Department of Transport and Main Roads

PROJECT DOCUMENT
REFERENCE ONLY

Project Specific Technical Specification

Transport and Main Roads
PSTS008 SCMS Certificate Profile

July 2019

Queensland
Government

Document control sheet

Contact for enquiries and proposed changes

If you have any questions regarding this document or if you have a suggestion for improvements, please contact:

Contact officer	Stuart Allen-Keeling
Title	Principal Advisor (Cooperative & Automated Vehicles) - Security
Phone	+61 7 3066 8203

Version history

Version	Date	Nature of change	Author	Reviewer
0.99	16/05/2018	Initial Draft	David Rowe (TCA)	Ed Yoon (ISS)
1.0	16/05/2018	Removed padding from SSP	Stuart Allen-Keeling (QLD TMR)	Ed Yoon (ISS)
1.01	18/05/2018	made rollover scheme consistent with requirements – moved from draft standard to published standard (1.3.1)	Stuart Allen-Keeling (QLD TMR)	Ed Yoon (ISS)
1.02	31/05/2018	added ability for C-ITS-S to send MAP	Stuart Allen-Keeling (QLD TMR)	Ed Yoon (ISS)
1.03	06/06/2018	added CTL AID	Stuart Allen-Keeling (QLD TMR)	-not reviewed/published-added to next version
1.04	14/6/2018	Pure ETSI complaint review. Removed Linkage Values as a revocation option. Removed additional error codes from SCMS (wait values).	Stuart Allen-Keeling (QLD TMR)	Ed Yoon (ISS)
1.1	17/7/2019	Permissions expanded to reflect a potential for wider C-ITS deployment. Reduced EC 6 to 3 years in line with Europe. Changed RCA CRL ITS-AID to match Europe. Remove TLM related permissions from the Root and replace with a standalone TLM profile.	Stuart Allen-Keeling (QLD TMR)	Ed Yoon (ISS)

PROJECT DOCUMENT
REFERENCE ONLY

Copyright

http://creativecommons.org/licenses/by/3.0/au/

© State of Queensland (Department of Transport and Main Roads) 2018

Contents

PROJECT DOCUMENT
REFERENCE ONLY

PROJECT DOCUMENT REFERENCE ONLY

1 Introduction

The following content sets out the security certificate profile for use in the TMR project. The SCMS for TMR will follow the most up-to-date ETSI standards while also considering the Australian context, pilot environment and its objectives.

The key standards for security certificates for reference are:

ETSI TS 103 097 v.1.3.1 (2017-10)

ETSI TS 102 941 v1.3.1 (2018-05)

Unless specified otherwise, the certificate profile is identical to the ETSI standards. The following sections outline the parameter settings and any differences to ETSI standards to be implemented.

The following sections are included for reference:

1. Artefact summary and certificate rollover – the implementation of ETSI security certificates.
2. Certificate Profile
3. ITS-AID and SSPs – the listing of permissions applied to ITS-S

In place of requirements set by a Policy Authority, a security attestation stating a provider's security implementation may be a prerequisite to being granted access to the SCMS environment.

2 Definition of terms

Table 2.1 – Acronyms

Acronym	Term
AA	Authorisation Authority (an SCMS component)
ASN.1	Abstract Syntax Notation One
AT	Authorisation tickets
C2CCC	Car to Car Communication Consortium
*****CA**	Certificate Authorities
CAM	Cooperative awareness message (EU)
CAVI	Cooperative and Automated Vehicle Initiative
CEN	European committee for standardization
C-ITS	Cooperative intelligent transport systems
C-ITS-S	Central ITS station
*****CPOC**	C-ITS Point of Contact
*****CRL**	Certificate Revocation List
CTL	Certificate Trust List
*****DE**	ServiceProviderID: Octet 1-3 are a combination of country code (10 bits) and provider ID (14 bit) {DE Provider from CEN ISO/TS 19321:2015}. This should be a registered value, but a placeholder will be used in the TMR pilot as follows:
DENM	Decentralised environmental notification message (EU)
DSRC	Dedicated short range communications
EA	Enrolment Authority (an SCMS component)
EC	Enrolment Certificate
ETSI	European Telecommunications Standards Institute
ETSI TR	European Telecommunications Standards Institute Technical Report
ETSI TS	European Telecommunications Standards Institute Technical Standard
IEEE	Institute of Electrical and Electronic Engineers
ISO	International Organization for Standardization
ISO/TS	International Organization for Standardization Technical Standard

