ETSI TS 102 867 V1.1.1 (2012-06)

Intelligent Transport Systems (ITS);
Security;
Stage 3 mapping for IEEE 1609.2

Reference
DTS/ITS-0050013

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://ipr.etsi.org).

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

Foreword

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

1 Scope

The present document specifies the use of the mechanisms of IEEE 1609.2 [1] within the ITS communications architecture defined in EN 302 665 [3] to provide a stage 3 implementation for a subset of the security services defined in TS 102 731 [2].

The present document identifies:

- Those areas where IEEE 1609.2 [1] provides a security service defined in TS 102 731 [2].
- Those areas where IEEE 1609.2 [1] needs to be extended or modified in a minor way to provide security services defined in TS 102 731 [2] and suitable for CAM and DENM.
- Those areas where IEEE 1609.2 [1] does not provide a basis for a security service defined in TS 102 731 [2] and consumed by CAM and DENM.

In those cases where IEEE 1609.2 [1] does not fully provide a required service, the present document identifies the requirements for that service but does not specify that service in full. The present document should therefore be seen not as a full specification of security for CAM and DENM but as a subset of that specification.

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.

[1] IEEE Std. 1609.2 draft D12 (January 2012): "Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages".

NOTE: Available from http://ieeexplore.ieee.org/xpl/mostRecentIssue.jsp?reload=true&punumber=6140528.

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

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

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 TS 102 636-3: "Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 3: Network architecture".

[i.3] Wassenaar agreement: "Lists of Dual Use Goods and Technologies and Munitions List; Category 5; Part 2".

NOTE: Available from http://www.wassenaar.org.

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in IEEE 1609.2 [1], TS 102 731 [2] and TS 102 636-3 [i.2] apply.

3.2 Abbreviations

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

BSM	Basic Safety Message
CA	Certificate Authority
CAM	Cooperative Awareness Message
CME	Connection Management Entity
CRL	Certificate Revocation List
CSR	Certificate Signing Request
DENM	Decentralized Environmental Notification Message
ITS-AID	Intelligent Transport Systems - Application Identifier
ITS-S	ITS Station
MAC	Message Authentication Code
PSID	Provider Service Identifier
RSA	Rivest Shamir Adleman
Rx	Receiver
SSP	Service Specific Permissions
TVRA	Threat Vulnerability and Risk Analysis
Tx	Transmitter

4 Assessment of the ability of IEEE 1609.2 to provide the security services defined in TS 102 731

4.1 Summary

Table 1 summarizes the capabilities of IEEE 1609.2 [1] in relation to the stage 2 ITS security services [2]. The level of support in IEEE 1609.2 [1] for each ITS security service is identified using a traffic light key where green indicates full explicit support, amber indicates partial support, and red indicates no support.

Table 1: Identification of stage 2 services covered by IEEE 1609.2 [1] at stage 3

Security Service Group	Stage 2 service		Stage 3 mapping definition (IEEE 1609.2 [1])
	Security Service at Tx	Security service at Rx	
Enrolment	Obtain Enrolment Credentials		Supported through Certificate Signing Request certificates
		Remove Enrolment Credentials	Supported through Certificate Signing Request certificates
	Update Enrolment Credentials		Supported through Certificate Signing Request certificates
Authorisation	Obtain Authorization Ticket		Supported through Certificate Signing Request Certificates
	Update Authorization Ticket		Supported through Certificate Signing Request Certificates
	Publish Authorization Status		Supported through Certificate Revocation Lists
	Update Local Authorization Status Repository		Supported through Certificate Revocation Lists and CRL Requests
	Add authorisation credential to single message		Supported through Signed Messages
		Validate authorisation credential of received message	Supported through processing of incoming signed messages
Security Association management	Establish Security Association	Establish Security Association	Not supported (note 1)
	Remove Security Association	Remove Security Association	Not supported (note 1)
	Update Security Association	Update Security Association	Not supported (note 1)
Authentication services	Authenticate ITS user	Authenticate ITS user	Supported for single messages through signed messages. No concept of authenticating a user for prolonged communications
	Authenticate ITS network	Authenticate ITS network	Supported for single messages through signed messages. No concept of authenticating the network for prolonged communications
Confidentiality services	Encrypt single outgoing message		Supported through encrypted messages
		Decrypt single incoming message	Supported through encrypted messages
	Send secured message using Security Association		Not supported (note 1)
		Receive secured message using Security Association	Not supported (note 1)
Integrity services	Insert check value		Supported through signed messages. No concept of providing a check value within a prolonged communications session.
		Validate check value	Supported through signed messages. No concept of providing a check value within a prolonged communications session.

Security Service Group	Stage 2 service		Stage 3 mapping definition (IEEE 1609.2 [1])
	Security Service at Tx	Security service at Rx	
	Calculate check value		Supported through signed messages. No concept of providing a check value within a prolonged communications session.
Replay Protection services	Timestamp message		Supported
		Validate timestamp	Supported
	Insert sequence number		Not supported
		Validate sequence number	Not supported
	Insert challenge		Not supported
		Use received challenge	Not supported
	Validate use of challenge		Not supported
Accountability services		Record incoming message	Not supported
	Record outgoing message		Not supported
Plausibility validation		Validate data plausibility	Basic support (note 2)
		Validate dynamic parameters	Basic support (note 2)
		Validate timestamp	Supported
		Validate sequence number	Not supported
Remote management	Activate ITS transmission		Not supported
	Deactivate ITS transmission		Not supported
Report Misbehaving ITS-S	Report Misbehaviour	Report Misbehaviour	Not supported
NOTE 1: IEEE 1609.2 [1] does not explicitly support the management of session based security associations but does support on the fly security associations by identifying the trust hierarchy and security service applied to the message in the body and content of the public key certificate.			
NOTE 2: IEEE provides basic data plausibility and dynamic parameter validation: messages may be rejected on the grounds of generation time too far in the past, expiry time in the past, generation time or expiry time in the future, or geographic location too far away, where "too far" is parameterizable. More sophisticated plausibility and parameter validation may be carried out by services outside the scope of IEEE 1609.2 [1].			

