Telecommunications Standards Advisory Committee (TSAC)

Technical Specification

Dedicated Short-Range Communications in Intelligent Transport Systems

IMDA TS DSRC
Issue 1, October 2016

Info-communications Media Development Authority of Singapore
Resource Management & Standards
10 Pasir Panjang Road
#10-01 Mapletree Business City
Singapore 117438

Acknowledgement

The Info-communications Media Development Authority of Singapore (IMDA) and the Telecommunications Standards Advisory Committee (TSAC) would like to acknowledge the following members of the TSAC Working Group 3 Intelligent Transport Systems (ITS) – Dedicated Short Ranged Communication (DSRC) Task Force (TSAC WG6 ITS-DSRC TF) for their invaluable contributions to the preparation of this Technical Specification:

IMDA TS DSRC Issue 1, October 2016	Technical Specification for Dedicated Short-Range Communications (DSRC) in Intelligent Transport Systems (ITS)
Chairman(s)	Dr Jaya Shankar; Department Head, Institute for Infocomm Research (I²R), A*STAR (Chairman)
	Dr Zander Lei; Senior Researcher, Huawei Singapore Research Center (Co-Chairman)
Chief Editor	Dr Zander Lei; Senior Researcher, Huawei Singapore Research Center
Editors	Dr Guan Yong Liang; Associate Professor, Nanyang Technological University
	Mr Paul Mellon; Systems Engineer, Kapsch TrafficCom Pte Ltd
	Mr Katayan Riyas; Manager, I²R, A*STAR
	Mr Mike Cheong; Account Manager, Rohde & Schwarz
	Mr Colin Yap; Senior Engineer, LTA
	Mr Luoyi Huang; Senior Engineer, Denso
Secretary	Mr Colin Yap; Senior Engineer, LTA

List of TSAC WG3 ITS-DSRC TF Members (2015-2018)

S/N	Organisation	Name
1	ATiS (TSAC WG6 Chairman)	Mr Yip Yew Seng, Chairman, TSAC WG 6
2	Continental Automotive Singapore	Mr Dan Chia, Senior Manager
3	Delphi Electronics & Safety, Singapore	Dr Teo Kiat Choon, Manager
4	DENSO International Asia Pte Ltd	Mr Bruce Eng, General Manager
5		Mr Luoyi Huang, Senior Engineer
6	D'Crypt Pte Ltd	Dr. Antony Ng, CEO
7	Huawei Singapore Research Center	Dr Zander Lei, Senior Researcher
8	IBM	Mr Pankaj Lunia, ASEAN Business Manager
9	IMDA	Mr Andy Phang, Senior Manager
10		Mr Lim Wei Li, Manager
11		Ms Tan Siew Guat, Manager
12		Dr Jaya Shankar; Department Head

13	Institute for Infocomm Research (I²R), A-STAR	Mr Katayan Riyas, Manager
14	Kapsch TrafficCom Pte Ltd	Mr Johan Ahlberg, Sales Director
15		Mr Paul Mellon, Systems Engineer
16	National University of Singapore	Dr Masaaki Sato, Visiting Senior Research Fellow
17	LTA	Mr Chang Mook Choong, Deputy Director
18		Mr Chan Hin Phung, Senior Manager
19		Mr Ong Beng Kee, Manager
20		Ms Goh Lee Ming, Manager
21		Mr Colin Yap, Senior Engineer
22		Mr Francis Tan, Senior Engineer
23	Mitsubishi Heavy Industries Engine System Asia Pte. Ltd.	Mr Yamamoto Masayuki, Project Director
24		Mr Kamimura Yoichi, Deputy Manager
25	NCS Pte Ltd	Mr Eddie Lim Sing Loong, Account Director
26	Nanyang Polytechnic	Mr Tan Keng Chuah, Manager
27	Nanyang Technological University	Dr Guan Yong Liang, Associate Professor
28	NXP Semiconductors Singapore Pte Ltd	Mr Marcus Lim Ah Sui, Senior Applications Manager
29	Power Automation	Mr Kerk See Gim, Project Director
30	Quantum Inventions Pte Ltd	Mr Mohit Sindhwani, Head
31	Rohde & Schwarz	Mr Mike Cheong, Account Manager
32	Singapore Police Force	Mr Toh Keng Han, Programme Manager
33	ST Electronics (Info-Comm Systems)	Mr Nixon Ng Ho Kwong, Senior Director
34		Dr Albert Ng Kim Chwee, Deputy Division Manager
35	Toyota Tsusho Asia Pacific Pte. Ltd.	Mr Richard Lee, General Manager
36	Watchdata Technologies Pte Ltd	Mr James Cai Mao, Director

Telecommunications Standards Advisory Committee (TSAC)

The TSAC advises IMDA on the setting of ICT standards as well as on the development and recommendation of specifications, standards, information notes, guidelines and other forms of documentation for adoption and advancement of the standardisation effort of the Singapore ICT industry (hereafter termed "IMDA Standards").

Telecommunications standards-setting in Singapore is achieved with the assistance of TSAC, where professional, trade and consumer interest in telecommunications standards is represented on the TSAC with representatives from network and service operators, equipment suppliers and manufacturers, academia and researchers, professional bodies and other government agencies.

List of TSAC Members (2015-2018)

TSAC Chairman:

Mr Raymond Lee	Director (Resource Management & Standards) Info-communications Media Development Authority of Singapore

TSAC Members:

Mr Lim Yuk Min (TSAC Vice-Chairman)	Senior Executive Consultant (Resource Management and Standards) Info-communications Media Development Authority of Singapore
Mr Darwin Ho Kang Ming	Member Association of Telecommunications Industry of Singapore (ATIS)
Mr Yip Yew Seng	Honorary Secretary Association of Telecommunications Industry of Singapore (ATIS)
Dr Oh Ser Wah	Head, Strategic Planning Office Institute for Infocomm Research
Mr Denis Seek	CTO M1 Limited
Mr Tan Tiong Heng	Deputy Director, Engineering M1 Limited
Mr Goh Kim Soon	Senior Vice President MediaCorp Pte Ltd
Mr Lim Chin Siang	Director, Technology Info-communications Media Development Authority of Singapore
Ms Tan Sze Siang	Director, Digital Broadcasting Deployment Office Info-communications Media Development Authority of Singapore
Assoc Prof Guan Yong Liang	Nanyang Technological University School of Electrical & Electronic Engineering
Ms Lim Siew Eng	Director, Centre of Innovation Nanyang Polytechnic
Assoc Prof Tham Chen Khong	National University of Singapore Department of Electrical & Computer Engineering
Dr Yu Changyuan	National University of Singapore Department of Electrical & Computer Engineering
Mr Widjaja Suki	Director, Products, Business Development & Process Netlink Trust Pte Ltd
Mr Ronald Lim	Head, Regulatory Nucleus Connect Pte Ltd
Mr Neo Yong Chiang	Chief Information Officer Republic Polytechnic
Mr Manik Narayan Saha	Singapore Infocomm Technology Federation
Assoc Prof Steven Wong Kai Juan	Programme Director Singapore Institute of Technology
Assoc Prof Ian Thng Li-Jin	Programme Director

	Singapore Institute of Technology
Dr Wong Woon Kwong	Director, Research and Industry Collaborations Singapore University of Technology and Design
Mr Kuan Wai Mun	Associate Director, Radio Network Quality Singapore Telecommunications Ltd
Mr Lew Yoon Heng	Senior Engineering Manager Singapore Telecommunications Ltd
Mr Adrian Goh	Deputy Director, Standards SPRING Singapore
Mr Lim Eng Huat	Vice President Starhub Ltd
Mr Hong Tse Min	Assistant Director, Resource Management and Standards Info-communications Media Development Authority of Singapore
Ms Woo Yim Leng	Senior Manager, Resource Management and Standards Info-communications Media Development Authority of Singapore

This page is intentionally left blank.

Content

Dedicated Short-Range Communications (DSRC) Standards for Intelligent Transport Systems (ITS)

1 Scope

1.1 This Specification is established based on the current standards for wireless connectivity, which include the IEEE 802.11 with modifications to the PHY and MAC Layer to provide reliable and low latency communications in vehicles, Dedicated Short Range Communication (DSRC) in the 5 GHz spectrum, the IEEE 1609 wireless access vehicular environment (WAVE) for security and network management.

1.2 The Specification is intended for developing Intelligent Transportation Systems (ITS) for improving traffic management, transportation safety and mobility, and an ITS architecture for Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communications envisaged in the Smart Nation.

2 References

In establishing the technical requirements of this Specification, reference has been made to the following documents:

[1] IEEE Std 802.11-2012[1], IEEE Standard for Information technology – Telecommunication and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications

[2] IEEE Std 1609.2-2016, IEEE Standard for Wireless Access in Vehicular Environment (WAVE) - Security Services for Applications and Management Messages

[3] IEEE Std 1609.3-2016, IEEE Standard for Wireless Access in Vehicular Environment (WAVE) - Networking Services

[4] IEEE Std 1609.4-2016, IEEE Standard for Wireless Access in Vehicular Environment (WAVE) - Multi Channel Operation

[5] IEEE Std 1609.11-2010, IEEE Standard for Wireless Access in Vehicular Environment (WAVE) - Over-the-Air Electronic Payment Data Exchange Protocol for Intelligent Transportation Systems (ITS)

[6] IEEE Std 1609.12-2016, IEEE Standard for Wireless Access in Vehicular Environment (WAVE) - Identifier Allocations

[7] SAE (Society of Automotive Engineers) J2735-2009[2], Dedicated Short Range Communications (DSRC) Message Set Dictionary

[8] IEEE Std 1609.0-2013, IEEE Guide for Wireless Access In Vehicular Environment (WAVE) Architecture

[9] IEC CISPR 32, Electromagnetic Compatibility of Multimedia Equipment – Emission Requirements

[10] IEC 60950-1, International Electrotechnical Commission – Safety of Information Technology Equipment

[1] IEEE publications are available from the Institute of Electrical and Electronics Engineers, Inc, 445 Hoes Lane, Piscataway, NJ 08854, USA (http://standards.ieee.org/). The IEEE standards or products referred to in this clause are trademarks of the Institute of Electrical and Electronics Engineers, Inc.

