow across relationship *rc* from *Responder's Security Association Management* to *Security Association Responder Agent*. It contains the service elements specified in table 24.

Table 24: Contents of the Initiate SA Received information flow

Service elements	Allowed values	Request	Confirm
Initiator's identifier	Enrolment Credentials	M	
Security Association identifier	Octet string	M	M
Result	- Success - Failure		M
Cause of rejection	- Administrative reasons		O (note)
NOTE: This service element shall be included if the registration result is "Rejected".			

7.3.2.1.1.3 SA Parameter Establishment

SA Parameter Establishment is a confirmed information flow across relationship *re* from *Initiator-side SA Parameter Establishment* to *Responder-side SA Parameter Establishment Invocation.*

Prerequisites: This information flow is undertaken in response to *SA Parameter Invocation*.

Table 25: Contents of the SA Parameter Establishment information flow

Service elements	Allowed values	Request	Confirm
Possible Security Associations	Set of Security Association Parameters supported by the sending ITS-S	M	
Result	- Success - Failure		M
Security Association	Set of Security Association Parameters supported by the Initiator and the Responder		O (note 1)
Security Association Identifier	Octet string		O (note 1)
Cause of rejection	- No parameters in common with responder		O (note 2)
NOTE 1: This service element shall be included if the parameter establishment result is "Success". NOTE 2: This service element shall be included if the parameter establishment result is "Failure".			

7.3.2.1.1.4 SA Key Establishment

7.3.2.1.1.4.1 Send Responder Key

Send Responder Key is an unconfirmed information flow across relationship *rb* from *Responder's Security Association Management* to *Initiator's Security Association Management.* It contains the service elements specified in table 26.

Table 26: Contents of the Send Responder Key information flow

Service elements	Allowed values	Request
Security Association Identifier	Octet string	M
Encryption key	Public key	O (note 1)
Encryption key reference	(note 2)	O (note 1)
Key authorization ticket		M
NOTE 1: At least one of these elements shall be included in the information flow. NOTE 2: The value of this service element depends upon the nature of the user of the SA.		

7.3.2.1.1.4.2 Initiator Keying Material

Initiator Keying material is a confirmed information flow across relationship *rb* from *Responder's Security Association Management* to *Initiator's Security Association Management.* It contains the service elements specified in table 27.

Table 27: Contents of the Initiator Keying Material information flow

Service elements	Allowed values	Request	Confirm
Security Association Identifier	Octet string	M	M
Initiator's keying material	Cryptographically secure random string encrypted using the Responder's public key	M	
Response	- The string encrypted in the Initiator's keying material - A hash of the string encrypted in the Initiator's keying material - Other valid information demonstrating the use of the key(s) derived from the Initiator's keying material		M

NOTE: The number of keys, their type and the means by which they are derived from the underlying secure random string are all outside the scope of the present document.

7.3.2.1.1.4.3 Send Initiator Key

Send Initiator Key is an unconfirmed information flow across relationship *rb* from *Initiator's Security Association Management* to *Responder's Security Association Management.* It contains the service elements specified in table 28.

Table 28: Contents of the Send Initiator Key information flow

Service elements	Allowed values	Request
Security Association Identifier		M
Encryption key	Public key	O (note 1)
Encryption key reference	(note 2)	O (note 1)
Key authorization ticket		M
NOTE 1: At least one of these elements shall be included in the information flow. NOTE 2: The value of this service element depends upon the nature of the user of the SA.		

7.3.2.1.1.4.4 Responder Keying Material

Responder Keying Material is a confirmed information flow across relationship *rb* from *Initiator's Security Association Management* to *Responder's Security Association Management.* It contains the service elements specified in table 29.

Table 29: Contents of the Responder Keying Material information flow

Service elements	Allowed values	Request	Confirm
Security Association Identifier	Octet string	M	M
Responder's keying material	Cryptographically secure random string encrypted using the Initiator's public key	M	
Response	- The string encrypted in the Responder's keying material - A hash of the string encrypted in the Responder's keying material - Other valid information demonstrating the use of the key(s) derived from the Responder's keying material		M

NOTE: The number of keys, their type and the means by which they are derived from the underlying secure random string are all beyond the scope of the present document.

7.3.2.1.1.5 Responder Authorization

7.3.2.1.1.5.1 Send Responder Authorization Context

Send Responder Authorization Context is an unconfirmed information flow across relationship *rb* from *Initiator's Security Association Management* to *Responder's Security Association Management.* . It contains the service elements specified in table 30.

Table 30: Contents of the Send Responder Authorization Context information flow

Service elements	Allowed values	Request
Security Association Identifier	Octet string	M
Authorization ticket		M
Explicit context description	Character string	O (note 1)
Context description reference	(note 2)	O (note 1)
NOTE 1: At least one of these elements shall be included in the information flow if the authorization ticket does not contain a description of the authorization context. NOTE 2: The value of this service element depends upon the nature of the user of the SA.		

7.3.2.1.1.5.1 Send Responder Authorization Key

Send Responder Authorization Key is an unconfirmed information flow across relationship *rb* from *Responder's Security Association Management* to *Initiator's Security Association Management*. It contains the service elements specified in table 31.

Table 31: Contents of the Send Responder Authorization Key information flow

Service elements	Allowed values	Request
Security Association Identifier	Octet string	M
Encryption key	Public key	O (note 1)
Encryption key reference	Network address	O (note 1)
Authorization ticket		O (note 2)
Authorization ticket reference	(note 4)	O (note 2)
Authorization code	- Cryptographic signature generated with a public key - Cryptographic signature generated with a symmetric key	O (note 3)
NOTE 1: At least one of these service elements shall be included in the information flow if the Authorization ticket does not include the relevant public encryption key. NOTE 2: At least one of these service elements shall be included in the information flow. NOTE 3: This service element shall be included in he information flow if the Authorization ticket does not contain the relevant public encryption key. NOTE 4: The value of this service element depends upon the nature of the user of the SA.		

7.3.2.1.1.5.2 Responder Authorization Challenge

Responder Authorization Challenge is a confirmed information flow across relationship *rb* from *Initiator's Security Association Management* to *Responder's Security Association management*. It contains the service elements specified in table 32.

Table 32: Contents of the Responder Authorization Challenge information flow

Service elements	Allowed values	Request	Confirm
Security Association Identifier	Octet string	M	M
Encryption challenge	Cryptographically secure random string encrypted using the Responder's authorization public key	O (note 1)	
Authentication challenge	Cryptographically secure random string encrypted using the Responder's authorization public key	O (note 1)	
Response	- The string encrypted in the Challenge - A hash of the string encrypted in the Challenge - Other valid information demonstrating the use of the key(s) derived from the Challenge		O (note 2)
Authorization ticket			O (note 3)
Authorization code	- Cryptographic signature generated with a public key - Cryptographic signature generated with a symmetric key		O (note 3)
NOTE 1: One of these service elements shall be included in the information flow. NOTE 2: Mandatory if the Encryption challenge element is included in the Request information flow. NOTE 3: Mandatory if the Authentication challenge is included in the Request information flow.			

7.3.2.1.1.5.3 Initiator Authorization

7.3.2.1.1.5.4 Send Initiator Authorization Key

Initiator Authorization Using Public-Key Encryption: Send Key is an unconfirmed information flow across relationship *rb* from *Responder's Security Association Management* to *Initiator's Security Association Management.* It contains the service elements specified in table 33.

