Ruckus Wireless™ SmartCell Gateway™ 200

Standard Compliance Report for SmartZone 3.4.1

Part Number 800-71381-001 Rev A
Published October 2016

www.ruckuswireless.com

Copyright Notice and Proprietary Information

Destination Control Statement

Technical data contained in this publication may be subject to the export control laws of the United States of America. Disclosure to nationals of other countries contrary to United States law is prohibited. It is the reader’s responsibility to determine the applicable regulations and to comply with them.

Disclaimer

THIS DOCUMENTATION AND ALL INFORMATION CONTAINED HEREIN (“MATERIAL”) IS PROVIDED FOR GENERAL INFORMATION PURPOSES ONLY. RUCKUS AND ITS LICENSORS MAKE NO WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, WITH REGARD TO THE MATERIAL, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT AND FITNESS FOR A PARTICULAR PURPOSE, OR THAT THE MATERIAL IS ERROR-FREE, ACCURATE OR RELIABLE. RUCKUS RESERVES THE RIGHT TO MAKE CHANGES OR UPDATES TO THE MATERIAL AT ANY TIME.

Limitation of Liability

IN NO EVENT SHALL RUCKUS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES, OR DAMAGES FOR LOSS OF PROFITS, REVENUE, DATA OR USE, INCURRED BY YOU OR ANY THIRD PARTY, WHETHER IN AN ACTION IN CONTRACT OR TORT, ARISING FROM YOUR ACCESS TO, OR USE OF, THE MATERIAL.

Trademarks

Ruckus Wireless, Ruckus, the bark logo, ZoneFlex, FlexMaster, ZoneDirector, SmartMesh, Channelfly, Smartcell, Dynamic PSK, and Simply Better Wireless are trademarks of Ruckus Wireless, Inc. in the United States and other countries. All other product or company names may be trademarks of their respective owners.

Contents

Index

About This Report

This *SmartCell Gateway™ (SCG) 200 Compliance Report* lists the 3GPP / RFC compliance test report for SCG. It contains the test topology and compliance matrix support for SCG.

This report is for service operators and system administrators who are responsible for managing, configuring, and troubleshooting Ruckus Wireless devices. Consequently, it assumes a basic working knowledge of local area networks, wireless networking, and wireless devices.

NOTE: This report assumes that the SmartCell Gateway has already been installed as described in the *Getting Started Guide*.

Most user guides and release notes are available in Adobe Acrobat Reader Portable Document Format (PDF) or HTML on the Ruckus Wireless Support Web site at https://support.ruckuswireless.com/contact-us.

Document Conventions

Table 1 and Table 2 list the text and notice conventions that are used throughout this guide.

Table 1. Text conventions

Convention	Description	Example
`monospace`	Represents information as it appears on screen	`[Device name]>`
`monospace bold`	Represents information that you enter	`[Device name]>` **`set ipaddr 10.0.0.12`**
default font bold	Keyboard keys, software buttons, and field names	On the **Start** menu, click **All Programs**.
italics	Screen or page names	Click **Advanced Settings.** The *Advanced Settings* page appears.

Table 2. Notice conventions

Notice Type	Description
NOTE	Information that describes important features or instructions
CAUTION!	Information that alerts you to potential loss of data or potential damage to an application, system, or device
WARNING!	Information that alerts you to potential personal injury

Terms Used

Table 3 lists the terms used in the compliance report.

Table 3. Terms used

Term	Description
Fully compliant	Implemented as specified in the section including optional aspects of the specification.
Compliant	Implemented all mandatory aspects of the functionality. Optional aspects may not be supported.
Partially compliant	Some aspects of the mandatory part have not been implemented.
Non-compliant	Not implemented as specified. If applicable, proprietary implementations are explained with a note.
Not applicable	Refers to requirements but is not relevant to this version of the SCG.
No requirement	Indicates that there are no requirements to be implemented or the section is empty.

Related Documentation

For a complete list of documents that accompany this release, refer to the Release Notes.

Online Training Resources

To access a variety of online Ruckus Wireless training modules, including free introductory courses to wireless networking essentials, site surveys, and Ruckus Wireless products, visit the Ruckus Wireless Training Portal at: https://training.ruckuswireless.com

Documentation Feedback

Ruckus Wireless is interested in improving its documentation and welcomes your comments and suggestions. You can email your comments to Ruckus Wireless at:

docs@ruckuswireless.com

When contacting us, please include the following information:

- Document title
- Document part number (on the cover page)
- Page number (if appropriate)

For example:

- SCG-200 Standard Compliance Report for SmartZone 3.4.1
- Part number: 800-71381-001
- Page 88

SCG and 3GPP Compliance Report 1

In this chapter:

Overview

This compliance report lists the 3GPP / RFC compliance test report for the SCG-200. It contains the test topology and compliance matrix support. This document shows the test results for all the supported features.

NOTE: Refer to About This Report for conventions used in this report.

NOTE: If the compliance statement is identical for all sections below a certain level, the sub-sections may not be itemized.

3GPP SCG to WLAN

Table 4 lists the 3GPP inter-working of the SCG to WLAN. This is based on 3GPP TS 22.234 compliance aspects.

Table 4. 3GPP SCG to WLAN

Section Number	Section Title	Support	Comments
1	Scope	No requirement	Informative
2	References	No requirement	Informative
3	Definitions and abbreviations	No requirement	Informative
3.1	Definitions	No requirement	Informative
3.2	Abbreviations	No requirement	Informative
4	General description	Compliant	UE requirements are out of scope for this report
5	High level requirements	No requirement	
5.1	Service principles	No requirement	
5.1.1	Numbering	Compliant	
5.1.2	USIM and UICC	Partially compliant	Complaint to SIM only
5.1.3	Roaming	Compliant	
5.1.4	Charging	Compliant	Supports off line charging
5.1.5	Subscription	Fully compliant	
5.1.6	Emergency calls	Not applicable	

Table 4. 3GPP SCG to WLAN

Section Number	Section Title	Support	Comments
5.1.7	Inter-working between PLMN and WLANs	No requirement	
5.1.7.1	General	Compliant	IPv6 does not support TTG calls. Service continuity is dependent on the core network.
5.1.7.2	Simultaneous connection to I-WLANs and 3GPP systems	Partially compliant	Simultaneous connection for PS and WLAN and depends on the core network and UE support. Does not support when a user tries using the same UICC/SIM credentials from different devices.
6	Service requirements	No requirement	
6.1	Network selection	Not applicable	Based on user equipment requirements
6.2	Operator determined barring	Not complaint	
6.3	Support of PS domain services	Compliant	QoS is not implemented in data path. *Best effort* approach is used.
6.4	Support for service continuity	Not applicable	
6.5	Support of LCS	Not applicable	To be supported in the future release
6.6	Support of IFOM	Not applicable	
7	Charging	Compliant	Supports off line charging

3GPP SCG to WLAN System Description

Table 5 lists the 3GPP inter-working of the SCG to WLAN as per the system description. This is based on 3GPP TS 23.234 compliance aspects.

Table 5. 3GPP SCG to WLAN system description

Section Number	Section Title	Support	Comments
1	Scope	No requirement	Informative
2	References	No requirement	Informative
3	Definitions, abbreviations and symbols	No requirement	Informative
3.1	Definitions	No requirement	Informative
3.2	Symbols	No requirement	Informative
3.3	Abbreviations	No requirement	Informative
4	WLAN radio networks inter-working with 3GPP	Fully compliant	Informative
5	High-level requirements and principles	No requirement	
5.1	Access control	Fully compliant	
5.1.1	WLAN impacts	Compliant	
5.1.2	Existing 3GPP element impacts	Compliant	Supports HLR. Diameter and HSS is not supported
5.1.3	Requirements for WLAN direct IP access	Fully compliant	
5.1.4	Requirements for WLAN 3GPP IP access	Compliant	Does not support Diameter
5.1.4.1	Requirement for private network access from WLAN 3GPP IP access	Fully compliant	
5.1.4.2	Requirements for support of IMS emergency calls	Not applicable	
5.1.5	WLAN access authorization	Compliant	
5.1.6	3GPP WLAN attach	Compliant	Supports HLR. HSS is not supported
5.2	Void	No requirement	
5.3	User identity	No requirement	Does not support Diameter

Table 5. 3GPP SCG to WLAN system description

Section Number	Section Title	Support	Comments
5.3.1	General	Fully compliant	
5.3.2	NAI username	Compliant	
5.3.3	NAI realm name	Fully compliant	
5.3.4	NAI decoration for roaming	Fully compliant	
5.3.5	NAI decoration for IMS emergency call service	Not applicable	
5.4	Network advertisement and selection	No requirement	
5.4.1	Description of the issue	Fully compliant	Does not support Diameter
5.4.2	I-WLAN access network advertisement and selection	No requirement	
5.4.2.1	Case of IEEE 802.11 WLANs	No requirement	
5.4.2.1.1	General	Fully compliant	
5.4.2.1.2	WLAN access network advertisement	Compliant	
5.4.2.1.3	I-WLAN access network selection	Compliant	
5.4.2.2	Case of other WLANs	No requirement	
5.4.3	PLMN advertisement and selection	No requirement	
5.4.3.1	General	Compliant	
5.4.3.2	Network advertisement	Compliant	
5.4.3.3	Network selection	Compliant	
5.5	Authentication methods	Compliant	
5.6	Service authorization principles for WLAN 3GPP IP Access	Fully compliant	
5.6.1	Accessing home network provided services	Compliant	
5.6.2	Accessing visited network provided services	Compliant	
5.6.3	External IP network selection	Compliant	
5.7	IP connectivity for WLAN 3GPP IP access	No requirement	
5.7.1	Principles	Compliant	
5.7.2	Tunneling requirements	Compliant	
5.7.3	Void	No requirement	

Table 5. 3GPP SCG to WLAN system description

Section Number	Section Title	Support	Comments
5.8	Roaming requirements for WLAN 3GPP IP access	Compliant	
5.9	Routing enforcement and policy enforcement for WLAN 3GPP IP access	No requirement	
5.9.1	Purpose for routing enforcement and policy enforcement	Partially Compliant	QoS is not implemented in data path
5.9.2	Routing enforcement in the WLAN AN	Compliant	
5.9.3	Routing and policy enforcement in HPLMN	Compliant	
5.9.4	Routing and policy enforcement in the VPLMN	Partially Compliant	
5.10	IP address allocation for the WLAN UE	No requirement	
5.10.1	General	Compliant	
5.10.2	Static and dynamic remote IP address	Compliant	
5.11	Charging	Partially Compliant	Supports off line charging
5.12	AAA protocol requirements	Compliant	
5.13	QoS support	Not applicable	QoS is not implemented in data path
6	Inter-working architecture	No requirement	
6.1	Reference model	No requirement	
6.1.1	Non roaming WLAN inter-working reference model	Compliant	Does not support OCS, HSS and SLF
6.1.2	Roaming WLAN inter-working reference model	Compliant	Supports Wa,Wu,Wd,Wm,Wi,Wz and Gr interfaces
6.2	Network elements	No requirement	
6.2.1	WLAN UE	Not applicable	
6.2.1.1	Void	No requirement	
6.2.2	3GPP AAA proxy	Compliant	
6.2.3	3GPP AAA server	Compliant	
6.2.4	HLR/HSS	Compliant	HSS is not supported

Table 5. 3GPP SCG to WLAN system description

Section Number	Section Title	Support	Comments
6.2.5	WLAN access gateway	Compliant	
6.2.5.1	Policy enforcement	Compliant	
6.2.5.2	Void	No requirement	
6.2.6	Packet Data Gateway	Compliant	
6.2.7	Subscription Locater Function (SLF)	Not applicable	
6.2.8	Offline charging system	Compliant	
6.2.9	Online charging system	Not applicable	
6.3	Reference points	No requirement	
6.3.1	Wa reference point	No requirement	
6.3.1.1	General description	Compliant	
6.3.1.2	Functionality	Compliant	
6.3.2	Wx reference point	Not applicable	
6.3.3	D'/Gr' reference point	Compliant	
6.3.4	Wo reference point	Not applicable	
6.3.5	Wf reference point	Compliant	
6.3.6	Wg reference point	Compliant	
6.3.7	Wn reference point	Compliant	
6.3.8	Wp reference point	Fully Compliant	
6.3.9	Wi reference point	Fully Compliant	
6.3.10	Wm reference point	Fully Compliant	
6.3.11	Wd reference point	No requirement	
6.3.11.1	General description	Fully Compliant	
6.3.11.2	Functionality	Compliant	
6.3.12	Wu reference point	Fully Compliant	Interface is through AP
6.3.13	Ww reference point	No requirement	
6.3.13.1	General description	Compliant	Interface is through AP
6.3.13.2	Functionality	Fully Compliant	
6.3.14	Dw reference point	Not applicable	

Table 5. 3GPP SCG to WLAN system description

Section Number	Section Title	Support	Comments
6.3.15	Wy reference point	Not applicable	
6.3.16	Wz reference point	Fully Compliant	
6.4	Protocols	Fully Compliant	
6.4.1	Remote IP layer	Fully Compliant	
6.4.2	Tunneling layer	Fully Compliant	
6.4.3	Transport IP layer	Compliant	
6.5	WLAN user profile	Compliant	
7	Procedures	No requirement	
7.1	I-WLAN and VPLMN selection procedure	No requirement	
7.1.1	Initial network selection	Compliant	
7.1.2	Network re-selection	Fully Compliant	
7.2	WLAN access authentication and authorization	Compliant	
7.3	Subscriber profile update	No requirement	
7.3.0	WLAN direct access authorization information update procedure	Compliant	HSS is not supported. Authorization update is through CoA
7.3.1	Access and service authorization information update procedure	Compliant	HSS is not supported. Access and service authorization update is through CoA
7.4	Cancelling WLAN registration	Compliant	Cancellation is either through disconnect message from AAA sever or cancel location or delete subscriber data message from HLR
7.5	Disconnecting a subscriber by WLAN	Compliant	
7.6	Disconnecting a subscriber by Online charging system	Not applicable	
7.7	Charging offline charged subscribers	Compliant	

Table 5. 3GPP SCG to WLAN system description

Section Number	Section Title	Support	Comments
7.8	Charging online charged subscribers	Not applicable	
7.9	W-APN resolution and tunnel establishment	Compliant	
7.9.1	Void	No requirement	
7.9.2	Subsequent authentication	Fully Compliant	
7.9.3	Use of DNS	Compliant	IPv6 is not supported. Multiple PDG addresses cannot be configured against a single FQDN
7.9.4	Subsequent tunnel establishment	Fully Compliant	
7.10	Tunnel disconnection procedures	Fully Compliant	
7.10.1	WLAN UE initiated tunnel disconnection	Fully Compliant	
7.10.2	Network initiated tunnel disconnection	Fully Compliant	
7.10.3	Disconnection of the last tunnel for WLAN UE	Not applicable	Single tunnel is created for a particular user equipment
7.11	WLAN UE initiated WLAN access disconnection	Compliant	
7.12	User identity to HSS resolution	Not applicable	
7.13	Disconnecting a subscriber through external AAA server	No requirement	
7.13.1	Tunnel disconnection through external AAA server initiate	Compliant	Cancellation is either through disconnect message from AAA sever

3GPP System to WLAN UE Network Protocols

Table 6 lists the 3GPP inter-working of the SCG to WLAN as per the user equipment network protocols. This is based on 3GPP TS 24.234 compliance aspects.

Table 6. 3GPP System to WLAN UE network protocols

Section Number	Section Title	Support	Comments
1	Scope	No requirement	Informative
2	References	No requirement	Informative
3	Definitions, abbreviations and symbols	No requirement	Informative
3.1	Definitions	No requirement	Informative
3.2	Symbols	No requirement	Informative
3.3	Abbreviations	No requirement	Informative
4	3GPP WLAN inter-working system	Fully compliant	Informative
4.2	WLAN UE identities	No requirement	
4.2.1	General	Fully compliant	
4.2.2	Root NAI	Not applicable	
4.2.3	Decorated NAI	Not applicable	
4.2.4	Alternative NAI	Not applicable	
4.2.5	Username	Fully compliant	
4.3	Scanning procedure	No applicable	User requirement
4.3.1	IEEE 802.11 WLANs	Not applicable	User requirement
4.3.2	Other WLAN technologies	Not applicable	UE requirement
4.4	Network discovery	No requirement	
4.4.1	General	Not applicable	UE requirement
4.4.2	WLAN UE procedures	Not applicable	UE requirement
5	Network selection	Not applicable	UE requirement
5.1	General	Not applicable	UE requirement
5.2	PLMN selection	Not applicable	UE requirement
5.2.1	WLAN UE I-WLAN selection procedure	Not applicable	UE requirement
5.2.2	Void	Not requirement	
5.2.3	Manual PLMN selection mode procedure	Not applicable	UE requirement

Table 6. 3GPP System to WLAN UE network protocols

Section Number	Section Title	Support	Comments
5.2.4	Automatic PLMN selection mode procedure	Not applicable	UE requirement
5.2.5	Network selection for emergency cases	Not applicable	
5.2.5.1	General	Not applicable	
5.2.5.2	Manual PLMN selection for emergency case	Not applicable	
5.2.5.3	Automatic PLMN selection for emergency case	Not applicable	
5.2.5.4	Network selection in case of UICC-less terminal	Not applicable	
5.3	Void	Not Requirement	
5.4	User restriction and steering roaming	No requirement	
5.4.1	WLAN UE procedures	No requirement	
5.4.1.1	General	Not applicable	UE requirement
5.4.1.2	Automatic network selection mode	Not applicable	UE requirement
5.4.1.3	Manual network selection mode	Not applicable	UE requirement
5.4.1.4	Steering of roaming	Not applicable	UE requirement
5.4.2	3GPP AAA procedures	Compliant	
6	WLAN UE to 3GPP network protocols	No requirement	
6.1	WLAN UE to 3GPP AAA server protocols	No requirement	
6.1.1	WLAN access authentication and authorization protocols	No requirement	
6.1.1.1	General	No requirement	
6.1.1.1.1	Non emergency calls	Compliant	
6.1.1.1.2	WLAN access authentication and authorization in emergency case	Not applicable	Emergency call is not supported
6.1.1.2	WLAN UE procedures	No requirement	
6.1.1.2.1	Identity management	Compliant	
6.1.1.2.2	User identity privacy	Compliant	
6.1.1.2.3	EAP-AKA based authentication	Compliant	
6.1.1.2.4	EAP-SIM based authentication	Compliant	