[2] SAE publications are available from the Society of Automotive Engineers, 400 Commonwealth Drive, Warrendale, PA 15096, USA (http://www.sae.org/).

3 Definition and Abbreviations

For the purpose of this document, the following terms and definitions apply.

3.1 Definitions

The industrial, scientific and medical (ISM) band: radio bands (portions of the radio spectrum) that are reserved internationally for the use of radio frequency (RF) energy for industrial, scientific and medical purposes other than telecommunications.

Vehicle to Infrastructure (V2I), Infrastructure to Vehicle (I2V): direct communication from a vehicle to road infrastructure or road infrastructure to vehicles using the 5.9 GHz DSRC frequency spectrum

Vehicle to vehicle (V2V): direct vehicle(s) to vehicle(s) communication using the 5.9 GHz DSRC frequency spectrum

3.2 Abbreviations

ASTM	American Society for Testing Material
AV	Autonomous Vehicle
BSM	Basic Safety Message
CCC	Compliance Checking Communication
CCH	Control Channel
CEN	European Committee for Standardization
CEPT	European Conference of Postal and Telecommunications Administrations
C-ITS	Cooperative ITS
DSRC	Dedicated Short Range Communications
EDCA	Enhanced Distributed Channel Access
EFC	Electronic Fee Collection
EIRP	Equivalent Isotropic Radiated Power
EMF	Electromagnetic Fields
EPS	Electronic Parking System
ETSI	European Telecommunications Standards Institute
FCC	Federal Communications Commission
GNSS	Global Navigation Satellite System
ICNIRP	International Commission on Non-Ionizing Radiation Protection
IEEE	Institute of Electrical and Electronic Engineers
IP	Internet Protocol
IPv6	Internet Protocol version 6
ISO	International Organization for Standardization
ISM	Industrial, Scientific and Medical
ITS	Intelligent Transportation Systems
LAC	Location Augmentation Communication
LLC	Logical Link Control
MAC	Media Access Control
OBU	On Board Unit
PER	Packet Error Rate
PHY	Physical
PSID	Provider Service Identifier
RF	Radio Frequency
RSU	Road Side Unit
SAE	Society of Automotive Engineers
SCH	Service Channel
SPaT	Signal Phase and Timing

STA	Station
TCP	Transmission Control Protocol
TIM	Traveller Information Message
UDP	User Datagram Protocol
V2I	Vehicle to Infrastructure
V2V	Vehicle to Vehicle
VMS	Variable Message Sign
WAVE	Wireless Access in Vehicular Environments
WG	Working Group
WSA	WAVE Service Advertisement
WLAN	Wireless Local Area Network
WSM	WAVE Short Message
WSMP	WAVE Short Message Protocol

4 General Requirements

4.1 Design of DSRC Devices

The DSRC device shall be designed to meet the following requirements:

a) The DSRC device shall not be constructed with any external or readily accessible control which permits the adjustment of its operation in a manner that is inconsistent with this Specification;

b) The DSRC device shall be marked with the supplier/manufacturer's name or identification mark, and the supplier/manufacturer's model or type reference. The markings shall be legible, indelible and readily visible; and

c) DSRC devices shall have different power classes as defined in this Specification, corresponding to the varied communication zones. DSRC devices shall transmit only the power needed to communicate within the communications zone, and must take steps to limit the signal within the zone to the maximum extent practicable. DSRC devices consist of Road Side Unit ("RSU") and On Board Unit ("OBU"). RSU may have additional conditions on antenna height and power as defined in § 5.

4.2 Safety Requirements

4.2.1 Where appropriate, the DSRC device shall be tested according to measurement methods and limits for:

a) Electromagnetic Compatibility (EMC) emissions from the direct DC power or AC mains power input/output ports defined in IEC CISPR 32 [9]; and

b) Electrical safety defined in the IEC 60950-1 [10].

4.2.2 Where appropriate, the DSRC device shall comply with the International Commission on Non-Ionising Radiation Protection ("ICNIRP") guidelines for limiting exposure to time-varying electromagnetic field ("EMF") in the frequency range up to 300 GHz.

4.2.3 It should be noted that compliance with any radiation safety standard does not by itself confer immunity from legal obligations and requirements imposed by national health or safety authorities.

5 Technical Requirements for DSRC

5.1 Category of Use Cases

Description of use cases for DSRC is given as general information in Annex A of this Specification. Use cases may be broadly categorised as follows:

a) Localisation
b) Electronic Parking Management
c) Traffic Signal Control Management
d) Traffic Information
e) Safety Applications
f) Emergency Applications
g) Kiosk Related Services
h) Other ITS Application and Services

Emphasis is on Congestion Management in the ITS. The DSRC deployed according to this Specification, should have taken these factors into consideration: the communication range (10m – 1000m), the need for control channel, antenna beam directionality, differentiation of channel usage (public, private and V2V) and urgency, and the possibility of overlapping cells (in radio coverage) and network congestion.

5.2 Protocol Stack

Components of the 5.9 GHz DSRC protocol stack for Singapore are as shown in Figure 1, based on the IEEE 1609 family of WAVE standards.

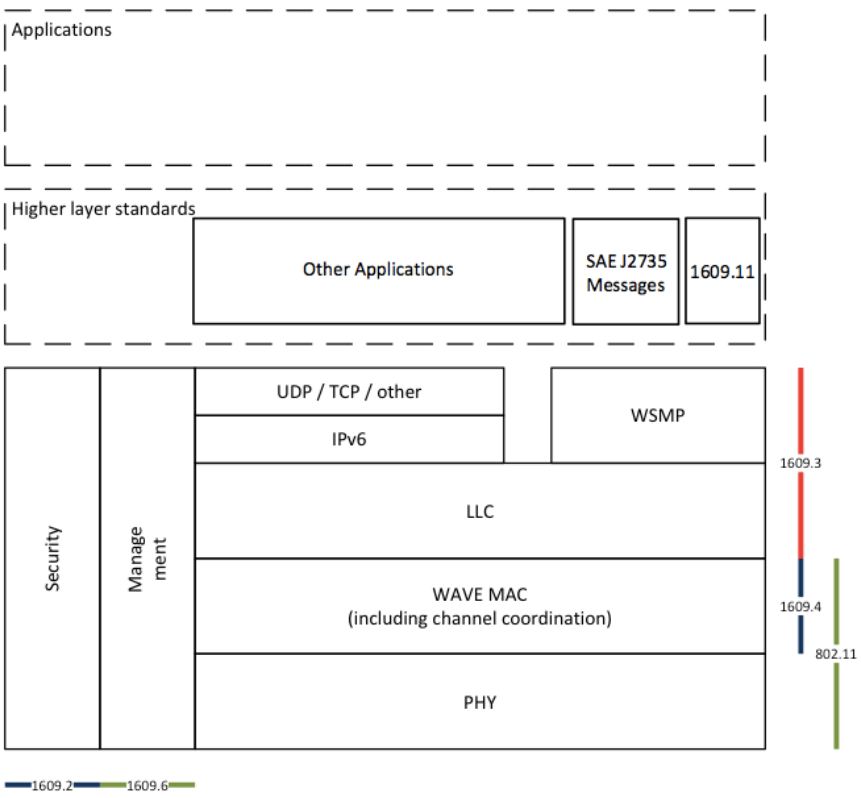


Figure 1: The Singapore 5.9 GHz DSRC Protocol Stack (Based on the IEEE 1609.0 WAVE Architecture)

5.3 DSRC Devices and Conformity Assessment Requirements

5.3.1 DSRC devices shall be able to support at minimum the features of the WAVE protocol standards implemented by Service Provider(s) as outlined in the Protocol Implementation Conformance Statement (PICS) Tables given in Annex B of this Specification.

5.3.2 The WAVE protocol requirements specific to the DSRC implementation(s) of the Singapore Service Provider(s) are based the following IEEE standards:

a) IEEE 802.11 WLAN MAC and PHY layer specifications, operating Outside the Context of a Basic service set (OCB)
The DSRC device shall comply with the statement of mandatory and optional features set out in the PICS Table B.1 of this Specification for an implementation of IEEE 802.11 [1].

b) IEEE 1609.4 for Multi-Channel Operations
The DSRC device shall comply with the statement of mandatory and optional features set out in the PICS Table B.2 of this Specification for an implementation of IEEE 1609.4 [4].

c) IEEE 1609.3 for Networking Services
The DSRC device shall comply with the statement of mandatory and optional features set out in the PICS Table B.3 of this Specification for an implementation of IEEE 1609.3 [3]. The DSRC device shall also comply with the IEEE 1609.2 security profile, SSP specification, and additional certificate constraints that apply to the WSA (Annex H of IEEE 1609.3).

d) IEEE 1609.11 [5] for Over-the-Air Electronic Payment Data Exchange Protocol for ITS
This is an application-level DSRC-based standard, which specifies a payment protocol, referencing to the ISO standards. This standard defines a basic level of technical interoperability for electronic payment equipment, i.e. OBU and RSU.

e) IEEE 1609.12 [6] for Identifier Allocations
This specifies the allocation of Provider Service Identifier (PSID) for use with the IEEE 1609 family of standards. For example, it may be used by a Service Provider to identify its advertised application-service opportunities by means of the PSID values in the WSA messages it transmits.

f) IEEE 1609.2 for Security Services for Applications and Management Messages
This standard defines secure message formats and processing for use by Wireless Access in Vehicular Environments (WAVE) devices, including methods to secure WAVE management messages and methods to secure application messages. It also describes administrative functions necessary to support the core security functions.