Acronym	Term
ITA	International Telegraph Alphabet
*****ITIS**	Permits the use of ISO 14823:2017 and general containers. Excludes ITIS and Vienna codes.
ITS	Intelligent transport systems
ITS-AID	ITS Application object Identifier
ITS-S	ITS station
IVI	In-vehicle Information
IVIM	In-vehicle Information Messages
MAP	Cooperative ITS message, broadcasting geography/topology of intersection
MAPEM	MapData extended Message
*****MSB**	Most Significant Bit
PSID	Physical Security ID
PSTS	Project Specific Technical Specification
RCA	Root Certificate Authority (an SCMS component)
R-ITS-S	Roadside ITS station
*****RLT**	Road and Lane Topology
SCMS	Security credential management system
SPaT	Signal phase and timing (cooperative message)
SPATEM	Signal Phase and Timing Extended Message
SSP	Security Service Provider
TLM	Trust List Manager
TMR	Queensland Department of Transport and Main Roads
V-ITS-S	Vehicle ITS station

PROJECT DOCUMENT
REFERENCE ONLY

Table 2.2 – Definitions

Term	Term Description
Certificate	The public part of an asymetric cryptrographic key pair defined under 1609.2
C-ITS-F	Back-end C-ITS Facility including C-ITS-S (router and SCMS certificate addition), Maintenance tool, spatial service, integration and messaging engine, data capture system and logging service, and monitoring system
DSRC	Dedicated short range communications = 5.9Ghz (approx. 300m range) US terminology.
ITS-AID	ITS Application object Identifier. An ITS application object is a generic term for either ITS application class, or ITS application, or ITS message set. Identifiers are unique and assigned by an ITS registration authority.
ITS-S	ITS station - includes C-ITS-S, R-ITS-S and V-ITS-S
Message	Message (image, audio and metadata) for presentation via the HMI

3 Reference documents

Table 3.1 – Referenced documents – External

Document ID	Document Name / Description
ISO 14823 (2017-05)	Intelligent transport systems -- Graphic data dictionary
ISO/TS 19321:2015	Intelligent transport systems - Cooperative ITS - Dictionary of in-vehicle information (IVI) data structures
ETSI TS 102 941 V1.2.1(2018-05)	Intelligent Transport Systems (ITS); Security; Trust and Privacy Management
ETSI TS 103 097 V1.3.1 (2017-10)	Intelligent Transport Systems (ITS); Security; Security Header and Certificate Formats
ETSI TR 103 415 V1.1.1 (2018-04)	Intelligent Transport Systems (ITS); Security; Pre-Standardization study on pseudonym change management
IEEE 1609.2:2016	Wireless Access in Vehicular Environments--Security Services for Applications and Management Messages

PROJECT DOCUMENT
REFERENCE ONLY

4 Artefact summary and certificate rollover

This section lists the profile to be implemented as the initial / baseline TMR security certificate profile. This follows the referenced ETSI standards except where stated.

4.1 Specification of certificate format

The certificate format for TMR is defined as per ETSI TS 103 097 v1.3.1. Particular parameters are defined as follows:

toBeSigned

region -- where used: *identifiedRegion* will be used and set to *CountryOnly* (Uint16) populating '36' corresponding to Australia

assuranceLevel -- optional in profile, but not used – set to zero

4.2 Trust and privacy management

4.2.1 General

Specific characteristics of certificate requests, responses and characteristics are listed below:

- The canonical identifier of the ITS-S will be assigned by the client device
- An enrolment request includes the profile information of the ITS-S as one of: vehicle (V-ITS-S); Roadside (R-ITS-S) and Central (C-ITS-S) stations.

4.2.2 Certificate validity and rotation

EC will be issued to be valid for the duration of the TMR project. Reissuing of EC is not anticipated.

Each V-ITS-S will be initialised with 720 ATs. These ATs will be divided onto 'AT pools' of 60 with the ATs in each AT pool being valid for **one-week-and-one-hour,** 12 weeks in total. This allows some overlap of AT validity when managing 'top ups' of ATs.

The following rotation principles are based on ETSI TR 103 415 (C2C-CC). The following requirements are to be followed for V-ITS-S:

- AT validity period – 1 week plus 1 hour (overlap)
- 60 parallel ATs (may have up to 120 during overlap period)
- Maximum of 720 ATs loaded at one time
- Change at station start-up
- Identity change after a random time period between 10 to 30 minutes
- Valid AT reuse – allowed (no limit)
- ATs will be selected randomly from the pool of 60, however, may not include the current AT
- Lock AT for 15 minutes after sending safety critical message (e.g. DENM)
- EC validity - 3 years (EC rollover outside of scope)

And for R-ITS-S:

- No requirement for anonymity
- 1 parallel ATs (may have up to 2 during overlap)
- Maximum of 12 ATs loaded at one time
- No identity change required – new AT only
- No lockout required
- AT follows validity period of V-ITS-S ATs
- EC validity - 3 years (EC rollover outside of scope)

C-ITS-S is not required to renew or rotate either EC or AT.