Table 33: Contents of the Send Initiator Authorization Key information flow

Service elements	Allowed values	Request
Security Association Identifier	Octet string	M
Encryption key	Public key	O (note 1)
Encryption key reference	Network address	O (note 1)
Authorization ticket		O (note 2)
Authorization ticket reference	(note 4)	O (note 2)
Authorization code	- Cryptographic signature generated with a public key - Cryptographic signature generated with a symmetric key	O (note 3)
NOTE 1: At least one of these service elements shall be included in the information flow if the Authorization ticket does not include the relevant public encryption key. NOTE 2: At least one of these service elements shall be included in the information flow. NOTE 3: This service element shall be included in the information flow if the Authorization ticket does not contain the relevant public encryption key. NOTE 4: The value of this service element depends upon the nature of the user of the SA.		

7.3.2.1.1.5.5 Initiator Authorization Challenge

Initiator Authorization Challenge is an information flow across relationship *rb* from *Initiator's Security Association Management* to *Responder's Security Association Management.* It contains the service elements specified in table 34.

Table 34: Contents of the Initiator Authorization Challenge information flow

Service elements	Allowed values	Request	Confirm
Security Association Identifier	Octet string	M	M
Encryption challenge	Cryptographically secure random string encrypted using the Responder's authorization public key	O (note 1)	
Authentication challenge	Cryptographically secure random string encrypted using the Responder's authorization public key	O (note 1)	
Response	- The string encrypted in the Challenge - A hash of the string encrypted in the Challenge - Other valid information demonstrating the use of the key(s) derived from the Challenge		O (note 2)
Authorization ticket			O (note 3)
Authorization code	- Cryptographic signature generated with a public key - Cryptographic signature generated with a symmetric key		O (note 3)
NOTE 1: One of these service elements shall be included in the information flow. NOTE 2: Mandatory if the Encryption challenge service element is included in the Request information flow. NOTE 3: Mandatory if the Authentication challenge service element is included in the Request information flow.			

7.3.2.1.1.6 SA Establishment Complete

SA Establishment Complete is an unconfirmed information flow across relationship *rc* from *Responder's Security Association Management* to *Security Association Responder Agent*. It contains the service elements specified in table 35.

Table 35: Contents of the SA Establishment Complete information flow

Service elements	Allowed values	Request
Security Association Identifier	Octet string	M
Establishment result	- Success - Failure	
Failure cause	Unable to match security parameters with Initiator	O (note)
NOTE: This service element shall be included in the information flow if the establishment result is "Failure".		

7.3.2.1.1.7 Examples of information flow sequences

A stage 3 standard for the Establish Security Association security service shall provide procedures in support of the information flow sequences specified in clause 7.3.2.1.1.7.1. In addition, signalling procedures shall be provided to cover other sequences arising from, for example, error situations and interactions with other security services.

7.3.2.1.1.7.1 Establish Security Association

Figure 22 shows the information flow for an ITS-S successfully establishing an SA with another ITS-S.

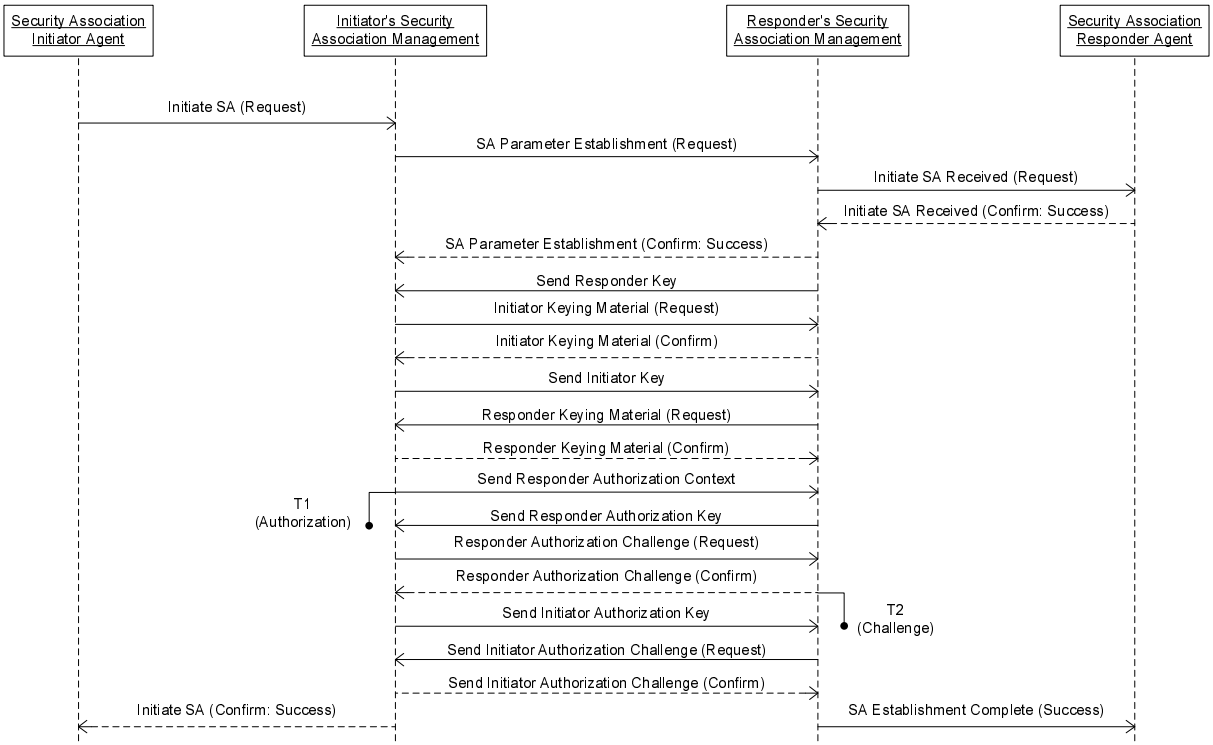


Figure 22: Successful establishment of a Security Association

Figure 23 shows an example information flow for an ITS-S unsuccessfully attempting to establish an SA with another ITS-S.

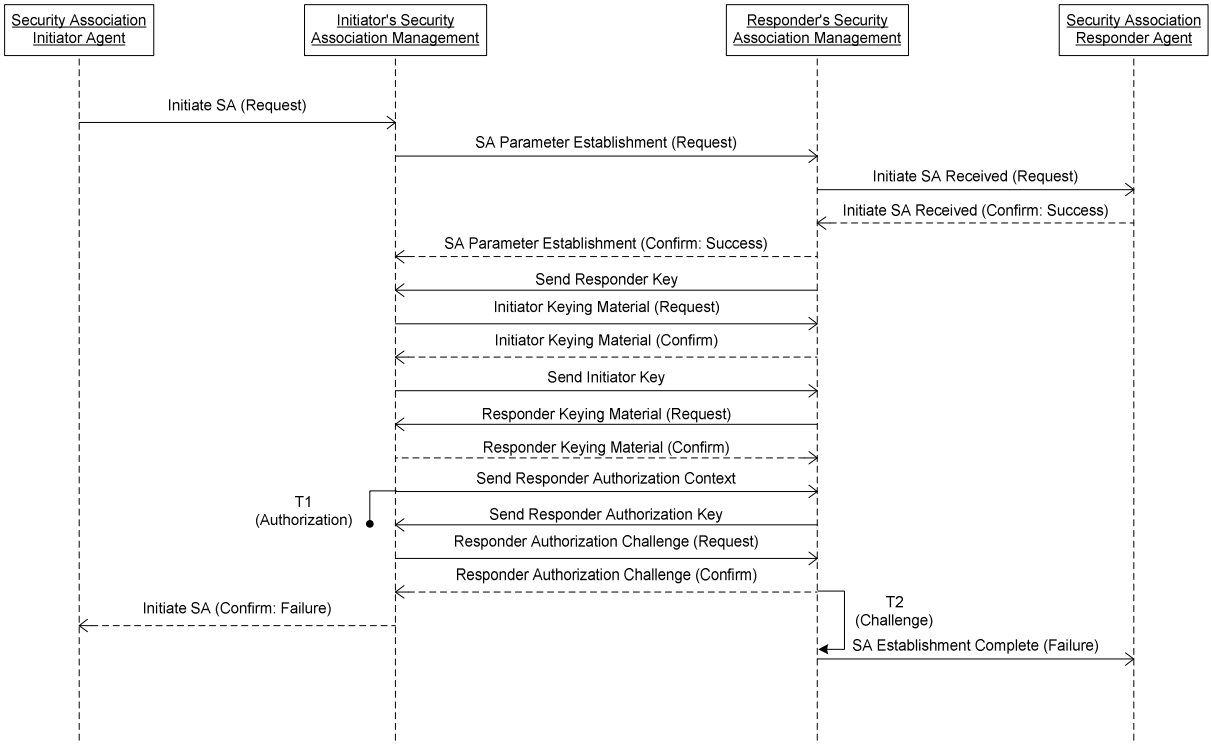


Figure 23: Unsuccessful establishment of a Security Association

7.3.3 Update security association

The Update Security Association security service removes an existing SA and establishes a new SA with the parameters required by the Initiator.