The DSRC device shall comply with the statement of mandatory and optional features set out in the PICS Table B.4 of this Specification for an implementation of IEEE 1609.2 [6].

g) SAE J2735 [7] DSRC Message Set Dictionary
This standard defines a set of messages that may be used for V2V and V2I safety exchanges. Examples are not limited to the use of the broadcast type Basic Safety Message (BSM) as a WSM for probe data collection and V2V safety applications; use of the Signal Phase and Timing (SPAT) and the Map Data (MAP) messages as WSMs to broadcast traffic signal and map data to vehicles from an intersection roadside; and the use of the broadcast type Traveller Information Message (TIM) as a WSM for travel times, parking information and hazard warnings.

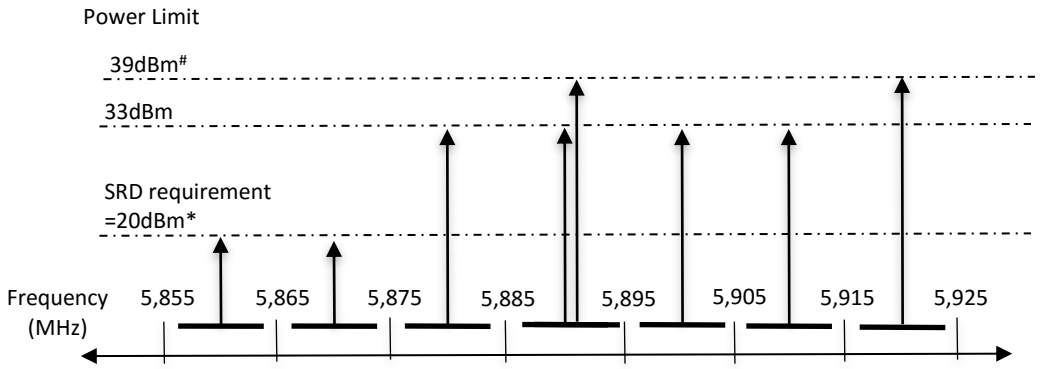
5.4 Spectrum Allocation and Power Limits

5.4.1 The 5.9 GHz frequency spectrum from 5.855 GHz to 5.925 GHz has been allocated for operation of DSRC in Singapore. For DSRC devices, the available spectrum is divided into seven 10MHz channels, as illustrated in Figure 2.

5.4.2 The DSRC device shall comply with the maximum field strength or radio frequency (RF) output power[3]

[3] Equivalent Isotropic Radiated Power (e.i.r.p.) is a product of the power supplied to the antenna and the maximum

illustrated in Figure 2, operating in its intended frequency band or frequencies. It is notable that there are two power limits defined for the spectrum from 5.885 GHz to 5.895 GHz, which will be elaborated in § 5.1010 (Communication Services).



Higher RF emission power shall be approved only on an exceptional basis
* Reference to IMDA TS SRD for maximum allowable RF output power

Figure 2: DSRC Spectrum Power Limit

5.5 Power Classes, Antenna Height and Communication Zones

5.5.1 There are four classes of DSRC devices in terms of output power defined in this Specification, as shown in Table 1. A DSRC device shall meet both the Max output power and the EIRP limit requirements. This is in line with the FCC rule in the USA, except for the Class D EIRP requirement. An indicative communication zone of each class is also shown in Table 1.

5.5.2 Table 1 shall also be applicable to any RSU with an antenna height not exceeding 8 meters from the roadway bed surface[4].

Table 1: Power Classification

Power Class	Max output power[5] (mW)	EIRP Limit[6] (dBm)	Communication Zones (m, indicative)
A	1	23	15
B	10	23	100
C	100	33	400
D[7]	760	39	1000

5.5.3 For any RSU with an antenna height exceeding 8 meters but not exceeding 15 meters above the roadway bed surface, Table 1 shall be applicable together with a reduction factor of 20 log(Ht/8) in dB, where Ht is the height of the radiation centre of the antenna in meters above the roadway bed surface. The EIRP is measured as the maximum EIRP toward the horizon or horizontal, whichever is greater, of the gain associated with the main or centre of the transmission beam. The RSU antenna height shall not exceed 15 meters above the roadway bed surface.

5.6 Spectrum Mask, Interference, and Coexistence

5.6.1 For any DSRC device using the 10 MHz channel spacing, the transmitted power spectral density shall

antenna gain, relative to an isotropic antenna, and is used for frequencies above 1 GHz. There is a constant difference of 2.15 dB between e.i.r.p. and e.r.p. [e.i.r.p. (dBm) = e.r.p. (dBm) + 2.15]

[4] Separate antenna height mounting approval(s) should be obtained from the relevant authorities.

[5] Max output power refers to the power level at the input of antenna, or its equivalent using an isotropic antenna.

[6] The EIRP limit is only applicable to devices operating in channels 176-184 (5.875 – 5.925 GHz), which are defined in Table 5. Devices operating in channel 172 or 174 shall (i) operate based on non-protection basis; and (ii) comply with all the requirements set out in the IMDA TS SRD for the 5.8 GHz band.

[7] The Power Class D DSRC devices and RSU are restricted for public safety uses only.

have a 0 dBr bandwidth not exceeding 9 MHz and shall not exceed the spectrum mask created, using the permitted power spectral density levels as specified in Table 2, based on the IEEE 802.11 [1].

5.6.2 For any DSRC device, the out-of-band (below 5845 MHz or above 5935 MHz) emissions shall not exceed an EIRP of −30 dBm/MHz.

Table 2: Spectrum Mask

Power Class	Permitted Power Spectrum Density (dBr/MHz)				
	+/- 4.5MHz	+/- 5MHz	+/- 5.5MHz	+/- 10MHz	+/- 15MHz
A	0	-10	-20	-28	-40
B	0	-16	-20	-28	-40
C	0	-26	-32	-40	-50
D	0	-35	-45	-55	-65

5.7 Receiver Minimum Input Sensitivity

5.7.1 The receiver sensitivity is defined as the min Rx signal level at the antenna connector required for a given pack error rate and modulation scheme. The minimum input level for receiver sensitivity shall be no more than 10% PER of occurrence, based on Table 3.

Table 3: Receiver Minimum Input Sensitivity

Modulation	Coding Rate	Minimum Sensitivity (dBm) (10 MHz channel spacing)
BPSK	1/2	-85
BPSK	3/4	-84
QPSK	1/2	-82
QPSK	3/4	-80
16QAM	1/2	-77
16QAM	3/4	-73
64QAM	2/3	-69
64QAM	3/4	-68

5.8 Receiver Adjacent and Non-Adjacent Channel Rejection

5.8.1 The adjacent/non-adjacent channel rejection, i.e. the power difference between the interfering and the desired channel, which measures the ability of a receiver to demodulate and decode a desired signal in the presence of an interfering signal in an adjacent or nonadjacent channel. The desired signal power is set 3 dB above the minimum sensitivity. The power of the interfering signal in the adjacent/non-adjacent channel is increased until the measured PER of the wanted signal reaches 10%.

5.8.2 The receiver adjacent/non-adjacent channel rejection under specified conditions shall be equal to or greater than the limits based on Table 4.

Table 4: Receiver Adjacent and Non-Adjacent Channel Rejection Requirements

Modulation	Coding Rate	Adjacent Channel Rejection (dB)	Non-adjacent rejection (dB)
BPSK	1/2	28	42
BPSK	3/4	27	41
QPSK	1/2	25	39
QPSK	3/4	23	37

16QAM	1/2	20	34
16QAM	3/4	16	30
64QAM	2/3	12	26
64QAM	3/4	11	25

5.9 Channel Types

5.9.1 Operation of Control Channel (CCH) and Service Channel (SCH) will be deployed in Singapore, and altogether 7 channels have been defined as shown in Table 5. In an ascending order in frequency, Channel 172 and Channel 174 are assigned as the ISM-Band Public/Private Service Channel (ISM-CH1 and ISM-CH2). Channel 176 is assigned as the V2V Safety Service Channel (SfCH), while Channel 178 is assigned as the CCH. Channel 180 and Channel 182 are assigned as the Public/Private Service Channel (PP-SCH) and the Public Channel (PUB-SCH) for Road Pricing Service respectively. Lastly, Channel 184 is assigned as the Long Range Service Channel (LR-SCH).

Table 5: Channel Types

Channel No.	Centre Frequency (MHz)	Channel Name	Channel Type
172	5860	ISM Band Public/Private Channel (ISM-SCH1)	Service Channel
174	5870	ISM Band Public/Private Channel (ISM-SCH2)	Service Channel
176	5880	V2V Safety Channel (SfCH)	Service Channel
178	5890	Control Channel (CCH)	Control Channel
180	5900	Public/Private Channel (PP-SCH)	Service Channel
182	5910	Public Channel (PUB-SCH)	Service Channel
184	5920	Long Range Channel (LR-SCH)	Service Channel

Note: The actual carrier centre frequency for any given channel shall be maintained within the range fc +/- 20ppm.