5 Stage 2 security service implementation based on IEEE 1609.2

TS 102 731 [2] models the functional entities, and the relationships between them, as well as the detail of the information flows for each of the security services identified as necessary to counter the risks identified in the ITS TVRA from TR 102 893 [i.1]. The relevant models are copied here for ease of reference. This clause details how these entities, relationships, and flows shall be implemented by an implementation based on IEEE 1609.2 [1].

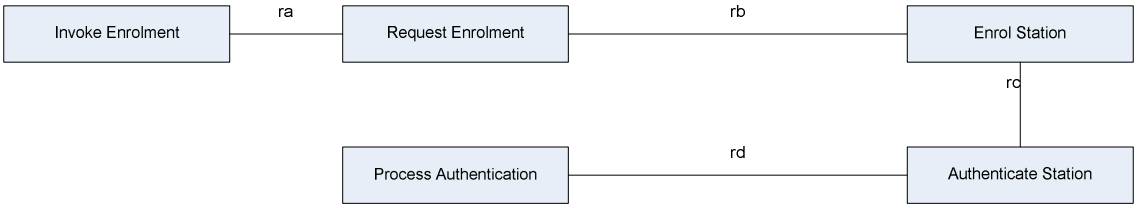

Figure 1: Functional model for the Obtain Enrolment Credentials security service

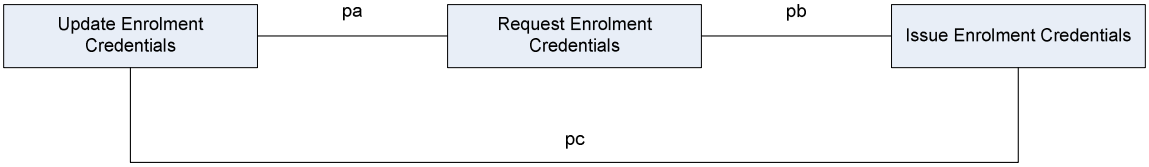

Figure 2: Functional model for the Update Enrolment Credentials security service

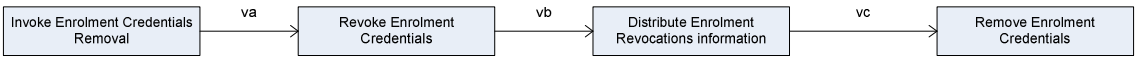

Figure 3: Functional model for the Remove Enrolment Credentials security service

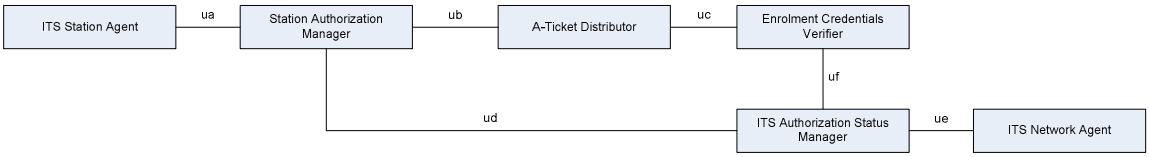

Figure 4: Functional model for the Authorization Tickets security services

5.1 Services directly mappable to IEEE 1609.2

5.1.1 Enrolment service

The Enrolment Credential in ETSI ITS shall be implemented as an IEEE 1609.2 [1] Certificate Signing Request Certificate (CSR Certificate).

5.1.1.1 Enrolment request

The information flow sequence Request Enrolment Credentials defined in TS 102 731 [2] shall be implemented as follows.

- The request flow shall be implemented as an IEEE 1609.2 ToBeEncrypted message of type certificate_request as defined in clause 6.2.27 of IEEE 1609.2 [1], with fields set as specified in table 2.
- If enrolment was successful, the confirm flow shall be implemented using a 1609Dot2Data structure of type encrypted_message, encapsulating a ToBeEncrypted message of type certificate_response as defined in clauses 6.2.1 and 6.2.7 of IEEE 1609.2 [1], with fields set as specified in table 3.
- If enrolment was unsuccessful, the confirm flow shall be implemented using a 1609Dot2Data structure of type encrypted_message, encapsulating a ToBeEncrypted message of type certificate_request_error as defined in clauses 6.2.1 and 6.2.7 of IEEE 1609.2 [1], with fields set as specified in table 4.

In each table, if there is no entry for a field in a given IEEE 1609.2 [1] structure, then that field for the purposes of the present document is identical to the IEEE 1609.2 [1] use of that field.

Table 6 explicitly maps the information elements of TS 102 731 [2] to the fields in IEEE 1609.2 [1] for clarity.

NOTE: The present document maps protocol messages described in IEEE 1609.2 [1] only to the message sequence visible at reference point rb defined in TS 102 731 [2]. The authentication exchange visible at reference point rd defined in TS 102 731 [2] is embedded in the IEEE 1609.2 [1] message exchange.