The functional model of the "Update Security Association" security service is specified in clause 7.3.1.1. The functional entities involved and the relationships between them are shown in figure 21.

7.3.3.1 Information flows

7.3.3.1.1 Definition of information flows

7.3.3.1.1.1 Update SA

Update SA is a confirmed information flow across relationship ra from *Security Association Initiator Agent* to *Initiator's Security Association Management*. It contains the service elements specified in table 36.

Table 36: Contents of the Update SA information flow

Service elements	Allowed values	Request	Confirm
Existing Security Association identifier	Octet string	M	M
New Security Association identifier	Octet string		O (note)
Update operation	- Update SA identifier - Update SA keys - Update SA identifier and keys	M	
Result	- Accepted - Rejected		M
NOTE: This service element shall be included in the information flow if the returned result is "Accepted" and the Update operation was "Update SA identifier" or "Update SA identifier and keys".			

7.3.3.1.1.2 SA Identifier Update

SA Identifier Update is a confirmed information flow across relationship *rb* from *Initiator's Security Association Management* to *Responder's Security Association Management.* It contains the service elements specified in table 37.

Table 37: Contents of the SA Identifier Update information flow

Service elements	Allowed values	Request	Confirm
Existing Security Association identifier	Octet string encrypted using the keys associated with the existing SA	M	O (note 1)
New Security Association identifier	Octet string encrypted using the keys associated with the existing SA	M	M (note 2)
Result	- Accepted - Rejected		M
NOTE 1: This service element shall be included in the information flow if the returned result is "Rejected". NOTE 2: This service element contains the Initiator's proposed new SA identifier if the returned result is "Accepted" or a different new SA identifier if the result is "Rejected".			

7.3.3.1.1.3 SA Identifier Update Response

SA Identifier Update Response is an unconfirmed information flow across relationship *rb* from *Initiator's Security Association Management* to *Responder's Security Association Management.* It contains the service elements specified in table 38.

Table 38: Contents of the SA Identifier Update Response information flow

Service elements	Allowed values	Request
Existing Security Association identifier	Octet string encrypted using the keys associated with the existing SA	O (note)
New Security Association identifier	Octet string encrypted using the keys associated with the existing SA	M
Result	- Accepted - Rejected	M
NOTE: This service element shall be included in the information flow if the returned result is "Accepted".		

7.3.3.1.1.4 SA Key Update

SA Key Update is a confirmed information flow across relationship *rb* from *Initiator's Security Association Management* to *Responder's Security Association Management.* It contains the service elements specified in table 39.

Table 39: Contents of the SA Key Update information flow

Service elements	Allowed values	Request	Confirm
Security Association identifier	Octet string	M (note 1)	M
New keying material	- Encryption key - Cryptographic string from which the encryption key can be derived	M (note 1)	
Responder keying material requested			O
Responder keying material	- Encryption key - Cryptographic string from which the key can be derived		O (note 1, note 2)
Result	- Accepted - Rejected		M
Rejection reason	- Decryption failure - Unable to encrypt with Initiator key - Unwilling to change key.		O (note 3)
NOTE 1: This service element shall be encrypted using the existing keys associated with the SA. NOTE 2: This service element shall be included if the Responder keying material requested service element was included in the associated Request flow. NOTE 3: This service element shall be included if the returned result is "Rejected".			

7.3.3.1.1.5 SA Key Update Response

SA Key Update Response is an unconfirmed information flow across relationship *rb* from *Initiator's Security Association Management* to *Responder's Security Association Management.* It contains the service elements specified in table 40.

Table 40: Contents of the SA Key Update Response information flow

Service elements	Allowed values	Request
Security Association identifier	Octet string encrypted using the keys associated with the existing SA	M
Result	- Accepted - Rejected	M
Rejection reason	- Decryption failure - Unwilling to change key.	O (note)
NOTE: This service element shall be included in the information flow if the returned result is "Accepted".		

7.3.3.1.1.6 SA Updated

SA Updated is an unconfirmed information flow across relationship *rc* from *Responder's Security Association Management* to *Security Association Responder Agent*. It contains the service elements specified in table 41.

Table 41: Contents of the SA Updated information flow

Service elements	Allowed values	Request
Existing Security Association identifier	Octet string	M
Update operation	- SA identifier updated - SA keys updated	M
New Security Association identifier	Octet string	O (note)
NOTE: This service element shall be included in the information flow if the Update operation service element is "SA identifier updated" or "SA identifier and keys update".		

7.3.3.1.1.7 Examples of information flow sequences

A stage 3 standard for the Update Security Association security service shall provide procedures in support of the information flow sequences specified in clauses 7.3.3.1.1.7.1 and 7.3.3.1.1.7.2. In addition, signalling procedures shall be provided to cover other sequences arising from, for example, error situations and interactions with other security services.

7.3.3.1.1.7.1 Update SA Identifier

Figure 24 shows the information flow for an ITS-S successfully updating the identifier of an established SA using an identifier selected by the Responder.

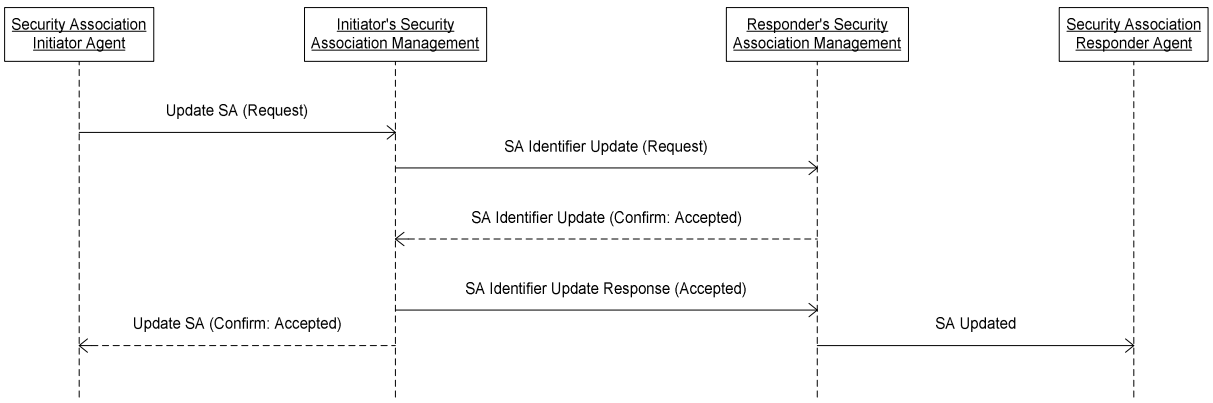


Figure 24: Successful update of a Security Association identifier

Figure 25 shows an example information flow for an ITS-S unsuccessfully attempting to update the identifier of an established SA using an identifier selected by the Responder.