Table 6. 3GPP System to WLAN UE network protocols

Section Number	Section Title	Support	Comments
6.1.1.2.4.1	Interoperability cases	Not applicable	UE requirement
6.1.1.2.5	Reauthentication	Not applicable	UE requirement
6.1.1.2.6	Protected result indicators	Compliant	
6.1.1.2.7	UE procedure in emergency case	Not applicable	Emergency call is not supported
6.1.1.3	3GPP AAA server procedure	No requirement	
6.1.1.3.1	Identity management	Compliant	
6.1.1.3.2	User identity privacy	Compliant	
6.1.1.3.3	EAP SIM and EAP AKA based authentication	Compliant	
6.1.1.3.4	3GPP AAA server operation beginning of authentication	compliant	
6.1.1.3.4.1	Interoperability cases	Compliant	
6.1.1.3.5	Reauthentication	Compliant	
6.1.1.3.6	WLAN access authorization	Compliant	
6.1.1.3.7	Protected result indicators	Non Compliant	
6.1.1.3.8	3GPP AAA server procedures in emergency case	No Applicable	Emergency call is not supported
7	Parameter coding	No requirement	
7.1	General	No requirement	
7.3	Pseudonym	Compliant	
7.4	Void	No requirement	
7.5	Operator controlled PLMN selector for WLAN access	Not applicable	UE requirement
7.6	User controlled WLAN specific identifier list	Not applicable	UE requirement
7.6a	Operator controlled WLAN specific identifier list	Not applicable	UE requirement
7.7	Supported PLMNs list for WLAN access	Not applicable	UE requirement
7.8	Reauthentication identity	Complaint	
7.9	I-WLAN last registered PLMN	Not applicable	UE requirement
7.10	HPLMN priority file	Not applicable	UE requirement

Table 6. 3GPP System to WLAN UE network protocols

Section Number	Section Title	Support	Comments
7.11	HPLMN direct access	Not applicable	UE requirement
8	Tunnel management procedures	No requirement	
8.1	General	Compliant	QoS, IPsec is not supported
8.2	Tunnel establishment procedure	No requirement	
8.2.1	WLAN UE procedures	No requirement	
8.2.1.1	General	Compliant	IPsec is not supported.
8.2.1.2	Selection of remote tunnel endpoint	Compliant	
8.2.1.3	WLAN UE initiated tunnel establishment	No requirement	
8.2.1.3.1	WLAN UE initiated tunnel establishment with authentication to the 3GPP AAA server	Partially-compliant	Ruckus proprietary tunnel established model
8.2.1.3.2	WLAN UE initiated tunnel establishment with additional authentication to external AAA server	Not applicable	
8.2.1.4	Void	No requirement	
8.2.1.5	Void	No requirement	
8.2.1.6	In place rekeying of existing security association	Not applicable	IPsec is not supported
8.2.1.7	Additional tunnel establishment	Not applicable	IPsec is not supported
8.2.1.8	WLAN UE procedures for the Emergency Case	Not applicable	Emergency call is not supported
8.2.1.9	QoS provisioning support	Not applicable	No QoS support
8.2.2	PDG Procedures	No requirement	
8.2.2.1	General	Partially-Compliant	IPsec is not supported
8.2.2.2	WLAN UE initiated tunnel establishment	No requirement	
8.2.2.2.1	WLAN UE initiated tunnel establishment with authentication to the 3GPP AAA Server	Compliant	IPsec is not supported

Table 6. 3GPP System to WLAN UE network protocols

Section Number	Section Title	Support	Comments
8.2.2.2.2	WLAN UE initiated tunnel establishment with additional authentication to an External AAA Server	Compliant	
8.2.2.3	Void	No requirement	
8.2.2.4	Void	No requirement	
8.2.2.5	Additional tunnel establishment and in place rekeying	Not applicable	IPsec is not supported
8.2.2.6	PDG procedures in the emergency case	Not applicable	Emergency call not supported.
6.4.2	QoS provisioning support	Not applicable	No QoS support
8.3	Tunnel disconnection procedures	No requirement	
8.3.1	WLAN UE procedures	No requirement	
8.3.1.1	General	Not applicable	IPsec is not supported
8.3.1.2	PDG Initiated tunnel disconnection procedures	Not applicable	IPsec is not supported
8.3.1.3	WLAN UE procedures in emergency cases	Not applicable	Emergency call is not supported
8.3.2	PDG procedure	No requirement	
8.3.2.1	General	Not applicable	IPsec is not supported
8.3.2.2	WLAN UE initiated tunnel disconnection procedures	Not applicable	IPsec is not supported
8.3.2.3	PDG procedures in emergency case	Not applicable	Emergency call is not supported
8.4	Timers and counters for tunnel management	Not applicable	IPsec is not supported
8.5	Void	No requirement	

3GPP SCG with WLAN PLMN Support

Table 7 lists the 3GPP inter-working of the SCG to WLAN with PLMN support packet based services. This is as per WLAN access and PDN. This is based on 3GPP TS 29.161 compliance aspects.

Table 7. 3GPP SCG with WLAN PLMN support

Section Number	Section Title	Support	Comments
1	Scope	No requirement	Informative
2	References	No requirement	Informative
3	Definitions, abbreviations and symbols	No requirement	Informative
3.1	Definitions	No requirement	Informative
3.2	Abbreviations	No requirement	Informative
3.3	Symbols	No requirement	Informative
4	Network characteristics	No requirement	Informative
4.1	Key characteristics of PLMN	Compliant	
4.2	Key characteristics of IP networks	Compliant	
5	Inter-working classifications	Compliant	
6	Access reference configuration	Compliant	Supports HLR but not HSS
7	Subscription checking	Compliant	
8	Inter-working with PDN (IP)	Compliant	
8.1	General	Fully compliant	
8.2	PDN inter-working model	Compliant	IPv6 is not supported
8.2.1	Access to Internet, intranet or ISP through packet domain	Compliant	
8.2.1.1	Transparent access to the Internet	Compliant	
8.2.1.2	IPv4 non transparent access to intranet or ISP	Compliant	
8.2.1.3	IPv6 non transparent access to intranet or ISP	Not applicable	
8.2.1.3.1	Tunnel establishment and intranet/ISP access authorization	Not applicable	
8.2.1.3.2	IPv6 stateless address auto configuration	Not applicable	

Table 7. 3GPP SCG with WLAN PLMN support

Section Number	Section Title	Support	Comments
8.2.1.3.3	IPv6 stateful address auto configuration	Not applicable	
8.3	Numbering and addressing	Compliant	
8.4	Charging	Compliant	Supports off line charges
8.5	DNS server	Compliant	
8.6	IP multicast access	Not applicable	
9	Inter-working with PDN (DHCP)	No requirement	
9.1	General	Compliant	
9.2	Address allocation by intranet or ISP	Compliant	
9.3	Other configuration by Intranet or ISP (IPv6 only)	Not applicable	
10	Inter-working between packet domains	Compliant	
11	Usage of RADIUS on Wi interface	Compliant	
11.1	RADIUS authentication and authorization	Compliant	
11.2	RADIUS accounting	Compliant	
11.3	Authentication, authorization and accounting message flows	Compliant	
11.4	List of RADIUS attributes	Compliant	
11a	Usage of diameter on Wi interface	Not applicable	
12	Usage of RADIUS on Pp interface	Not applicable	

3GPP SCG to WLAN

Table 8 lists the 3GPP inter-working of the SCG to WLAN. This is based on 3GPP TS 29.234 compliance aspects.

Table 8. 3GPP SCG to WLAN

Section Number	Section Title	Support	Comment
1	Scope	No requirement	Informative
2	References	No requirement	Informative
3	Definitions, abbreviations and symbols	No requirement	Informative
3.1	Definitions	No requirement	Informative
3.2	Symbols	No requirement	Informative
3.3	Abbreviations	No requirement	Informative
4	Wa description	No requirement	Informative
4.1	Functionality	Compliant	
4.2	Protocols	Compliant	
4.3	Procedures description	No requirement	
4.3.1	WLAN access authentication and authorization	Compliant	Diameter is not supported
4.3.1.1	WLAN access authentication and authorization for emergency case	Not applicable	
4.3.2	Immediate purging of a user from WLAN access	Compliant	Diameter is not supported
4.3.2.1	Emergency case	Not applicable	
4.3.3	Ending a session	Compliant	
4.3.4	WLAN access authorization information update procedure	Compliant	
4.4	Information element contents	No requirement	
4.4.1	RADIUS based information elements contents	Compliant	
4.4.2	Diameter based Information elements contents	Not applicable	Diameter is not supported
4.5	Accounting signaling across Wa interface	Compliant	
4.5.1	RADIUS	Fully compliant	

Table 8. 3GPP SCG to WLAN

Section Number	Section Title	Support	Comment
4.5.1.1	RADIUS attributes in accounting messages	Compliant	
4.5.2	Diameter	Not applicable	
5	Wd description	No requirement	
5.1	Functionality	Compliant	
5.2	Protocols	Compliant	Diameter is not supported
5.3	3GPP AAA proxy and 3GPP AAA server behavior when inter-working with RADIUS/ diameter WLAN ANs	Compliant	
5.3.1	Requirements in 3GPP AAA proxy for RADIUS/Diameter translation agent	Compliant	
5.3.1.1	Conversion of RADIUS request to Diameter request	Not applicable	
5.3.1.2	Conversion of Diameter response to RADIUS response	Not applicable	
5.3.1.3	3GPP AAA proxy advertisement of RADIUS or Diameter client to 3GPP AAA server	Not applicable	
5.3.1.4	Managing the transaction state and session state information	Compliant	
5.4	Procedures description	No requirement	
5.4.1	WLAN access authentication and authorization	Compliant	
5.4.2	Immediate purging of a user from WLAN access	Compliant	
5.4.3	Ending a session	Compliant	
5.4.4	Authorization information update procedure	Compliant	
5.5	Information elements contents	No requirement	
5.5.1	Authentication procedures	Not applicable	
5.5.2	Abort session requests and answer AVPs	Not applicable	
5.5.3	Session termination request and answer AVPs	Not applicable	

Table 8. 3GPP SCG to WLAN

Section Number	Section Title	Support	Comment
5.5.4	RADIUS based Information elements contents for authentication and authorization	Compliant	
5.5.5	RADIUS based Information elements contents for accounting	Compliant	
6	Wx description	Not applicable	
7	Void	No requirement	
8	Wm description	Not applicable	Wm interface is applicable on the SCG, where RADIUS is used instead of Diameter.
9	Wg description	Not applicable	
10	Information elements contents	Not applicable	
11	Pr description	Not applicable	
12	User identity to HSS resolution	Not applicable	

3GPP SCG to GTPV2-c

Table 9 lists the 3GPP inter-working of the SCG to GTPV2-c. This is based on 3GPP TS 29.274 compliance aspects.

Table 9. 3GPP SCG to GTPV2-c

Section Number	Section Title	Support	Comment
1	Scope	No requirement	Informative
2	References	No requirement	Informative
3	Definitions, symbols and abbreviations	No requirement	Informative
4	General	No requirement	
4.1	GTP Tunnel	Partially compliant	S2a and S5/S8 interfaces are supported. The SCG is used from the WiFi offload perspective and acts as SGW. Either S2a/ S5/S8 are not used. Piggybacking is not supported.
4.2	Protocol stack	No requirement	
4.2.0	General	Compliant	Only port 2123 is supported for control messages. Piggybacking is not supported.
4.2.1	UDP header and port numbers	No requirement	
4.2.1.0	General	Fully compliant	
4.2.1.1	Initial messages	Fully compliant	
4.2.1.2	Triggered messages	Compliant	
4.2.1.3	Piggybacked messages	Not applicable	Piggybacking is not supported.
4.2.2	IP header and IP addresses	No requirement	
4.2.2.1	Initial messages	Partially compliant	The SCG is used from the WiFi offload perspective and acts as SGW.
4.2.2.2	Triggered messages	Compliant	
4.2.2.3	Piggybacked messages	Not applicable	Piggybacking is not supported.
4.2.3	Layer 2	Fully compliant	
4.2.4	Layer 1	No requirement	

Table 9. 3GPP SCG to GTPV2-c

Section Number	Section Title	Support	Comment
4.2.5	Messages with GTPv2 defined reply. Classification of initial and triggered messages	Partially compliant	The SCG is used from the WiFi offload perspective and supported messages are provided in Event Compliance - GTPv2-c.
4.3	Transmission order and bit definitions	Fully compliant	
5	GTP header for control plane	No requirement	
5.1	General format	Fully compliant	
5.2	Controlplane GTP extension header	No requirement	
5.3	GTP-C header for echo and version not supported messages	Partially compliant	Supports messages but not decoding of version. The SCG (SGW) does not initiate the message as it is initiates tunnel creation.
5.4	EPC specific GTP-C header	Compliant	Piggybacking is not supported.
5.5	Usage of the GTPv2-C Header	No requirement	
5.5.1	General	Fully compliant	
5.5.2	Conditions for sending TEID=0 in GTPv2-C header	Partially compliant	Supports S2a/S5/S8.
5.6	Format of the GTPv2-C message	Fully compliant	
6	GTP-C message types and message formats	No requirement	
6.0	General	Fully compliant	
6.1	Message format and type values	No requirement	
6.1.0	Message type	Partially compliant	
6.1.1	Presence requirements of information elements	Compliant	
6.1.2	Grouped information element	Compliant	Supports Grouped IE but not multiple instances and dedicated bearers

Table 9. 3GPP SCG to GTPV2-c

Section Number	Section Title	Support	Comment
6.1.3	Information element instance	Fully compliant	
6.2	Message granularity	Compliant	Supported messages are provided in this chapter
7	GTP-C messages	No requirement	
7.1	Path management messages	No requirement	Refer to the clarification provided in Compliance for GTPv2 Section 7.1.
7.1.0	General	Fully compliant	
7.1.1	Echo request	Compliant	Only Recovery IE is sent
7.1.2	Echo response	Compliant	Only Recovery IE is sent
7.1.3	Version not supported indication	Compliant	The SCG decodes but does not initiate the message
7.2	Tunnel management messages	No requirement	Supported messages are provided in Compliance for GTPv2 Section 7.2.
7.2.0	General	Fully compliant	
7.2.1	Create session request	Compliant	Supports S2a and S5/S8 but not SGW terminated session request. Refer to the clarification provided in Compliance for GTPv2 Section 7.2.1 and Bearer Context Attributes for Section 7.2.1.
7.2.2	Create session response	Partially compliant	Refer to the clarification provided in Compliance for GTPv2 Section 7.2.2 and Bearer Context Attributes for Section 7.2.2.
7.2.3	Create bearer request	Not applicable	Dedicated bearers are not supported
7.2.4	Create bearer response	Not applicable	
7.2.5	Bearer resource command	Not applicable	Not required as the SCG does not interact with MME
7.2.6	Bearer resource failure indication	Not applicable	

Table 9. 3GPP SCG to GTPV2-c

Section Number	Section Title	Support	Comment
7.2.7	Modify bearer request	Non-compliant	Message sent on S2a interface also. Refer to the clarification provided in Compliance for GTPv2 Section 7.2.7 and Bearer Context Attributes for Section 7.2.7
7.2.8	Modify bearer response	Non-compliant	Refer to the clarification provided in Compliance for GTPv2 Section 7.2.8 and Bearer Context Attributes for Section 7.2.8
7.2.9	Delete session request and delete bearer request	No requirement	
7.2.9.1	Delete session request	Compliant	Refer to the clarification provided in Compliance for GTPv2 Section 7.2.9.1
7.2.9.2	Delete bearer request	Compliant	Refer to the clarification provided in Compliance for GTPv2 Section 7.2.9.2 and Bearer Context Attributes for Section 7.2.9.2
7.2.10	Delete session response and delete bearer response	No requirement	
7.2.10.1	Delete session response	Compliant	Refer to the clarifications provided in Compliance for GTPv2 Section 7.2.10.1
7.2.10.2	Delete bearer response	Compliant	Refer to the clarification provided in Compliance for GTPv2 Section 7.2.10.2 and Bearer Context Attributes for Section 7.2.10.2
7.2.11	Downlink data notification messages	Not applicable	
7.2.12	Delete indirect data forwarding tunnel request	Not applicable	
7.2.13	Delete indirect data forwarding tunnel response	Not applicable	

Table 9. 3GPP SCG to GTPV2-c

Section Number	Section Title	Support	Comment
7.2.14	Modify bearer command and failure indication	No requirement	
7.2.14.1	Modify bearer command	Compliant	Refer to the clarification provided in Compliance for GTPv2 Section 7.2.14.1 and Bearer Context Attributes for Section 7.2.14.1
7.2.14.2	Modify bearer failure indication	Compliant	Refer to the clarification provided in Compliance for GTPv2 Section 7.2.14.2
7.2.15	Update bearer request	Compliant	Clarification provided in Compliance for GTPv2 Section 7.2.15 and Bearer Context Attributes for Section 7.2.15
7.2.16	Update bearer request	Compliant	Clarification provided in Compliance for GTPv2 Section 7.2.16 and Bearer Context Attributes for Section 7.2.16
7.2.17	Delete bearer command and failure indication	Not applicable	
7.2.18	Create indirect data forwarding tunnel request	Not applicable	
7.2.19	Create indirect data forwarding tunnel response	Not applicable	
7.2.20	Void	No requirement	
7.2.21	Release access bearers request	Not applicable	
7.2.22	Release access bearers response	Not applicable	
7.2.23	Stop paging indication	Not applicable	
7.2.24	Modify access bearers request	Not applicable	
7.2.25	Modify access bearers response	Not applicable	

Table 9. 3GPP SCG to GTPV2-c

Section Number	Section Title	Support	Comment
7.3	Mobility management messages	No requirement	All the messages under Mobility Management Messages section are not supported. They are not required from the WiFi offload perspective
7.4	CS Fallback and SRVCC related messages	No requirement	All the messages under CS fall back and SRVCC related messages section are not supported. They are not required from the WiFi offload perspective
7.5	Non-3GPP access related messages	No requirement	All the messages under Non-3GPP access related messages section are not supported. They are not required from the WiFi offload perspective
7.6	Reliable delivery of signaling messages	Compliant	
7.7	Error handling	No requirement	
7.7.0	Handling piggybacked messages	Not applicable	Not supported
7.7.1	Protocol errors	Fully compliant	
7.7.2	Different GTP versions	Compliant	Version not supported will be decoded at SCG. SCG does not initiate version not supported message. GTPv0 is not supported
7.7.3	GTP message o invalid length	Compliant	
7.7.4	Unknown GTP message	Fully compliant	
7.7.5	Unexpected GTP message	Fully compliant	
7.7.6	Missing information elements	Fully compliant	
7.7.7	Invalid length information element	Fully compliant	
7.7.8	Semantically incorrect information element	Fully compliant	

Table 9. 3GPP SCG to GTPV2-c

Section Number	Section Title	Support	Comment
7.7.9	Unknown or unexpected information element	Fully compliant	
7.7.10	Repeated information elements	Fully compliant	
7.7.11	TFT error handling	Fully compliant	Dedicated bearer is not supported
7.8	Path failure	Fully compliant	
7.9	Restoration and recovery	Not applicable	
7.10	Fallback to GTPv1 mechanism	Not applicable	Fall back is not supported
7.11	Fallback to GTPv0	Not applicable	Fall back is not supported
7.12	Trace management messages	Not applicable	
7.13	MBMS messages	Not applicable	
8	GTP-C information elements	No requirement	
8.1	Information element types	Compliant	Supported IE types are provided in Section 4 under the respective message types
8.2	Information element format	No requirement	
8.2.1	General	Fully compliant	
8.2.2	Handling ASN.1/PER encoded parameters	Not applicable	
8.3	International mobile subscriber identity	Fully compliant	
8.4	Cause	Compliant	
8.5	Recovery (restart counter)	Fully compliant	
8.6	Access Point Name (APN)	Fully compliant	
8.7	Aggregate Maximum Bit Rate (AMBR)	Fully compliant	QoS is not implemented in the data path
8.8	EPS Bearer ID (EBI)	Fully compliant	
8.9	IP address	Fully compliant	
8.10	Mobile Equipment Identity (MEI)	Not applicable	
8.11	MSISDN	Fully compliant	