Table 2: Fields in IEEE 1609.2 [1] structures to support enrolment request

Structure	Field	Value
ToBeSignedCertificateRequest	subject_type	message_csr
	Cf	does not include encryption_key
PsidArray	Type	specified
	permissions_list	A list of the ETSI ITS-AIDs to be supported by the enrolment credentials

Table 3: Fields in IEEE 1609.2 [1] structures to support confirmation of successful enrolment request

Structure	Field	Value
The ToBeSignedCertificate in the last Certificate in the certificate chain	subject_type	message_csr
	cf	does not include encryption_key

Table 4: Fields in IEEE 1609.2 [1] structures to support confirmation of unsuccessful enrolment request

Structure	Field	Value
ToBeEncryptedCertificateRequestError	reason	Depends on reason for rejection: - Canonical Identity unknown = canonical_identity_unknown - User not permitted to enrol = request_denied - User authentication failed = verification_failure

Table 5: Parameters to the WaveCertificateRequest-RequestCertificate.request primitive to support enrolment request

Name	Value
RequestIndex	Locally determined. Shall not be the same as the RequestIndex provided to an outstanding certificate request from the same higher layer
CertificateType	Message CSR
Permissions	An array of the appropriate ITS-AIDs
Identifier	A canonical identity determined according to the rules to be specified by ETSI
GeographicRegion	An identifier for the requested area of validity of the enrolment credentials, of the format specified in IEEE 1609.2 [1] or otherwise by ETSI
Lifetime	Lifetime determined according to the rules to be specified in ETSI

Table 6: Contents of the Enrolment Request information flow

Service elements	Allowed values	IEEE 1609.2 [1] Equivalent	Request	Confirm
Canonical identity	Character string: Permanent identifier	The name field, to be set according to the rules to be specified in ETSI.	M	M
ITS-S Key	Public or symmetric key identifier	public_key field in ToBeSignedCertificateRequest	M	
Network identifier	Character string	Root CA certificate, identified by SignerID		M
Network challenge	Randomly generated character string	Challenge role fulfilled by request_time in ToBeSignedCertificateRequest	M	
Registration result	- Accepted - Rejected	Implicit: either certificate or encrypted ToBeEncryptedCertificateRequestError is returned		M
List of enrolment credentials	Temporary identities	Certificate		O (note 1)
Cause of rejection	- Canonical identity unknown - User not permitted to enrol - User authentication failed	ToBeEncryptedCertificateRequestError: - Canonical Identity unknown = canonical_identity_unknown - User not permitted to enrol = request_denied - User authentication failed = verification_failure		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".				

5.1.1.2 Update Enrolment Credentials

The information flow sequence Update Enrolment Credentials defined in TS 102 731 [2] shall be implemented as follows.

- The request flow shall be implemented using a 1609Dot2Data of type encrypted_message, encapsulating a ToBeEncrypted message of type certificate_request as defined in clauses 6.2.1 and 6.2.27 of IEEE 1609.2 [1], with fields set as specified in table 7.
- If enrolment was successful, the confirm flow shall be implemented using a 1609Dot2Data of type encrypted_message, encapsulating a ToBeEncrypted message of type certificate_response as defined in clauses 6.2.1 and 6.2.27 of IEEE 1609.2 [1], with fields set as specified in table 8.
- If enrolment was unsuccessful, the confirm flow shall be implemented using a 1609Dot2Data of type encrypted_message, encapsulating a ToBeEncrypted message of type certificate_request_error as defined in clauses 6.2.1 and 6.2.7 of IEEE 1609.2 [1], with fields set as specified in table 9.

In each table, if there is no entry for a field in a given IEEE 1609.2 [1] structure, then that field is identical for the purposes of the present document to the IEEE 1609.2 [1] use of that field.

NOTE: The present document maps protocol messages described in IEEE 1609.2 [1] only to the message sequence visible at reference point pa defined in TS 102 731 [2].

Table 7: Fields in IEEE 1609.2 [1] structures to support enrolment update

Structure	Field	Value
ToBeSignedCertificateRequest	subject_type	message_csr
	cf	does not include encryption_key
PsidArray	type	Specified
	permissions_list	A list of the ETSI ITS-AIDs to be supported by the enrolment credentials

Table 8: Fields in IEEE 1609.2 [1] structures to support confirmation of successful enrolment update

Structure	Field	Value
The ToBeSignedCertificate in the last Certificate in the certificate chain	subject_type	message_csr
	cf	does not include encryption_key

Table 9: Fields in IEEE 1609.2 [1] structures to support confirmation of unsuccessful enrolment update

Structure	Field	Value
ToBeEncryptedCertificateRequestError	reason	Depends on reason for rejection: - Canonical Identity unknown = canonical_identity_unknown - User not permitted to enrol = request_denied - User authentication failed = verification_failure

Table 10: Contents of the Update Enrolment Credentials information flow

Service elements	Allowed values	IEEE 1609.2 [1] equivalent	Request	Confirm
Canonical identity	Character string: Permanent identifier	The name field, to be set according to the rules to be specified in ETSI.	M	
ITS-S Key	Public or symmetric key	public_key field in ToBeSignedCertificateRequest	M	
Update request result	- Accepted - Rejected	Implicit: either certificate or encrypted ToBeEncryptedCertificateRequestError is returned		M
List of enrolment credentials	Temporary identities	Certificate		O (note 1)
Cause of rejection	- Canonical identity unknown - User not permitted to request enrolment credentials - Failed to create enrolment credentials	ToBeEncryptedCertificateRequestError - Canonical Identity unknown = canonical_identity_unknown - User not permitted to request enrolment credentials = request_denied, csr_cert_unauthorized, csr_cert_expired, csr_cert_revoked, csr_cert_unknown - User authentication failed = verification_failure		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".				