- No requirement for anonymity
- No lockout required
- AT and EC validity set to 3 years.

Where not specifically defined above, the following validity periods shall be used:

Entity	**Max. Private Key Usage period**	**Maximum Validity time**
Root-CA	3y	8y
EA	2y	5y
AA	4y	5y
EC	3y	3y
TLM	3y	4y

y = years

PROJECT DOCUMENT REFERENCE ONLY

4.2.3 CTL

The Australian CTL (ACTL) containing the list of trusted Root Certificate Authorities (RCAs) is published by the Trust List Manager (TLM) as per ETSI TS 102 941.

The CTL of Root-subordinates (i.e. published by the RCA) is managed per ETSI TS 102 941.

4.2.4 CRL

A CRL of certificate authorities can be published by the RCA.

The CRL will be implemented as per ETSI standard (i.e. *ToBeSignedCrl*).

Delta CTLs and delta CRLs are computed as per ETSI TS 102 941.

5 Certificate profile

This section contains a Certificate Profile that is designed to be used by C-ITS pilots across Australia. It is based on ETSI C-ITS standards and is therefore subject to change through agreement/consultation with all subscribers.

5.1 Over-the-air certificate requests

Top-ups of ATs will occur over-the-air using 3G/4G. This tests an important aspect of the C-ITS environment, preventing the need to vehicles to connect to a specific network or device in order to top up certificates.

6 PSID / ITS-AID and SSPs

6.1 PSID / ITS-AID allocation:

PSID / ITS-AID is a managed number space, registered as per the requirements of ISO 17419.

The number space is currently being managed in an agreement between SDOs while a registrar for C-ITS identifiers is being established. The current assignments are available on the following webpage:

http://standards.iso.org/iso/ts/17419/TS17419%20Assigned%20Numbers/TS17419_ITS-AID_AssignedNumbers.pdf

or from the IEEE Registration Authority web page here:

https://standards.ieee.org/products-services/regauth/psid/public.html

PROJECT DOCUMENT
REFERENCE ONLY

6.2 Assignments:

This part lists all the relevant PSID / ITS-AID for the SCMS. For SSP assignment, see the relevant device profile (vehicle, R-ITS-S, central-ITS-S and Certificate Authorities). The assignments are kept as liberal as possible to allow for the greatest use of the SCMS by pilots and future deployments.

6.2.1 V-X flows:

This table lists the PSID values used for V-X and C-F information flows (i.e. V-V, V-I, C-F, C-V)[1]

These are encoded in *appPermissions*:

[1] See TMR use cases for further information. C = central ITS station; F = field device (effectively, an R-ITS-S / infrastructure).

Table 6.1 – PSID Values for V-X and C-F information flows

Message(s)	PSID / ITS-AID	SSP range	Notes
CAM	36 (0x24)	Octet 0: version control Octet 1-2: SSP Octet 3-30: reserved	
DENM	37 (0x25)	Octet 0: version control Octet 1-3: SSP Octet 4-30: reserved	
SPAT (TLM)	137 (0x89)	Octet 0: version control Octet 1: SSP Octet 2-30: reserved	
MAP (RTL)	138 (0x8a)	Octet 0: version control Octet 1: SSP Octet 2-30: reserved	
IVI	139 (0x8b)	Octet 0: version control Octet 1-3: service provider ID Octet 4-5: parameter	

6.2.2 SCMS flows:

This table lists the PSID values used to communicate with and within the SCMS.

These are encoded in certIssuePermissions and appPermissions as detailed in the notes:

Table 6.2 – PSID Values for communication with and within the SCMS

Message(s)	PSID / ITS-AID	SSP range	Notes
Secured Certificate Request Service	623 (0x026f)	Octet 0: version control Octet 1: SSP	Certificate request messages
Certificate revocation list service	622 (0x026e)	Octet 0: version control	
CTL publishing	624 (0x0270)	Octet 0: version control Octet 1: SSP	
Misbehaviour reporting for common applications	38 (0x26)		Not to be issued At this stage, misbehaviour reporting is not supported in end-entity-certificates. This may be introduced at a later date.

PROJECT DOCUMENT REFERENCE ONLY

7 Device Profiles

This section provides a set of device profiles for vehicles, R-ITS-Ss and central stations for reference.

SSPs are listed following for format used in ETSI standards as below:

Reference:

0								1								2							
0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7
Octet 0								Octet 1								Octet 2 etc.							

For each octet, the most significant bit (MSB) is the leftmost bit.

7.1 V-ITS-S Profile

This section lists the ITS-AID and SSP assignment for vehicles in the TMR pilot. The ITS-AID and SSP assignments apply to both EC and AT except where otherwise noted.