Table 9. 3GPP SCG to GTPV2-c

Section Number	Section Title	Support	Comment
8.12	Indication	Fully compliant	Value is set to 0 in Create Session Request
8.13	Protocol Configuration Options (PCO)	Not applicable	Will be decoded in case it is received in Create Session Response. It is not sent from SCG
8.14	PDN Address Allocation (PAA)	Fully compliant	
8.15	Bearer QoS	Fully compliant	QoS is not implemented in the data path
8.16	Flow QoS	Not applicable	
8.17	RAT type	Fully compliant	In S5/S8 value will be EUTRAN, for S2a it will be WLAN
8.18	Serving network	Fully compliant	
8.19	EPS Bearer Level Traffic Flow Template (Bearer TFT)	Not applicable	Will be decoded in case it is received in Create Session Response. It is not sent from SCG
8.20	Traffic Aggregate Description (TAD)	Not applicable	
8.21	User Location Information (ULI)	Compliant	
8.21.1	CGI field	Not applicable	
8.21.2	SAI field	Fully compliant	
8.21.3	RAI field	Fully compliant	
8.21.4	TAI field	Not applicable	
8.21.5	ECGI field	Not applicable	
8.21.6	LAI field	Not applicable	
8.22	Fully Qualified TEID (F-TEID)	Fully compliant	
8.23	TMSI	Not applicable	
8.24	Global CN-Id	Not applicable	
8.25	S103 PDN Data Forwarding Info (S103PDF)	Not applicable	
8.26	S1-U Data Forwarding (S1UDF)	Not applicable	
8.27	Delay value	Not applicable	

Table 9. 3GPP SCG to GTPV2-c

Section Number	Section Title	Support	Comment
8.28	Bearer context	Fully compliant	
8.29	Charging Id	Fully compliant	
8.30	Charging characteristics	Fully compliant	
8.31	Trace Information	Not applicable	
8.32	Bearer flags	Not applicable	
8.33	Void	Not applicable	
8.34	PDN type	Fully compliant	
8.35	Procedure Transaction ID (PTI)	Not applicable	
8.36	Void	Not applicable	
8.37	Void	Not applicable	
8.38	MM context	Not applicable	
8.39	PDN connection	Not applicable	
8.40	PDU numbers	Not applicable	
8.41	Packet TMSI (P-TMSI)	Not applicable	
8.42	P-TMSI signature	Not applicable	
8.43	Hop counter	Not applicable	
8.44	UE time zone	Not applicable	
8.45	Trace reference	Not applicable	
8.46	Complete request message	Not applicable	
8.47	GUTI	Not applicable	
8.48	Fully Qualified Container (F-Container)	Not applicable	
8.49	Fully Qualified Cause (F-Cause)	Not applicable	
8.50	Selected PLMN ID	Not applicable	
8.51	Target identification	Not applicable	
8.52	Void	Not applicable	
8.53	Packet Flow ID	Not applicable	
8.54	RAB context	Not applicable	
8.55	Source RNC PDCP context info	Not applicable	

Table 9. 3GPP SCG to GTPV2-c

Section Number	Section Title	Support	Comment
8.56	Port number	Not applicable	
8.57	APN restriction	Fully compliant	This value is set to the least restrictive type
8.58	Selection mode	Fully compliant	The value is set to “MS or network provided APN, subscription verified”
8.59	Source identification	Not applicable	
8.60	Void	Not applicable	
8.61	Change reporting action	Not applicable	Will be decoded in case it is received in Create Session Response. It is not sent from SCG.
8.62	Fully Qualified PDN Connection Set Identifier (FQ-CSID)	Not applicable	
8.63	Channel needed	Not applicable	
8.64	eMLPP priority	Not applicable	
8.65	Node type	Not applicable	
8.66	Fully Qualified Domain Name (FQDN)	Not applicable	
8.67	Private extension	Not applicable	Will be decoded in case it is received in any supported message. It is not sent from SCG.
8.68	Transaction Identifier (TI)	Not applicable	
8.69	MBMS session duration	Not applicable	
8.70	MBMS service area	Not applicable	
8.71	MBMS session identifier	Not applicable	
8.72	MBMS flow identifier	Not applicable	
8.73	MBMS IP multicast distribution	Not applicable	
8.74	MBMS distribution acknowledge	Not applicable	
8.75	User CSG Information (UCI)	Not applicable	
8.76	CSG information reporting action	Not applicable	
8.77	RFSP index	Not applicable	

Table 9. 3GPP SCG to GTPV2-c

Section Number	Section Title	Support	Comment
8.78	CSG ID	Not applicable	
8.79	CSG Membership Indication (CMI)	Not applicable	
8.80	Service indicator	Not applicable	
8.81	Detach type	Not applicable	
8.82	Local Distinguished Name (LDN)	Not applicable	
8.83	Node features	Not applicable	
8.84	MBMS time to data transfer	Not applicable	
8.85	Throttling	Not applicable	
8.86	Allocation/Retention Priority (ARP)	Not applicable	
8.87	EPC timer	Not applicable	
8.88	Signaling Priority Indication	Not applicable	
8.89	Temporary Mobile Group Identity (TMGI)	Not applicable	
8.90	Additional MM context for SRVCC	Not applicable	
8.91	Additional flags for SRVCC	Not applicable	
8.92	Max MBR/APN-AMBR(MMBR)	Not applicable	
8.93	MDT configuration	Not applicable	
8.94	Additional Protocol Configuration Options (APCO)	Not applicable	
8.95	Absolute time of MBMS data transfer	Not applicable	
8.96	H(e)NB information reporting	Not applicable	
8.97	IPv4 Configuration Parameters (IP4CP)	Not applicable	
9	Security	Not applicable	
10	IP - Networking technology used by GTP	No requirement	

Table 9. 3GPP SCG to GTPV2-c

Section Number	Section Title	Support	Comment
10.1	IP version	Compliant	IPv6 is not supported
10.2	IP fragmentation	Not applicable	
11	Notification of supported features between peer GTP-C entities	No requirement	
11.1	General	No requirement	
11.1.1	Introduction	Fully compliant	
11.1.2	Defining a feature	Fully compliant	
11.2	Dynamic discovery of supported features	No requirement	
11.2.1	General	Not applicable	
11.2.2	Features supported by direct peer GTP-C entities	Not applicable	

3GPP SCG to WLAN Security

Table 10 lists the 3GPP inter-working of the SCG to WLAN as per the security protocols. This is based on 3GPP TS 33.234 compliance aspects.

Table 10. 3GPP SCG to WLAN security

Section Number	Section Title	Support	Comments
1	Scope	No requirement	Informative
2	References	No requirement	Informative
3	Definitions and abbreviations	No requirement	Informative
3.1	Definitions	No requirement	Informative
3.2	Abbreviations	No requirement	Informative
4	Security requirements for 3GPP-WLAN inter-working	No requirement	Informative
4.1.1	Non roaming WLAN inter-working reference model	Compliant	OCS, SLF and HSS are not supported.
4.1.2	Roaming WLAN inter-working reference model, access to HPLMN services	Compliant	
4.1.3	Roaming WLAN inter-working reference model, access to VPLMN services	Compliant	
4.1.4	Network elements	Compliant	
4.1.5	Reference points description	No requirement	
4.2	Security requirements	No requirement	
4.2.1	General	Fully compliant	
4.2.2	Signaling and user data protection	Compliant	
4.2.3	User identity privacy	Fully compliant	
4.2.4	WLAN-UE functional split	No requirement	
4.2.4.1	General	Compliant	
4.2.4.2	Generic security requirements on local interface	Compliant	
4.2.4.3	Communication over local interface via a blue tooth link	Not applicable	
4.2.5	Link layer security requirements	Compliant	
4.2.5.1	Void	No requirement	

Table 10. 3GPP SCG to WLAN security

Section Number	Section Title	Support	Comments
4.2.5.2	Void	No requirement	
4.2.5.3	Void	No requirement	
4.2.6	UE-initiated tunneling	Compliant	
4.2.7	Requirements on IP based access networks other than WLAN	Compliant	
4.2.8	Requirements for support of emergency call	Not applicable	
4.2.9	Requirements for support of emergency call for a non UICC terminal	Not applicable	
5	Security features	No requirement	
5.1	Authentication of the subscriber and the network and security association management	No requirement	
5.1.1	End to end WLAN access authentication (WLAN direct IP access)	Fully compliant	
5.1.2	Transport of authentication WLAN access signaling over the WLAN radio interface	Compliant	
5.1.3	Transport of WLAN access authentication signaling between the WLAN access network and the 3GPP AAA proxy server	Compliant	Does not support Diameter.
5.1.4	Transport of authentication signaling between the 3GPP AAA proxy server and AAA server	Compliant	
5.1.5	Transport of WLAN access authentication signaling between the 3GPP AAA server and HSS	Not applicable	
5.1.6	User Identity privacy in WLAN access	Compliant	
5.1.7	Reauthentication in WLAN access	Compliant	
5.1.8	Security association management for UE initiated tunnels (WLAN 3GPP IP access)	Fully compliant	
5.2	Confidentiality protection	No requirement	
5.2.1	Confidentiality protection in WLAN direct IP access	Compliant	

Table 10. 3GPP SCG to WLAN security

Section Number	Section Title	Support	Comments
5.2.2	Confidentiality protection in WLAN 3GPP IP access	Fully compliant	
5.3	Integrity protection	No requirement	
5.3.1	Integrity protection in WLAN direct IP access	Compliant	
5.3.2	Integrity protection in WLAN 3GPP IP access	Fully compliant	
5.4	Void	No requirement	
5.5	Immediate service termination	Compliant	
5.6	WLAN UE functionality split	Not applicable	
5.7	Simultaneous access control	Fully compliant	
6	Security mechanisms	No requirement	
6.1	Authentication and key agreement	Fully compliant	
6.1.1	USIM-based WLAN access authentication	Fully compliant	
6.1.1.1	EAP/AKA procedure	Compliant	
6.1.2	GSM SIM based WLAN access authentication	Compliant	
6.1.2.1	EAP SIM procedure	Compliant	
6.1.3	EAP support in smart cards	Not applicable	
6.1.4	Fast reauthentication mechanisms in WLAN access	Compliant	
6.1.4.1	EAP/AKA procedure	Compliant	
6.1.4.2	EAP/SIM procedure	Compliant	
6.1.4.3	Fallback to full authentication from fast reauthentication	Compliant	
6.1.5	Mechanisms for setting up UE-initiated tunnels (WLAN 3GPP IP access)	Not applicable	Does not support IPsec.
6.1.6	Void	No requirement	
6.2	Confidentiality mechanisms	No requirement	
6.2.1	Confidentiality mechanisms in WLAN direct IP access	Compliant	

Table 10. 3GPP SCG to WLAN security

Section Number	Section Title	Support	Comments
6.2.2	Confidentiality mechanisms in WLAN 3GPP IP access	Not applicable	Does not support IPsec.
6.3	Integrity mechanisms	No requirement	
6.3.1	Integrity mechanisms in WLAN direct IP access	Compliant	
6.3.2	Integrity mechanisms in WLAN 3GPP IP access	Not applicable	
6.4	Temporary identity management	No requirement	
6.4.1	Temporary identity generation	Compliant	
6.4.2	Key management	Compliant	
6.4.3	Impact on permanent user identities	Compliant	
6.4.4	Acknowledged limitations	Compliant	
6.4.5	UE behavior on receiving requests for sending IMSI-based user identity	Compliant	
6.5	Profile of IKEv2	Not applicable	
6.6	Profile of IPsec ESP	Not applicable	
6.6A	Profile for PDG certificates	Not applicable	
6.7	WLAN UE split inter-working	Not applicable	The SCG provides the WiFi offload solution.
7	Support for emergency call over I-WLAN for a non UICC terminal	Not applicable	

3GPP SCG to Packet Switched Domain Charging Protocols

Table 11 lists the 3GPP inter-working of the SCG to packet switched domain charging protocols. This is based on 3GPP TS 32.251 compliance aspects.

Table 11. 3GPP SCG to Packet Switched Domain Charging

Section Number	Section Title	Support	Comments
1	Scope	No requirement	
2	References	No requirement	
3	Definitions, symbols and abbreviations	No requirement	
3.1	Definitions	No requirement	
3.2	Symbols	No requirement	
3.3	Abbreviations	No requirement	
4	Architecture considerations	No requirement	
4.1	High level EPS architecture	No requirement	
4.2	PS domain offline charging architecture	Partially compliant	The SCG acts as CDF and the CDR is transferred from the SCG to the configured CGF on the Ga interface.
4.3	PS domain online charging architecture	Not applicable	
5	PS domain charging principles and scenarios	No requirement	
5.1	PS charging principles	No requirement	
5.1.1	Requirements	Partially complaint	A unique id is used for charging. The data volume is calculated separately for uplink and downlink. The SCG provides the duration, data and time.
5.1.2	Charging information	Complaint	The SCG collects the charging information for IP-CAN bearer.
5.1.3	Identifiers and correlation	Not applicable	

Table 11. 3GPP SCG to Packet Switched Domain Charging

Section Number	Section Title	Support	Comments
5.2	PS domain offline charging scenarios	No requirement	
5.2.1	Basic principles	Partially compliant	The SCG supports only S-CDR.
5.2.1.1	IP-CAN bearer charging		
5.2.1.2	MM context charging	Not applicable	
5.2.1.3	Flow based Bearer Charging (FBC)	Not applicable	
5.2.1.4	SMS charging	Not applicable	
5.2.1.5	LCS charging	Not applicable	
5.2.1.6	MBMS context charging for GPRS	Not applicable	
5.2.1.6A	MBMS context charging for EPS	Not applicable	
5.2.1.7	IP Flow Mobility (IFOM) charging	Not applicable	
5.2.1.8	Sponsored data connectivity charging	Not applicable	
5.2.2	Rf message flows	Partially complaint	The SCG uses RADIUS for accounting.
5.2.2.1	Triggers for charging events from S-GW	Fully complaint	Aip triggers Cip process for CDR generation.
5.2.2.2	Triggers for charging events from P-GW	Not applicable	
5.2.2.3	Triggers for charging events from ePDG	Not applicable	
5.2.2.4	Triggers for charging events from MME	Not applicable	
5.2.3	CDR generation	Complaint	The SCG supports generation of SCDR for TTG call on enabling same on the SCG UI.
5.2.3.1	Triggers for S-CDR charging information collection	Fully complaint	

Table 11. 3GPP SCG to Packet Switched Domain Charging

Section Number	Section Title	Support	Comments
5.2.3.1.1	Triggers for S-CDR charging information addition	Complaint	Supports only one container.
5.2.3.1.2	Triggers for S-CDR closure	Complaint	
5.2.3.2	Triggers for M-CDR charging information collection	Not applicable	
5.2.3.3	Triggers for SGW-CDR charging information collection	Not applicable	
5.2.3.4	Triggers for PGW-CDR charging information collection	Not applicable	
5.2.3.5	Triggers for SMS-CDR charging information collection	Not applicable	
5.2.3.6	Triggers for LCS-CDR charging information collection	Not applicable	
5.2.3.7	Triggers for S-MB-CDR and G-MB-CDR charging information collection for MBMS context charging for GPRS	Not applicable	
5.2.3.7A	Triggers for MBMS-GW-CDR charging information collection for MBMS context charging for EPS	Not applicable	
5.2.3.8	Triggers ePDG-CDR charging information collection	Not applicable	
5.2.4	Void	No requirement	
5.2.5	Ga record transfer flows	Complaint	Ga interface is used between the SCG and CGF for CDR transmission.
5.2.6	Bp CDR file transfer	Not applicable	
5.3	PS domain online charging scenarios	Not applicable	
6	Definition of charging information	No requirement	
6.1A	Rf message content	No requirement	

Table 11. 3GPP SCG to Packet Switched Domain Charging

Section Number	Section Title	Support	Comments
6.1A.1	Summary of offline charging message formats	Not applicable	RADIUS protocol is used, Does not support Diameter.
6.1A.2	Structure for the accounting message formats	Not applicable	
6.1A.2.1	Accounting request message	Not applicable	
6.1A.2.2	Accounting answer message	Not applicable	
6.1B	CDR content description on Bp interface	Not applicable	
6.1.1	IP CAN bearer charging data in SGSN (S-CDR)	Fully compliant	
6.1.2	IP CAN bearer charging data in S-GW (SGW-CDR)	Not applicable	
6.1.3	FBC IP CAN bearer charging data in P-GW (PGW-CDR)	Not applicable	
6.1.4	Mobile station mobility management data in SGSN (M-CDR)	Not applicable	
6.1.5	SMS-MO data in SGSN/MME (S-SMO-CDR)	Not applicable	
6.1.6	SMS-MT data in SGSN/MME (S-SMT-CDR)	Not applicable	
6.1.7	Mobile terminated location request (LCS-MT-CDR)	Not applicable	
6.1.8	Mobile originated location request (LCS-MO-CDR)	Not applicable	
6.1.9	Network induced location request (LCS-NI-CDR)	Not applicable	
6.1.10	MBMS bearer context charging data in SGSN (S-MB-CDR)	Not applicable	
6.1.11	MBMS bearer context charging data in GGSN (G-MB-CDR)	Not applicable	

Table 11. 3GPP SCG to Packet Switched Domain Charging

Section Number	Section Title	Support	Comments
6.1.12	MBMS bearer context charging data in MBMS GW (MBMS-GW-CDR)	Not applicable	
6.1.13	IP CAN bearer charging data in ePDG (ePDG-CDR)	Not applicable	
6.2	Data description for PS online charging	Not applicable	
6.2.1	Diameter message contents	Not applicable	
6.3	PS charging specific parameters	Not applicable	
6.3.1	Definition of PS charging information	Not applicable	
6.3.1.1	PS charging information assignment for service information	Not applicable	
6.3.1.1a	SMS over MME charging information assignment for service information	Not applicable	
6.3.1.2	Definition of the PS Information	Not applicable	
6.3.2	Detailed message format for offline charging	Not applicable	Does not support Diameter.
6.3.3	Detailed message format for online charging	Not applicable	
6.4	Void	Not applicable	
6.5	Bindings for EPC offline charging	Not applicable	

3GPP SCG to WLAN Offline Charging

Table 12 lists the 3GPP inter-working of the SCG to WLAN offline charging protocols. The SCG acts as the hosted AAA server. This is based on 3GPP TS 32.252 compliance aspects.