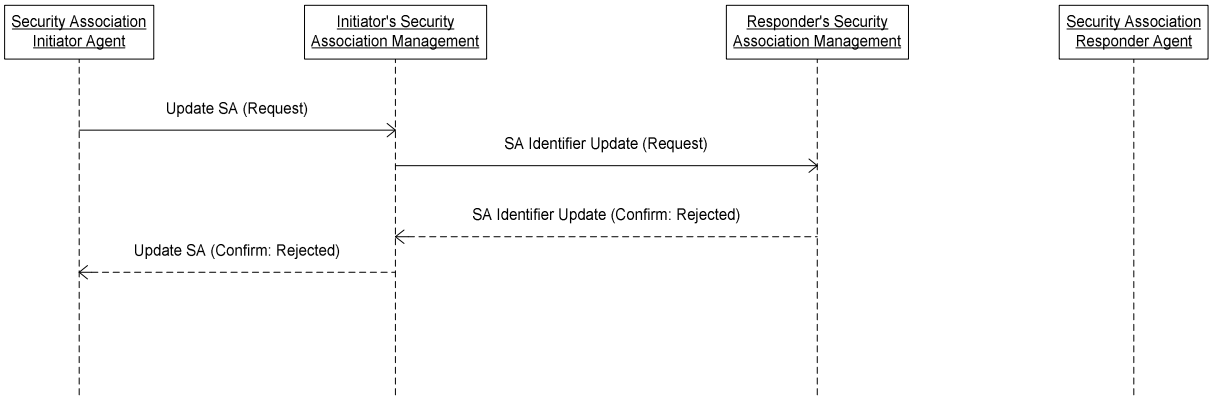


Figure 25: Unsuccessful update of a Security Association identifier

7.3.3.1.1.7.2 Update SA keys

Figure 26 shows the information flow for an ITS-S successfully updating the security keys associated with an established SA using keying material selected by the Initiator.

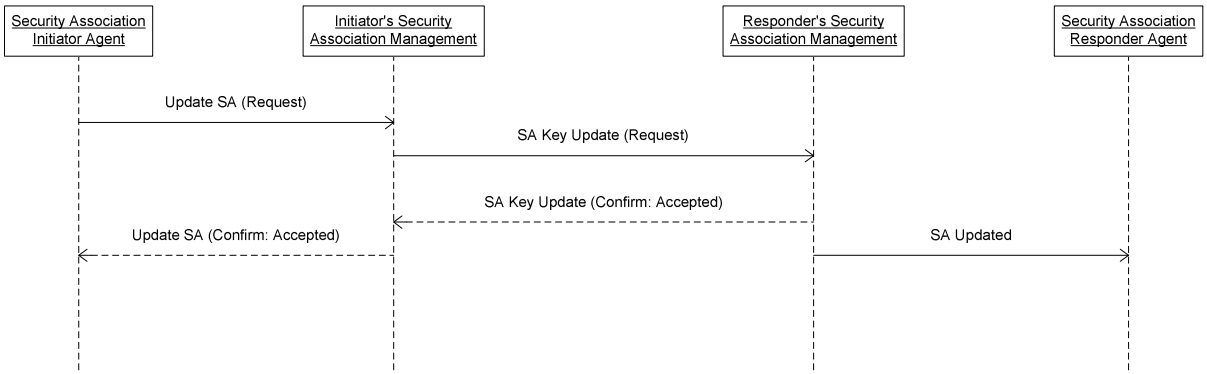


Figure 26: Successful update of a Security Association keys

Figure 27 shows an example information flow for an ITS-S unsuccessfully attempting to update the security keys associated with an established SA using keying material selected by the Initiator.

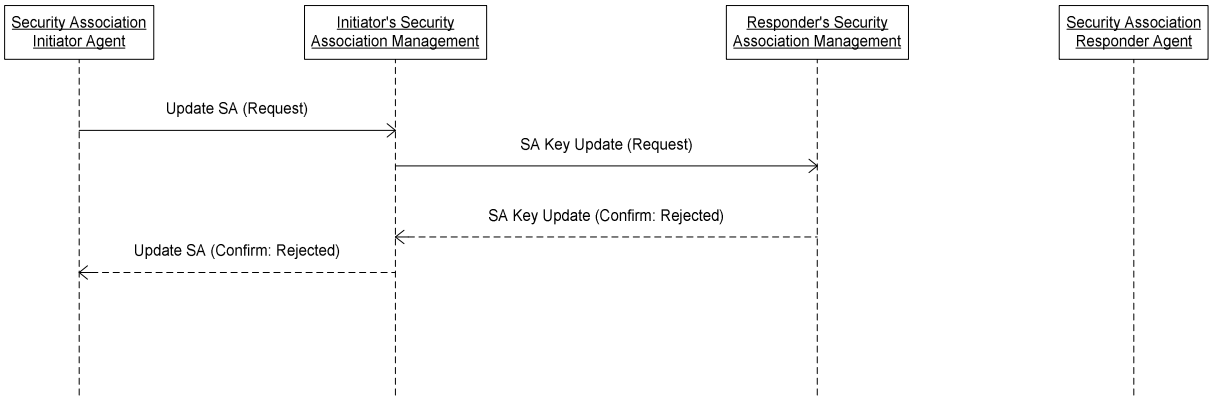


Figure 27: Unsuccessful update of a Security Association keys

7.3.4 Send Secured Message

The *Send Secured Message* security service encrypts and authenticates an ITS message before it is transmitted to its destination.

This security service involves no exchange of information with entities outside the ITS-S.

7.3.5 Receive Secured Message

The *Receive Secured Message* security service authenticates and decrypts a secured ITS message received by the ITS-S.

This security service involves no exchange of information with entities outside the ITS-S.

7.3.6 Remove security association

The *Remove Security Association* security service marks a specified SA as invalid and, optionally, informs the Responder.

The functional model of the "Remove Security Association" security service is specified in clause 7.3.1.1. The functional entities involved and the relationships between them are shown in figure 21.

7.3.6.1 Information flows

7.3.6.1.1 Definition of information flows

7.3.6.1.1.1 Remove SA

Remove SA is a confirmed information flow across relationship *ra* from *Security Association Initiator Agent* to *Initiator's Security Association Manager*. It contains the service elements specified in table 42.

Table 42: Contents of the Remove SA information flow

Service elements	Allowed values	Request	Confirm
Security Association identifier	Octet string	M	M
Result	- Accepted - Rejected		M
Rejection reason	- Unknown SA Identifier - SA Identifier already marked invalid		O (note)
NOTE: This service element shall be included if the returned result is "Rejected".			

7.3.6.1.1.2 SA Removal

SA Removal is a confirmed information flow across relationship *rb* from *Initiator's Security Association Management* to *Responder's Security Association Management*. It contains the service elements specified in table 43.

Table 43: Contents of the SA Removal information flow

Service elements	Allowed values	Request	Confirm
Security Association identifier	Octet string encrypted using the keys associated with the existing SA	M	M
Result	- Accepted - Rejected		M
Rejection reason	- Unknown SA Identifier - SA Identifier already marked invalid		O (note)
NOTE: This service element shall be included if the returned result is "Rejected".			

7.3.6.1.1.3 SA Removed

SA removed is an unconfirmed information flow across relationship *rc* from *Responder's Security Association Management* to *Security Association Responder Agent*. It contains the service elements specified in table 44.

Table 44: Contents of the SA Removed information flow

Service elements	Allowed values	Request
Security Association identifier	Octet string encrypted using the keys associated with the existing SA	M

7.3.6.1.1.4 Examples of information flows

A stage 3 standard for the Remove Security Association security service shall provide procedures in support of the information flow sequences specified in clause 7.3.6.1.1.4.1. In addition, signalling procedures shall be provided to cover other sequences arising from, for example, error situations and interactions with other security services.