5.9.2 Both PUB-SCH and LR-SCH are public channels that only government agencies and their designated entities are allowed to install and operate DSRC devices. LR-SCH is for applications requiring a large coverage area. PUB-SCH is dedicated to Road Pricing related applications that are managed by LTA.

5.9.3 SfCH is dedicated to V2V Safety applications, whereas CCH is used for WSMP messages and management messages.

5.9.4 PP-SCH, ISM-SCH1, and ISM-SCH2 are Service Channels that can be used by both government agencies and private entities.

5.9.5 Only operation of 10 MHz channel will be allowed. Operation of 20 MHz channel by combining two 10 MHz channels will not be allowed.

5.10 Communication Services

5.10.1 CCH communications and SCH communications are delivered by the IEEE 1609 WAVE protocols, supporting various applications running on a DSRC device. CCH is a “rendezvous” channel that allows multiple-channel-capable DSRC devices to tuning on at the same time to find each other. Only WSMs, WSA, and management frames are allowed on the CCH. V2V safety messages and IP packages (UDP, TCP) are not allowed on the CCH.

5.10.2 SCH is the “service delivery” channel where applications data is transferred. The data allowed on SCH

is dependent on the SCH types:

- Only BSM that conveys information supporting V2V safety-related use cases are permitted on the V2V SCH.
- All messages and application data that are not conveyed on CCH and V2V Safety channel are allowed on any of the public or private channels.

5.10.3 Operation on one SCH requires one DSRC radio interface. Operation on more than one SCH is allowed, which may require additional radio interfaces to operate at the same time. For example, it requires a DSRC device to be equipped with 2 DSRC radio interfaces to operate on both PUB-SCH and SfCH at the same time.

5.10.4 A DSRC device (RSU) providing services or applications on SCH may advertise its services using WSA on CCH. An OBU may listen to CCH for WSA and switch to the advertise SCH for the interested services. It is noted that the power limit for transmitting advertising messages on CCH is tied to the power limit of each SCH. Specifically, the power limits of advertising on CCH for LR-SCH and other SCHs are 39dBm and 33dBm respectively, as illustrated in Figure 2.

5.10.5 Services may also be provided on a predefined SCH without advertising on CCH. In this case, a DSRC device may stay on the interested SCH and does not need to switch to CCH periodically.

5.11 User Priority

The IEEE 1609.4 [4] standard for multi-channel operations provides safety and non-safety applications up to eight levels of MAC sublayer priority, using User Priority (UP) and related Access Category (AC) of QoS enhanced distributed channel access (EDCA) as specified in IEEE 802.11 [1].

Annex A

DSRC Use Cases

A.1 Localisation

The Next Generation (NG) Congestion Management System may introduce service applications where one or several RSUs placed along the roadside may provide location augmentation to the OBU attached in the vehicle.

A.2 Electronic Parking Management

With the implementation of the NG Congestion Management System, the existing EPS can be upgraded together with the OBUs, leveraging the 5.9 GHz DSRC for parking payment transactions through means of both frontend and backend payment. This is also applicable to vehicle access controls for private residential premises, etc.

A.3 Traffic Signal Control Management

With placement of RSUs along the routes to the traffic junctions, traffic data may be collected from the vehicles On-Board Unit (OBU) to better manage the traffic control functions for applications such as adaptive phasing of traffic lights at the junctions. This is also applicable to vehicle priority for emergency vehicles (ambulances, fire engines, etc.) and in public transportation (e.g. buses) at the traffic junctions.

A.4 Traffic Information

These are use cases identified for disseminating traffic information, namely, in-vehicle Variable Message System (VMS), Warnings (Road Conditions, Obstruction, Road Works, Low Height Clearance, etc.), Stop Light Assistance, Curve Speed Assistance and Parking Availability to the OBU attached in the vehicle. Within the control of privacy rules, anonymous traffic data such as location and speed may be collected for traffic analysis.

A.5 Safety Applications

These are use cases of the V2V Safety Channel (SfCH) for Intersection Collision Warning Avoidance, Cooperative Vehicle System – Platooning, Cooperative Adaptive Cruise Control (CACC) and Cooperative Collision Warning. Specific services for the Autonomous Vehicle (AV), as well as for alerting vehicles of approaching emergency vehicles are also be included under safety applications.

A.6 Emergency Applications

Live video obtained from DSRC devices may be sent to a control centre to provide the required information as supporting evidence.

A.7 Kiosk Related Services

Diagnostic data such as automotive repair records, firmware/software updates may be provided through a service kiosk. Drivers' daily log may be collect through a kiosk for better planning and control in fleet management. Value added services such as purchasing data (music, videos and maps), food takeaways or fuel may be provided through a service kiosk.

A.8 Other ITS Application and services

Pedestrians and cyclists may carry DSRC devices to alert approaching vehicles to slow down and drive with caution. Notifications may be sent to vehicles registered for services such as advertisements or receiving other valued information.

Annex B

Protocol Implementation Conformance Statement (PICS)

An ITS Service Provider may use the PICS to indicate which features are supported by an implementation of DSRC; a consumer of DSRC devices may employ the PICS to note the features required for a particular deployment. A tester may use the PICS as a checklist against which to verify the conformance of the DSRC device.

Notes: An entry of the form <pred>:<S> in the Status column indicates that the status <S> applies if the item identified by <pred> is identified in the Support column as being present.

Valid status values in the Status column are M, O, O<n>, and C<n>.

A status of M indicates a mandatory feature.
A status of O indicates an optional feature.
A status of O<n> indicates a mutual condition such that the feature is optional, but that support of at least one of the items that have status O<n> is mandatory.
A status of C<n> indicates a mutual condition such that support of only one of the items that have status C<n> is mandatory.

Table B.1: PICS of an Implementation of IEEE 802.11 [1]

Item	Feature	References	Status	Support
CF2.1	Independent station (RSU/OBU) operating outside the context of a BSS (dot11OCBActivated is true)	§ 11.19 of IEEE 802.11 [1]	CF17: M	
CF17	5.9 GHz OFDM PHY	§ 5.4, § 5.5, § 5.6, § 5.7 and § 5.8 of this Spec. Note 1	M	
FT26	Timing Advertisement frame	§ 7 of IEEE 802.11 [1]	O	
FR26	Timing Advertisement frame	§ 7 of IEEE 802.11 [1]	O	
AD4	Wildcard BSSID	§ 7.1.3.3.3, § 7.2.2 of IEEE 802.11 [1]	CF2.1:M	
AD5	MAC and PHY operation resumes with appropriate MIB attributes in less than 2 TU	§ 11.19 of IEEE 802.11 [1]	CF2.1:M	
QD8	Default EDCA parameters for communications outside context of BSS	§ 7.3.2.29, § 9.9.1.2 of IEEE 802.11 [1]	CF2.1:M	
Note 1: DSRC devices (RSU/OBU) shall be classified for operation in this band by their max output power and EIRP limit as listed in Table 1 of this Spec, and comply with the spectrum mask requirement for their class listed in Table 2 and defined in § 5.6.1 of this Spec.				

Table B.2: PICS of an Implementation of IEEE 1609.4 [4]

Item	Feature	Value	IEEE 1609.4 [4]	Status	Support
M1.	OCBActivated communication	( )[a]	5.1	M	
M2.	Operation on CCH	( )[b]	5.2	O4	
M2.1.	Continuous CCH access		6.3.1	O	
M3.	Operation on SCH	( )[c]	5.2	O4	
M3.1.	Continuous SCH access		6.3.1	O	
M4.	Mixed operation		5.2	O	
M4.1.	Immediate access		6.3.3	O	
M4.2.	Alternating access		6.3.2	O	
M4.2.1.	Use common time reference		5.2.2, 6.2.1	M	
M4.2.1.1.	Derive timing from GPS		6.2.3	O5	
M4.2.1.2.	Derive timing from Timing Advertisement frame		6.2.3	O5	
M4.2.1.3.	Derive timing from other timing source	( )[d]	6.2.3	O5	
M4.2.2.	Guard interval on transmit		6.2.5	M	
M4.2.3.	Medium busy at end of guard interval		6.2.5	M	
M5.	Transmit		5.3.2	O2	
M5.1.	EDCA and user priority		5.4	M	
M5.2.	Cancel transmissions		5.3.2	O	
M5.3.	Send TA		6.2.6	O	
M5.4.	Send other IEEE 802.11 frames	( )[e]	6.4	O	
M5.5.	Send WSM		5.3.3	O3	
M5.5.1.	Expiry time		5.3.3	O	
M5.6.	Send IPv6		5.3.4	O3	
M6.	Receive		5.3.5	O2	
M6.1.	Receive TA		6.2.7	O	
M6.2.	Receive WSM		5.3.3	O3	
M6.3.	Receive IPv6		5.3.4	O3	
M7.	Device readdressing		6.6	O	
M8.	MIB maintenance		6.5	—	
M8.1.	Managed WAVE device		3.1, 6.5	O	
M8.2.	IEEE 1609.4 MIB per Annex E		6.5	M8.1: M	
M8.3.	Other MIB	( )[f]	6.5	O	

[a] Enter number of simultaneous channels supported.
[b] List supported control channel(s), and operating class.
[c] List supported service channel(s), and operating class.
[d] Indicate device's timing source(s).
[e] Enter IEEE 802.11 management frames/service request primitives supported.
[f] Enter references to other management information bases supported.