Table 12. 3GPP SCG to WLAN Offline Charging

Section Number	Section Title	Support	Comments
1	Scope	No requirement	Informative
2	References	No requirement	Informative
3	Definitions, symbols and abbreviations	No requirement	Informative
3.1	Definitions	No requirement	Informative
3.2	Symbols	No requirement	Informative
3.3	Abbreviations	No requirement	Informative
4	Architecture considerations	No requirement	Informative
4.1	High level WLAN architecture	No requirement	Informative
4.2	WLAN offline charging architecture	Complaint	The SCG acts as CTF (integrated component of AAA server and CDF). Supports WLAN-AN-CDR for PDG calls.
4.3	WLAN online charging architecture	Not applicable	
5	WLAN charging principles and scenarios	Complaint	
5.1	WLAN charging principles	Complaint	
5.1.1	WLAN direct IP access charging	Fully complaint	
5.1.2	WLAN 3GPP IP access charging	Complaint	
5.2	WLAN offline charging scenarios	No requirement	
5.2.1	Basic principles	No requirement	
5.2.1.1	Direct IP access	Complaint	Supports RADIUS.
5.2.1.2	3GPP IP access	Fully complaint	
5.2.2	Wf message flows	Not applicable	
5.2.2.1	Message Flows - WLAN session when WLAN access network supports accounting	Not applicable	

Table 12. 3GPP SCG to WLAN Offline Charging

Section Number	Section Title	Support	Comments
5.2.2.2	Message Flows - WLAN session when WLAN access network does not support accounting	Not applicable	
5.2.3	WLAN-AN-CDR generation	Fully complaint	Supports generation of W LAN– AN -CDR for PDG calls (AP / Datablade LBO)
5.2.4	WLAN-CDR generation	Fully complaint	
5.2.4.1	Triggers for WLAN-CDR charging information collection	Complaint	
5.2.4.1.1	Triggers for WLAN-CDR charging information addition	complaint	
5.2.4.1.2	Triggers for WLAN-CDR closure	Complaint	
5.2.5	Ga record transfer flows	Complaint	
5.2.6	B_w CDR file transfer		
5.3	WLAN online charging scenarios	Not applicable	
5.3.1	Basic principles	Not applicable	
5.3.2	Wo message flows	Not applicable	
5.3.2.1	Message flows - WLAN session where WLAN access network supports diameter credit control	Not applicable	
5.3.2.2	Message flows - WLAN session where WLAN access network support RADIUS/ diameter accounting (version 1)	Not applicable	
5.3.2.3	Message flows - WLAN session where WLAN access network support RADIUS/ diameter accounting (version 2)	Not applicable	
5.3.2.4	Message flows - WLAN session where WLAN access network does not support RADIUS/diameter accounting	Not applicable	
6	Definition of charging information	No requirement	
6.1	Data description for WLAN offline charging	No requirement	

Table 12. 3GPP SCG to WLAN Offline Charging

Section Number	Section Title	Support	Comments
6.1.1	Rf message contents	Compliant	Internal compliance since both, CTF and CDR reside in the SCG.
6.1.1.1	WLAN direct IP access charging message contents	Compliant	
6.1.1.1.1	Charging *data* request message	Compliant	
6.1.1.1.2	Charging data response message	Compliant	
6.1.2	GTP' message contents	Fully complaint	GTP' is used between the SCG and CGF.
6.1.3	CDR description on the Bw interface	Fully compliant	
6.1.3.1	CDR field types	Fully compliant	
6.1.3.2	CDR content	Fully compliant	
6.1.3.2.1	WLAN direct IP access CDR (WLAN-AN-CDR)	Complaint	
6.1.3.2.2	WLAN 3GPP IP access charging message contents	Complaint	
6.2	Data description for WLAN online charging	Not applicable	
6.2.1	Ro message contents	Not applicable	
6.2.1.1	WLAN direct IP access charging message contents	Not applicable	
6.2.1.1.1	Debit/reserve unit request message	Not applicable	
6.2.1.1.2	Debit/reserve unit response message	Not applicable	
6.2.1.2	WLAN 3GPP IP access charging message contents	Not applicable	
6.2.1.2.1	Debit/reserve unit request message	Not applicable	
6.2.1.2.2	Debit/reserve unit response message	Not applicable	
6.2.2	Detailed message formats	Not applicable	
6.2.2.1	WLAN direct IP access charging message contents	Not applicable	

Table 12. 3GPP SCG to WLAN Offline Charging

Section Number	Section Title	Support	Comments
6.2.2.2	WLAN 3GPP IP access charging message contents	Not applicable	
6.3	WLAN charging specific parameters	Not applicable	
6.3.1.1	WLAN charging information assignment for service-information	Not applicable	
6.3.1.2	Definition of WLAN information	Not applicable	
6.3.2	Formal WLAN charging parameter description	Not applicable	
6.3.2.1	WLAN charging information for CDRs	Not applicable	
6.3.2.2	Definition of the WLAN charging events	Not applicable	

3GPP SCG to GPRS Tunneling

Table 13 lists the 3GPP inter-working of the SCG to GPRS tunneling protocols. This is based on 3GPP TS 29.060 compliance aspects.

Table 13. 3GPP SCG to GPRS Tunneling

Section Number	Section Title	Support	Comments
1	Scope	No requirement	Informative
2	References	No requirement	Informative
3	Definitions and abbreviations	No requirement	Informative
3.1	Definitions	No requirement	Informative
3.2	Abbreviations	No requirement	Informative
4	General	Partially compliant	Used from the Wi-Fi offload perspective. The SCG acts as SGSN while interacting with GGSN. Does not support RAN, Iu (UTRAN-SGSN) and Gn (SGSN-SGSN) interfaces.
5	Transmission order and bit definitions	Fully compliant	

Table 13. 3GPP SCG to GPRS Tunneling

Section Number	Section Title	Support	Comments
6	GTP header	Compliant	Does not support NPDU and extension headers. Sequence numbers are present for GTPC but absent for GTPU.
6.1	Extension headers	Not applicable	
6.1.1	PDCP PDU number	Not applicable	
6.1.2	Suspend request	Not applicable	
6.1.3	Suspend response	Not applicable	
6.1.4	MBMS support indication	Not applicable	
7	GTP messages and message formats	No requirement	
7.1	Message formats	Compliant	Messages supported are listed in Compliance for GTPv1Section 7.1 .
7.1.1	Presence requirements of information elements	No requirement	
7.2	Path management messages	Compliant	Messages exchanged only between the SCG (SGSN) and GGSN.
7.2.1	Echo request	Compliant	Does not support private extension.
7.2.2	Echo response	Compliant	Does not support private extension.
7.2.3	Version not supported	Compliant	
7.2.4	Supported extension headers notification	Not applicable	
7.3	Tunnel management messages	No requirement	
7.3.1	Create PDP context request	Compliant	Refer to information in Compliance for GTPv1 Section 7.3.1.
7.3.2	Create PDP context response	Compliant	Attributes accepted as part of response is provided in Compliance for GTPv1 Section 7.3.2.
7.3.3	Update PDP context request	Compliant	Attributes sent in this message is provided in Compliance for GTPv1 Section 7.3.3.

Table 13. 3GPP SCG to GPRS Tunneling

Section Number	Section Title	Support	Comments
7.3.4	Update PDP context response	Compliant	Attributes decoded in this message is provided in Compliance for GTPv1 Section 7.3.4.
7.3.5	Delete PDP context request	Compliant	Attributes sent in this message is provided in Compliance for GTPv1Section 7.3.5.
7.3.6	Delete PDP context response	Compliant	Attributes sent in this message is provided in Compliance for GTPv1 Section 7.3.6.
7.3.7	Error indication	Compliant	The SCG (SGSN) handles and deletes the session if the message is initiated by GGSN. The SCG (SGSN) does not initiate it.
7.3.8	PDU notification request	Not applicable	
7.3.9	PDU notification response	Not applicable	
7.3.10	PDU notification reject request	Not applicable	
7.3.11	PDU notification reject response	Not applicable	
7.4	Location management messages	Not applicable	
7.5	Mobility management messages	Not applicable	
7.6	Reliable delivery of signaling messages	Compliant	
7.7	Information elements	Compliant	Supported Information elements are provided in this chapter.
7.7.1	Cause	Compliant	
7.7.2	IMSI	Fully complaint	
7.7.3	RAI	Fully complaint	
7.7.4	TLLI	Not applicable	
7.7.5	P-TMSI	Not applicable	
7.7.6	Reordering required	Not applicable	
7.7.7	Authentication triplet	Not applicable	
7.7.8	MAP cause	Not applicable	

Table 13. 3GPP SCG to GPRS Tunneling

Section Number	Section Title	Support	Comments
7.7.9	P-TMSI signature	Not applicable	
7.7.10	MS validated	Not applicable	
7.7.11	Recovery	Fully compliant	
7.7.12	Selection mode	Not applicable	
7.7.13	Tunnel endpoint identifier date I	Fully compliant	
7.7.14	Tunnel endpoint identifier control plane	Fully compliant	
7.7.15	Tunnel endpoint identifier date I1	Not applicable	
7.7.16	Teatdown Ind	Fully compliant	
7.7.17	NSAPI	Fully compliant	
7.7.18	RANAP cause	Not applicable	
7.7.19	RAB context	Not applicable	
7.7.20	Radio priority SMS	Not applicable	
7.7.21	Radio priority	Not applicable	
7.7.22	Packet flow Id	Not applicable	
7.7.23	Charging characteristics	Complaint	
7.7.24	Trace reference	Not applicable	
7.7.25	Trace type	Not applicable	
7.7.25A	MS not reachable reason	Not applicable	
7.7.25B	Radio priority LCS	Not applicable	
7.7.26	Charging Id	Not applicable	
7.7.27	End user address	Complaint	
7.7.28	MM context	Not applicable	
7.7.29	PDP context	Not applicable	
7.7.30	Access point name	Fully complaint	
7.7.31	Protocol configuration options	Fully complaint	
7.7.32	GSN address	Fully complaint	
7.7.33	MSISDN	Fully complaint	
7.7.34	QOS profile	Fully complaint	

Table 13. 3GPP SCG to GPRS Tunneling

Section Number	Section Title	Support	Comments
7.7.35	Authentication quintuplet	Not applicable	
7.7.36	TFT	Not applicable	
7.7.37	Target identification	Not applicable	
7.7.38	UTRAN transparent container	Not applicable	
7.7.39	RAB setup information	Not applicable	
7.7.40	Extension header type list	Not applicable	
7.7.41	Trigger Id	Not applicable	
7.7.42	OMC Identity	Not applicable	
7.7.43	RAN transport container	Not applicable	
7.7.44	Charging gateway address	Complaint	Supports only IPv4.
7.7.45	PDP context prioritization	Not applicable	
7.7.45A	Additional RAB setup information	Not applicable	
7.7.46	Private extension	Not applicable	
7.7.47	SGSN number	Not applicable	
7.7.48	Common flags	Not applicable	
7.7.49	APN restriction	Not applicable	
7.7.50	RAT type	Complaint	
7.7.51	User location information	Not applicable	
7.7.52	MS time zone	Not applicable	
7.7.53	IMEI (SV)	Not applicable	
7.7.54	CAMEL charging information container	Not applicable	
7.7.55	MBMS UE context	Not applicable	
7.7.56	Temporary mobile group identity	Not applicable	
7.7.57	RIM routing address	Not applicable	
7.7.58	MBMS protocol configuration options	Not applicable	
7.7.59	MBMS session duration	Not applicable	
7.7.60	MBMS service area	Not applicable	

Table 13. 3GPP SCG to GPRS Tunneling

Section Number	Section Title	Support	Comments
7.7.61	Source RNC PDCP context info	Not applicable	
7.7.62	Additional trace Info	Not applicable	
7.7.63	Hop counter	Not applicable	
7.7.64	Selected PLMN Id	Not applicable	
7.7.65	MBMS session identifier	Not applicable	
7.7.66	MBMS 2G/3G indicator	Not applicable	
7.7.67	Enhanced NSAPI	Not applicable	
7.7.68	Additional MBMS trace info	Not applicable	
7.7.69	MBMS session repetition number	Not applicable	
7.7.70	MBMS time to data transfer	Not applicable	
7.7.71	Void	No requirement	
7.7.72	BSS container	Not applicable	
7.7.73	Cell identification	Not applicable	
7.7.74	PDU numbers	Not applicable	
7.7.75	BSSGP cause	Not applicable	
7.7.76	Required MBMS bearer capabilities	Not applicable	
7.7.77	RIM routing address discriminator	Not applicable	
7.7.78	List of set-up PFCs	Not applicable	
7.7.79	PS handover XID parameters	Not applicable	
7.7.80	Reliable inter RAT handover info	Not applicable	
8	Controlplane (GTP-C)	Compliant	
8.1	Controlplane protocol	Fully compliant	
8.2	Usage of the GTP-C header	Compliant	
9	GTP-U	Fully compliant	
9.1	GTP-U protocol entity	Fully compliant	
9.1.1	Handling of sequence numbers	Not applicable	Does not support sequence numbers.
9.2	GTP-U service access points and primitives	Not applicable	

Table 13. 3GPP SCG to GPRS Tunneling

Section Number	Section Title	Support	Comments
9.3	Protocol stack	Fully compliant	
9.3.1	Usage of the GTP-U header	Fully compliant	
9.3.1.1	Usage of sequence number	Not applicable	Sequence number is supported only for control plane.
9.4	Tunneling between SGSNs	Not applicable	The SCG provides a Wi-Fi offload solution.
9.5	Tunneling between source RNC and target RNC	Not applicable	
9.6	Tunneling between GGSNs	Not applicable	
10	Path protocols	No requirement	
10.1	UDP/IP	Fully compliant	
10.1.1	UDP header	No requirement	
10.1.1.1	Request messages	Fully compliant	
10.1.1.2	Response messages	Fully compliant	
10.1.1.3	Encapsulated T-PDUs	Fully compliant	
10.1.1.4	Error indication, RAN information Relay, Version not supported and supported extension header notification	Compliant	
10.1.2	IP header	Fully compliant	
10.1.2.1	Request messages and encapsulated T-PDUs	Fully compliant	
10.1.2.2	Response messages	Fully compliant	
10.1.2.3	Error indication, RAN information Relay, Version not supported and supported extension header notification	Compliant	
11	Error handling	No requirement	
11.1	Protocol errors	Compliant	
11.1.1	Different GTP versions	Compliant	Supports GTPv1 and GTPv2. Does not support Fallback.

Table 13. 3GPP SCG to GPRS Tunneling

Section Number	Section Title	Support	Comments
11.1.2	GTP message too short	Fully compliant	
11.1.3	Unknown GTP signaling message	Fully compliant	
11.1.4	Unexpected GTP signaling message	Fully compliant	
11.1.5	Missing mandatory present information element	Fully compliant	
11.1.6	Invalid length	Fully compliant	
11.1.7	Invalid mandatory information element	Fully compliant	
11.1.8	Invalid optional information element	Fully compliant	
11.1.9	Unknown information element	Fully compliant	
11.1.10	Out of sequence information elements	Fully compliant	
11.1.11	Unexpected information element	Fully compliant	
11.1.12	Repeated information elements	Fully compliant	
11.1.13	Incorrect optional information elements	Fully compliant	
11.2	Path failure	Fully compliant	
11.3	MS detach	Fully compliant	
11.4	Restoration and recovery	Fully compliant	
12	Security provided to GTP communication over Gn and Gp interfaces	Not applicable	Security is provided only for mobility management messages, which is not supported.
13	IP, networking technology used by GTP	No requirement	
13.1	IP version	Fully compliant	Does not support IPv6.
13.2	IP fragmentation	Not applicable	Path MTU is set as less.
13.2.1	MO direction	Not applicable	
13.2.2	MT direction	Not applicable	
13.2.3	Tunneling from old to new SGSN	Not applicable	
14	GTP parameters	No requirement	

Table 13. 3GPP SCG to GPRS Tunneling

Section Number	Section Title	Support	Comments
14.1	Timers	Compliant	
14.2	Others	Compliant	

RFC Compliance

2

In this chapter:

Network Access Identifier - RFC 4282

Table 14 lists the RFC compliance 4282 for the SCG based on the network access identifier.

Table 14. Network access identifier - RFC 4286

Section Number	Section Title	SCG as		Ruckus AP	Comments
		Proxy Server	Hosted AAA Server		
1	Introduction	No requirement		No requirement	Informative
1.1	Terminology	No requirement		No requirement	Informative
1.2	Requirements language	No requirement		No requirement	
1.3	Purpose	No requirement		No requirement	
2	NAI definition	No requirement		No requirement	
2.1	Formal syntax	Fully compliant		Fully compliant	
2.2	NAI length considerations	Fully compliant		Fully compliant	
2.3	Support for username privacy	Non compliant		Non compliant	It is recommended to omit the user name rather than the fixed username.
2.4	International character sets	Compliant		Compliant	Does not support bidirectional characters.
2.5	Compatibility with email username	Fully compliant		Fully compliant	
2.6	Compatibility with DNS	Fully compliant		Fully compliant	
2.7	Realm construction	Partially compliant		Partially compliant	Does not support mediating realm.
2.8	Examples	No requirement		No requirement	Informative

Table 14. Network access identifier - RFC 4286

Section Number	Section Title	SCG as		Ruckus AP	Comments
		Proxy	Hosted AAA Server		
3	Security considerations	No requirement		No requirement	
4	IANA considerations	No requirement		No requirement	
Appendix A	Changes from RFC 2486	No requirement		No requirement	Informative

EAP-SIM - RFC 4186

Table 15 lists the RFC compliance 4186 for the SCG based on the EAP-SIM.

Table 15. EAP-SIM - RFC 4186

Section Number	Section Title	SCG Proxy Mode		SCG - Hosted AAA Mode	Comment
		AP-SCG	SCG-AAA		
1	Introduction	No requirement		No requirement	Descriptive
2	Terms	No requirement		No requirement	Informative
3	Overview	No requirement		No requirement	Informative
4	Operation	No requirement		No requirement	Informative
4.1	Version negotiation	Fully compliant		Fully compliant	
4.2	Identity management	No requirement		No requirement	
4.2.1	Format, generation and usage of peer identities	No requirement		No requirement	
4.2.1.1	General	No requirement		No requirement	Informative
4.2.1.2	Identity privacy support	No requirement		No requirement	Informative
4.2.1.3	Username types in EAP-SIM identities	Fully compliant		Fully compliant	

Table 15. EAP-SIM - RFC 4186

Section Number	Section Title	SCG Proxy Mode		SCG - Hosted AAA Mode	Comment
		AP-SCG	SCG-AAA		
4.2.1.4	Username decoration	Fully compliant		Not complaint	Only pre-pending string is allowed to decorate the username in non 3GPP proxy mode.
4.2.1.5	NAI realm portion	Not applicable		Not applicable	Requirement for PEER.
4.2.1.6	Format of the permanent username	Not applicable		Fully compliant	Informative
4.2.1.7	Generating pseudonyms and fast reauthentication identities by the server	Not applicable		Compliant	
4.2.1.8	Transmitting pseudonyms and fast reauthentication identities to the peer	Fully compliant		Fully compliant	
4.2.1.9	Usage of the pseudonym by the peer	Not applicable		Not applicable	PEER (STA) requirement.
4.2.1.10	Usage of the fast reauthentication Identity by the peer	Not applicable		Not applicable	PEER (STA) requirement.
4.2.2	Communicating the peer identity to the server	No requirement		No requirement	
4.2.2.1	General	Fully compliant		Fully compliant	
4.2.2.2	Fully compliant	Fully compliant		Fully compliant	Fully compliant.
4.2.3	Choice of identity for the EAP-response/identity	Not applicable		Not applicable	Requirement for PEER.