7.3.6.1.1.4.1 Remove Security Association

Figure 28 shows the information flow for an ITS-S successfully removing an established SA.

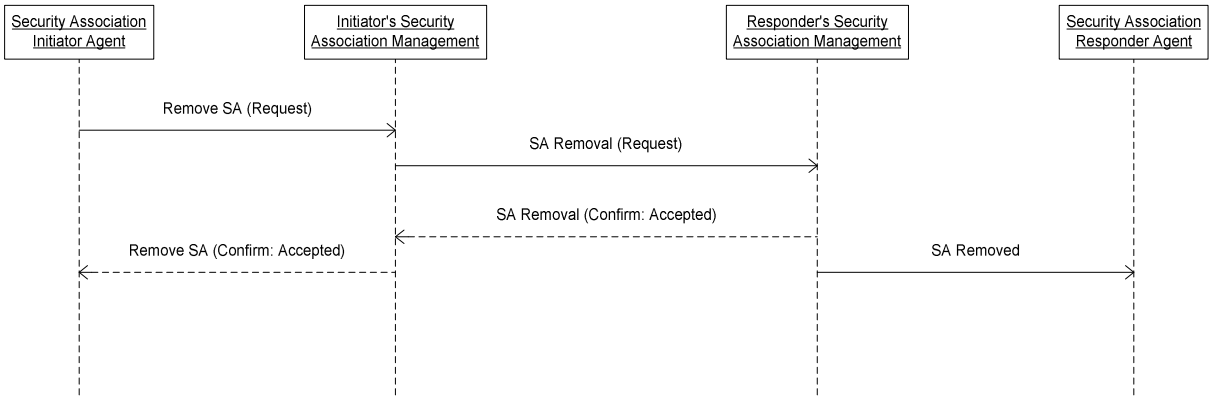


Figure 28: Successful removal of a Security Association

Figure 29 shows an example information flow for an ITS-S unsuccessfully attempting to remove an established SA.

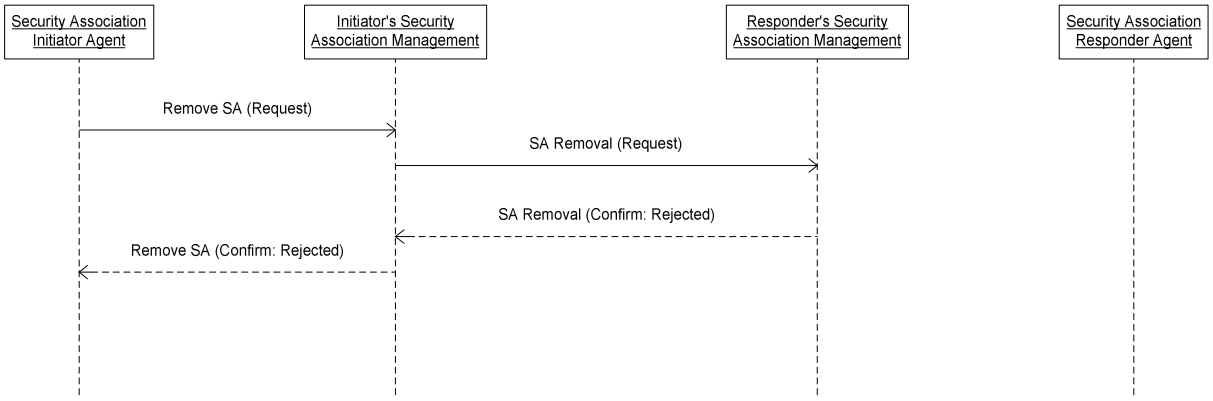


Figure 29: Unsuccessful removal of a Security Association

7.4 Single message services

7.4.1 Authorize Single Message

The Authorize Single Message security service invokes other sub-services in order to authorize a single outgoing ITS message.

This security service involves no exchange of information with entities outside the ITS-S.

7.4.2 Validate Authorization on Single Message

The Validate Authorization on Single Message security service invokes other sub-services in order to validate the authorization of a single incoming ITS message by evaluating the authorization tickets attached to the message, the authorization code associated with the message and the timestamp of the message.

This security service involves no exchange of information with entities outside the ITS-S.

7.4.3 Encrypt Single Message

7.4.3.1 Overview

The Encrypt Single Message security service invokes other subservices to acquire the appropriate cryptographic keys in order to encrypt a single outgoing ITS message.

This security service involves no exchange of information with entities outside the ITS-S.

7.4.4 Decrypt Single Message

7.4.4.1 Overview

The Decrypt Single Message security service invokes other subservices to acquire the appropriate cryptographic keys in order to decrypt a single incoming ITS message encrypted for that particular ITS-S.

This security service involves no exchange of information with entities outside the ITS-S.

7.5 Integrity services

NOTE: Check values can be either cryptographically generated and validated or non-cryptographic.

7.5.1 Calculate Check Value

The Calculate Check Value security service computes a checksum or cyclic redundancy check value for an outgoing message at the Networking and Transport layer of the ITS protocol stack.

NOTE: The primary purpose of a checksum is to make it possible to detect message corruption during transmission. A cyclic redundancy check, however, is used in order to make the correction of transmission errors possible.

This security service involves no exchange of information with entities outside the ITS-S.

7.5.2 Validate Check Value

The Validate Check Value security service compares the checksum or cyclic redundancy check value received in an ITS Networking and Transport layer message with its own calculation of what the value should be. Any message that contains a checksum value that is different from the calculated value can be rejected.

This security service involves no exchange of information with entities outside the ITS-S.

7.5.3 Insert Check Value

The Insert Check Value security service adds a checksum or cyclic redundancy check value into an outgoing message at the Networking and Transport layer of the ITS protocol stack.

This security service involves no exchange of information with entities outside the ITS-S.

7.6 Replay Protection services

7.6.1 Replay Protection Based on Timestamp

The Replay Protection Based on Timestamp security service provides a timestamp for inclusion in an outgoing message. For an incoming message, the Replay Protection Based on Timestamp service maintains a list of recently received messages and rejects messages that match previously received messages or messages whose timestamp is too old.

7.6.2 Replay Protection Based on Sequence Number

The Replay Protection Based on Sequence Number service provides a sequence number for inclusion in an outgoing message. For an incoming message, the Replay Protection Based on Sequence Number service rejects messages whose sequence number is not consistent with the expected sequence number.

7.7 Accountability services

NOTE: Data stored has to be stored in accordance with the legislation that applies in the region of operation.

7.7.1 Record Incoming Message in Audit Log

The Record Incoming Message in Audit Log security service is used by the ITS-S to record events for audit purposes and for the purpose of ensuring that the ITS-S can be held accountable according to the messages received.

This security service involves no exchange of information with entities outside the ITS-S.

NOTE: May be used to support a repudiation service.

7.7.2 Record outgoing message in Audit Log

The Record Outgoing Message in Audit Log security service is used by the ITS-S to record events for audit purposes and for the purpose of ensuring that the ITS-S can be held accountable according to the messages that it sends.

This security service involves no exchange of information with entities outside the ITS-S.

NOTE: May be used to support a repudiation service.

7.8 Plausibility validation

7.8.1 Validate Data Plausibility

The Validate Data Plausibility security service compares information such a geographic position, time-of-day and vehicle speed and direction received in an incoming ITS message and compares it with recently received data form available sources to validate whether the newly received information can be trusted on the basis of its plausibility.

This security service involves no exchange of information with entities outside the ITS-S.

7.9 Remote management

The ITS-S Remote Management security services enable the ITS infrastructure to remotely manage an ITS-S. The services are only used in cases of misbehaviour or in circumstances where the ITS-S is causing sever harm to the ITS network and/or users. In the best interest of ITS, it is important to ensure mutual and confirmed authentication between the ITS infrastructure and the ITS-S. There are only two remote management services specified:

- Activate ITS transmission.
- Deactivate ITS transmission.