Table B.3: PICS of an Implementation of IEEE 1609.3 [3]

Item	Feature	Value	IEEE 1609.3 [3]	Status	Support
N1.	**DATA PLANE**		—	—	
N1.1.	LLC		5.2	M	
N1.1.1.	LLC extensions for WSMP		7.5	N1.3:M	
N1.2.	IPv6		5.3, 6.4	O1	
N1.2.1.	Use stateless configuration		6.4	O	
N1.2.2.	IP readdressing		6.4.2	M	
N1.2.3.	Send IP datagrams		5.3	O2	
N1.2.4.	Receive IP datagrams		5.3	O2	
N1.2.4.1.	Receive by link-local address		6.4	M	
N1.2.4.2.	Receive by global address		6.4	M	
N1.2.4.3.	Receive by host multicast addresses		6.4	O3	
N1.2.4.4.	Receive by router multicast addresses		6.4	O3	
N1.2.5.	UDP		5.4	O	
N1.2.6.	TCP		5.4	O	
N1.2.7.	Other IETF protocols	( )[a]	5.4	O	
N1.3.	WSMP		5.5	O1	
N1.3.1.	WSM reception		5.5.3	O4	
N1.3.1.1.	Check WSMP Version number	( )[b]	5.5.3, 8.3.2	M	
N1.3.1.2.	Check Subtype field	( )[r]	5.5.3, 8.3.2	M	
N1.3.1.3.	Check TPID field	( )[s]	5.5.3, 8.3.2	M	
N1.3.1.4.	WAVE Info Elem Extension field		8.1.1	M	
N1.3.1.5.	Deliver message based on Address Info (PSID)		5.5.3	M	
N1.3.2.	WSM transmission		5.5.2	O4	
N1.3.2.1.	Insert WSMP Version number		8.3.2	M	
N1.3.2.2.	Insert Address Info (PSID)		8.3.3	M	
N1.3.2.3.	Outbound message size	( )[c]	5.5.2	M	
N1.3.2.4.	Transmit channel number		8.3.4.2	O	
N1.3.2.5.	Transmit data rate		8.3.4.3	O	
N1.3.2.6.	Transmit Power Used		8.3.4.4	O	
N1.3.2.7.	Channel Load		8.3.4.5	O	
N1.3.2.8.	Insert Subtype features	( )[r]	8.3.2	M	
N1.3.2.9.	Insert TPID features	( )[s]	8.3.2	M	

Table B.3: PICS of an Implementation of IEEE 1609.3 [3] Cont'd

Item	Feature	Value	IEEE 1609.3 [3]	Status	Support
N2.	**MANAGEMENT PLANE**		—	—	
N2.1.	User role		6.2.1	O	
N2.1.1.	Receive WSAs over WSMP		6.3.2	O5	
N2.1.2.	Verify and accept Secured WSA		6.3.3, 8.2.1	O5	
N2.1.3.	Accept Unsecured WSA		6.3.3, 8.2.1	O5	
N2.1.4.	WAVE Info Elem Extension fields		8.1.1	M	
N2.1.5.	Calculate avail service link quality		6.3.4	O	
N2.1.6.	WSA header		8.2.2	M	
N2.1.6.1.	Check WSA Version number	( )[d]	8.2.2.2	M	
N2.1.6.2.	Check WSA Identifier		8.2.2.4	O	
N2.1.6.3.	Check Content Count		8.2.2.5	O	
N2.1.6.4.	WSA header Info Element Ext field		8.2.2.6	M	
N2.1.6.4.1.	Repeat Rate		8.2.2.6.1	O	
N2.1.6.4.2.	2DLocation		8.2.2.6.2	O	
N2.1.6.4.3.	3DLocation		8.2.2.6.3	O	
N2.1.6.4.4.	Advertiser Identifier		8.2.2.6.4	O	
N2.1.6.4.5.	Other info elements	( )[e]	8.2.2.6	O	
N2.1.7.	Service Info Segment		8.2.3	M	
N2.1.7.1.	Number of Service Info Instances	( )[f]	8.2.3	M	
N2.1.7.2.	WAVE Information Element Extension		8.2.3.5	M	
N2.1.7.2.1.	PSC		8.2.3.5.1	O	
N2.1.7.2.2.	IPv6 Address		8.2.3.5.2	O	
N2.1.7.2.3.	Service Port		8.2.3.5.3	O	
N2.1.7.2.4.	Provider MAC Address		8.2.3.5.4	O	
N2.1.7.2.5.	RCPI Threshold		8.2.3.5.5	O	
N2.1.7.2.6.	WSA Count Threshold		8.2.3.5.6	O	
N2.1.7.2.6.1.	WSA Count Threshold Interval		8.2.3.5.7	O	
N2.1.7.2.7.	Other info elements	( )[g]	8.2.3.5	O	
N2.1.8.	Channel Info Segment		8.2.4	M	
N2.1.8.1.	Number of Channel Info Instances	( )[h]	8.2.4	M	
N2.1.8.2.	WAVE Info Elem Extension field		8.2.4.8	M	
N2.1.8.2.1.	EDCA Parameter Set		8.2.4.8.1	O	
N2.1.8.2.2.	Channel Access		8.2.4.8.2	O	
N2.1.8.2.3.	Other info elements	( )[i]	8.2.4.8	O	

Table B.3: PICS of an Implementation of IEEE 1609.3 [3] Cont'd

Item	Feature	Value	IEEE 1609.3 [3]	Status	Support
N2.1.9.	WAVE Router Advertisement		8.2.5.1	O	
N2.1.9.1.	WAVE Info Elem Extension field		8.2.5.7	M	
N2.1.9.1.1.	Secondary DNS		8.2.5.7.1	O	
N2.1.9.1.2.	Gateway MAC Address		8.2.5.7.2	O	
N2.1.9.1.3.	Other info elements	( )[j]	8.2.5.7	O	
N2.2.	Provider role		6.2.1	O	
N2.2.1.	Send Service Advertisements over WSMP		6.2.3.3	M	
N2.2.1.1.	Send Secured WSA		6.2.4.2.1, 8.2.1	O6	
N2.2.1.2.	Send Unsecured WSA		6.2.4.2.1, 8.2.1	O6	
N2.2.2.	Send repeated advertisements		6.2.4.2.1	O	
N2.2.3.	Change ongoing advertisements		6.2.2.2, 6.2.4.2.2	O	
N2.2.4.	Delete application-service		6.2.3.6	O	
N2.2.5.	WSA header		8.2.2	M	
N2.2.5.1.	Set WSA Version		8.2.2.2	M	
N2.2.5.2.	Set WSA Identifier		8.2.2.4	M	
N2.2.5.3.	Set Content Count		8.2.2.5	M	
N2.2.6.	WSA header Info Element Ext field		8.2.2.6	M	
N2.2.6.1.	Repeat Rate		8.2.2.6.1	O	
N2.2.6.2.	2DLocation		8.2.2.6.2	O	
N2.2.6.3.	3DLocation		8.2.2.6.3	O	
N2.2.6.4.	Advertiser Identifier		8.2.2.6.4	O	
N2.2.6.5.	Other info elements	( )[k]	8.2.2.6	O	
N2.2.7.	Service Info Segment		8.2.3	M	
N2.2.8.	Number of Service Info Instances	( )[l]	8.2.3	M	
N2.2.9.	WAVE Info Elem Extension field		8.2.3.5	O	
N2.2.9.1.	PSC		8.2.3.5.1	O	
N2.2.9.2.	IPv6 Address		8.2.3.5.2	O	
N2.2.9.3.	Service Port		8.2.3.5.3	O	
N2.2.9.4.	Provider MAC Address		8.2.3.5.4	O	
N2.2.9.5.	RCPI Threshold		8.2.3.5.5	O	
N2.2.9.6.	WSA Count Threshold		8.2.3.5.6	O	
N2.2.9.6.1.	WSA Count Threshold Interval		8.2.3.5.7	O	
N2.2.9.7.	Other info elements	( )[m]	8.2.3.5	O	

Table B.3: PICS of an Implementation of IEEE 1609.3 [3] Cont'd

Item	Feature	Value	IEEE 1609.3 [3]	Status	Support
N2.2.10.	Channel Info Segment		8.2.4	M	
N2.2.11.	Number of Channel Info Instances	( )[n]	8.2.4	M	
N2.2.12.	WAVE Info Elem Extension field		8.2.4.8	O	
N2.2.12.1.	EDCA Parameter Set		8.2.4.8.1	O	
N2.2.12.2.	Channel Access		8.2.4.8.2	O	
N2.2.12.3.	Other info elements	( )[o]	8.2.4.8	O	
N2.2.13.	Send WRA		8.2.5	O	
N2.2.13.1.	WAVE Info Elem Extension field		8.2.5.7	O	
N2.2.13.1.1.	Secondary DNS		8.2.5.7.1	O	
N2.2.13.1.2.	Gateway MAC address		8.2.5.7.2	O	
N2.2.13.1.3.	Other info elements	( )[p]	8.2.5.7	O	
N2.3.	Timing advertisement		—		
N2.3.1.	Timing Advertisement generation		6.2.4.3	O	
N2.4.	MIB maintenance		6.5	—	
N2.4.1.	Managed WAVE device		6.5	O	
N2.4.2.	MIB per standard		6.5	N2.4.1: M	
N2.4.3.	Other MIB	( )[q]	6.5	O	

[a] List protocols supported.
[b] List version numbers supported.
[c] Enter maximum WAVE Short Message length.
[d] List version numbers supported.
[e] List any other WSA header WAVE Information Elements processed on reception.
[f] Enter maximum number of Service Info Instances processed on reception.
[g] List any other Service Info Segment WAVE Information Elements processed on reception.
[h] Enter maximum number of Channel Info Instances processed on reception.
[i] List any other Channel Info Segment WAVE Information Elements processed on reception.
[j] List any other WAVE routing advertisement WAVE Information Elements processed on reception.
[k] List any other WSA header WAVE Information Elements supported on transmission.
[l] Enter maximum number of Service Info Instances supported on transmission.
[m] List any other Service Info Segment WAVE Information Elements supported on transmission.
[n] Enter maximum number of Channel Info Instances supported on transmission.
[o] List any other Channel Info Segment WAVE Information Elements supported on transmission.
[p] List any other WAVE routing advertisement WAVE Information Elements supported on transmission.
[q] List any other MIBs supported.
[r] List Subtype values supported.
[s] List TPID values supported.