PROJECT DOCUMENT
REFERENCE ONLY

7.1.1 CAM:

ITS-AID: 36 (0x24)

SSP version: 1

SSP allocation: default – no SSP

0								1								2							
0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

7.1.2 DENM:

ITS-AID: 37 (0x25)

SSP version: 1

SSP allocation: permissions for all DENM excepting:

excepting:

- Roadworks (3)
- rescueAndRecoveryWorkinProgress(15); and
- emergencyVehicleApproaching(95)

0								1								2							
0	0	0	0	0	0	0	1	1	1	0	1	1	1	1	1	1	0	1	1	1	1	1	1

3							
1	1	1	0	1	1	1	1

7.1.3 Security Management:

Note: this permission applies only to the EC

ITS-AID: 623 (0x26f)

SSP version: 1

SSP allocation: can sign enrolment request messages and authorisation request messages.

0								1							
0	0	0	0	0	0	0	1	1	1	0	0	0	0	0	0

7.2 R-ITS-S Profile

This section lists the ITS-AID and SSP assignment for roadside units in the TMR pilot. The ITS-AID and SSP assignments apply to both EC and AT except where otherwise noted.

7.2.1 CAM:

ITS-AID: 36 (0x24)

SSP version: 1

SSP allocation: CenDsrcTollingZone/ProtectedCommunicationZonesRSU

0								1								2							
0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

PROJECT DOCUMENT
REFERENCE ONLY

7.2.2 DENM:

ITS-AID: 37 (0x25)

SSP version: 1

SSP allocation: permissions for all DENM cause codes enabling C-ITS-S message to be sent solely over or rebroadcast from the R-ITS-S

0								1								2							
0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

3							
1	1	1	1	1	1	1	1

7.2.3 IVI:

ITS-AID: 139 (0x8b)

SSP version: 1

ServiceProviderID: Octet 1-3 are a combination of country code (10 bits) and provider ID (14 bit) {DE Provider from CEN ISO 19321}. This should be a registered value, but a placeholder will be used in the TMR pilot as follows:.

Country code (1100011100) + provider ID (11111111111111)

Note: Text for country code is ITA2 encoded

SSP allocation:

0								1								2							
0	0	0	0	0	0	0	1	1	1	0	0	0	1	1	1	0	0	1	1	1	1	1	1

3								4								5							
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0

7.2.4 SPAT/TLM

ITS-AID: 137 (0x89)

SSP version: 1 (ETSI TS 103 301 V1.1.1 (2016-11))

SSP allocation:

SSP	Octet	Bit
Information about Intersection state without advisory speed (see bit position 1) and Maneuver assisting information (see Bit position 4) {SPATEM.spat.intersections.IntersectionState }	1	0
General status of the traffic controller {SPATEM.spat.intersections.IntersectionState.status	1	1
Advisory speed {SPATEM.spat.intersections. IntersectionState.states.MovementState.statetime-speed.MovementEvent.speeds. AdvisorySpeed}	1	2
Public transport prioritization {SPATEM.spat.intersections. IntersectionState.regional.SEQUENCE. regExtValue. IntersectionState-aggGrpC.activePrioritizations}	1	3

Maneuver assisting information {SPATEM.spat.intersections.IntersectionState.maneuverAssistList}
and
{SPATEM.spat.intersections. IntersectionState.states.MovementState.maneuverAssistList}
	1	4

PROJECT DOCUMENT
REFERENCE ONLY

0								1							
0	0	0	0	0	0	0	1	1	1	1	1	1	0	0	0

Note: The CAVI pilot is using ETSI TS 103 301 V1.1.1 (2016-11) rather than the updated ETSI TS 103 301 V1.2.1 (2018-08).

The SSP values in these standards was compressed/reduced from 5 to 3 values with manoeuvre assist being moved from bit position 4 to bit position 2. The standard did not increment the SSP version, it kept it as ‘1’. Which means that a client has to guess which SSP version it is performing its comparison against. To maintain compatibility with v1.1.1 we propose to use the superset of the 2 standards. This should be fine as long as permissions are checked using a bitwise comparison rather than an absolute comparison.

7.2.5 MAP/RLT

ITS-AID: 138 (0x8a)

SSP version: 1

SSP allocation:

SSP	Octet	Bit
Road and lane topology controlled by a traffic light controller without speed limits (see Bit position 2) {MAPEM}	1	0
Road and lane topology not using traffic light controller (see Bit position 2) {MAPEM}	1	1
Speed limits included in the road and lane topology {MAPEM.map.intersections IntersectionGeometry.speedLimits}	1	2

PROJECT DOCUMENT
REFERENCE ONLY

0								1							
0	0	0	0	0	0	0	1	1	1	1	0	0	0	0	0

Note: Under ETSI TS 103 301 V1.1.1 (2016-11), Octet Position 1, Bit Position 1 is only allowed to be set to “0: certificate not allowed to sign”. This is believed to be a misprint.