5.1.1.3 Remove Enrolment Credentials

The information flow sequence Remove Enrolment Credentials defined in TS 102 731 [2] shall be implemented as follows.

- The request flow shall be implemented using a 1609Dot2Data of type encrypted_message, encapsulating a ToBeEncrypted message of type certificate_request_error as defined in clauses 6.2.1 and 6.2.27 of IEEE 1609.2 [1], with fields set as specified in table 3. This shall be sent in response to an enrolment request, or enrolment update request, authorization request, or authorization update request.

NOTE 1: IEEE 1609.2 [1] does not provide a mechanism for the Enrolment Authority to pre-emptively contact a unit whose enrolment credentials have been removed.

- The confirm flow shall be implemented using a 1609Dot2Data of type encrypted_message, encapsulating a ToBeEncrypted message of type certificate_response_acknowledgement as defined in clauses 6.2.1 and 6.2.27 of IEEE 1609.2 [1].

In each table, if there is no entry for a field in a given IEEE 1609.2 [1] structure, then the use of that field for the purposes of the present document is identical to the IEEE 1609.2 [1] use of that field.

Table 6 explicitly maps the information elements of TS 102 731 [2] to the fields in IEEE 1609.2 [1] for clarity.

NOTE 2: The present document maps protocol messages described in IEEE 1609.2 [1] only to the message sequence visible at reference point vb defined in TS 102 731 [2].

Table 11: Fields in IEEE 1609.2 [1] structures to support remove enrolment credentials request

Structure	Field	Value		
ToBeEncryptedCertificateRequestError	reason	csr_cert_expired or csr_cert_revoked		

Table 12: Contents of the Remove Enrolment Credentials information flow

Service elements	Allowed values	IEEE 1609.2 [1] Equivalent	Request	Confirm
Enrolment credential	Temporary identity previously allocated by the ITS infrastructure	Signature on response	M	
Enrolment credential removal request	Removal request field	Implicit from receipt of certificate request error	M	
Removal request result	Accepted Rejected	"accepted" if ACK is received, "rejected" if not		M
Cause of rejection	- Enrolment credential unknown - Removal failed - Distribution failed	Not supported		O

5.1.2 Authorization Service

The Authorization Ticket in ETSI ITS shall be implemented as an IEEE 1609.2 [1] messaging certificate.

5.1.2.1 Request Authorization

The information flow sequence Request Authorization defined in TS 102 731 [2] shall be implemented as follows.

- The request flow shall be implemented using a 1609Dot2Data of type encrypted_message, encapsulating a ToBeEncrypted message of type certificate_request as defined in clauses 6.2.1 and 6.2.27 of IEEE 1609.2 [1], with fields set as specified in table 13.
- If enrolment was successful, the confirm flow shall be implemented using a 1609Dot2Data of type encrypted_message, encapsulating a ToBeEncrypted message of type certificate_response as defined in clauses 6.2.1 and 6.2.27 of IEEE 1609.2 [1], with fields set as specified in table 14.
- If enrolment was unsuccessful, the confirm flow shall be implemented using a 1609Dot2Data of type encrypted_message, encapsulating a ToBeEncrypted message of type certificate_request_error as defined in clauses 6.2.1 and 6.2.27 of IEEE 1609.2 [1], with fields set as specified in table 15.

In each table, if there is no entry for a field in a given IEEE 1609.2 [1] structure, then the use of that field for the purposes of the present document is identical to the IEEE 1609.2 [1] use of that field.

Table 17 explicitly maps the information elements of TS 102 731 [2] to the fields in IEEE 1609.2 [1] for clarity.

NOTE: The present document maps protocol messages described in IEEE 1609.2 [1] only to the message sequence visible at reference point ub defined in TS 102 731 [2]. The authentication exchange visible at reference point ud defined in TS 102 731 [2] is embedded in the IEEE 1609.2 [1] message exchange.

Table 13: Fields in IEEE 1609.2 [1] structures to support authorization request

Structure	Field	Value
ToBeSignedCertificateRequest	subject_type	message_identified_localized, message_identified_not_localized, or message_anonymous
	cf	does not include encryption_key
IdentifiedScope, IdentifiedNotLocalizedScope	subject_name	An identity string set according to the rules to be specified by ETSI
AnonymousScope	additional_data	A string determined according to the rules to be specified by ETSI. May be blank if ETSI so specifies
AnonymousScope, IdentifiedScope	region	An identifier for the requested area of validity of the enrolment credentials, of the format specified in IEEE 1609.2 [1] or otherwise by ETSI
PsidSspArray	type	specified
	permissions_list	A list of the ETSI ITS-AIDs to be supported by the enrolment credentials, and the associated SSPs to be specified by ETSI

Table 14: Fields in IEEE 1609.2 [1] structures to support confirmation of successful authorization request