Table B.4: PICS of an Implementation of IEEE 1609.2 [6]

Item	Security configuration (top-level)	IEEE 1609.2 [6]	Status	Support
Security Services (A.2.3.1 [6])				
S1.	Support secure data service		O1	
S1.1.	**Secure data exchange entity (SDEE) identification**	4.2.2.1	S1: M	
S1.1.1.	Support only one SDEE	4.2.2.1	S1.1: C1	
S1.1.2.	Distinguish between SDEEs	4.2.2.1	S1.1: C1	
S1.2.	**Generate secured protocol data unit (SPDU)**		S1: O2	
S1.2.1.	Create Ieee1609Dot2Data containing unsecured data	4.2.2.2.2	S1.2: O3	
S1.2.2.	Create Ieee1609Dot2Data containing valid SignedData	4.2.2.2.3, 5.2, 5.3.1, 5.3.3, 5.3.7, 6.3.4, 6.3.9, 9.3.9.1	S1.2: O3	
S1.2.2.1.	Using a valid HashAlgorithm	6.3.5	S1.2.2: M	
S1.2.2.1.1.	Support signing with hash algorithm SHA-256	6.3.5	S1.2.2: M	
S1.2.2.1.2.	Support signing with hash algorithm other than SHA-256	6.3.5	S1.2.2: O	
S1.2.2.2.	Containing a Signed Data payload	6.3.6	S1.2.2: M	
S1.2.2.2.1.	… with payload containing data	6.3.7	S1.2.2.2: O4	
S1.2.2.2.2.	… with payload containing extDataHash	6.3.7	S1.2.2.2: O4	
S1.2.2.2.3.	… with generationTime in the security headers	6.3.9, 6.3.11	S1.2.2.2: O	
S1.2.2.2.4.	… with expiryTime in the security headers	6.3.9, 6.3.11	S1.2.2.2: O	
S1.2.2.2.5.	… with generationLocation in the security headers	6.3.9, 6.3.12	S1.2.2.2: O	
S1.2.2.2.6.	… with p2pcdLearningRequest in the security headers	6.3.9, 6.3.25	S1.2.2.2: O	
S1.2.2.2.7.	… with missingCrlIdentifier in the security headers	6.3.9, 6.3.16	S1.2.2.2: O	
S1.2.2.2.8.	… with encryptionKey in the security headers	6.3.9, 6.3.18	S1.2.2.2: O	
S1.2.2.2.8.1.	… … with a PublicEncryptionKey 6.3.9,	6.3.18, 6.3.19	S1.2.2.2.8: O	
S1.2.2.2.8.2.	… … with a SymmetricEncryptionKey	6.3.9, 6.3.18, 6.3.20	S1.2.2.2.8: O5	
S1.2.2.3.	Support a SignerIdentifier	6.3.24	S1.2.2: M	
S1.2.2.3.1.	… of type digest	6.3.26	S1.2.2.3: O6	
S1.2.2.3.2.	… of type certificate	6.4.2	S1.2.2.3: O6	

Table B.4: PICS of an Implementation of IEEE 1609.2 [6] Cont'd

Item	Security configuration (top-level)	IEEE 1609.2 [6]	Status	Support
Security Services (A.2.3.1 [6])				
S1.2.2.3.2.1.	… … maximum number of Certificates in the chain	5.1.2.2	S1.2.2.3.2. 8: M > 8: O	Enter number: ( )
S1.2.2.3.3.	… of type self	6.3.24	S1.2.2.3: O6	
S1.2.2.4.	Support a Signature	6.3.28	S1.2.2: M	
S1.2.2.4.1.	… a ecdsa256Signature	6.3.29	S1.2.2.4: M	
S1.2.2.4.1.1.	… … using NIST p256	6.3.29	S1.2.2.4.1: O7	
S1.2.2.4.1.2.	… … using Brainpool p256r1	6.3.29	S1.2.2.4.1: O7	
S1.2.2.4.1.3.	… … with a x-only *r* value	6.3.23	S1.2.2.4.1: O8	
S1.2.2.4.1.4.	… … with a compressed *r* value	6.3.23	S1.2.2.4.1: O8	
S1.2.2.4.1.5.	… … with an uncompressed *r* value	6.3.23	S1.2.2.4.1: O8	
S1.2.2.5.	Determine that certificate used to sign data is valid (part of a consistent chain, valid at the current time and location, hasn't been revoked)	5.2, 6.4.2	S1.2.2: M	
S1.2.2.5.1.	Determine that the region is correct	6.4.8, 6.4.17	S1.2.2.5: O	
S1.2.2.5.1.1.	Support a circularRegion	6.4.17, 6.4.18	S1.2.2.5.1: O9	
S1.2.2.5.1.2.	Support a rectangularRegion	6.4.17, 6.4.20	S1.2.2.5.1: O9	
S1.2.2.5.1.2.1.	Maximum number of rectangularRegions supported	6.4.17, 6.4.20	S1.2.2.5.1.2 8: M > 8: O	Enter number: ( )
S1.2.2.5.1.3.	Support a polygonalRegion	6.4.17, 6.4.21	S1.2.2.5.1: O9	
S1.2.2.5.1.3.1.	Maximum number of points in a polygonalRegion	6.4.17, 6.4.21	S1.2.2.5.1.3 8: M > 8: O	Enter number: ( )
S1.2.2.5.1.4.	Support identifiedRegion	6.4.17, 6.4.22	S1.2.2.5.1: O9	
S1.2.2.5.1.4.1.	Maximum number of identifiedRegions supported	6.4.17, 6.4.22	S1.2.2.5.1.4: 8: M > 8: O	Enter number: ( )
S1.2.2.5.1.4.2.	Support IdentifiedRegion of type CountryOnly	6.4.22, 6.4.23	S1.2.2.5.1.4: O10	
S1.2.2.5.1.4.3.	Support IdentifiedRegion of type CountryAndRegions	6.4.22, 6.4.24	S1.2.2.5.1.4: O10	
S1.2.2.5.1.4.4.	Support IdentifiedRegion of type CountryAndSubregions	6.4.22, 6.4.25	S1.2.2.5.1.4: O10	

Table B.4: PICS of an Implementation of IEEE 1609.2 [6] Cont'd

Item	Security configuration (top-level)	IEEE 1609.2 [6]	Status	Support
Security Services (A.2.3.1 [6])				
S1.2.2.5.2.	Determine that the certificate has the proper appPermissions	6.4.8, 6.4.28	S1.2.2.5: O	
S1.2.2.5.2.1.	Maximum number of PsidSsp in the appPermissions sequence	6.4.8, 6.4.28	S1.2.2.5.2 8: M > 8: O	Enter number: ( )
S1.2.2.6.	Determine that key and certificate used to sign are a valid pair	5.3.7	S1.2.2: M	
S1.2.2.7.	Support signing with explicit certificates	6.4.6	S1.2.2.5: O11	
S1.2.2.8.	Support signing with implicit certificates	5.3.2, 6.4.5	S1.2.2.5: O11	
S1.2.2.9.	Generate elliptic curve digital signature algorithm (ECDSA) keypairs using a high-quality random number generator	5.3.6	S1.2.2.4.1: M	
S1.2.3.	Create Ieee1609Dot2Data containing EncryptedData	4.2.2.3.2, 5.3.4, 6.3.30	S1.2: O2	
S1.2.3.1.	Generate Elliptic Curve Integrated Encryption Scheme (ECIES) ephemeral keypairs using a high-quality random number generator	5.3.4, 5.3.5, 5.3.6	S1.3.3: M	
S1.2.3.2.	Maximum number of recipients supported	6.3.30	S1.2.3 8:M > 8: O	Enter number: ( )
S1.2.3.3.	Containing PreSharedKeyRecipientInfo	6.3.31, 6.3.1	S1.2.3.2: O12	
S1.2.3.3.1.	Containing symmRecipientInfo	6.3.31, 6.3.2	S1.2.3.2: O12	
S1.2.3.3.2.	Containing certRecipientInfo	6.3.31, 6.3.3	S1.2.3.2: O12	
S1.2.3.3.3.	Containing signedDataRecipientInfo	6.3.31, 6.3.3	S1.2.3.2: O12	
S1.2.3.3.4.	Containing rekRecipientInfo	6.3.31, 6.3.3	S1.2.3.2: O12	
S1.2.3.4.	Support public-key encryption	6.3.5	S1.2.3: O13	
S1.2.3.4.1.	… using ECIES-256	6.3.5	S1.2.3.4: M	
S1.2.3.4.1.1.	… … using NIST p256	6.3.5	S1.2.3.4.1: O14	
S1.2.3.4.1.2.	… … using Brainpool p256r1	6.3.5	S1.2.3.4.1: O14	
S1.2.3.4.1.3.	Support encrypting to an uncompressed encryption key	6.3.18	S1.2.3.4.1: O15	
S1.2.3.4.1.4.	Support encrypting to a compressed encryption key	6.3.18	S1.2.3.4.1: O15	
S1.2.3.4.1.5.	Support encrypting to an encryption key included in an explicit cert	6.3.18	S1.2.3.4.1: O16	
S1.2.3.4.1.6.	Support encrypting to an encryption key included in an implicit cert	6.3.18	S1.2.3.4.1: O16	