7.2.6 Security Management:

Note: this permission applies only to the EC

ITS-AID: 623 (0x26f)

SSP version: 1

SSP allocation: can sign enrolment request messages and authorisation request messages.

0								1							
0	0	0	0	0	0	0	1	1	1	0	0	0	0	0	0

7.3 C-ITS-S Profile

This section lists the ITS-AID and SSP assignment for the central ITS-S in the TMR pilot. The ITS-AID and SSP assignments apply to both EC and AT except where otherwise noted.

7.3.1 MAP/RLT

ITS-AID: 138 (0x8a)

SSP version: 1

SSP allocation:

SSP	Octet	Bit
Road and lane topology controlled by a traffic light controller without speed limits (see Bit position 2) {MAPEM}	1	0
Road and lane topology not using traffic light controller (see Bit position 2) {MAPEM}	1	1
Speed limits included in the road and lane topology {MAPEM.map.intersections IntersectionGeometry.speedLimits}	1	2

PROJECT DOCUMENT
REFERENCE ONLY

0								1							
0	0	0	0	0	0	0	1	1	1	1	0	0	0	0	0

Note: Under ETSI TS 103 301 V1.1.1 (2016-11), Octet Position 1, Bit Position 1 is only allowed to be set to “0: certificate not allowed to sign”. This is believed to be a misprint.

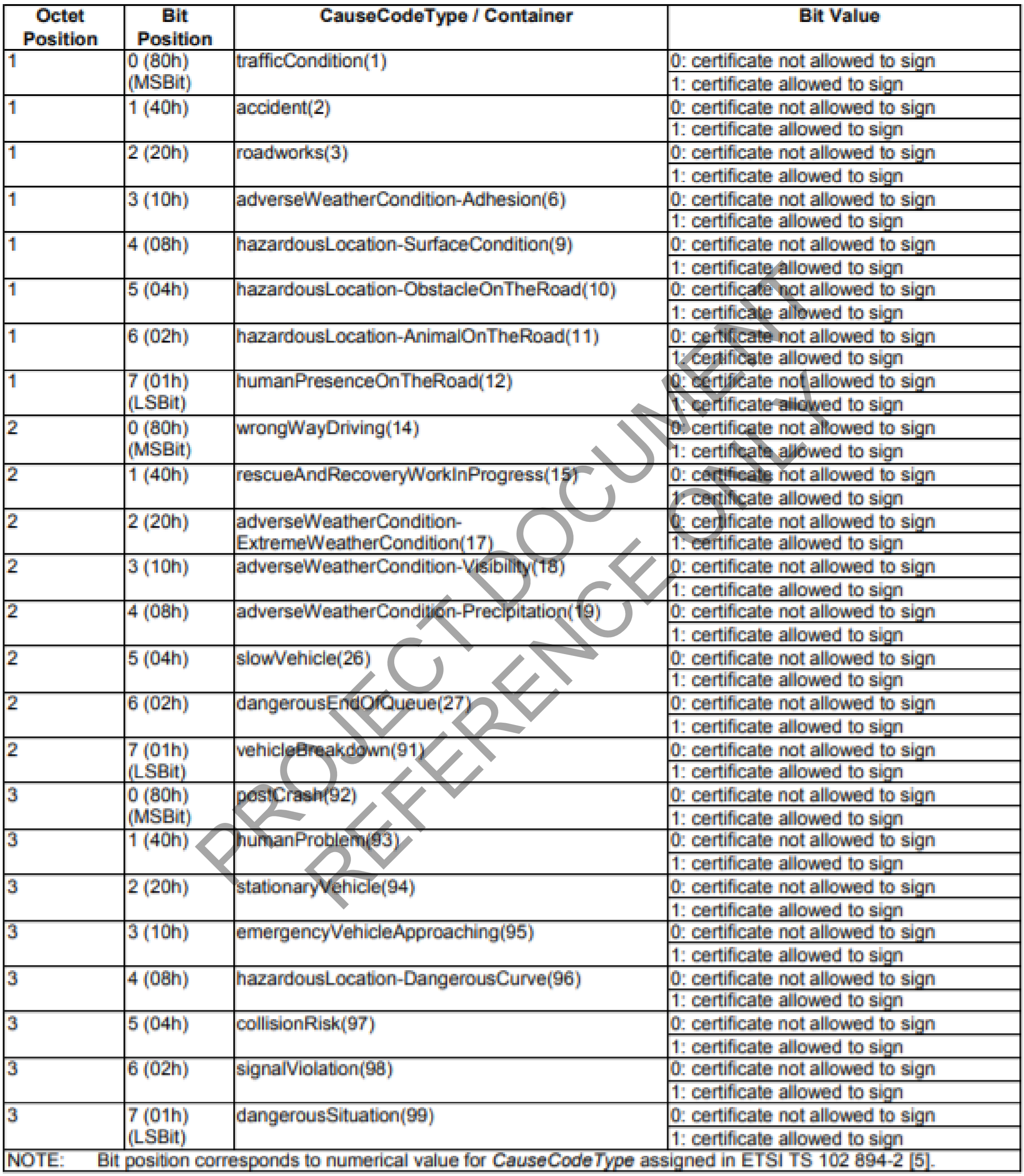
7.3.2 DENM:

ITS-AID: 37 (0x25)

SSP version: 1

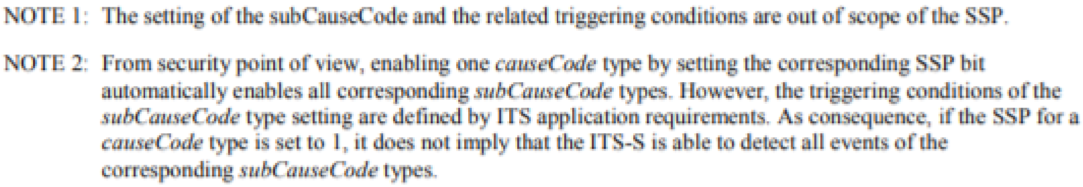
SSP allocation: permissions for all DENM cause codes

Table 9: SSP Definitions for DENM



Octet Position	Bit Position	CauseCodeType / Container	Bit Value
1	0 (80h) (MSBit)	trafficCondition(1)	0: certificate not allowed to sign 1: certificate allowed to sign
1	1 (40h)	accident(2)	0: certificate not allowed to sign 1: certificate allowed to sign
1	2 (20h)	roadworks(3)	0: certificate not allowed to sign 1: certificate allowed to sign
1	3 (10h)	adverseWeatherCondition-Adhesion(6)	0: certificate not allowed to sign 1: certificate allowed to sign
1	4 (08h)	hazardousLocation-SurfaceCondition(9)	0: certificate not allowed to sign 1: certificate allowed to sign
1	5 (04h)	hazardousLocation-ObstacleOnTheRoad(10)	0: certificate not allowed to sign 1: certificate allowed to sign
1	6 (02h)	hazardousLocation-AnimalOnTheRoad(11)	0: certificate not allowed to sign 1: certificate allowed to sign
1	7 (01h) (LSBit)	humanPresenceOnTheRoad(12)	0: certificate not allowed to sign 1: certificate allowed to sign
2	0 (80h) (MSBit)	wrongWayDriving(14)	0: certificate not allowed to sign 1: certificate allowed to sign
2	1 (40h)	rescueAndRecoveryWorkInProgress(15)	0: certificate not allowed to sign 1: certificate allowed to sign
2	2 (20h)	adverseWeatherCondition-ExtremeWeatherCondition(17)	0: certificate not allowed to sign 1: certificate allowed to sign
2	3 (10h)	adverseWeatherCondition-Visibility(18)	0: certificate not allowed to sign 1: certificate allowed to sign
2	4 (08h)	adverseWeatherCondition-Precipitation(19)	0: certificate not allowed to sign 1: certificate allowed to sign
2	5 (04h)	slowVehicle(26)	0: certificate not allowed to sign 1: certificate allowed to sign
2	6 (02h)	dangerousEndOfQueue(27)	0: certificate not allowed to sign 1: certificate allowed to sign
2	7 (01h) (LSBit)	vehicleBreakdown(91)	0: certificate not allowed to sign 1: certificate allowed to sign
3	0 (80h) (MSBit)	postCrash(92)	0: certificate not allowed to sign 1: certificate allowed to sign
3	1 (40h)	humanProblem(93)	0: certificate not allowed to sign 1: certificate allowed to sign
3	2 (20h)	stationaryVehicle(94)	0: certificate not allowed to sign 1: certificate allowed to sign
3	3 (10h)	emergencyVehicleApproaching(95)	0: certificate not allowed to sign 1: certificate allowed to sign
3	4 (08h)	hazardousLocation-DangerousCurve(96)	0: certificate not allowed to sign 1: certificate allowed to sign
3	5 (04h)	collisionRisk(97)	0: certificate not allowed to sign 1: certificate allowed to sign
3	6 (02h)	signalViolation(98)	0: certificate not allowed to sign 1: certificate allowed to sign
3	7 (01h) (LSBit)	dangerousSituation(99)	0: certificate not allowed to sign 1: certificate allowed to sign
NOTE: Bit position corresponds to numerical value for *CauseCodeType* assigned in ETSI TS 102 894-2 [5].			