Structure	Field	Value
The ToBeSignedCertificate in the last Certificate in the certificate chain	subject_type	message_identified_localized, message_identified_not_localized, or message_anonymous, as requested in the request
	cf	does not include encryption_key
IdentifiedScope, IdentifiedNotLocalizedScope	subject_name	An identity string set according to the rules to be specified by ETSI.
AnonymousScope	additional_data	A string determined according to the rules to be specified by ETSI
AnonymousScope, IdentifiedScope	region	An identifier for the requested area of validity of the enrolment credentials, of the format specified in IEEE 1609.2 [1] or otherwise by ETSI
PsidSspArray	type	specified
	permissions_list	A list of the ETSI ITS-AIDs to be supported by the enrolment credentials, and the associated SSPs to be specified by ETSI

Table 15: Fields in IEEE 1609.2 [1] structures to support confirmation of unsuccessful enrolment request

Structure	Field	Value
ToBeEncryptedCertificateRequest-Error	reason	Depends on reason for rejection: - Enrolment credentials unknown = csr_cert_unkown - A-Tickets request disabled = request_denied - No permission to use ITS application = csr_cert_unauthorized - Authorization request failed = verification_failure

Table 16: Parameters to the WaveCertificateRequest-RequestCertificate.request primitive to support authorization request

Name	Value
RequestIndex	Locally determined. Shall not be the same as the RequestIndex provided to an outstanding certificate request from the same higher layer
CertificateType	message_identified_localized, message_identified_not_localized, or message_anonymous
Permissions	An array of the appropriate ITS-AIDs and SSPs, determined according to rules to be specified by ETSI.
Identifier	A canonical identity determined according to the rules to be specified by ETSI
GeographicRegion	An identifier for the requested area of validity of the enrolment credentials, of the format specified in IEEE 1609.2 [1] or otherwise by ETSI
Lifetime	Lifetime determined according to the rules to be specified by ETSI

Table 17: Contents of the Request Authorization information element

Service elements	Allowed values	IEEE 1609.2 [1] Equivalent	Request	Confirm
Enrolment Credentials	Temporary identity previously allocated by the ITS infrastructure	CSR certificate used to sign certificate request	M	
A-Tickets Request	List of ITS applications for which authorization is requested	permissions field within scope in CertRequestSpecificData (note 3)	M	
ITS-S Key	Public or symmetric key	public_key field in ToBeSignedCertificateRequest	M	
A-Tickets Request result	Accepted Rejected	Implicit: given by whether response is a certificate or a certificate request error.		M
List of A-tickets	Temporary authorization parameters	Certificate		O (note 1)
Cause of rejection	- Enrolment credentials unknown - A-Tickets request disabled - No permission to use ITS application - Authorization request failed	Supported by CertificateRequestErrorCode		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".				

5.1.2.2 Update Authorization Ticket

A service with equivalent security properties to the information flow sequence Update Authorization defined in TS 102 731 [2] shall be implemented identically to Request Authorization, except that the ITS-S requesting an authorization ticket shall run the Authorization Request information flow with an existing ITS-S Key.

5.1.2.3 Publish Authorization Status

The Authorization Status Update Information in ETSI ITS shall be implemented as an IEEE 1609.2 [1] Certificate Revocation List (CRL).

The present document maps protocol messages described in IEEE 1609.2 [1] only to the message sequence visible at reference point ud defined in TS 102 731 [2].

There is no confirmation message.

Table 18: Fields in IEEE 1609.2 [1] structures to support publish authorization status request

Structure	Field	Value
ToBeSignedCrl	type	id_and_expiry
	expiring_entries	list of CertID8s of expired certificates

Table 19: Contents of the Authorization Status information flow

Service elements	Allowed values	IEEE 1609.2 [1] Equivalent	Request	Confirm
Authoritative Credentials	Trustworthy and Assured Identity of the Authority requesting the authorization status update	CRL signing certificate	M	
Authorization Status Update Information	List of authorization status updates	CRL	O	

5.1.2.4 Update Local Authorization Status Repository

The information flow sequence Update Local Authorization Status Repository defined in TS 102 731 [2] shall be implemented as follows.

- The request flow shall be implemented using a 1609Dot2Data of type crl_request, as defined in clause 5of IEEE 1609.2 [1].
- The confirm flow shall be implemented using a 1609Dot2Data of type crl, as defined in clause 5 of IEEE 1609.2 [1], with fields set as specified in table 20.

In each table, if there is no entry for a field in a given IEEE 1609.2 [1] structure, then the ETSI use of that field is identical to the IEEE 1609.2 [1] use of that field.

The present document maps protocol messages described in IEEE 1609.2 [1] only to the message sequence visible at reference point ud defined in TS 102 731 [2].

Table 21 explicitly maps the information elements of TS 102 731 [2] to the fields in IEEE 1609.2 [1] for clarity.

Table 20: Fields in IEEE 1609.2 [1] structures to support confirm flow of Update Repository

Structure	Field	Value
ToBeSignedCrl	type	id_and_expiry
	expiring_entries	list of CertID8s of expired certificates

Table 21: Contents of the Update Repository information element

Service elements	Allowed values	IEEE 1609.2 [1] equivalent	Request	Confirm
Authorization ticket	Temporary identity previously allocated by the ITS infrastructure	CrlRequests are not signed in IEEE 1609.2 [1]	O	
Specific Status Information	Description of needed status information	CrlRequest	M	
Repository Update Request	- Accepted - Rejected	Implicit: requests are always accepted if successfully received, so the if the requester receives the confirm message that implies "accepted".		M
Authorization Status Update Information	List of authorization status updates	Crl		O (note 1)
Cause of rejection	- Enrolment credentials unknown - Repository update disabled - Repository update failed	Not supported: Requests are always accepted if successfully received.		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".				