Table B.4: PICS of an Implementation of IEEE 1609.2 [6] Cont'd

Item	Security configuration (top-level)	IEEE 1609.2 [6]	Status	Support
Security Services (A.2.3.1 [6])				
S1.2.3.4.2.	… using a different algorithm introduced at a later date	6.3.6	S1.2.3.4: O	
S1.2.3.5.	Support symmetric encryption	6.3.7	S1.2.3: O13	
S1.2.3.5.1.	… using AES-128	5.3.8, 6.3.7	S1.2.3.5: M	
S1.2.3.5.2.	… using a different algorithm introduced at a later date	6.3.3	S1.2.3.5: O	
S1.3.	**Receive secured protocol data unit (SPDU)**		S1: O2	
S1.3.1.	Support preprocessing SPDUs	4.2.2.3.1	S1.3.2.3.1, S3.2 S3.3: M	
S1.3.2.	Verify Ieee1609Dot2Data containing SignedData	4.2.2.3.2, 5.2, 5.3.1, 5.3.3, 5.3.7, 6.3.4, 6.3.9	S1.3: O17	
S1.3.2.1.	Using a valid HashAlgorithm		S1.3.2: M	
S1.3.2.1.1.	Verify signed data using HashAlgorithm SHA-256	6.3.5	S1.3.2.1: M	
S1.3.2.1.2.	Verify signed data using a HashAlgorithm other than SHA-256	6.3.5	S1.3.2.1: O	
S1.3.2.2.	Containing a Signed Data payload	6.3.6	S1.3.2: M	
S1.3.2.2.1.	… with payload containing data	6.3.7	S1.3.2.2: O18	
S1.3.2.2.2.	… with payload containing extDataHash	6.3.7	S1.3.2.2: O18	
S1.3.2.2.3.	… with generationTime in the security headers	6.3.9, 6.3.11	S1.3.2.2: O	
S1.3.2.2.4.	… with expiryTime in the security headers	6.3.9, 6.3.11	S1.3.2.2: O	
S1.3.2.2.5.	… with generationLocation in the security headers	6.3.9, 6.3.12	S1.3.2.2: O	
S1.3.2.2.6.	… with missingCertIdentifier in the security headers	6.3.9, 6.3.25	S1.3.2.2: O	
S1.3.2.2.7.	… with missingCrlIdentifier in the security headers	6.3.9, 6.3.16	S1.3.2.2: O	
S1.3.2.2.8.	… with encryptionKey in the security headers	6.3.9, 6.3.18	S1.3.2.2: O	
S1.3.2.2.8.1.	… … with a PublicEncryptionKey	6.3.9, 6.3.18, 6.3.19	S1.3.2.2.8: O19	
S1.3.2.2.8.2.	… … with a SymmetricEncryptionKey	6.3.9, 6.3.18, 6.3.20	S1.3.2.2.8: O19	

Table B.4: PICS of an Implementation of IEEE 1609.2 [6] Cont'd

Item	Security configuration (top-level)	IEEE 1609.2 [6]	Status	Support
Security Services (A.2.3.1 [6])				
S1.3.2.3.	Support a SignerIdentifier	6.3.24	S1.3.2: M	
S1.3.2.3.1.	… of type digest	6.3.26	S1.3.2.3: O20	
S1.3.2.3.2.	… of type certificate	6.4.2	S1.3.2.3: O20	
S1.3.2.3.2.1.	… … maximum number of Certificates in the chain	5.1.2.2	S1.3.2.3.2 1: M > 1: O	Enter number: ( )
S1.3.2.3.3.	… of type self		S1.3.2.3: O20	
S1.3.2.4.	Support a Sig nature	6.3.28	S1.3.2: M	
S1.3.2.4.1.	… a ecdsa256Signature	6.3.29	S1.3.2.4:M	
S1.3.2.4.1.1.	… … using NIST p256	6.3.29	S1.3.2.4.1: O21	
S1.3.2.4.1.2.	… … using Brainpool p256r1	6.3.29	S1.3.2.4.1: O21	
S1.3.2.4.1.3.	… … with a x-only *r* value	6.3.23	S1.3.2.4.1: O22	
S1.3.2.4.1.4.	… … with a compressed *r* value	6.3.23	S1.3.2.4.1: O22	
S1.3.2.4.1.5	… … with a compressed *r* value and fast verification	6.3.23	S1.3.2.4.1: O22	
S1.3.2.4.1.6.	… … with a uncompressed *r* value	6.3.23	S1.3.2.4.1: O22	
S1.3.2.4.1.7.	… … with a uncompressed *r* value and fast verification	6.3.23	S1.3.2.4.1: O22	
S1.3.2.5.	SignedData verification fails if the certificate is not valid (part of a consistent chain, valid at the current time and location, hasn't been revoked)	5.2, 6.4.2	S1.3.2: M	
S1.3.2.5.1.	Reject data based on generation location being inconsistent with certificate	6.4.8, 6.4.17	S1.3.2.5: O	
S1.3.2.5.1.1.	… using a circularRegion	6.4.17, 6.4.18	S1.3.2.5.1: O23	
S1.3.2.5.1.2.	Support a rectangularRegion	6.4.17, 6.4.20	S1.3.2.5.1: O23	
S1.3.2.5.1.3.	Maximum number of rectangularRegions supported	6.4.17, 6.4.20	S1.3.2.5.1.2 8: M > 8: O	Enter number: ( )
S1.3.2.5.1.4.	Support a polygonalRegion	6.4.17, 6.4.21	S1.3.2.5.1: O23	
S1.3.2.5.1.5.	Maximum number of points in a polygonalRegion	6.4.17, 6.4.21	S1.3.2.5.1.4 8: M > 8: O	Enter number: ( )
S1.3.2.5.1.6.	Support identifiedRegion	6.4.17, 6.4.22	S1.3.2.5.1 8: M > 8: O	Enter number: ( )

Table B.4: PICS of an Implementation of IEEE 1609.2 [6] Cont'd

Item	Security configuration (top-level)	IEEE 1609.2 [6]	Status	Support
Security Services (A.2.3.1 [6])				
S1.3.2.5.1.6.1.	Maximum number of identifiedRegions supported	6.4.17, 6.4.22	S1.3.2.5.1.6: 8: M > 8: O	Enter number: ( )
S1.3.2.5.1.6.2.	Support IdentifiedRegion of type CountryOnly	6.4.22, 6.4.23	S1.3.2.5.1.6: O24	
S1.3.2.5.1.6.3.	Support IdentifiedRegion of type CountryAndRegions	6.4.22, 6.4.24	S1.3.2.5.1.6: O24	
S1.3.2.5.1.6.4.	Support IdentifiedRegion of type CountryAndSubregions	6.4.22, 6.4.25	S1.3.2.5.1.6: O24	
S1.3.2.5.1.7.	Maximum number of identifiedRegions supported	6.4.17, 6.4.22	S1.3.2.5.1.6 8:M > 8: O	Enter number: ( )
S1.3.2.5.2.	Reject data if the certificate does not have the proper appPermissions	6.4.8, 6.4.28	S1.3.2.5: O	
S1.3.2.5.3.	Maximum number of PsidSsp in the appPermissions sequence	6.4.8, 6.4.28	S1.3.2.5 8: O > 8: O	Enter number: ( )
S1.3.2.5.4.	Determine that the assuranceLevel is an acceptable level	6.4.8, 6.4.27	S1.3.2.5: O	
S1.3.2.6.	Support verifying SPDUs signed with explicit authorization certificates	6.4.5	S1.3.2: O25	
S1.3.2.7.	Support verifying SPDUs signed with implicit authorization certificates	5.3.2, 6.4.5	S1.3.2: O25	
S1.3.2.8.	Support explicit certificate authority (CA) certificates	6.4.2, 6.4.6	S1.3.2: M	
S1.3.2.9.	Support receiving implicit CA certificates	6.4.2, 6.4.5	S1.3.2: O	
S1.3.2.10.	SignedData verification fails in the following circumstances:	6.3.4	S1.3.2: M	
S1.3.2.10.1.	… SPDU-Parsing: Invalid Input	6.3.4	S1.3.2.10: M	
S1.3.2.10.2.	… SPDU-Parsing: Unspported critical information field	6	S1.3.2.10: M	
S1.3.2.10.3.	… SPDU-Parsing: Certificate not found	4.3, 6.3.13, 6.3.14, 6.3.15	S1.3.2.10: M	
S1.3.2.10.4.	… SPDU-Parsing:Generation time not available	4.3, 6.3.13, 6.3.14, 6.3.15	S1.3.2.10: M	
S1.3.2.10.5.	… SPDU-Parsing:Generation location not available	4.3, 6.3.13, 6.3.14, 6.3.15	S1.3.2.10: M	
S1.3.2.10.6.	… SPDU-Certificate-Chain: Not enough information to construct chain	5.1.2	S1.3.2.10: M	
S1.3.2.10.7.	… SPDU-Certificate-Chain: Chain ended at untrusted root	5.1.2	S1.3.2.10: M	