PROJECT DOCUMENT
REFERENCE ONLY



NOTE 1: The setting of the subCauseCode and the related triggering conditions are out of scope of the SSP.

NOTE 2: From security point of view, enabling one *causeCode* type by setting the corresponding SSP bit automatically enables all corresponding *subCauseCode* types. However, the triggering conditions of the *subCauseCode* type setting are defined by ITS application requirements. As consequence, if the SSP for a *causeCode* type is set to 1, it does not imply that the ITS-S is able to detect all events of the corresponding *subCauseCode* types.

SSP allocation:

0								1								2							
0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

3							
1	1	1	1	1	1	1	1

7.3.3 IVI

ITS-AID: 139 (0x8b)

SSP version: 1

ServiceProviderID: Octet 1-3 are a combination of country code (10 bits) and provider ID (14 bit) {DE Provider from CEN ISO 19321}. This should be a registered value, but a placeholder will be used in the TMR pilot as follows:.

Country code (1100011100) + provider ID (11111111111111)

Note: Text for country code is ITA2 encoded

SSP allocation:

Permits the use of ISO 14823 and general containers. Excludes ITIS and Vienna codes.

PROJECT DOCUMENT
REFERENCE ONLY

SSP	Octet	Bit
ISO/TS 14823 [i.3] traffic sign pictogram (danger warning) {IVIM.ivi.optional.gic.GicPart.roadSignCodes.RSCode.code. iso14823.pictogramCode.serviceCategoryCode.trafficSignPictogram. dangerWarning}	4	1
ISO/TS 14823 [i.3] traffic sign pictogram (regulatory) {IVIM.ivi.optional.gic.GicPart.roadSignCodes.RSCode.code. iso14823.pictogramCode.serviceCategoryCode. trafficSignPictogram.regulatory}	4	2
ISO/TS 14823 [i.3] traffic sign pictogram (informative) {IVIM.ivi.optional.gic.GicPart.roadSignCodes.RSCode.code. iso14823.pictogramCode.serviceCategoryCode. trafficSignPictogram.informative}	4	3
ISO/TS 14823 [i.3] public facilities pictogram {IVIM.ivi.optional.gic.GicPart.roadSignCodes.RSCode.code. iso14823.pictogramCode.serviceCategoryCode. publicFacilitiesPictogram}	4	4

ISO/TS 14823 [i.3] ambient or road conditions pictogram (ambient condition) {IVIM.ivi.optional.gic.GicPart.roadSignCodes.RSCode.code. iso14823.pictogramCode.serviceCategoryCode. ambientOrRoadContitionPictogram.ambientCondition}	4	5
ISO/TS 14823 [i.3] ambient or road conditions pictogram (road condition) {IVIM.ivi.optional.gic.GicPart.roadSignCodes.RSCode.code. iso14823.pictogramCode.serviceCategoryCode. ambientOrRoadContitionPictogram.roadCondition}	4	6
Lane status {IVIM.ivi.optional.gic.GicPart. laneStatus}	5	0
Road configuration container {IVIM.ivi.optional.rcc}	5	1
Text container {IVIM.ivi.optional.tc}	5	2
Layout Container {IVIM.ivi.optional.lac}	5	3
IVI Status (negation) {IVIM.ivi.mandatory.iviStatus}	5	4

0								1								2							
0	0	0	0	0	0	0	1	1	1	0	0	0	1	1	1	0	0	1	1	1	1	1	1

3								4								5							
1	1	1	1	1	1	1	1	0	1	1	1	1	1	1	0	1	1	1	1	1	0	0	0

PROJECT DOCUMENT REFERENCE ONLY

7.3.4 Security Management:

Note: this permission applies only to the EC

ITS-AID: 623 (0x26f)