7.9.1 Functional model

7.9.1.1 Functional model description

The functional model for the Remote Management security services comprises the following functional entities:

- In The ITS-S:
  - ITS Transmission Manager.
  - ITS Station Agent.
- In the ITS infrastructure:
  - ITS Network Agent.
  - ITS Transmission Controller.

The following relationships exist between the functional entities:

sa: between *ITS Network Agent* and *ITS Transmission Controller*;

sb: between *ITS Transmission Controller* and *ITS Transmission Manager*;

sc: between *ITS Transmission Manager* and *ITS Station Agent*.

The functional entities and the relationships between them are shown in figure 30.

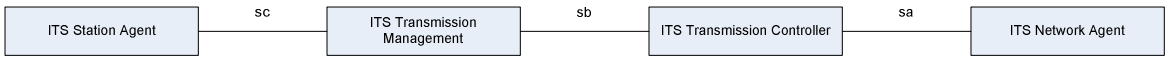


Figure 30: Functional model for the Remote Management security services

7.9.1.1.1 Description of functional entities

7.9.1.1.1.1 ITS Network Agent

The *ITS Network Agent* functional entity detects the need to terminate or restart ITS transmissions from an ITS-S and initiates transmission deactivation or activation procedures.

7.9.1.1.1.2 ITS Transmission Controller

On request from the *ITS Network Agent* functional entity the *ITS Transmission Controller* functional entity uses secure communication to command the remote station to deactivate or activate its ITS transmissions.

7.9.1.1.1.3 ITS Transmission Manager

The *ITS Transmission Manager* functional entity validates the relevant security associations and authoritative security parameters related to a received request to deactivate or activate ITS transmissions and forwards the request to the ITS Station Agent functional entity.

7.9.1.1.1.4 ITS Station Agent

On request from the *ITS Transmission Manager* functional entity, the *ITS Station Agent* functional entity terminates or restarts the specified ITS transmissions.

7.9.2 Activate ITS transmission

The Active ITS Transmission security service enables the ITS infrastructure to enable the transmission of ITS messages on a specific ITS-S.

The functional model of the "Activate ITS Transmission" security service is specified in clause 7.9.1. The functional entities involved and the relationships between them are shown in figure 30.

7.9.2.1 Information flows

7.9.2.1.1 Remote Activate Transmission

Remote Activate Transmission is a confirmed information flow across relationship *sa* from *ITS Network Agent* to *ITS Transmission Controller*. It contains the service elements specified in table 45.

Table 45: Contents of the Remote Activate Transmission information flow

Service elements	Allowed values	Request	Confirm
Target station identity	Enrolment identity of the ITS-S	M	M
ITS Transmission	Specification of the kind of ITS Transmission to restart or initiate	M	
Activation result	- Success - Failure		M
Cause of failure	- Station identity unknown - Activate process disabled - Activate process refused - Activate process failed		O (note)
NOTE: This service element shall be included if the activation result is "Failure".			

7.9.2.1.2 Activate Transmission

Activate Transmission is a confirmed information flow across relationship *sb* from *ITS Transmission Controller* to *ITS Transmission Manager*. It contains the service elements specified in table 46.

Table 46: Contents of the Activate Transmission information flow

Service elements	Allowed values	Request	Confirm
ITS network authority	Authoritative identity (note 2)	M	
Target station identity	Enrolment identity of the ITS-S (note 2)	M	M
ITS Transmission	Specification of the kind of ITS Transmission to restart or initiate	M	
Activation result	Success Failure		M
Cause of failure	- Station identity unknown - Activate process disabled - Activate process refused - Activate process failed		O (note 1)
NOTE 1: This service element shall be included if the activation result is "Failure". NOTE 2: Encrypted with ITS-S key and cryptographically signed with ITS infrastructure authoritative key.			

7.9.2.1.3 Transmission Activation

Transmission Activation is a confirmed information flow across relationship *sc* from *ITS Transmission Manager* to *ITS Station Agent*. It contains the service elements specified in table 47.

Table 47: Contents of the Transmission Activation information flow

Service elements	Allowed values	Request	Confirm
ITS network authority	Authoritative identity	M	
Target station Identity	Enrolment identity of the ITS-S	M	
ITS Transmission	Specification of the kind of ITS Transmission to restart or initiate	M	
Activation result	Success Failure		M
Cause of failure	- Activate process disabled - Activate process refused - Activate process failed		O (note)
NOTE: This service element shall be included if the activation result is "Failure".			

7.9.2.1.4 Examples of information flow sequences

A stage 3 standard for the Activate ITS Transmission security service shall provide procedures in support of the information flow sequences specified in clause 7.9.2.1.4.1. In addition, signalling procedures shall be provided to cover other sequences arising from, for example, error situations and interactions with other security services.

7.9.2.1.4.1 Activate ITS Transmission

Figure 31 shows the information flow for successful activation of ITS transmission from a remote ITS-S.

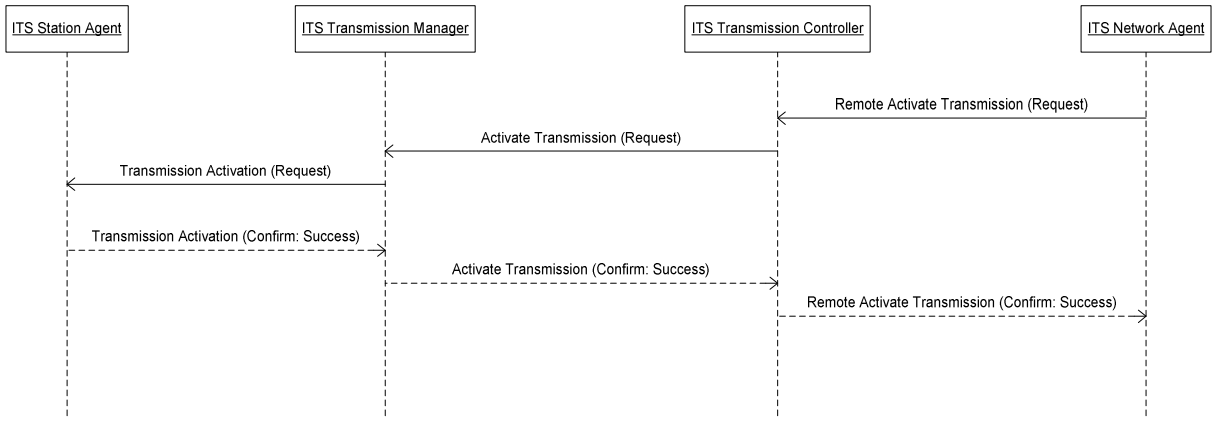


Figure 31: Successful remote activation of ITS transmission

Figure 32 shows an example information flow for an unsuccessful attempt to activate ITS transmission from a remote ITS-S.