5.1.3 Authorize Single Message

The service Authorize Single Message shall be implemented as follows.

There shall be an IEEE 1609.2 [1] Security Profile for use by the higher layer to set the value of *SignMessages* to "true" or "adaptive". The specific security profiles for CAM and DENM are defined in clause 6 of the present document.

The sender shall create a 1609Dot2Data of type signed, signed_partial_payload, or signed_external_payload using the WaveSecurityServices-SignedMessage primitive and setting the parameters to the primitive as defined in the security profile.

5.1.4 Validate Authorization on Single Message

The service Validate Authorization on Single Message shall be implemented as follows.

There shall be an IEEE 1609.2 [1] Security Profile for use by the higher layer to set the value of *VerifyMessages* to "true" or "adaptive". The specific security profiles for CAM and DENM are defined in clause 6 of the present document.

The receiver shall process the incoming message using the WaveSecurityServices-SecuredMessageDataExtraction and WaveSecurityServices-SignedMessageValidation primitives and setting the parameters to the primitive as defined in the security profile.

5.1.5 Encrypt single outgoing message

The service Encrypt Single Outgoing Message shall be implemented as follows.

There shall be an IEEE 1609.2 [1] Security Profile for use by the higher layer to set the value of *EncryptMessages* to "always", "if possible," or "adaptive". The specific security profiles for CAM and DENM are defined in clause 6 of the present document.

The sender shall process the outgoing message using the WaveSecurityServices-EncryptedMessage primitive and setting the parameters to the primitive as defined in the security profile.

5.1.6 Decrypt single incoming message

The service Decrypt Single Incoming Message shall be implemented as follows.

There shall be an IEEE 1609.2 [1] Security Profile for use by the higher layer to set the value of *EncryptMessages* to "always", "if possible," or "adaptive". The specific security profiles for CAM and DENM are defined in clause 6 of the present document.

The receiver shall process the incoming message using the WaveSecurityServices-SecuredMessageDataExtraction primitive and setting the parameters to the primitive as defined in the security profile.

5.1.7 Calculate check value

The service Calculate check value shall be implemented as follows.

There shall be an IEEE 1609.2 [1] Security Profile for use by the higher layerto set the value of *SignMessages* to "true" or "adaptive". The specific security profiles for CAM and DENM are defined in clause 6 of the present document.

The sender shall create a 1609Dot2Data of type signed, signed_partial_payload, or signed_external_payload using the WaveSecurityServices-SignedMessage primitive and setting the parameters to the primitive as defined in the security profile.

The receiver shall process the incoming message using the WaveSecurityServices-SecuredMessageDataExtraction and WaveSecurityServices-SignedMessageValidation primitives and setting the parameters to the primitive as defined in the security profile.

5.1.8 Validate check value

The service Validate Check Value shall be implemented as follows.

There shall be an IEEE 1609.2 [1] Security Profile for use by the higher layer to set the value of *SignMessages* to "true" or "adaptive". The security profile shall set the value of *VerifyMessages* to "true" or "adaptive". The specific security profiles for CAM and DENM are defined in clause 6 of the present document.

The receiver shall process the incoming message using the WaveSecurityServices-SecuredMessageDataExtraction and WaveSecurityServices-SignedMessageValidation primitives and setting the parameters to the primitive as defined in the security profile.

5.1.9 Insert check value

The service Insert check value shall be implemented as follows.

There shall be an IEEE 1609.2 [1] Security Profile for use by the higher layer. The security profile shall set the value of *SignMessages* to "true" or "adaptive". The specific security profiles for CAM and DENM are defined in clause 6 of the present document.

The sender shall create a 1609Dot2Data of type signed, signed_partial_payload, or signed_external_payload using the WaveSecurityServices-SignedMessage primitive and setting the parameters to the primitive as defined in the security profile.

5.1.10 Replay Protection Based on Timestamp

The service Replay Protection Based on Timestamp shall be implemented as follows.

The sender shall create a 1609Dot2Data of type signed, signed_partial_payload, or signed_external_payload using the WaveSecurityServices-SignedMessage primitive and setting the parameters to the primitive as defined in the security profile.

The receiver shall process the incoming message using the WaveSecurityServices-SecuredMessageDataExtraction and WaveSecurityServices-SignedMessageValidation primitives and setting the parameters to the primitive as defined in the security profile.

There shall be an IEEE 1609.2 [1] Security Profile for use by the higher layer used to set the value of *SignMessages* to "true" or "adaptive". The security profile shall have the value of *DetectReplay* set to *true*. The specific security profiles for CAM and DENM are defined in clause 6 of the present document.

5.1.11 Validate data plausibility

The service Validate data plausibility shall be implemented as follows.

There shall be an IEEE 1609.2 [1] Security Profile for use by the higher layer to set the value of *SignMessages* to "true" or "adaptive". The specific security profiles for CAM and DENM are defined in clause 6 of the present document. The security profile shall set at least one of the following values to "TRUE":

- CheckValidityBasedOnGenerationTime;
- CheckValidityBasedOnExpiryTime; and
- CheckValidityBasedOnGenerationLocation.

The following values shall be set appropriately to the calling application:

- MessageValidityPeriod;
- MessageValidityDistance;
- GenerationTimeConfidenceMultiplier; and
- GenerationLocationHorizontalConfidenceMultiplier.