Table 15. EAP-SIM - RFC 4186

Section Number	Section Title	SCG Proxy Mode		SCG - Hosted AAA Mode	Comment
		AP-SCG	SCG-AAA		
4.2.4	Server operation in the beginning of EAP-SIM exchange	Not applicable		Fully compliant	
4.2.5	Processing of EAP-request/SIM/start by the peer	Not applicable		Not applicable	Requirement for PEER.
4.2.6	Attacks against identity privacy	Not applicable		Not Applicable	Requirement for PEER.
4.2.7	Processing of AT_IDENTITY by the server	Not applicable		Fully compliant	
4.3	Message sequence examples (informative)	No requirement		No requirement	Informative
4.3.1	Full authentication	Fully compliant		Fully compliant	
4.3.2	Fast reauthentication	Fully compliant		Fully compliant	
4.3.3	Fallback to full authentication	Fully compliant		Fully compliant	
4.3.4	Requesting the permanent identity 1	Fully compliant		Fully compliant	
4.3.5	Requesting the permanent identity 2	Fully compliant		Fully compliant	
4.3.6	Three EAP-SIM/start roundtrips	Fully compliant		Fully compliant	
5	Fast reauthentication	No requirement		No requirement	
5.1	General	Not applicable		Fully compliant	
5.2	Comparison to UMTS AKA	No requirement		No requirement	Informative
5.3	Fast reauthentication identity	Not applicable		Fully compliant	

Table 15. EAP-SIM - RFC 4186

Section Number	Section Title	SCG Proxy Mode		SCG - Hosted AAA Mode	Comment
		AP-SCG	SCG-AAA		
5.4	Fast reauthentication procedure	Not applicable		Fully compliant	
5.5	Fast reauthentication procedure when counter Is too small	Not applicable		Fully compliant	Unable to verify.
6	EAP-SIM notifications	No requirement		No requirement	
6.1	General	No requirement		No requirement	Informative
6.2	Result indications	Not compliant		Not compliant	
6.3	Error cases	No requirement			
6.3.1	Peer operation	Not applicable		Not applicable	Requirement for PEER.
6.3.2	Server operation	Fully compliant		Not compliant	
6.3.3	EAP failure	Fully compliant		Fully compliant	
6.3.4	EAP success	Partially compliant		Partially compliant	Does not support AT_RESULT_IND .
7	Key generation	Not applicable		Fully compliant	
8	Message format and protocol extensibility	No requirement		No requirement	
8.1	Message format	Fully compliant		Fully compliant	
8.2	Protocol extensibility	Compliant		Compliant	Supports EAP-SIM version 1.
9	Messages	No requirement		No requirement	
9.1	EAP-request/SIM/start	Fully Compliant		Fully Compliant	Supports EAP-SIM version 1.
9.2	EAP-response/SIM/ start	Fully compliant		Fully compliant	Peer operation.

Table 15. EAP-SIM - RFC 4186

Section Number	Section Title	SCG Proxy Mode		SCG - Hosted AAA Mode	Comment
		AP-SCG	SCG-AAA		
9.3	EAP-request/SIM/ challenge	Compliant		Compliant	Does not support AT_RESULT_IND .
9.4	EAP-response/SIM/ challenge	Fully compliant		Fully compliant	Peer operation
9.5	EAP-request/SIM/ reauthentication	Compliant		Compliant	Does not support AT_RESULT_IND .
9.6	EAP-response/SIM/ reauthentication	Compliant		Compliant	Peer operation. Does not support AT_RESULT_IND .
9.7	EAP response/SIM/ client error	Fully compliant		Fully compliant	Peer operation.
9.8	EAP request/SIM/ notification	Not compliant		Not compliant	
9.9	EAP response/SIM/ notification	Not compliant		Not compliant	
10	Attributes	No requirement		No requirement	Informative
10.1	Table of attributes	No requirement		No requirement	Informative
10.2	AT_VERSION_LIST	Fully compliant		Fully compliant	
10.3	AT_SELECTED_VERSION	Fully compliant		Fully compliant	Peer operation.
10.4	AT_NONCE_MT	Fully compliant		Fully compliant	Peer operation.
10.5	AT_PERMANENT_ID_REQ	Fully compliant		Fully compliant	
10.6	AT_ANY_ID_REQ	Fully compliant		Fully compliant	
10.7	AT_FULLAUTH_ID_REQ	Fully compliant		Fully compliant	

Table 15. EAP-SIM - RFC 4186

Section Number	Section Title	SCG Proxy Mode		SCG - Hosted AAA Mode	Comment
		AP-SCG	SCG-AAA		
10.8	AT_IDENTITY	Fully compliant		Fully compliant	Peer operation.
10.9	AT_RAND	Not applicable		Fully Compliant	The SCG passes the attribute between NAS and AAA server using a proxy mode.
10.10	AT_NEXT_PSEUDONYM	Fully compliant		Compliant	Realm is sent. The SCG passes the attribute between NAS and AAA server using a proxy mode.
10.11	AT_NEXT_REAUTH_ID	Fully compliant		Fully compliant	The SCG passes the attribute between NAS and AAA server using a proxy mode.
10.12	AT_IV, AT_ENCR_DATA, and AT_PADDING	Fully compliant		Fully compliant	The SCG passes the attribute between NAS and AAA server using a proxy mode.
10.13	AT_RESULT_IND	Not compliant		Not compliant	

Table 15. EAP-SIM - RFC 4186

Section Number	Section Title	SCG Proxy Mode		SCG - Hosted AAA Mode	Comment
		AP-SCG	SCG-AAA		
10.14	AT_MAC	Fully compliant		Full compliant	The SCG passes the attribute between NAS and AAA server using a proxy mode.
10.15	AT_COUNTER	Not applicable		Fully compliant	
10.16	AT_COUNTER_TOO_SMALL	Not applicable		Fully compliant	Peer operation
10.17	AT_NONCE_S	Not applicable		Fully compliant	
10.18	AT_NOTIFICATION	Not compliant		Not compliant	
10.19	AT_CLIENT_ERROR_CODE	Fully compliant		Fully compliant	
11	IANA considerations	No requirement		No requirement	
12	Security considerations	No requirement		No requirement	
12.1	A3 and A8 algorithms	Not applicable		Fully compliant	

Table 15. EAP-SIM - RFC 4186

Section Number	Section Title	SCG Proxy Mode		SCG - Hosted AAA Mode	Comment
		AP-SCG	SCG-AAA		
12.2	Identity protection	Fully compliant	Not compliant	Compliant	RADIUS messages are sent to the SCG using the SSH tunnel. A secure connection is not available since the SCG and AAA server are both assumed to be in operator core. The SCG supports pseudonym based authentication.
12.3	Mutual authentication and triplet exposure	Not applicable	Not compliant	Not compliant	Communication between the SCG and AAA/ HLR is unsecured.
12.4	Flooding the authentication center	Not compliant		Not compliant	
12.5	Key derivation	Not applicable		Fully complaint	
12.6	Cryptographic separation of keys and session independence	Not applicable		Fully complaint	
12.7	Dictionary attacks	Fully compliant		Fully compliant	
12.8	Credentials reuse	No requirement		No requirement	
12.9	Integrity and replay protection, and confidentiality	Fully compliant		Fully compliant	

Table 15. EAP-SIM - RFC 4186

Section Number	Section Title	SCG Proxy Mode		SCG - Hosted AAA Mode	Comment
		AP-SCG	SCG-AAA		
12.10	Negotiation attacks	Fully compliant		Fully compliant	
12.11	Protected result indications	Not compliant		Not compliant	
12.12	Man-in-the-middle attacks	Fully complaint	Not compliant	Not compliant	
12.13	Generating random numbers	Not applicable		Fully complaint	
13	Security claims	Not applicable		Fully complaint	
Appendix A	Test vectors	No requirement		No requirement	Informative
A.1	EAP-request/identity	No requirement		No requirement	Informative
A.2	EAP-response/identity	No requirement		No requirement	Informative
A.3	EAP-request/SIM/start	No requirement		No requirement	Informative
A.4	EAP-response/SIM/ start	No requirement		No requirement	Informative
A.5	EAP-request/SIM/ challenge	No requirement		No requirement	Informative
A.6	EAP-response/SIM/ challenge	No requirement		No requirement	Informative
A.7	EAP success	No requirement		No requirement	Informative
A.8	Fast reauthentication	No requirement		No requirement	Informative
A.9	EAP-request/SIM/re-authentication	No requirement		No requirement	Informative
A.10	EAP-response/SIM/re-authentication	No requirement		No requirement	Informative
Appendix B	Pseudo-random number generator	No requirement		No requirement	Informative

EAP-AKA - RFC 4187

Table 16 lists the RFC compliance 4187 for the SCG based on the EAP-AKA.

Table 16. EAP-AKA - RFC 4187

Section Number	Section Title	SCG as Proxy		SCG - Hosted AAA Mode	Comment
		Ruckus AP	SCG		
1	Introduction and motivation	No requirement		No requirement	Informative
2	Terms and conventions used in this document	No requirement		No requirement	Informative
3	Protocol overview	Fully compliant		Fully compliant	
4	Operation	No requirement		No requirement	
4.1	Identity management	No requirement		No requirement	
4.1.1	Format, generation and usage of peer identities	No requirement		No requirement	
4.1.1.1	General	No requirement		No requirement	Informative
4.1.1.2	Identity privacy support	Fully compliant		Fully compliant	
4.1.1.3	Username types in EAP-AKA identities	Fully compliant		Fully compliant	
4.1.1.4	Username decoration	Fully compliant	Not applicable	Fully compliant	
4.1.1.5	NAI realm portion	Fully compliant		Fully compliant	
4.1.1.6	Format of the permanent username	Fully compliant		Fully compliant	
4.1.1.7	Generating pseudonyms and fast reauthentication identities by the server	Fully compliant		Fully compliant	
4.1.1.8	Transmitting pseudonyms and fast reauthentication identities to the peer	Fully compliant		Fully compliant	
4.1.1.9	Usage of the pseudonym by the peer	Fully compliant		Fully compliant	

Table 16. EAP-AKA - RFC 4187

Section Number	Section Title	SCG as Proxy		SCG - Hosted AAA Mode	Comment
		Ruckus AP	SCG		
4.1.1.10	Usage of the fast reauthentication identity by the peer	Fully compliant		Fully compliant	
4.1.2	Communicating the peer identity to the server	No applicable		No applicable	Requirement for PEER
4.1.2.1	General	Fully compliant		Fully compliant	
4.1.2.2	Relying on EAP-response/ identity discouraged	Fully compliant		Fully compliant	
4.1.3	Choice of identity for the EAP-response/identity	Not applicable		Not applicable	Requirement for PEER
4.1.4	Server operation in the beginning of EAP-AKA exchange	Fully compliant		Fully compliant	
4.1.5	Processing of EAP-request/ AKA-identity by the peer	Not applicable		Not applicable	Requirement for PEER
4.1.6	Attacks against identity privacy	Not applicable		Not applicable	Requirement for PEER
4.1.7	Processing of AT_IDENTITY by the server	Fully compliant		Fully compliant	
4.2	Message sequence examples (informative)	No requirement		No requirement	Informative
4.2.1	Usage of AT_ANY_ID_REQ	No requirement		No requirement	Informative
4.2.2	Fallback on full authentication	No requirement		No requirement	Informative
4.2.3	Requesting the permanent identity 1	No requirement		No requirement	Informative
4.2.4	Requesting the permanent identity 2	No requirement		No requirement	Informative
4.2.5	Three EAP/AKA-identity round trips	No requirement		No requirement	Informative
5	Fast reauthentication	No requirement		No requirement	

Table 16. EAP-AKA - RFC 4187

Section Number	Section Title	SCG as Proxy		SCG - Hosted AAA Mode	Comment
		Ruckus AP	SCG		
5.1	General	Fully compliant		Fully compliant	
5.2	Comparison to AKA	No requirement		No requirement	Informative
5.3	Fast reauthentication identity	Fully compliant		Fully compliant	
5.4	Fast reauthentication procedure	Fully compliant		Fully compliant	
5.5	Fast reauthentication procedure when the counter is too small	No requirement		No requirement	
6	EAP-AKA notifications	No requirement		No requirement	
6.1	General	Non-compliant		Non-compliant	
6.2	Result indications	Non-compliant		Non-compliant	
6.3	Error cases	No requirement		No requirement	
6.3.1	Peer operation	Not applicable		Not applicable	
6.3.2	Server operation				Needs to be verified
6.3.3	EAP failure	Compliant		Compliant	Does not support AT_NOTIFICATION
6.3.4	EAP success			Compliant	Does not support AT_RESULT_IND and AT_NOTIFICATION
7	Key generation	Fully compliant		Fully compliant	
8	Message format and protocol extensibility	No requirement		No requirement	
8.1	Message format	Fully compliant		Fully compliant	
8.2	Protocol extensibility				

Table 16. EAP-AKA - RFC 4187

Section Number	Section Title	SCG as Proxy		SCG - Hosted AAA Mode	Comment
		Ruckus AP	SCG		
9	Messages	No requirement		No requirement	Informative
9.1	EAP-request/AKA-identity	Fully compliant		Fully compliant	
9.2	EAP-response/AKA-identity	Not applicable		Not applicable	Requirement for PEER
9.3	EAP-request/AKA-challenge	Compliant		Compliant	Does not support AT_RESULT_IND
9.4	EAP-response/AKA-challenge	Not applicable		Not applicable	Requirement for PEER
9.5	EAP-response/AKA-authentication-reject	Not applicable		Not applicable	Requirement for PEER
9.6	EAP-response/AKA-synchronization-failure	Not applicable		Not applicable	Requirement for PEER
9.7	EAP-request/AKA-reauthentication	Fully compliant		Fully compliant	AT_CHECK CODE is not verified
9.8	EAP-response/AKA-reauthentication	Not applicable		Not applicable	Requirement for PEER
9.9	EAP-response/AKA-client-error	Not applicable		Not applicable	Requirement for PEER
9.10	EAP-request/AKA-notification	Non compliant		Non compliant	Does not support AT_NOTIFICATION
9.11	EAP-response/AKA-notification	Not applicable		Not applicable	Requirement for PEER
10	Attributes	No requirement		No requirement	
10.1	Table of attributes	No requirement		No requirement	Informative
10.2	AT_PERMANENT_ID_REQ	Fully compliant		Fully compliant	

Table 16. EAP-AKA - RFC 4187

Section Number	Section Title	SCG as Proxy		SCG - Hosted AAA Mode	Comment
		Ruckus AP	SCG		
10.3	AT_ANY_ID_REQ	Fully compliant		Fully compliant	
10.4	AT_FULLAUTH_ID_REQ	Fully compliant		Fully compliant	
10.5	AT_IDENTITY	Fully compliant		Fully compliant	
10.6	AT_RAND	Fully compliant		Fully compliant	
10.7	AT_AUTN	Fully compliant		Fully compliant	
10.8	AT_RES	Fully compliant		Fully compliant	
10.9	AT_AUTS	Fully compliant		Fully compliant	
10.10	AT_NEXT_PSEUDONYM	Fully compliant		Fully compliant	
10.11	AT_NEXT_REAUTH_ID	Fully compliant		Fully compliant	
10.12	AT_IV, AT_ENCR_DATA, and AT_PADDING	Fully compliant		Fully compliant	
10.13	AT_CHECKCODE	Fully compliant		Fully compliant	AT_CHECK CODE is not verified
10.14	AT_RESULT_IND	Non compliant		Non compliant	
10.15	AT_MAC	Fully compliant		Fully compliant	
10.16	AT_COUNTER	Fully compliant		Fully compliant	
10.17	AT_COUNTER_TOO_SMALL				
10.18	AT_NONCE_S	Fully compliant		Fully compliant	
10.19	AT_NOTIFICATION	Non compliant		Non compliant	
10.20	AT_CLIENT_ERROR_CODE	Fully compliant		Fully compliant	
11	IANA and protocol numbering considerations	Compliant		Compliant	Does not support AT_RESULT _IND & AT_NOTIFIC ATION
12	Security considerations	No requirement		No requirement	
12.1	Identity protection	Fully compliant		Fully compliant	

Table 16. EAP-AKA - RFC 4187

Section Number	Section Title	SCG as Proxy		SCG - Hosted AAA Mode	Comment
		Ruckus AP	SCG		
12.2	Mutual authentication	Fully compliant		Fully compliant	Not verified
12.3	Flooding the authentication center	Non compliant		Non compliant	Does not support rate limiting
12.4	Key derivation	No requirement		No requirement	Informative
12.5	Brute force and dictionary attacks	No requirement		No requirement	Informative
12.6	Protection, replay protection, and confidentiality	Fully compliant		Fully compliant	
12.7	Negotiation attacks	No requirement		No requirement	Informative
12.8	Protected result indications	Non compliant		Non compliant	
12.9	Man-in-the-middle attacks	Fully compliant		Fully compliant	Not verified
12.10	Generating random numbers	Fully compliant		Fully compliant	Not verified
13	Security claims	No requirement		No requirement	Informative
Appendix A	Pseudo random number generator	No requirement		No requirement	Informative

RADIUS Support for EAP - RFC 3579

Table 17 lists the RFC compliance 3579 for the SCG based on the EAP.