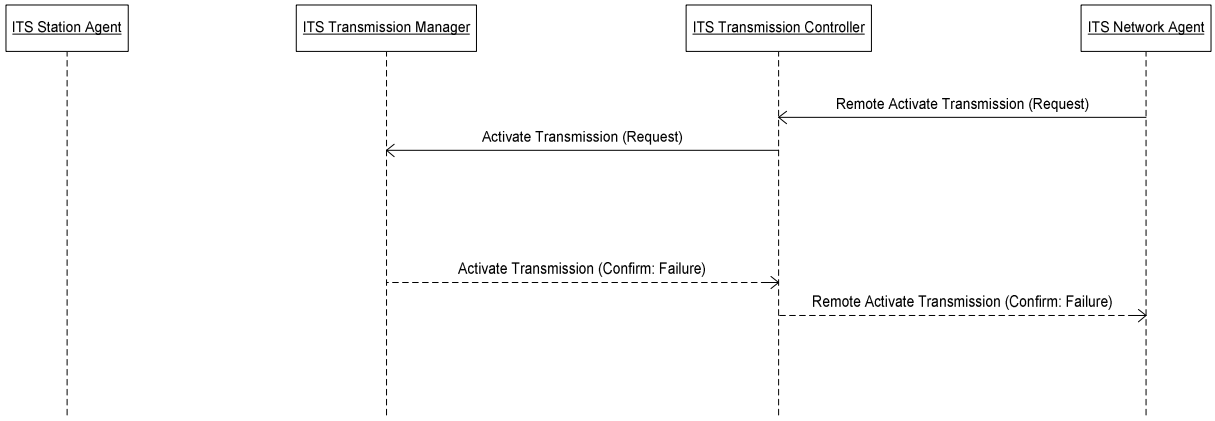


Figure 32: Unsuccessful remote activation of ITS transmission

7.9.3 Deactivate ITS transmission

The Deactivate ITS Transmission security service enables the ITS infrastructure to remotely stop certain ITS transmission or all ITS transmission locally on an ITS-S.

The functional model of the "Deactivate ITS Transmission" security service is specified in clause 7.9.1. The functional entities involved and the relationships between them are shown in figure 30.

7.9.3.1 Information flows

7.9.3.1.1 Definition of information flows

7.9.3.1.1.1 Remote Deactivate Transmission

Remote Deactivate Transmission is a confirmed information flow across relationship *sa* from *ITS Network Agent* to *ITS Transmission Controller*. It contains the service elements specified in table 48.

Table 48: Contents of the Remote Deactivate Transmission information flow

Service elements	Allowed values	Request	Confirm
Target station Identity	Enrolment identity of the ITS-S	M	M
ITS Transmission	Specification of the kind of ITS Transmission to restart or initiate	M	
Deactivation result	- Success - Failure		M
Cause of failure	- Station identity unknown - Deactivate process disabled - Deactivate process refused - Deactivate process failed		O (note)
NOTE: This service element shall be included if the deactivation result is "Failure".			

7.9.3.1.1.2 Deactivate Transmission

Deactivate Transmission is a confirmed information flow across relationship *sb* from *ITS Transmission Controller* to *ITS Transmission Management*. It contains the service elements specified in table 49.

Table 49: Contents of the Deactivate Transmission information flow

Service elements	Allowed values	Request	Confirm
ITS network authority	Authoritative identity (note 2)	M	
Target station Identity	Enrolment identity of the ITS-S (note 2)	M	M
ITS Transmission	Specification of the kind of ITS Transmission to restart or initiate	M	
Deactivation result	- Success - Failure		M
Cause of failure	- Station identity unknown - Deactivate process disabled - Deactivate process refused - Deactivate process failed		O (note 1)
NOTE 1: This service element shall be included if the deactivation result is "Failure". NOTE 2: Encrypted with ITS-S key and cryptographically signed with ITS infrastructure authoritative key.			

7.9.3.1.1.3 Transmission Deactivation

Transmission Deactivation is a confirmed information flow across relationship s*c* from *ITS Transmission Management* to *ITS Station Agent*. It contains the service elements specified in table 50.

Table 50: Contents of the Transmission Deactivation information flow

Service elements	Allowed values	Request	Confirm
ITS network authority	Authoritative identity	M	
Target station Identity	Enrolment identity of the ITS-S	M	
ITS Transmission	Specification of the kind of ITS Transmission to restart or initiate	M	
Deactivation result	- Success - Failure		M
Cause of failure	- Deactivate process disabled - Deactivate process refused - Deactivate process failed		O (note)
NOTE: This service element shall be included if the deactivation result is "Failure".			

7.9.3.1.1.4 Examples of information flow sequences

A stage 3 standard for the Activate ITS Transmission security service shall provide procedures in support of the information flow sequences specified in clause 7.9.3.1.1.4.1. In addition, signalling procedures shall be provided to cover other sequences arising from, for example, error situations and interactions with other security services.

7.9.3.1.1.4.1 Deactivate ITS Transmission

Figure 33 shows the information flow for the successful deactivation of ITS transmission at a remote ITS-S.

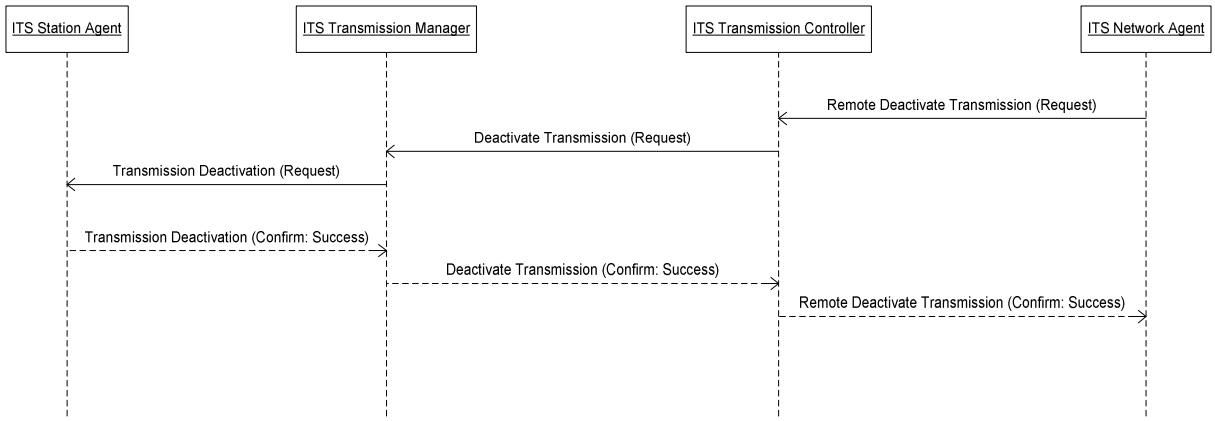


Figure 33: Successful remote deactivation of ITS transmission

Figure 34 shows an example information flow for an unsuccessful attempt to deactivate ITS transmission at a remote ITS-S.

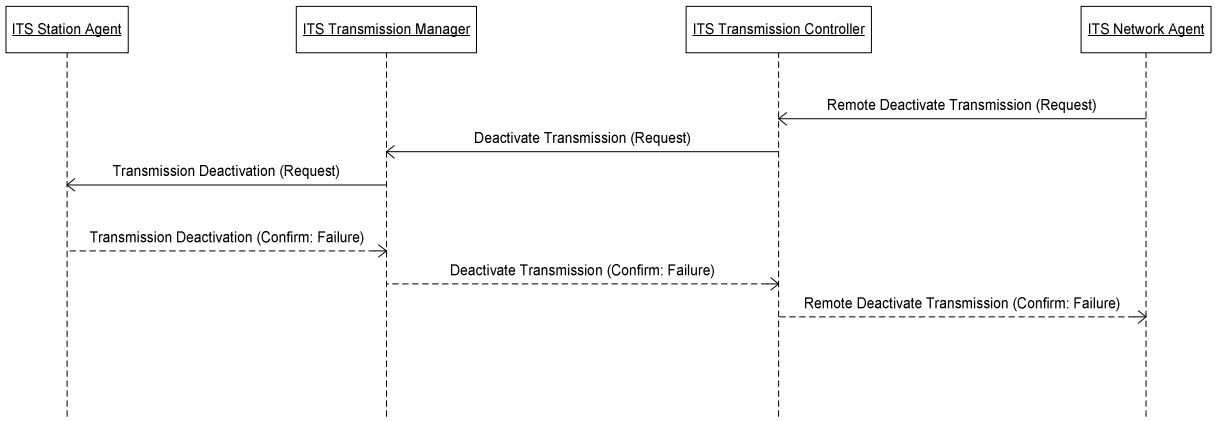


Figure 34: Unsuccessful remote deactivation of ITS transmission

7.10 Report Misbehaving ITS-S

7.10.1 Report misbehaviour

The Report Misbehaviour security service is used by an ITS-S to report suspicious activity to the ITS infrastructure.