Table B.4: PICS of an Implementation of IEEE 1609.2 [6] Cont'd

Item	Security configuration (top-level)	IEEE 1609.2 [6]	Status	Support
Security Services (A.2.3.1 [6])				
S1.3.2.10.8.	… SPDU-Certificate-Chain: Chain was too long for implementation	5.1.2	S1.3.2.10: M	
S1.3.2.10.9.	… SPDU-Certificate-Chain: Certificate revoked	5.1.2	S1.3.2.10: M	
S1.3.2.10.10.	… SPDU-Certificate-Chain: Overdue CRL	5.1.2	S1.3.2.10: M	
S1.3.2.10.11.	… SPDU-Certificate-Chain: Inconsistent expiry times	5.1.2	S1.3.2.10: M	
S1.3.2.10.12.	… SPDU-Certificate-Chain: Inconsistent start times	5.1.2	S1.3.2.10: M	
S1.3.2.10.13.	… SPDU-Certificate-Chain: Inconsistent chain permissions	5.1.2	S1.3.2.10: M	
S1.3.2.10.14.	… SPDU-Crypto: Verification failure	5.3.1	S1.3.2.10: M	
S1.3.2.10.15.	… SPDU-Consistency: Future certificate at generation time	5.2.3	S1.3.2.10:M	
S1.3.2.10.16.	… SPDU-Consistency: Expired certificate at generation time	5.2.3	S1.3.2.10: M	
S1.3.2.10.17.	… SPDU-Consistency: Expiry date too early	5.2.3	S1.3.2.10:M	
S1.3.2.10.18.	… SPDU-Consistency: Expiry date too late	5.2.3	S1.3.2.10: M	
S1.3.2.10.19.	… SPDU-Consistency: Generation location outside validity region	5.2.3	S1.3.2.10: M	
S1.3.2.10.20.	… SPDU-Consistency: Unauthorized PSID	5.2.3	S1.3.2.10: M	
S1.3.2.10.21.	… SPDU-Internal-Consistency: Expiry time before generation time	6.4.8, 6.4.14, 5.2.3	S1.3.2.10: M	
S1.3.2.10.22.	… SPDU-Internal-Consistency: extDataHash doesn't match	5.2.3	S1.3.2.10: M	
S1.3.2.10.23.	… SPDU-Local-Consistency: PSIDs don't match	5.2.3	S1.3.2.10: O	
S1.3.2.10.24.	… SPDU-Local-Consistency: Chain was too long for SDEE	5.2.3	S1.3.2.10: M	
S1.3.2.10.25.	… SPDU-Relevance: SPDU Too Old	5.2.4	S1.3.2.10: O	
S1.3.2.10.26.	… SPDU-Relevance: Future SPDU	5.2.4	S1.3.2.10: O	
S1.3.2.10.27.	… SPDU-Relevance: Expired SPDU	5.2.4	S1.3.2.10: O	
S1.3.2.10.28.	… SPDU-Relevance: SPDU Too Distant	5.2.4	S1.3.2.10: O	
S1.3.2.10.29.	… SPDU-Relevance: Replayed SPDU	5.2.4	S1.3.2.10: O	

Table B.4: PICS of an Implementation of IEEE 1609.2 [6] Cont'd

Item	Security configuration (top-level)	IEEE 1609.2 [6]	Status	Support
Security Services (A.2.3.1 [6])				
S1.3.3.	Decrypt Ieee1609Dot2Data containing EncryptedData	4.2.2.3.3, 5.3.5, 6.3.30	S1.3: O17	
S1.3.3.1.	Generate ECIES keypairs using a high-quality random number generator	5.3.4, 5.3.5, 5.3.6	S1.3.3: M	
S1.3.3.2.	Maximum number of RecipientInfos supported in an incoming EncryptedData	6.3.30	S1.3.3: 8: M > 8: O	Enter number: ( )
S1.3.3.2.1.	Containing symmRecipientInfo	6.3.31, 6.3.1	S1.3.3.2: O26	
S1.3.3.2.2.	Containing certRecipientInfo	6.3.31, 6.3.3	S1.3.3.2: O26	
S1.3.3.2.3.	Containing signedDataRecipientInfo	6.3.31, 6.3.3	S1.3.3.2: O26	
S1.3.3.2.4.	Containing rekRecipientInfo	6.3.31, 6.3.3	S1.3.3.2: O26	
S1.3.3.3.	Support decrypting using a public-key algorithm	6.3.5	S1.3.3: O27	
S1.3.3.3.1.	… using ECIES-256	6.3.5	S1.3.3.3: M	
S1.3.3.3.1.1.	… … using NIST p256	6.3.5	S1.3.3.3: O28	
S1.3.3.3.1.2.	… … using Brainpool p256r1	6.3.5	S1.3.3.3: O28	
S1.3.3.3.2.	… using a different algorithm introduced at a later date	6.3.6	S1.3.3.3: O	
S1.3.3.4.	Support decrypting using a symmetric algorithm	6.3.7	S1.3.3: O27	
S1.3.3.4.1.	... using AES-128	6.3.7	S1.3.3.4: M	
S1.3.3.4.2.	… using a different algorithm introduced at a later date	6.3.3	S1.3.3.4: O	
Certificate Revocation List (CRL) Verification Entity (A.2.3.2 [6])				
S2.	Support CRL Validation Entity	7	O1	
S2.1.	Correctly verify received CRL	7.4	S2: M	
S2.1.1.	…using hash ID-based revocation	5.1.3.5	S2.1: O29	
S2.1.1.1.	… of type fullHashCrl	7.3.2	S2.1.1: M	
S2.1.1.2.	… of type delta HashCrl	7.3.2	O	
S2.1.2.	… using linkage-based revocation	5.1.3.4	S2.1: O29	
S2.1.2.1.	… of type fullLinkedCrl	7.3.2	S2.1.2: M	
S2.1.2.2.	… of type delta LinkedCrl	7.3.2	O	
S2.1.2.3.	… containing individual linkage values	7.3.6	S2.1.2: M	
S2.1.2.4.	… containing group linkage values	7.3.6	O	

Table B.4: PICS of an Implementation of IEEE 1609.2 [6] Cont'd

Item	Security configuration (top-level)	IEEE 1609.2 [6]	Status	Support
Peer-to-Peer Certificate Distribution (P2PCD) Functionality (A.2.3.3 [6])				
S3.	Support P2PCD	8	O	
S3.1.	Number of supported SDEEs	8.2.6	S3.2: 1: O > 1: O	Enter number: ( )
S3.2.	**Support SSME and SDS operations for P2PCD in the requester role**	8.2.4.1	S3:O30	
S3.2.1.	Under at least one condition, trigger request processing on receiving a trigger SPDU	8.2.4.1	S3.2: M	Enter description of at least one condition under which request processing is triggered ( )
S3.2.2.	Do not trigger request processing on receiving a trigger SPDU for which a request is already active	8.2.4.1	S3.2: M	
S3.2.3.	Number of simultaneously active P2PCD learning requests	8.2.4.1,8.2.6	S3.2: 1: O > 1: O	
S3.2.4.	When request processing is triggered, include a P2PCD learning request in the next SPDU for the trigger SDEE except in the following exception cases	8.2.4.1	S3.2: M	
S3.2.4.1.	Do not include a P2PCD learning request if a learning request for the same certificate has been received within **p2pcd_observedRequestTimeout**	8.2.4.1	S3.2.4: O	
S3.2.4.2.	Only include one P2PCD learning request no matter how many learning requests have been triggered	8.2.4.1	S3.2.4: M	
S3.2.5.	Receive notifications from a P2PCDE that a P2PCD learning response has been received and use those to update the list of known certificates.	8.2.4.1	S3.2: M	
S3.3.	**Support SSME and SDS operations for P2PCD in the responder role**	8.2.4.2	S3: O30	
S3.3.1.	Trigger response processing on receiving a P2PCD learning request	8.2.4.2		
S3.3.2.	Number of simultaneously active P2PCD learning responses	8.2.4.1, 8.2.6	S3.3: 1: O > 1: O	

Table B.4: PICS of an Implementation of IEEE 1609.2 [6] Cont'd

Item	Security configuration (top-level)	IEEE 1609.2 [6]	Status	Support
Peer-to-Peer Certificate Distribution (P2PCD) Functionality (A.2.3.3 [6])				
S3.3.3.	Do not trigger response processing if less than **p2pcd_responseActiveTimeout** has passed since last triggered	8.2.4.2	S3.3: M	
S3.3.4.	Trigger sending response after random backoff time unless threshold number of responses have been observed	8.2.4.2	S3.3: M	
S3.3.5.	Increment number of responses observed based on input from P2PCDE	8.2.4.2	S3.3: M	
S3.4.	**Support P2PCDE operations for P2PCD**	8.2.4.2	S3:O30	
S3.4.1.	Receive responses and provide to SSME	8.2.4.1, 8.2.4.2, 8.3.1	S3.4: M	
S3.4.2.	Send responses when triggered by SSME	8.2.4.2, 8.3.1	S3.4: O	
S3.4.3.	Send responses over WSMP	8.2.4.2	S3.4.2: M	