The sender shall create a 1609Dot2Data of type signed, signed_partial_payload, or signed_external_payload using the WaveSecurityServices-SignedMessage primitive and setting the parameters to the primitive as defined in the security profile.

The receiver shall process the incoming message using the WaveSecurityServices-SecuredMessageDataExtraction and WaveSecurityServices-SignedMessageValidation primitives and setting the parameters to the primitive as defined in the security profile.

5.2 Security services defined in TS 102 731 not directly mappable to IEEE 1609.2

5.2.1 Security Associations

IEEE 1609.2 [1] does not provide services that map to the stage 2 services Establish Security Association, Update Security Association, Send Secured Message, Receive Secured Message, and Remove Security Association.

5.2.2 Replay Protection Based on Sequence Number

IEEE 1609.2 [1] messages are stateless and do not include a sequence number. A higher layer may provide services for replay protection based on sequence number. This higher layer may make use of the communications security services of IEEE 1609.2 [1].

5.2.3 Accountability services

Accountability services are provided at a higher layer than is addressed by IEEE 1609.2 [1]. This higher layer may make use of the communications security services of IEEE 1609.2 [1].

5.2.4 Activate / deactivate ITS transmission

The activate / deactivate ITS transmission service is a security service provided at a higher layer than is addressed by IEEE 1609.2 [1]. This higher layer may make use of the communications security services of IEEE 1609.2 [1].

5.2.5 Report Misbehaving ITS-S

Report Misbehaving ITS-S services are provided at a higher layer than is addressed by IEEE 1609.2 [1]. This higher layer may make use of the communications security services of IEEE 1609.2 [1].

6 Mapping of IEEE 1609.2 to ETSI CAM/DENM

NOTE: The use of IEEE 1609.2 [1] described for CAM/DENM in this clause makes no assumptions about the networking facility used.

6.1 Location of services within the stack

For CAM, and DENM the originator shall sign outgoing messages using IEEE 1609.2 [1] at the facilities layer in the stack. The CAM or DENM content shall form the payload of the *ToBeSignedData* element of the *SignedData* structure defined in clauses 6.2.7 and 6.2.3 of IEEE 1609.2 [1] respectively.

6.2 Security profiles

6.2.1 Overview

These security profiles are based on the template given in IEEE 1609.2 [1], annex B and use the terminology defined in that annex and elsewhere in IEEE 1609.2 [1].

6.2.2 Security Profile for CAM

This Security Profile is based on the security profile for the SAE J2735 BSM given in Annex C of IEEE 1609.2 [1].

6.2.2.1 General

Use1609Dot2 - true.

6.2.2.2 Secure messaging (sending)

Table 22

Field	Value	Notes
SignData	True	
SetGenerationTimeInSecurityHeaders	False	Use the generationTime field in the message
SetExpiryTimeInSecurityHeaders	False	CAM messages are transient and expire automatically
SetGenerationLocationInSecurity-Headers	False	The CAM message itself contains the generation location
TimeBetweenFullCertChain-Transmissions	Adaptive	Choice of how often to send a full certificate chain is a reliability issue rather than a security issue. A recipient cannot trust a sender's message until they have the full certificate chain. However, if all senders send the full certificate chain with every message, the resulting increase in overhead may cause congestion that results in a lower probability of a message being successfully received. This is a particularly important consideration for senders of CAM messages as CAM messages are sent frequently. See annex B for a discussion of the overhead due to IEEE 1609.2 [1] security mechanisms.
SignerIdentifierTypeIfNotFullCertChain	certificate digest	
SignerIdentifierCertChainLength	-1 if used	Full certificate chain, up to but not including the root
EncryptData	No	

6.2.2.3 Secure messaging (receiving)

Table 23

Field	Value	Notes
Verifydata	Adaptive	A receiver may verify messages when appropriate and needed
Check Validity Based on Generation Time	False	Not needed due to generationTime field in CAM message
GenerationTimeSource	n/a	
Check Validity Based on Expiry Time	False	Generation time is enough for the receiving ITS-S to judge relevance
ExpiryTimeSource	n/a	Expiry time is not used
Check Validity Based on Generation Location	False	Generation location is in message and location relevance check is carried out by receiving entity
Generation Location Source	n/a	
AcceptEncryptedData	False	
DetectReplay	False	A replayed message is simply a repeat of information, not an attack
DataValidityPeriod	n/a	
DataValidityDistance	n/a	
GenerationTimeConfidence Multiplier	n/a	
OverdueCRLTolerance	No	

6.2.2.4 Security management

Table 24

Field	Value	Notes
SigningKeyAlgorithm	ECDSA-224	
EncryptionAlgorithm	n/a	No encryption is applied

6.2.3 Security Profile for DENM without Geonetworking

This Security Profile is based on the security profile for the SAE J2735 BSM given in IEEE 1609.2 [1].

6.2.3.1 General

Use1609Dot2 - true.