7.10.1.1 Functional model

7.10.1.1.1 Functional model description

The functional model of the "Report Misbehaviour" security service comprises the following functional entities:

- In The ITS-S:
  - ITS Station Agent.
  - Station Reporting.

- In the ITS infrastructure:
  - Network Reporting.

The following relationships exist between the functional entities:

ma: between *ITS Station Agent* and *Station Reporting*;

mb: between *Station Reporting* and *Network Reporting*.

The functional entities and the relationships between them are shown in figure 35.

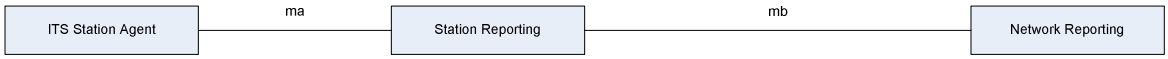


Figure 35: Functional model for the Report Misbehaviour security service

7.10.1.1.2 Description of functional entities

7.10.1.1.2.1 ITS Station Agent

The *ITS Station Agent* functional entity detects the need for the ITS-S to report a potential misbehaving ITS-S with which it is communicating.

7.10.1.1.2.2 Station Reporting

The *Station Reporting* functional entity prepares the misbehaviour report and publishes it to the ITS infrastructure.

7.10.1.1.2.3 Network Reporting

The *Network Reporting* functional entity receives a misbehaviour report from an ITS-S and initiates the appropriate procedures on behalf of the ITS infrastructure. The details of this procedure are not described in the present document.

7.10.1.2 Information flows

7.10.1.2.1 Definition of information flows

7.10.1.2.1.1 Misbehaviour Detected

Misbehaviour Detected is a confirmed information flow across relationship *ma* from *ITS Station Agent* to *Station Reporting*. It contains the service elements specified in table 51.

Table 51: Contents of the Misbehaviour Detected information flow

Service elements	Allowed values	Request	Confirm
Misbehaving station identity	Authorization ticket	M	
Reported behaviour	Free text string (note 2)	M	
Write Request result	- Accepted - Rejected		M
Cause of rejection	- Misbehaviour reporting disabled - Misbehaviour reporting failed		O (note 2)
NOTE 1: This service element shall be included if the write request result is "Rejected". NOTE 2: The format of the reported behaviour is beyond the scope of the present document.			

7.10.1.2.1.2 Report Misbehaviour

Report Misbehaviour is confirmed information flow across relationship *mb* from *Station Reporting* to *Network Reporting* . It contains the service elements specified in table 51.

Table 52: Contents of the Report Misbehaviour information flow

Service elements	Allowed values	Request	Confirm
Misbehaving station identity	Authorization Ticket(note 2)	M	
Reporting ITS-S	Enrolment credentials (note 2)	M	
Reported behaviour	Free text string (note 3)	M	
Write Request Result	- Accepted - Rejected		M
Cause of rejection	- Misbehaviour reporting disabled - Misbehaviour reporting failed		O (note 2)
NOTE 1: This service element shall be included if the write request result is "Rejected". NOTE 2: Encrypted using Authorization Authority Key and cryptographically signed using ITS-S key. NOTE 3 The format of the reported behaviour is beyond the scope of the present document.			

7.10.1.2.1.3 Examples of information flow sequences

A stage 3 standard for the Report Misbehaviour security service shall provide procedures in support of the information flow sequences specified in clause 7.10.1.2.1.3.1. In addition, signalling procedures shall be provided to cover other sequences arising from, for example, error situations and interactions with other security services.

7.10.1.2.1.3.1 Report Misbehaviour

Figure 36 shows the information flow for an ITS S successfully reporting the misbehaviour of another ITS-S to the ITS authority.

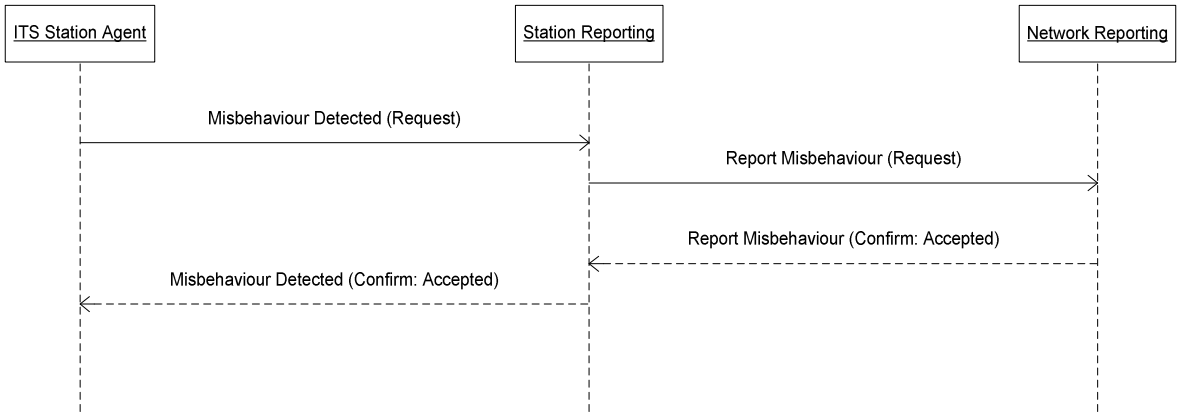


Figure 36: Successful reporting of misbehaviour

Figure 37 shows an example information flow for an ITS S unsuccessfully attempting to report the misbehaviour of another ITS-S to the ITS authority.

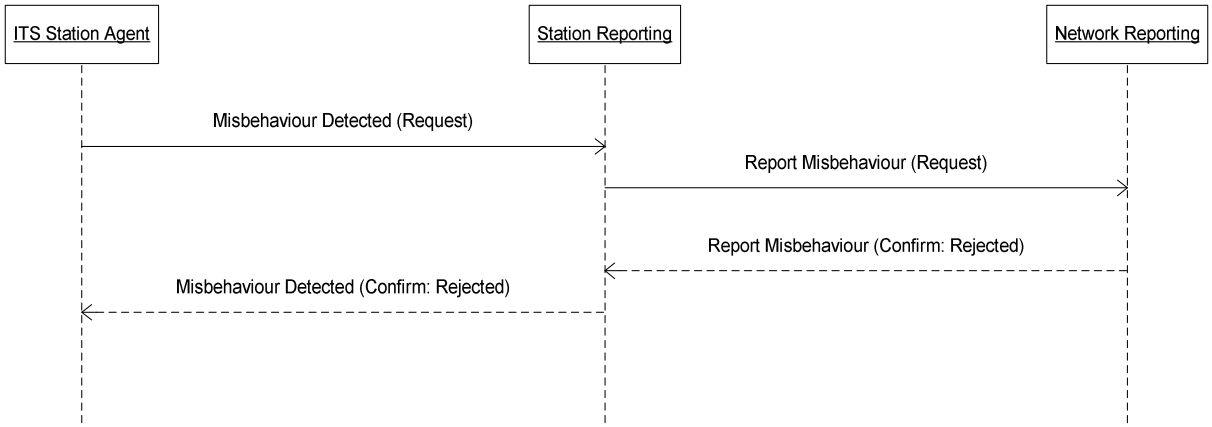


Figure 37: Unsuccessful reporting of misbehaviour

Annex A (informative): Bibliography

IETF RFC 2828 (2000): "Internet Security Glossary".

History

Document history		
V1.1.1	September 2010	Publication