SSP version: 1

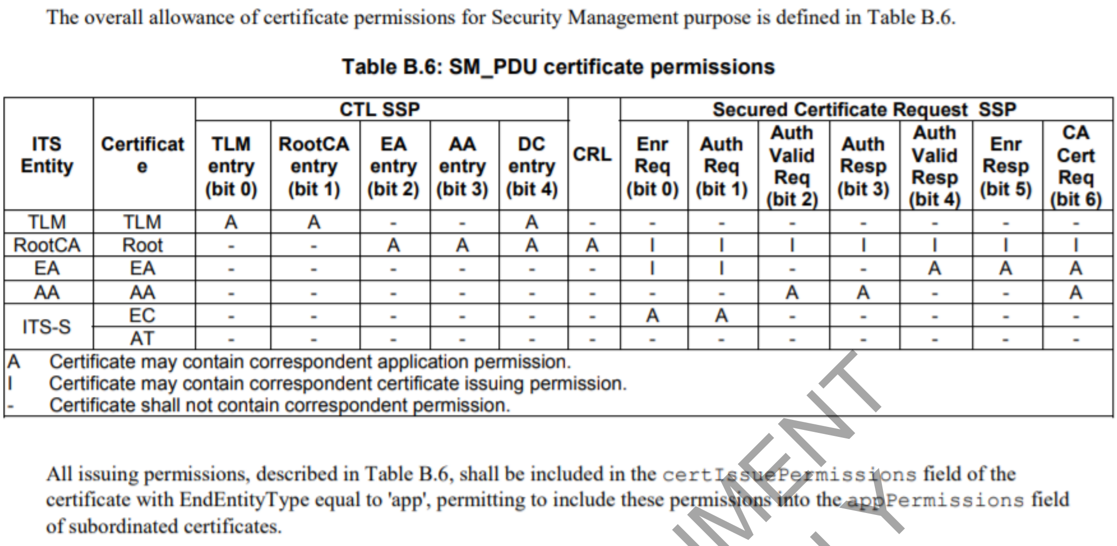
SSP allocation: can sign enrolment request messages and authorisation request messages.

0								1							
0	0	0	0	0	0	0	1	1	1	0	0	0	0	0	0

7.4 CA and TLM Profiles

This section lists the profiles for the various certificate authorities and the Australian trust list manager (ACTL).

Security Management certificate permissions are defined in ETSI TS 102 941 v1.3.1 as follows:



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

Table B.6: SM_PDU certificate permissions

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

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

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

PROJECT DOCUMENT
REFERENCE ONLY

CTL: ITS-AID 624 SSP values are defined in ETSI TS 102 941 v1.3.1 as follows:

Table B.1: CTL service-specific permissions

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

Only combinations of SSPs defined in the Table B.2 shall be allowed.

Table B.2: Allowed combinations of CTL SSPs

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

7.4.1 RCA

7.4.1.1 Security Management:

Certificate issuing permissions:

ITS-AID: 623 (0x26f)

SSP version: 1

SSP allocation: can sign all permissions as certificate issuing permission.

0								1							
0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	0

7.4.1.2 Certificate revocation list:

Application permissions:
ITS-AID: 622 (0x02-6E)
SSP version: 1
SSP allocation: Not applicable.

0							
0	0	0	0	0	0	0	1

7.4.1.3 Certificate trust list:

Application permissions:
ITS-AID: 624 (0x0270)
SSP version: 1
SSP allocation: can sign all permissions for the CTL.

0								1							
0	0	0	0	0	0	0	1	0	0	1	1	1	0	0	0

7.4.2 Enrolment Authority

7.4.2.1 Security Management:

Certificate issuing permissions:
ITS-AID: 623 (0x26f)
SSP version: 1
SSP allocation: can sign enrolment and authorisation request as certificate issuing permission.

0								1							
0	0	0	0	0	0	0	1	1	1	0	0	0	0	0	0

PROJECT DOCUMENT
REFERENCE ONLY

Note: For certificate issuing permissions, no restrictions are placed on PSID/SSP combinations that can be issued to end-entity-certificates in the certificate profile of CAs. The relevant CA and the policy authority will ensure that end-entity-certificates are issued with the correct profiles.

Application permissions:

ITS-AID: 623 (0x26f)

SSP version: 1

SSP allocation: can sign authorisation validation and enrolment response and CA certificate requests as application permission.

0								1							
0	0	0	0	0	0	0	1	0	0	0	0	1	1	1	0

7.4.3 Authorisation Authority

7.4.3.1 Security Management:

Certificate issuing permissions:

Note: For certificate issuing permissions, no restrictions are placed on PSID/SSP combinations that can be issued to end-entity-certificates in the certificate profile of CAs. The relevant CA and the policy authority will ensure that end-entity-certificates are issued with the correct profiles.

Application permissions:

ITS-AID: 623 (0x26f)

SSP version: 1

SSP allocation: can sign authorisation validation request, authorisation response and CA certificate requests as application permission.

0								1							
0	0	0	0	0	0	0	1	0	0	1	1	0	0	1	0

PROJECT DOCUMENT
REFERENCE ONLY

7.4.4 Trust List Manager (TLM)

7.4.4.1 Australian Certificate Trust List (ACTL):

Application permissions:

ITS-AID: 624 (0x0270)

SSP version: 1

SSP allocation: can sign all permissions for the ACTL.

0								1							
0	0	0	0	0	0	0	1	1	1	0	0	1	0	0	0

PROJECT DOCUMENT
REFERENCE ONLY