Table 17. RADIUS Support for EAP - RFC 3579

Section Number	Section Title	SCG as		Ruckus AP	Comments
		Proxy Server	Hosted AAA Server		
1	Introduction	No requirement		No requirement	
1.1	Specification of requirement	No requirement		No requirement	
1.2	Terminology	No requirement		No requirement	
2	RADIUS support for EAP	Complaint		Complaint	
2.1	Protocol overview	Partially complaint		Partially complaint	
2.2	Invalid packets	Partially complaint		Partially complaint	EAP-NAK and DOS attack is not supported
2.3	Retransmission	Not applicable		Not applicable	
2.4	Fragmentation	Fully complaint		Fully complaint	
2.5	Alternative uses	Not applicable		Not applicable	
2.6	Usage guidelines	Complaint		Complaint	
2.6.1	Identifier space	Complaint		Complaint	
2.6.2	Role reversal	Not applicable		Not applicable	
2.6.3	Conflicting messages	Complaint		Complaint	
2.6.4	Priority	Complaint		Complaint	
2.6.5	Displayable messages	Complaint		Complaint	
3	Attributes	Fully complaint		Fully complaint	
3.1	EAP message	Fully complaint		Fully complaint	
3.2	Message authenticator	Complaint		Complaint	

Table 17. RADIUS Support for EAP - RFC 3579

Section Number	Section Title	SCG as		Ruckus AP	Comments
		Proxy Server	Hosted AAA Server		
3.3	Table of attributes	Fully complaint		Fully complaint	
4.1	Security requirements	No requirement		No requirement	
4.2	Security protocol	Not applicable		Not applicable	IPSec is not used
4.3	Security Issues	Partially complaint		Partially complaint	
4.3.1	Privacy Issues	Not applicable		Not applicable	
4.3.2	Spoofing and hijacking	Partially complaint		Partially complaint	
4.3.3	Dictionary attacks	Not applicable		Not applicable	
4.3.4	Known plain text attacks	Not applicable		Not applicable	
4.3.5	Replay attacks	Not applicable		Not applicable	
4.3.6	Negotiation attacks	Not applicable		Not applicable	
4.3.7	Impersonation	No requirement		No requirement	
4.3.8	Man in the middle attacks	Not applicable		Not applicable	
4.3.9	Separation of authenticator and authentication server	Partially complaint		Partially complaint	
4.3.10	Multiple databases	No requirement		No requirement	
5	IANA considerations	No requirement		No requirement	
6	References	No requirement		No requirement	
6.1	Normative references	No requirement		No requirement	
6.2	Informative references	No requirement		No requirement	

EAP - RFC 3748

Table 18 lists the RFC compliance 3748 for the SCG based on the EAP.

Table 18. EAP - RFC 3748

Section Number	Section Title	SCG as		Ruckus AP	Comments
		Proxy Server	**Hosted AAA Server**		
1	Introduction	No requirement		No requirement	
1.1	Specification of requirements	No requirement		No requirement	
1.2	Terminology	No requirement		No requirement	
1.3	Applicability	No requirement		No requirement	
2	Extensible authentication protocol (EAP)	Fully compliant		Fully compliant	
2.1	Support for sequences	Fully compliant		Fully compliant	
2.2	EAP multiplexing model	No requirement		No requirement	
2.3	Pass through behavior	Compliant		Compliant	SCG does not support EAP. Fails for AAA RADIUS server and Diameter server
2.4	Peer-to-Peer operation	Compliant	Not applicable	compliant	SCG supports EAP-TLS in proxy mode
3	Lower layer behavior	No requirement		No requirement	
3.1	Lower layer requirements	Not applicable		Not applicable	
3.2	EAP usage within PPP	Not applicable		Not applicable	

Table 18. EAP - RFC 3748

Section Number	Section Title	SCG as		Ruckus AP	Comments
		Proxy Server	Hosted AAA Server		
3.2.	PPP configuration option format	Fully compliant		Fully compliant	
3.3	EAP usage within IEEE 802	Compliant		Compliant	
3.4	Lower layer indications	Not applicable		Not applicable	
4	EAP packet format	Fully compliant		Fully compliant	
4.1	Request and response	Compliant		Compliant	Code, identifier, length, type and data
4.2	Success and failure	Fully compliant		Fully compliant	
4.3	Retransmission behavior	Compliant		Compliant	
5	Initial EAP request/ response types	Compliant		Compliant	
5.1	Identity	Compliant		Compliant	Piggyback
5.2	Notification	No requirement		No requirement	Notification is optional as mentioned in the RFC
5.3	NAK	Not applicable		Not applicable	
5.3.1	Legacy NAK	Not applicable		Not applicable	
5.3.2	Expanded NAK	Not applicable		Not applicable	
5.4	MD5-challenge	Compliant		Compliant	NAK and expanded NAK

Table 18. EAP - RFC 3748

Section Number	Section Title	SCG as		Ruckus AP	Comments
		Proxy Server	Hosted AAA Server		
5.5	One-Time Password (OTP)	Not applicable		Not applicable	
5.6	Generic Token Card (GTC)	Not applicable		Not applicable	Not applicable
5.7	Expanded types	Not applicable		Not applicable	
5.8	Experimental	Not applicable		Not applicable	Not applicable
6	IANA considerations	No requirement		No requirement	
6.1	Packet codes	Fully compliant		Fully compliant	
6.2	Method types	No requirement		No requirement	
7	Security considerations	No requirement		No requirement	
7.1	Threat model	No requirement		No requirement	
7.2	Security claims	No requirement		No requirement	
7.2.1	Security claims terminology for EAP methods	No requirement		No requirement	
7.3	Identity protection	Compliant		Compliant	
7.4	Man-in-the-middle attacks	No requirement		No requirement	
7.5	Packet modification attacks	Not applicable		Not applicable	
7.6	Dictionary attacks	Not applicable		Not applicable	
7.7	Connection to an untrusted network	Not applicable		Not applicable	
7.8	Negotiation attacks	Not applicable		Not applicable	
7.9	Implementation idiosyncrasies	Not applicable		Not applicable	
7.10	Key derivation	Complaint		Complaint	

Table 18. EAP - RFC 3748

Section Number	Section Title	SCG as		Ruckus AP	Comments
		Proxy Server	Hosted AAA Server		
7.11	Weak cipher suites	Not applicable		Not applicable	
7.12	Link layer	Not applicable		Not applicable	
7.13	Separation of authenticator and backend authentication server	Not applicable	Complaint	Not applicable	
7.14	Clear text passwords	Not applicable		Not applicable	
7.15	Channel binding	Not applicable		Not applicable	
7.16	Protected result indications	No requirement		No requirement	
8	Acknowledgments	No requirement		No requirement	
9	References	No requirement		No requirement	
9.1	Normative references	No requirement		No requirement	
9.2	Informative references	No requirement		No requirement	

RADIUS - RFC 2865

Table 19 lists the RFC compliance 2865 for the SCG based on the RADIUS.

Table 19. RADIUS as per RFC 2865

Section Number	Section Title	SCG as		Ruckus AP	Comments
		Proxy Server	**Hosted AAA Server**		
1	Introduction	No requirement		No requirement	Informative
1.1	Specification of requirement	No requirement		No requirement	Informative
1.2	Terminology	No requirement		No requirement	Informative
2	Operation	Fully complaint		Fully complaint	
2.1	Challenge/ response	Fully complaint		Fully complaint	
2.2	Interoperation with PAP and CHAP	No requirement		No requirement	
2.3	Proxy	Fully complaint	Not applicable	Fully complaint	
2.4	Why UDP?	No requirement		No requirement	Informative
2.5	Retransmission hints	No requirement		No requirement	InformativeInformative
2.6	Keep-Alive considered harmful	No requirement		No requirement	Informative
3	Packet format	Fully complaint		Fully complaint	
4	Packet types	Fully complaint		Fully complaint	
4.1	Access request	Partial complaint		complaint	User password and CHAP password is not implemented.
4.2	Access accept	Fully complaint		Fully complaint	
4.3	Access reject	Fully complaint		Not applicable	

Table 19. RADIUS as per RFC 2865

Section Number	Section Title	SCG as		Ruckus AP	Comments
		Proxy Server	**Hosted AAA Server**		
4.4	Access challenge	Fully complaint		Fully complaint	
5	Attributes	Partial complaint		Partial complaint	
5.1	User name	Fully complaint		Fully complaint	
5.2	User password	Not applicable		Not applicable	
5.3	CHAP password	Not applicable		Not applicable	
5.4	NAS-IP address	Fully complaint		Fully complaint	
5.5	NAS port	Fully complaint		Fully complaint	
5.6	Service type	Complaint		Complaint	Framed and authorize (5176) is used.
5.7	Framed protocol	Not applicable		Not applicable	
5.8	Framed-IP address	Not applicable		Not applicable	
5.9	Framed-IP netmask	Not applicable		Not applicable	
5.10	Framed routing	Not applicable		Not applicable	
5.11	Filter Id	Not applicable		Not applicable	
5.12	Framed MTU	Complaint		Complaint	Used only in request.
5.13	Framed compression	Not applicable		Not applicable	
5.14	Login-IP-Host	Not applicable		Not applicable	
5.15	Login-Service	Not applicable		Not applicable	
5.16	Login-TCP-Port	Not applicable		Not applicable	
5.17	Unassigned	Not applicable		Not applicable	
5.18	Reply message	Partial complaint		Not applicable	Used only in reject.

Table 19. RADIUS as per RFC 2865

Section Number	Section Title	SCG as		Ruckus AP	Comments
		Proxy Server	**Hosted AAA Server**		
5.19	Callback number	Not applicable		Not applicable	
5.20	Callback Id	Not applicable		Not applicable	
5.21	Unassigned)	Not applicable		Not applicable	
5.22	Framed route	Not applicable		Not applicable	
5.23	Framed-IPX-network	Not applicable		Not applicable	
5.24	State	Partial complaint		Partial complaint	Access request sent by AP is not present.
5.25	Class	Not applicable		Not applicable	
5.26	Vendor specific	Fully complaint		Fully complaint	
5.27	Session timeout	Fully complaint		Not applicable	
5.28	Idle timeout	Fully complaint		Not applicable	
5.29	Termination-action	Not applicable		Not applicable	
5.30	Called-Station-Id	Fully complaint		Fully complaint	
5.31	Calling-Station-Id	Fully complaint		Fully complaint	
5.32	NAS identifier	Fully complaint		Fully complaint	
5.33	Proxy state	Fully complaint	Not applicable	Not applicable	
5.34	Login-LAT-Service	Not applicable		Not applicable	
5.35	Login-LAT-Node	Not applicable		Not applicable	
5.36	Login-LAT-Group	Not applicable		Not applicable	
5.37	Framed-AppleTalk-link	Not applicable		Not applicable	

Table 19. RADIUS as per RFC 2865

Section Number	Section Title	SCG as		Ruckus AP	Comments
		Proxy Server	**Hosted AAA Server**		
5.38	Framed-AppleTalk-network	Not applicable		Not applicable	
5.39	Framed-AppleTalk-zone	Not applicable		Not applicable	
5.40	CHAP challenge	Not applicable		Not applicable	
5.41	NAS port type	Complaint		Complaint	
5.42	Port limit	Not applicable		Not applicable	
5.43	Login-LAT-Port	Not applicable		Not applicable	
5.44	Table of attributes	Partial complaint		Partial complaint	
6	IANA considerations	No requirement		No requirement	

RADIUS - RFC 4372

Table 19 lists the RFC compliance 4372 for the SCG based on the dynamic authorization extension to remote authentication dial in user service (RADIUS).

Table 20. RADIUS - RFC 4372

Section Number	Section Title	Compliance	Comment
1.	Introduction	No requirement	
1.1	Motivation	No requirement	
1.2	Terminology	No requirement	
2	Operation	No requirement	
2.1.	Chargeable User Identify (CUI) attribute	Compliant	
2.2	CUI attribute	Compliant	
3	Attribute table	Compliant	
4	Diameter considerations	Not applicable	
5	IANA considerations	No requirement	
6	Security considerations	Compliant	
7	Acknowledgments	No requirement	
8	References	No requirement	
8.1	Normative references	No requirement	
8.2	Informative references	No requirement	

RADIUS - RFC 5176

Table 21 lists the RFC compliance 5176 for the SCG based on the dynamic authorization extensions to remote authentication dial in user service (RADIUS).

Table 21. RADIUS - RFC 5176

Section Number	Section Title	TTG	Non TTG	Comment
1.	Introduction	No requirement		
1.1	Applicability	No requirement		
1.2	Requirements language	No requirement		
1.3	Terminology	No requirement		
2	Overview	No requirement		
2.1.	Disconnect Messages (DM)	Compliant		No acct terminate cause in DM-ACK. (disconnect message acknowledgment)
2.2	Change of Authorization Messages (CoA)	Compliant		
2.3	Packet format	Compliant		Messages from DAC (Dynamic Authorization Client) need to be assigned to the SCG IP address rather than the NAS IP address.
3	Attributes	Compliant		Does not support IPv6.
3.1.	Proxy state	Compliant		
3.2	Authorize only	Partially compliant		Ruckus AP does not support CoA service type authorize only.
3.3	State	Compliant		
3.4	Message authenticator	Compliant		

Table 21. RADIUS - RFC 5176

Section Number	Section Title	TTG	Non TTG	Comment
3.5	Error cause	Compliant		Error cause attribute values 201, 202, 406, 502, 504, 507 and 508 are not supported in this release.
3.6	Table of attributes	Compliant		
4	Diameter considerations	Not applicable		
5	IANA considerations	No requirement		
6	Security considerations	No requirement		
6.1	Authorization issues	Compliant		
6.2	IPsec usage guidelines	Non-compliant		This feature is not supported.
6.3	Replay protection	Partially compliant		The event timestamp attribute is not included in CoA. DM request checks for duplication of SCG initiated CoA/DM.
7	Example traces	No requirement		
8	References	No requirement		
8.1	Normative references	No requirement		
8.2	Informative references	No requirement		
9	Acknowledgments	No requirement		

RADIUS Extension - RFC 2869

Table 22 lists the RFC compliance 2869 for the SCG based on the RADIUS extension.

Table 22. RADIUS Extension - RFC 2869

Section Number	Section Title	SCG as		Ruckus AP	Comments
		Proxy Server	Hosted AAA Server		
1	Introduction	No requirement		No requirement	Information
1.1	Specification of requirements	No requirement		No requirement	Information
1.2	Terminology	No requirement		No requirement	Information
2	Operation	No requirement		No requirement	Information
2.1	RADIUS support for interim accounting updates	Complaint		Complaint	Supports accounting interim.
2.2	RADIUS support for Apple remote access protocol	Not applicable		Not applicable	
2.3	RADIUS support for EAP (Extensible Authentication Protocol)	Fully compliant		Fully compliant	Supports EAP inside RADIUS.
2.3.1	Protocol overview	Fully compliant		Fully compliant	The SCG acts as both proxy and AAA server.
2.3.2	Retransmission	Compliant		Compliant	Session timeout is present only in *accept message.*
2.3.3	Fragmentation	Fully complaint		Fully complaint	
2.3.4	Examples	Not applicable		Not applicable	Does not support EAP-PPP.

Table 22. RADIUS Extension - RFC 2869

Section Number	Section Title	SCG as		Ruckus AP	Comments
		Proxy Server	Hosted AAA Server		
2.3.5	Alternative uses	Not Applicable		Not Applicable	Does not support encapsulated EAP.
3	Packet format	Complaint		Complaint	
4	Packet type	Complaint		Complaint	
5	Attributes	Partially compliant		Partially compliant	The SCG does not use all the listed attributes.
5.1	Acct-Input-Gigawords				
5.2	Acct-Output-Gigawords				
5.3	Event timestamp	Not applicable		Not applicable	
5.4	ARAP password	Not applicable		Not applicable	
5.5	ARAP features	Not applicable		Not applicable	
5.5	ARAP-zone-access	Not applicable		Not applicable	
5.7	ARAP security	Not applicable		Not applicable	
5.8	ARAP security-data	Not applicable		Not applicable	
5.9	Password retry	Not applicable		Not applicable	
5.10	Prompt	Not applicable		Not applicable	
5.11	Connect info	Fully compliant		Fully compliant	
5.12	Configuration token	No requirement		No requirement	Does not support this attribute.
5.13	EAP message	Fully compliant		Fully compliant	
5.14	Message authenticator	Fully compliant		Fully compliant	

Table 22. RADIUS Extension - RFC 2869

Section Number	Section Title	SCG as		Ruckus AP	Comments
		Proxy Server	Hosted AAA Server		
5.15	ARAP challenge-response	No requirement		No requirement	
5.16	Acct-interim-interval	Fully compliant		No requirement	Configuration is available in the SCG UI.
5.17	NAS-Port-Id	No requirement		No requirement	
5.18	Framed pool	No requirement		No requirement	
5.19	Table of attributes	Partially compliant		Partially compliant	The listed attributes are compliant
6	IANA considerations	No requirement		No requirement	
7	Security considerations	No requirement		No requirement	
7.1	Message authenticator security	Fully compliant		Fully compliant	
7.2	EAP security	Not applicable		Not applicable	
8	References	No requirement		No requirement	
9	Acknowledgments	No requirement		No requirement	
10	Chair's address	No requirement		No requirement	
11	Author's address	No requirement		No requirement	
12	Full copyright statement	No requirement		No requirement	

RADIUS Accounting - RFC 2866

Table 23 lists the RFC compliance 2866 for the SCG based on the RADIUS accounting.

Table 23. RADIUS Accounting - RFC 2866

Section Number	Section Title	PDG Support (AP generated accounting packets, proxied by the SCG)		TTG Support (SCG generated accounting packets)	Comments
		Ruckus AP	**SCG**		
1	Introduction	No requirement		No requirement	Informative
1.1	Specification of requirement	No requirement		No requirement	Informative
1.2	Terminology	No requirement		No requirement	Informative
2	Operation	Compliant	Fully complaint	Fully complaint	Accounting packets initiated from Ruckus AP's for PDG does not have a secondary server option.
2.1	Proxy	Not applicable	Fully complaint	Fully complaint	
3	Packet format	Fully complaint		Fully complaint	
4	Packet type	Fully complaint		Fully complaint	
4.1	Accounting request	Fully complaint		Fully complaint	For TTG, NAS port type is set to 0 (ASYNC) and no NAS port. For PDG, NAS port type is set to as (19), wireless 802.11.
4.2	Accounting response	Fully complaint		Fully complaint	
5	Attributes	Fully complaint		Fully complaint	

Table 23. RADIUS Accounting - RFC 2866

Section Number	Section Title	PDG Support (AP generated accounting packets, proxied by the SCG)		TTG Support (SCG generated accounting packets)	Comments
		Ruckus AP	**SCG**		
5.1	Acct – Status Type	Fully complaint	Compliant	Complaint	Accounting on/off Proxy is not supported for TTG Calls as SCG has other mechanisms to handle the same.
5.2	Acct – Delay- Time	Fully complaint		Fully complaint	
5.3	Acct – Input – Octates	Non complaint		Non complaint	The attribute is present in interim message. The RFC recommends that the attribute is present in *stop*.
5.4	Acct – Output – Octates	Non complaint		Non complaint	The attribute is present in interim message. The RFC recommends that the attribute is present in *stop*.
5.5	Acct-Session-Id	Fully complaint		Fully complaint	For TTG, the case value is assigned by GGSN/PGW.
5.5	Acct-Authentic	Complaint		Not applicable	Only RADIUS is used.
5.7	Acct-Session-Time	Non complaint		Non complaint	The attribute is present in interim message. The RFC recommends that the attribute is present in *stop*.