6.2.3.2 Secure messaging (sending)

Table 25

Field	Value	Notes
Signdata	True	
SetGenerationTimeInSecurityHeaders	False	Generation time is not needed
SetExpiryTimeInSecurityHeaders	False	Expiry time is contained in data payload
SetGenerationLocationInSecurityHeaders	False	Generation location is not needed for security purposes
TimeBetweenFullCertChainTransmissions	Adaptive	Choice of how often to send a full certificate chain is a reliability issue rather than a security issue. A recipient cannot trust a sender's message until they have the full certificate chain. However, if all senders send the full certificate chain with every message, the resulting increase in overhead may cause congestion that results in a lower probability of a message being successfully received. This is an important consideration for senders of repeated DENM. DENM that are sent only once shall always include the certificate chain. See annex B for a discussion of the overhead due to IEEE 1609.2 [1] security mechanisms.
SignerIdentifierTypeIfNotFullCertChain	certificate digest	
SignerIdentifierCertChainLength	-1 if used	
EncryptData	No	

6.2.3.3 Secure messaging (receiving)

Table 26

Field	Value	Notes
VerifyData	Adaptive	A receiver may verify messages when appropriate and needed
Check Validity Based on Generation Time	False	
GenerationTimeSource	n/a	Generation time is not used
Check Validity Based on Expiry Time	True	
ExpiryTimeSource	True	
Check Validity Based on Generation Location	False	Generation location is not used for security purposes
Generation Location Source	n/a	
AcceptEncryptedData	False	
DetectReplay	False	DENM payloads may repeat without this being a replay attack
DataValidityPeriod	n/a	Expiry time is not set in security headers
DataValidityDistance	n/a	Generation location is not used for security purposes
GenerationTimeConfidenceMultiplier	n/a	Generation time is not used for security purposes
Overdue CRL Tolerance	Adaptive	No minimum requirement

6.2.3.4 Security management

Table 27

Field	Value	Notes
SigningKeyAlgorithm	ECDSA-224	
EncryptionAlgorithm	n/a	No encryption

Annex A (informative): Cryptographic considerations

NOTE: Cryptographic technology is considered as a dual use technology, i.e. one that serves both military and civil purposes. Such technologies are sensitive and subject to controls in their application, their design, and their deployment, this annex summarises some of the areas to be considered in application of cryptography in ITS.

A.1 Export control

IEEE 1609.2 [1] uses elliptic curve cryptography that is subject to export control as defined in the Wassenaar agreement [i.3] when used for any function other than authentication or digital signature. Specifically restrictions on export can expect to be applied to any system using an "asymmetric algorithm" where the security of the algorithm is based on any of the following:

1) factorisation of integers in excess of 512 bits (e.g. RSA);

2) computation of discrete logarithms in a multiplicative group of a finite field of size greater than 512 bits (e.g. Diffie-Hellman over Z/pZ); or

3) discrete logarithms in a group other than mentioned above in excess of 112 bits (e.g. Diffie-Hellman over an elliptic curve).

The application of elliptic curve cryptographic algorithms in IEEE 1609.2 [1] for ITS is currently restricted to provision of data integrity protection and source authentication which may require export control subject to verification of export control authorities (as outlined in A.2).

NOTE: Where integrity verification mechanisms are a direct consequence of signature or authentication (e.g. using a Message Authentication Code (MAC)) this is assumed to be an integral part of the signature or authentication operation and not an additional function.

A.2 Signatories to the Wassenaar Arrangement

The Participating States of the Wassenaar Arrangement noted as of December 2010 are: Argentina, Australia, Austria, Belgium, Bulgaria, Canada, Croatia, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Japan, Latvia, Lithuania, Luxembourg, Malta, Netherlands, New Zealand, Norway, Poland, Portugal, Republic of Korea, Romania, Russian Federation, Slovakia, Slovenia, South Africa, Spain, Sweden, Switzerland, Turkey, Ukraine, United Kingdom and United States.

The signatories aim includes joint recognition of export control decisions and may also apply to decisions relating to export to countries that are not signatories to the agreement.

Annex B (informative): Overhead due to IEEE 1609.2 security processing

The described security mechanisms increase channel and computational resources requirements. The security overhead is described in table B.1.

Table B.1: IEEE 1609.2 [1] Overhead

IEEE 1609.2 [1] Signed Message overhead with no generation time, generation location, or expiry time, excluding overhead due to certificate	63 bytes (protocol_version (1) + type (1) + flags(1) + data length (4) + signature (56))
Overhead due to certificate digest	8 bytes
Field for sender's certificate	around 120 bytes
Field for each additional certificate in the sender's certificate chain	around 120 bytes
TOTAL Channel Overhead	If signer identifier type is certificate digest, around 80 bytes If signer identifier type is certificate or certificate chain: ~180 bytes for sender's certificate only ~300 bytes for sender + 1 CA certificate ~420 bytes for sender + 2 CA certificates …
TOTAL Computational Overhead (Note 1)	Original Sender: one ECDSA signature Final Receiver: If verification is performed, one ECDSA verification over payload + one ECDSA verification for every certificate in the chain that has not already been verified (note 2)
NOTE 1: Computational overhead will depend on the power and the cryptographic capabilities of the platform and may be significant or negligible. NOTE 2: A certificate is verified at or before the first time a message signed with that certificate is verified. Assuming that all messages are verified, ITS-S A's certificate will be verified by ITS-S B: (a) the first time a message from ITS-S A is received by ITS-S B; (b) if ITS-S A uses pseudonyms, any time ITS-S A changes to a different pseudonym. Assuming all encounters are at relative speeds of 240 km/h, and a radio range of 300 m, approximately one CAM message in every 45 (assuming 10 CAMs per second) will meet criterion (a); these messages will require two or more cryptographic verifications, while other messages will require a single cryptographic verification. In a more realistic model, the number of messages requiring two or more verifications will be less than one in 45. Likewise, if an ITS-S changes pseudonym every 5 minutes, then one message in 3 000 will meet criterion (b) and require an additional verification.	

History

Document history		
V1.1.1	June 2012	Publication