Table 23. RADIUS Accounting - RFC 2866

Section Number	Section Title	PDG Support (AP generated accounting packets, proxied by the SCG)		TTG Support (SCG generated accounting packets)	Comments
		Ruckus AP	SCG		
5.8	Acct-Input-Packets	Non complaint		Non complaint	The attribute is present in interim message. The RFC recommends that the attribute is present in *stop*.
5.9	Acct-Output-Packets	Non complaint		Non complaint	The attribute is present in interim message. The RFC recommends that the attribute is present in *stop*.
5.10	Acct-Terminate-Cause	Complaint		Complaint	Only a few causes have been implemented.
5.11	Acct-Multi-Session-Id	Fully compliant		Not applicable	
5.12	Acct-Link-Count	Fully compliant		Not applicable	
5.13	Table of attributes	Complaint		Complaint	
6	IANA considerations	No requirement		No requirement	
7	Security considerations	No requirement		No requirement	
8	Change log	No requirement		No requirement	
9	References	No requirement		No requirement	
10	Acknowledgments	No requirement		No requirement	
11	Chair's address	No requirement		No requirement	
12	Author's address	No requirement		No requirement	

Table 23. RADIUS Accounting - RFC 2866

Section Number	Section Title	PDG Support (AP generated accounting packets, proxied by the SCG)		TTG Support (SCG generated accounting packets)	Comments
		Ruckus AP	SCG		
13	Full copyright statement	No requirement		No requirement	

Lightweight Directory Access Protocol (LDAP) - RFC 4511

Table 24 lists the RFC compliance 4511 for SCG based on the Lightweight Directory Access Protocol (LDAP).

Table 24. LDAP Compliance- RFC 4511

Section Number	Section Title	Proxy Requirement	Comments
1	Introduction	No requirement	
2	Conventions	No requirement	
3	Protocol model	No requirement	
4	Element of protocol	No requirement	
4.1	Common elements	No requirement	
4.2	Bind operations	Compliant	
4.3	Unbind operation	Compliant	
4.4	Unsolicited notification	Not compliant	
4.5	Search operation	Compliant	
4.6	Modify operation	Not compliant	
4.7	Add operation	Not compliant	
4.8	Delete operation	Not compliant	
4.9	Modify DN operation	Not compliant	
4.10	Compare operation	Not compliant	
4.11	Abandon operation	Not compliant	

Table 24. LDAP Compliance- RFC 4511

Section Number	Section Title	Proxy Requirement	Comments
4.12	Extended operation	Not compliant	
4.13	Intermediate response message	Not compliant	
4.14	Start TLS operation	Not compliant	
5	Protocol encoding	Compliant	
5.2	Transmission Control Protocol (TCP)	Compliant	
5.3	Termination of the LDAP session	Compliant	Unbind
6	Security considerations	Compliant	Simple authentication
7	Acknowledgments	No requirement	
8	Normative references	No requirement	
9	Informative references	No requirement	

SNMP v3 Compliance

3

In this chapter:

The following section lists the module details RFC compliance 2571 for the SCG to SNMP v3.

Module Compliance

Figure 1 shows the module compliance based on RFC 2571.

Figure 1. Statement of module compliance

Test Name	Purpose	Status
3.1.2.1	Walk MIB to collect variables	WARNING
3.6.1	Check system group	FAILED
3.6.2	Check sysORTable	PASSED
3.6.3	Check SNMP group	PASSED
3.9.1	Detect missing object in GROUP	WARNING
3.9.2	Detect missing objects in MIBs	WARNING

Boundary Conditions Compliance

Figure 2 shows the statement of boundary conditions compliance for RFC 2571.

Figure 2. Boundary conditions compliance

Test Name	Purpose	Status
3.1.2.1	Walk MIB to collect variables	WARNING
3.5.1.1	snmpInASNParseErrs	PASSED
3.5.1.2	Request with non-minimal encoding	PASSED
3.5.1.3.1	snmpInASNParseErrs	PASSED
3.5.1.3.2	snmpInBadVersions	PASSED
3.5.1.3.3	Request with 129 sub-ids	PASSED
3.5.1.4	Request with smaller BER length	PASSED
3.5.1.5	Request with larger BER length	PASSED
3.5.1.7	Request with unexpected PDUs	PASSED
3.5.2.1	Request with non-zero errorStatus	PASSED
3.5.2.2	Request with non-zero errorIndex	PASSED
3.5.2.3	Request with zero varbinds	PASSED
3.5.2.4	Request without using NULL	PASSED
3.5.2.5	Request with tooBig varbinds	PASSED
3.5.2.6	Request with MAX and MIN req-ID	PASSED

SNMP GET Compliance

Figure 3 shows the statement of SNMP GET compliance for RFC 2571.

Figure 3. SNMP GET compliance

Test Name	Purpose	Status
3.1.2.1	Walk MIB to collect variables	WARNING
3.3.1.1	GET on each variable	PASSED
3.3.1.2	GET on padded OIDs	PASSED
3.3.1.3	GET on non-existent OIDs	WARNING
3.3.1.4	GET on incomplete OIDs	FAILED
3.3.2.1	GET variables in unrelated tables	PASSED
3.3.2.2	GET variables in unrelated tables	FAILED
3.3.2.3	GET variables within same table	PASSED

SNMP Bulk Compliance

Figure 4 shows the statement of SNMP bulk compliance for RFC 2571.

Figure 4. SNMP bulk compliance

Test Name	Purpose	Status
3.1.2.1	Walk MIB to collect variables	WARNING
3.2.1.1	BULK with 0 vbind	PASSED
3.2.1.2	BULK with vbinds	PASSED
3.2.1.2.0	BULK WALK with configurable M , R and acceptable	PASSED
3.2.1.3	BULK with R and 0 vbinds	PASSED
3.2.1.4	BULK with R and vbinds	PASSED
3.2.1.5	BULK with N and 0 vbind	PASSED
3.2.1.6	BULK with N and vbinds	PASSED
3.2.1.7	BULK with N, R and 0 vbind	PASSED
3.2.1.8	BULK with N, R and vbinds	PASSED
3.2.2.1	BULK with negative R and 0 vbind	PASSED
3.2.2.2	BULK with negative R and vbinds	PASSED
3.2.2.3	BULK with negative N and 0 vbind	PASSED
3.2.2.4	BULK with negative R and vbinds	PASSED
3.2.2.5	BULK with negative N, R and 0 vbind	PASSED
3.2.2.6	BULK with negative N, R and vbinds	PASSED
3.2.3.1	BULK from 0.0	PASSED
3.2.3.2	BULK from 1.0	PASSED
3.2.3.3	BULK from 2.0	PASSED
3.2.3.4	BULK walking MIBs	PASSED
3.2.4.1	BULK with arbitrary OIDs	WARNING
3.2.4.2	BULK with large instance-IDs	FAILED
3.2.4.3	BULK with padded OIDs	PASSED
3.2.4.4	BULK on unrelated tables	PASSED
3.2.4.5	BULK on unrelated variables	PASSED
3.2.4.6	BULK on columnar objects	WARNING
3.2.5.1	BULK with large N and vbinds	PASSED
3.2.5.2	BULK with large R and few vbinds	FAILED
3.2.5.2.1	BULK with large R and few vbinds	PASSED

SNMP Next Compliance

Figure 5 shows the statement of SNMP next compliance for RFC 2571.

Figure 5. SNMP next compliance

Test Name	Purpose	Status
3.1.2.1	Walk MIB to collect variables	WARNING
3.1.2.3	Walk by column and scalar	never run
3.1.1.1	NEXT request from 0.0	PASSED
3.1.1.2	NEXT request from 1.0	PASSED
3.1.1.3	NEXT request from 2.0	PASSED
3.1.2.2	Walk and check object syntax	FAILED
3.1.3.1	NEXT with arbitrary OIDs	FAILED
3.1.3.2	NEXT with large instance-IDs	FAILED
3.1.3.3	NEXT with padded OIDs	PASSED
3.1.4.1	NEXT on unrelated tables	PASSED
3.1.4.2	NEXT with unrelated variables	PASSED
3.1.4.3	NEXT on columnar objects	PASSED
3.1.5	Check Request-ID correlation	PASSED

SNMP Set Compliance

Figure 6 shows the statement of SNMP set compliance for RFC 2571.

Figure 6. SNMP set compliance

Test Name	Purpose	Status
3.1.2.1	Walk MIB to collect variables	WARNING
3.4.1	SET read-write objects	FAILED
3.4.1.1	SET non-existent objects	WARNING
3.4.1.2	SET on incomplete OIDs	FAILED
3.4.1.3	SET read-write & read-create objects atomically	FAILED
3.4.2	SET with invalid syntax	FAILED
3.4.3.1	SET Integer below range	FAILED
3.4.3.1.0	SET Integer with lower/upper value	UNINITIATED
3.4.3.2	SET Integer above range	FAILED
3.4.3.3	SET Integer below enumeration	FAILED
3.4.3.3.0	SET Integer with lower/upper enumeration	UNINITIATED
3.4.3.4	SET Integer above enumeration	FAILED
3.4.4.1	SET non-ASCII NVT string	FAILED
3.4.4.1.0	SET ASCII NVT string	UNINITIATED
3.4.4.2	SET with wrong NVT string	FAILED
3.4.4.3	SET string below SIZE	FAILED
3.4.4.3.0	SET string with upper/lower SIZE	UNINITIATED
3.4.4.4	SET string above SIZE	FAILED
3.4.5.1	SET read-only objects	FAILED

SNMP v2c Compliance

4

In this chapter:

The following section lists the module details RFC compliance 1901 for the SCG to SNMP v2c.

Module Compliance

Figure 7 shows the module compliance based on RFC 1901.

Figure 7. Statement of module compliance

SNMPv2c Tests for All MIBs Loaded -- Module Compliance Group

Test Name	Purpose	Status
2.1.2.1	Walk MIB to collect variables	PASSED
2.6.1	Check system group	FAILED
2.6.2	Check sysORTable	PASSED
2.6.3	Check SNMP group	PASSED
2.9.1	Detect missing object in GROUP	WARNING
2.9.2	Detect missing objects in MIBs	WARNING

Boundary Conditions Compliance

Figure 8 shows the statement of boundary conditions compliance for RFC 1901.

Figure 8. Boundary conditions compliance

SNMPv2c Tests for All MIBs Loaded -- Boundary Conditions Group

Test Name	Purpose	Status
2.1.2.1	Walk MIB to collect variables	PASSED
2.5.1.1	snmpInASNParseErrs	PASSED
2.5.1.2	Request with non-minimal encoding	PASSED
2.5.1.3.1	snmpInASNParseErrs	PASSED
2.5.1.3.2	snmpInBadVersions	PASSED
2.5.1.3.3	Request with 129 sub-ids	PASSED
2.5.1.4	Request with smaller BER length	PASSED
2.5.1.5	Request with larger BER length	PASSED
2.5.1.7	Request with unexpected PDUs	PASSED
2.5.2.1	Request with non-zero errorStatus	PASSED
2.5.2.2	Request with non-zero errorIndex	PASSED
2.5.2.3	Request with zero varbinds	PASSED
2.5.2.4	Request without using NULL	PASSED
2.5.2.5	Request with tooBig varbinds	PASSED
2.5.2.6	Request with MAX and MIN req-ID	PASSED
2.8.1	snmpInBadCommunityNames	PASSED

SNMP GET Compliance

Figure 9 shows the statement of SNMP GET compliance for RFC 1901.

Figure 9. SNMP GET compliance

SNMPv2c Tests for All MIBs Loaded -- GET Group

Test Name	Purpose	Status
2.1.2.1	Walk MIB to collect variables	PASSED
2.3.1.1	GET on each variable	FAILED
2.3.1.2	GET on padded OIDs	WARNING
2.3.1.3	GET on non-existent OIDs	WARNING
2.3.1.4	GET on incomplete OIDs	FAILED
2.3.2.1	GET variables in unrelated tables	FAILED
2.3.2.2	GET variables in unrelated tables	FAILED
2.3.2.3	GET variables within same table	FAILED

SNMP Bulk Compliance

Figure 10 shows the statement of SNMP bulk compliance for RFC 1901.

Figure 10. SNMP bulk compliance

SNMPv2c Tests for All MIBs Loaded -- BULK Group

Test Name	Purpose	Status
2.1.2.1	Walk MIB to collect variables	PASSED
2.2.1.1	BULK with 0 vbind	PASSED
2.2.1.2	BULK with vbinds	PASSED
2.2.1.2.0	BULK WALK with configurable M , R and	PASSED
2.2.1.3	BULK with R and 0 vbinds	PASSED
2.2.1.4	BULK with R and vbinds	PASSED
2.2.1.5	BULK with N and 0 vbind	PASSED
2.2.1.6	BULK with N and vbinds	PASSED
2.2.1.7	BULK with N, R and 0 vbind	PASSED
2.2.1.8	BULK with N, R and vbinds	PASSED
2.2.2.1	BULK with negative R and 0 vbind	PASSED
2.2.2.2	BULK with negative R and vbinds	PASSED
2.2.2.3	BULK with negative N and 0 vbind	PASSED
2.2.2.4	BULK with negative R and vbinds	PASSED
2.2.2.5	BULK with negative N, R and 0 vbind	PASSED
2.2.2.6	BULK with negative N, R and vbinds	PASSED
2.2.3.1	BULK from 0.0	PASSED
2.2.3.2	BULK from 1.0	PASSED
2.2.3.3	BULK from 2.0	PASSED
2.2.3.4	BULK walking MIBs	PASSED
2.2.4.1	BULK with arbitrary OIDs	WARNING
2.2.4.2	BULK with large instance-IDs	FAILED
2.2.4.3	BULK with padded OIDs	PASSED
2.2.4.4	BULK on unrelated tables	PASSED
2.2.4.5	BULK on unrelated variables	PASSED
2.2.4.6	BULK on columnar objects	PASSED
2.2.5.1	BULK with large N and vbinds	PASSED
2.2.5.2	BULK with large R and few vbinds	FAILED
2.2.5.2.1	BULK with large R and few vbinds	UNINITIATED

SNMP Set Compliance

Figure 11 shows the statement of SNMP set compliance for RFC 1901.

Figure 11. SNMP set compliance

SNMPv2c Tests for All MIBs Loaded -- SET Group

Test Name	Purpose	Status
2.1.2.1	Walk MIB to collect variables	PASSED
2.4.1	SET read-write objects	FAILED
2.4.1.1	SET non-existent objects	FAILED
2.4.1.2	SET on incomplete OIDs	FAILED
2.4.1.3	SET read-write & read-create objects ato	FAILED
2.4.2	SET with invalid syntax	FAILED
2.4.3.1	SET Integer below range	FAILED
2.4.3.1.0	SET Integer within range	UNINITIATED
2.4.3.2	SET Integer above range	FAILED
2.4.3.3	SET Integer below enumeration	FAILED
2.4.3.3.0	SET Integer with lower/upper enumeratio	UNINITIATED
2.4.3.4	SET Integer above enumeration	FAILED
2.4.4.1	SET non-ASCII NVT string	FAILED
2.4.4.1.0	SET ASCII NVT string	UNINITIATED
2.4.4.2	SET with wrong NVT string	FAILED
2.4.4.3	SET string below SIZE	FAILED
2.4.4.3.0	SET string with upper/lower SIZE	UNINITIATED
2.4.4.4	SET string above SIZE	FAILED
2.4.5.1	SET read-only objects	FAILED
2.4.5.2	SET varbinds order processing	FAILED
2.4.5.3	SET varbinds order processing	FAILED
2.4.6.1	SET varbinds value processing	FAILED
2.4.6.1.0	SET two varbinds with both correct value	UNINITIATED
2.4.6.2	SET varbinds value processing	FAILED
2.4.6.2.0	SET two varbinds with both bad values	UNINITIATED
2.5.1.6	SET with constructed value	FAILED
2.5.1.6.0	SET with primitive value	UNINITIATED

Event Compliance - GTPv1

A

In this appendix the following sections are the compliances for 3GPP SCG to GPRS Tunneling.

NOTE: This release is complaint with GPP TS Rel6. The following optional informational element from REL7 is added as part of *CREATE PDP REQUEST* - Common Flag IE, which is specified in section 7.7.48 of 3GPP TS 29.060 Rel 7.

Compliance for GTPv1Section 7.1

Table 25 lists the attributes and the interfaces for GTPv1 informational events compliance. This is in compliance for section 7.1.

NOTE: This compliance is for 3GPP SCG to GPRS Tunneling.

Table 25. Compliance for section 7.1

Message Type Value (Decimals)	Message
1	Echo request
2	Echo response
16	Create PDP context request
17	Create PDP context response
18	Update PDP context request
19	Update PDP context response
20	Delete PDP context request
21	Delete PDP context response

Compliance for GTPv1 Section 7.3.1

Messages are sent from SCG using the *create PDP request*. Supports only primary PDP context activation procedure. GGSN address can be configured as IPv4 address. IPv6 address is not supported. This is in compliance for section 7.3.1. Table 26 lists the attributes and the requirement.

NOTE: This compliance is for 3GPP SCG to GPRS Tunneling.

Table 26. Compliance for section 7.3.1

Attribute (IE)	Requirement	Reference
Tunnel endpoint identifier data I	Mandatory	7.7.13
NSAPI	Mandatory	7.7.17 - Value is set to 5

Table 26. Compliance for section 7.3.1

Attribute (IE)	Requirement	Reference
SGSN address for signaling	Mandatory	GSN address 7.7.32
SGSN address for user traffic	Mandatory	GSN address 7.7.32
Quality of Service profile	Mandatory	7.7.34
Routing Area Identity (RAI)	Optional	7.7.3
Recovery	Optional	7.7.11
Protocol configuration options	Optional	7.7.31
RAT type	Optional	7.7.50
IMSI	Conditional	7.7.2
Tunnel endpoint identifier control plane	Conditional	7.7.14
End user address	Conditional	7.7.27
Access Point name	Conditional	7.7.30
MSISDN	Conditional	7.7.33
Charging Characteristics	Conditional	7.7.23

Compliance for GTPv1 Section 7.3.2

Messages are received by the SCG using the *create PDP context response.* Supports QoS changes on the control plane but it does not affect the data plane. This is in compliance for section 7.3. 2. Table 27 lists the attributes and the requirement.

NOTE: This compliance is for 3GPP SCG to GPRS Tunneling.

Table 27. Compliance for Section 7.3.2

Attribute (IE)	Requirement	Reference
Cause	Mandatory	7.7.1
Recovery	Optional	7.7.11
Protocol configuration options	Optional	7.7.31
Charging gateway address	Optional	7.7.44
Tunnel endpoint identifier data I	Conditional	7.7.13

Table 27. Compliance for Section 7.3.2

Attribute (IE)	Requirement	Reference
Tunnel endpoint identifier control plane	Conditional	7.7.14
Charging Id	Conditional	7.7.26
End user address	Conditional	7.7.27
GGSN address for control plane	Conditional	GSN address 7.7.32
GGSN address for user traffic	Conditional	GSN address 7.7.32
Quality of Service profile	Conditional	7.7.34

Compliance for GTPv1 Section 7.3.3

Messages are sent by the SCG (SGSN) using the *update PDP context request.* This is in compliance for section 7.3.3. Table 28 lists the attributes and the requirement.

NOTE: This compliance is for 3GPP SCG to GPRS Tunneling.

Table 28. Compliance for Section 7.3.3

Attribute (IE)	Requirement	Reference
Tunnel endpoint identifier data I	Mandatory	7.7.13
NSAPI	Mandatory	7.7.17
SGSN address for control plane	Mandatory	GSN Address 7.7.32
SGSN address for user traffic	Mandatory	GSN Address 7.7.32
Quality of Service profile	Mandatory	7.7.34
Recovery	Optional	7.7.11
Protocol configuration options	Optional	7.7.31
RAT type	Optional	7.7.50
IMSI	Conditional	7.7.2
Tunnel endpoint Identifier control plane	Conditional	7.7.14

Messages are received by the SCG (SGSN) using the *update PDP context request.* Requests are initiated from the GGSN. The PCO sends the updated PDP from the GGSN. MS is not updated with this data. Table 29 lists the attributes and the requirement.

Table 29. Compliance for Section 7.3.3

Attribute (IE)	Requirement	Reference
NSAPI	Mandatory	7.7.17
IMSI	Optional	7.7.2
Recovery	Optional	7.7.11
Protocol configuration options	Optional	7.7.31
Quality of Service profile	Optional	7.7.34
End user address	Optional	7.7.27

Compliance for GTPv1 Section 7.3.4

Messages are received by the SCG (SGSN) using the *update PDP context response,* which is initiated by the GGSN. This is in compliance for section 7.3.4. Table 30 lists the attributes and the requirement.

NOTE: This compliance is for 3GPP SCG to GPRS Tunneling.

Table 30. Compliance for Section 7.3.4

Attribute (IE)	Requirement	Reference
Cause	Mandatory	7.7.1
Recovery	Optional	7.7.11
Protocol configuration options	Optional	7.7.31
Charging gateway address	Optional	7.7.44
Tunnel endpoint identifier data I	Conditional	7.7.13
Tunnel endpoint identifier control plane	Conditional	7.7.14
Charging Id	Conditional	7.7.26
GGSN address for control plane	Conditional	GSN Address 7.7.32

Table 30. Compliance for Section 7.3.4

GGSN address for user traffic	Conditional	GSN Address 7.7.32
Quality of Service profile	Conditional	7.7.34

Messages are sent by the SCG (SGSN) using the *update PDP context response.* Requests are sent to the GGSN. Table 31 lists the attributes and the requirement.

Table 31. Compliance for Section 7.3.4

Attribute (IE)	Requirement	Reference
Cause	Mandatory	7.7.1
Recovery	Optional	7.7.11
Quality of Service profile	Conditional	7.7.34

Compliance for GTPv1Section 7.3.5

Messages are sent by the SCG (SGSN) using the *delete PDP context request,* which is received by the GGSN. The SCG (SGSN) receives these messages when GGSN initiates it using the *delete PDP context request*. This is in compliance for section 7.3.5. Table 32 lists the attributes and the requirement.

NOTE: This compliance is for 3GPP SCG to GPRS Tunneling.

Table 32. Compliance for Section 7.3.5

Attribute (IE)	Requirement	Reference
Teardown Ind	Conditional	7.7.16
NSAPI	Mandatory	7.7.17

Compliance for GTPv1 Section 7.3.6

Messages are sent by the SCG (SGSN) using the *delete PDP context response,* which is received by the GGSN. The SCG (SGSN) also decodes these messages when GGSN initiates it using the *delete PDP context response*. This is in compliance for section 7.3.6. Table 33 lists the attributes and the requirement.

NOTE: This compliance is for 3GPP SCG to GPRS Tunneling.

Table 33. Compliance for Section 7.3.6

Attribute (IE)	Requirement	Reference
Cause	Mandatory	7.7.1

Event Compliance - GTPv2-c

B

In this appendix:

NOTE: This release is complaint to GPP TS Rel6. The following optional informational element from REL7 is added as part of *CREATE PDP REQUEST* - Common Flag IE, which is specified in section 7.7.48 of 3GPP TS 29.060 Rel 7.

Compliance for GTPv2 Section 7.1

Table 34 lists the path management messages that SCG (SGW) supports. This is in compliance for section 7.1 of 3GPP SCG to GTPV2-c. The SCG decodes the message, *version not supported* message when it is initiated at PGW. The SCG does not initiate the message since it initiates the tunnel creation.

NOTE: This compliance is for 3GPP SCG to GTPV2-c.

Table 34. Compliance for section 7.1

Message Type	Message
1	Echo request
2	Echo response

Compliance for GTPv2 Section 7.2

Table 35 lists the tunnel management message that SCG (SGW) supports. This is in compliance for section 7.2.

NOTE: Refer to 3GPP SCG to GTPV2-c.

Table 35. Compliance for section 7.2

Message Type	Message	Supported Interface
32	Create session request	S2a, S5/S8 intf
33	Create session response	S2a, S5/S8 intf
34	Modify bearer request	S2a,S5/S8 intf
35	Modify bearer response	S2a,S5/S8 int
36	Delete session request	S2a, S5/S8 intf
37	Delete session response	S2a, S5/S8 intf
64	Modify bearer command	S2a, S5/S8 intf
65	Modify bearer command failure	S2a, S5/S8 intf
97	Update bearer request	S2a, S5/S8 intf

Table 35. Compliance for section 7.2

Message Type	Message	Supported Interface
98	Update bearer response	S2a, S5/S8 intf
99	Delete bearer request	S2a, S5/S8 intf
100	Delete bearer response	S2a, S5/S8 intf

Compliance for GTPv2 Section 7.2.1

Messages are initiated by the SCG and sent to PGW using the *create session request*. This is in compliance for section 7.2.1. Table 36 lists the attributes and the interfaces.

NOTE: Refer to 3GPP SCG to GTPV2-c.

Table 36. Compliance for section 7.2.1

Attribute (IE)	Presence	Instance	Interface (S2a, S5/S8, Both)	Comments
AMBR	C	0	Both	
APN	M	0	Both	Value is APN NI+OI
Bearer Context	M		Both	A bearer context is created.
Charging Characteristics	C	0	Both	This attribute is received from the HLR/HSS. If the value is not received from the external entity, it takes the default value.
F-TEID	M	0	Both	The SCG generates TEID and sends F-TEID to the control plane.
IMSI	C	0	Both	
Indication	C	0	Both	Value is set to zero
Maximum APN Restriction	C	0	S5/S8	Value is set to zero.
MSISDN	C	0	Both	Received from HLR/HSS

Table 36. Compliance for section 7.2.1

Attribute (IE)	Presence	Instance	Interface (S2a, S5/S8, Both)	Comments
PAA	C	0	Both	This attribute is the PDN address allocation, which is set to 0.0.0.0.
PDN Type	C	0	Both	Value is set to IPV4.
RAT Type	M	0	Both	RAT type indicates the non-3GPP IP access technology type. It can either be configured in the SCG or hard coded to type, which is supported by the SCG. In S5/S8 the value is EUTRAN and for S2a it is WLAN.
Recovery	C	0	Both	This attribute is included when the peer node is contacted for the first time.
Selection Mode	C	0	Both	The value is set to “MS or network provided APN, subscription verified”.
Serving Network	C	0	Both	MCC and MNC configured in the SCG UI.
User Location Information (ULI)	C	0	S5/S8	The values are MCC and MNC from UE realm.

Bearer Context Attributes for Section 7.2.1

Table 37 lists the attributes and the interfaces for bearer context.

Table 37. Bearer Context content

Attribute (IE)	Presence	Instance	Interface (S2a, S5/S8, Both)	Comments
Bearer QoS	M	0	Both	Bearer Level QoS
EBI	M	0	Both	EPS Bearer ID
F-TEID	C	2	S5/S8	S5/S8-U SGW F-TEID
F-TEID	C	6	S2a	S2a-U TWAN F-TEID

Compliance for GTPv2 Section 7.2.2

Messages are received by the SCG using the *create session response*. It is initiated by PGW. This is in compliance for section 7.2. 2. Table 38 lists the attributes and the interfaces.

NOTE: Refer to 3GPP SCG to GTPV2-c.

NOTE: Quality of Service (QoS) is not implemented in the datapath.

Table 38. Compliance for section 7.2.2

Attribute (IE)	Presence	Instance	Interface (S2a, S5/S8, Both)	Comments
AMBR	C	0	Both	
APN Restriction	C	0	S5/S8	
Bearer Context	M	0	Both	This includes QoS, charging Id and other attributes.
Cause	M	0	Both	
Change Reporting Action	C	0	S5/S8	
F-TEID	C	1	Both	

Table 38. Compliance for section 7.2.2

Attribute (IE)	Presence	Instance	Interface (S2a, S5/S8, Both)	Comments
IP Address	C	0	S5/S8	The IP address is the charging gateway address.
PAA	C	0	Both	
Protocol Configuration Options (PCO)	O	0	S2a	
Recovery	C	0	Both	This attribute is included when the peer node is contacted for the first time.

Bearer Context Attributes for Section 7.2.2

Table 39 lists the attributes and the interfaces for bearer context.

Table 39. Bearer Context content

Attribute (IE)	Presence	Instance	Interface (S2a, S5/S8, Both)	Comments
Bearer Flags	O	0	S5/S8	Bearer flags
Bearer QoS	C	0	Both	Bearer level QoS
Cause	M	0	Both	Cause
Charging Id	O	0	Both	Charging Id
EBI	M	0	Both	EPS Bearer ID
F-TEID	C	2	S5/S8	S5/S8-U PGW F-TEID
F-TEID	C	5	S2a	S2a-U PGW F-TEID
TFT	O	0	Both	Bearer modification and TFT change.

Compliance for GTPv2 Section 7.2.7

The SCG sends *modify bearer request* S5/S8 and S2a. When a modification occurs in the datapath due to roaming, the *modify bearer request* is sent from the SCG to PGW indicating the modifications. This is in compliance for section 7.2. 7. Table 40 lists the attributes and the interfaces.

NOTE: Refer to 3GPP SCG to GTPV2-c.

NOTE: Messages are supported on S5/S8 interface but not S2a interface according to the 3GPP specification of 29.274 versions 11.3.0. Deviations from the specification has been taken since *modify bearer request* is the only message, which indicates changes in the datapath.

Bearer Context Attributes for Section 7.2.7

Table 40. Compliance for section 7.2.7

Attribute (IE)	Presence	Instance	Interface (S2a, S5/S8, Both)	Comments
Bearer Context	C	0	Both	Bearer contexts to be modified
F-TEID	C	0	Both	
Indication	C	0	Both	
RAT Type	C	0	Both	This attribute is sent on the S5/S8 interfaces if the RAT type is modified. The S5/S8 value is UTRAN and for S2a it is WLAN.
Recovery	C	0	Both	This attribute is included when the peer node is contacted for the first time.
Serving Network	C	0	Both	
ULI	C	0	Both	

Table 41 lists the attributes and the interfaces for bearer context.

Table 41. Bearer Context content

Attribute (IE)	Presence	Instance	Interface (S2a, S5/S8, Both)	Comments
EBI	M	0	Both	EPS Bearer ID
TEID	C	1	Both	Dataplane TEID indicating the change in the datapath.

Compliance for GTPv2 Section 7.2.8

The SCG received the *modify bearer response* from PGW. This is in compliance for section 7.2.8. Table 42 lists the attributes and the interfaces.

NOTE: Refer to 3GPP SCG to GTPV2-c.

Table 42. Compliance for section 7.2.8

Attribute (IE)	Presence	Instance	Interface (S2a, S5/S8, Both)	Comments
Cause	M	0	Both	Probable causes are request accepted, request accepted partiality, context not found, service not supported.
MSISDN	C	0	Both	
EBI	C	0	Both	
AMBR	C	0	Both	
Bearer Contexts	M	0	Both	Bearer Contexts modified
Change Reporting Action	C	0	Both	
Recovery	C	0	Both	This attribute is included when the peer node is contacted for the first time.

Bearer Context Attributes for Section 7.2.8

Table 43 lists the attributes and the interfaces for bearer context.

Table 43. Bearer Context content

Attribute (IE)	Presence	Instance	Interface (S2a, S5/S8, Both)	Comments
EBI	M	0	Both	EPS Bearer ID
TEID	C	1	Both	Dataplane TEID indicating the change in the datapath.
Charging Id	O	0	S5/S8	Charging id.

Compliance for GTPv2 Section 7.2.9.1

Messages are sent by the SCG in delete session request message. This is in compliance for section 7.2.9.1. Table 44 lists the attributes and the interfaces.

NOTE: Refer to 3GPP SCG to GTPV2-c.

Table 44. Compliance for section 7.2.9.1

Attribute (IE)	Presence	Interface (S2a, S5/S8, Both)	Comments
EBI	M	Both	Linked EPS Bearer ID (LBI)

Compliance for GTPv2 Section 7.2.9.2

Messages are received by the SCG in delete bearer request message. This is in compliance for section 7.2.9.2. Table 45 lists the attributes and the interfaces.

NOTE: Refer to 3GPP SCG to GTPV2-c.

Table 45. Compliance for section 7.2.9.2

Attribute (IE)	Presence	Instance	Interface (S2a, S5/S8, Both)	Comments
EBI	C	0	Both	Linked EPS Bearer ID (LBI)
EBI	C	1	Both	EPS Bearer IDs
Bearer Context	O	0	S5/S8	Failed bearer context
PCO	C	0	S5/S8	Protocol Configuration Options (PCO)

Bearer Context Attributes for Section 7.2.9.2

Table 46 lists the attributes and the interfaces for bearer context.

Table 46. Bearer Context content

Attribute (IE)	Presence	Instance	Interface (S2a, S5/S8, Both)	Comments
EBI	M	0	Both	EPS Bearer ID (LBI)
Cause	M	0	Both	This attribute indicates the reason for unsuccessful handling of the bearer.

Compliance for GTPv2 Section 7.2.10.1

Messages are received by the SCG in delete session response. This is in compliance for section 7.2.10.1. Table 47 lists the attributes and the interfaces.

NOTE: Refer to 3GPP SCG to GTPV2-c.

Table 47. Compliance for section 7.2.10.1

Attribute (IE)	Presence	Instance	Interface (S2a, S5/S8, Both)	Comments
Cause	M	0	Both	Cause value
Recovery	C	0	Both	This attribute is included when the peer node is contacted for the first time.
Private Extension	O	0	Both	Private extension

Compliance for GTPv2 Section 7.2.10.2

Messages are sent by the SCG in delete bearer response. This is in compliance for section 7.2.10.2. Table 48 lists the attributes and the interfaces.

NOTE: Refer to 3GPP SCG to GTPV2-c.

Table 48. Compliance for section 7.2.10.2

Attribute (IE)	Presence	Instance	Interface (S2a, S5/S8, Both)	Comments
Cause	M	0	Both	Cause value
EBI	C	0	Both	Linked EPS Bearer ID (LBI)
Bearer Context	O	0	Both	Failed bearer context, if the SCG fails to delete bearer
Recovery	C	0	Both	This attribute is included when the peer node is contacted for the first time.

Bearer Context Attributes for Section 7.2.10.2

Table 49 lists the attributes and the interfaces for bearer context.

Table 49. Bearer Context content

Attribute (IE)	Presence	Instance	Interface (S2a, S5/S8, Both)	Comments
EBI	M	0	Both	EPS Bearer ID (LBI)
Cause	M	0	Both	This attribute indicates the reason for unsuccessful handling of the bearer.

Compliance for GTPv2 Section 7.2.14.1

Messages are sent by the SCG in modify bearer response. This is in compliance for section 7.2.14.1. Table 50 lists the attributes and the interfaces.

NOTE: Refer to 3GPP SCG to GTPV2-c.

NOTE: .QoS change is supported only in the control plane. Services are not implemented in data plane.

Table 50. Compliance for section 7.2.14.1

Attribute (IE)	Presence	Instance	Interface (S2a, S5/S8, Both)	Comments
Bearer Contexts	M	0	Both	Modified bearer context
AMBR	M	0	Both	Aggregate Maximum Bit Rate (APN-AMBR)

Bearer Context Attributes for Section 7.2.14.1

Table 51 lists the attributes and the interfaces for bearer context.

Table 51. Bearer Context content for section 7.2.14.1

Attribute (IE)	Presence	Instance	Interface (S2a, S5/S8, Both)	Comments
EBI	M	0	Both	EPS Bearer ID (LBI)
Bearer QoS	C	0	Both	Bearer Level QoS

Compliance for GTPv2 Section 7.2.14.2

Messages are received by the SCG in modify bearer failure. This is in compliance for section 7.2.14.2. Table 52 lists the attributes and the interfaces.

NOTE: Refer to 3GPP SCG to GTPV2-c.

Table 52. Compliance for section 7.2.14.2

Attribute (IE)	Presence	Instance	Interface (S2a, S5/S8, Both)	Comments
Cause	M	0	Both	Cause value
Recovery	C	0	Both	This attribute is included when the peer node is contacted for the first time.
Private Extension	O	VS	Both	Private Extension

Compliance for GTPv2 Section 7.2.15

Messages are received by the SCG in update bearer request. This is in compliance for section 7.2. 15. Table 53 lists the attributes and the interfaces.

NOTE: Refer to 3GPP SCG to GTPV2-c.

Table 53. Compliance for section 7.2.15

Attribute (IE)	Presence	Instance	Interface (S2a, S5/S8, Both)	Comments
Bearer Contexts	M	0	Both	Modified bearer context
PCO	C	0	S5/S8	Protocol Configuration Option
AMBR	M	0	Both	Aggregate Maximum Bit Rate (APN-AMBR)
Private Extension	O	0	Both	Private Extension

Bearer Context Attributes for Section 7.2.15

Table 54 lists the attributes and the interfaces for bearer context.

Table 54. Bearer Context content

Attribute (IE)	Presence	Instance	Interface (S2a, S5/S8, Both)	Comments
EBI	M	0	Both	EPS Bearer ID (LBI)
Bearer QoS	C	0	Both	Bearer Level QoS
TFT	C	0	Both	Bearer modification and TFT change.
PCO	CO	0	S5/S8	Protocol Configuration Options (PCO)

Compliance for GTPv2 Section 7.2.16

Messages are sent by the SCG in update bearer response. This is in compliance for section 7.2. 16. Table 55 lists the attributes and the interfaces.

NOTE: Refer to 3GPP SCG to GTPV2-c.

Table 55. Compliance for section 7.2.16

Attribute (IE)	Presence	Interface (S2a, S5/S8, Both)	Comments
Cause	M	Both	Cause value
Bearer Context	M	Both	
Recovery	C	Both	This attribute is included when the peer node is contacted for the first time.
PCO	CO	S5/S8	Protocol Configuration Options (PCO), contains the PCO received from PDN GW in create session response.

Bearer Context Attributes for Section 7.2.16

Table 56 lists the attributes and the interfaces for bearer context.

Table 56. Bearer Context content

Attribute (IE)	Presence	Interface (S2a, S5/S8, Both)	Comments
EBI	M	Both	EPS Bearer ID (LBI)
Cause	M	Both	This attribute indicates if the bearer handling was successful. If unsuccessful it gives the reason.
Recovery	C	Both	

Index

Numerics

B

C

E

G

M

N

P

R

S

T

350 West Java Dr. Sunnyvale, CA 94089. USA
www.ruckuswireless.com