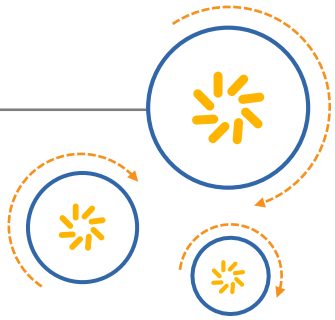
Qualcomm Technologies, Inc.



WLAN Offload via S2b Provisioning

Application Note

80-NP263-1 D

July 22, 2015

Qualcomm Technologies, Inc.
5775 Morehouse Drive
San Diego, CA 92121
U.S.A.

Revision history

Revision	Date	Description
A	Jun 2014	Initial release
B	Sep 2014	Updated Section 2.3.2; added Section 2.4
C	Feb 2015	Updated Section 2.1 and 2.2
D	Jul 2015	Updated Section 2.3.2

Contents

Tables

1 Introduction

1.1 Purpose

This document provides provisioning details to enable WLAN Offload over S2b/ePDG (IWLAN_S2b) functionality on Qualcomm Technologies, Inc. (QTI) MSM™ devices.

This document is intended for licensees, infrastructure vendors, and mobile operators interested in the enablement of WLAN Offload over S2b/ePDG (IWLAN_S2b).

1.2 Conventions

Function declarations, function names, type declarations, attributes, and code samples appear in a different font, for example, `#include`.

Shading indicates content that has been added or changed in this revision of the document.

1.3 Technical assistance

For assistance or clarification on information in this document, submit a case to QTI at https://support.cdmatech.com/.

If you do not have access to the CDMATech Support website, register for access or send email to support.cdmatech@qti.qualcomm.com.

2 WLAN Offload (S2b) configuration

This chapter describes NV settings needed to enable WLAN Offload over S2b on QTI MSM devices.

WLAN Offload configuration involves:

- Setting NV items
- Setting Android™-specific properties
- Setting provisioning properties in the PDN database
- Provisioning IWLAN connection parameters

2.1 WLAN offload configuration NV

Table 2-1 describes the settings for WLAN Offload config NV items.

Table 2-1 WLAN Offload configuration NV items

S #	NV item	Value		Description	Default	Recommendation
1.	70315	0	WLAN Offload Disabled	WLAN Offload configuration – Determines the WLAN Offload type	0 – WLAN Offload disabled	2 (for IWLAN_S2B support)
		1	WLAN Local Breakout			
		2	IWLAN_S2b and WLAN Local Breakout			
2.	69679	0x01		ds_apn_switching – Indicates whether the APN switching feature for attach and on demand PDNs is enabled	If the NV item is not set, the default behavior is to enable the APN switching feature; it should be turned off during runtime for backward compatibility.	0x01

S #	NV item	Value	Description	Default	Recommendation
3.	70316	0 to 500	data_wlan_throttle_timer – The data WLAN throttle timer (t_wlan) is the timer used to ensure that IWLAN RAT is throttled after a handoff is initiated from IWLAN to WWAN RATs following the loss of WLAN connectivity. The timer is in seconds.	120	120
4.	71567	0 to 255	epc_handoff_retry_count – Indicates the number of times handoff retries are attempted in case of failure before giving up handoff to a specific RAT	1	0
5.	72536	1 to 255	wifi_oos_linger_timer – Time in seconds after which the UE shall bring down WLAN LB iface when a WLAN Unavailable indication is received	180	180
6.	72554	1 to 5000	Data LTE MAPCON Hysteresis Timer – Timer in milliseconds for which LTE is assumed to be in service and continues to be provided as MPPM's WWAN preferred RAT after LTE goes OoS	1000	1000
7.	72555	1 to 5000	Data EHRPD MAPCON Hysteresis Timer – Timer in milliseconds for which EHRPD is assumed to be in service and continues to be provided as MPPM's WWAN preferred RAT after EHRPD goes OoS	2000	2000
8.	72556	1 to 5000	Data LTE MAPCON Wait (for ATTACH) Timer – Timer in milliseconds during which LTE is reported as MPPM's WWAN preferred RAT and is assumed to be in service (while waiting for LTE Attach procedure to complete)	3000	3000

2.2 WLAN Offload Linux Android properties

Table 2-2 describes settings specific to Linux Android properties.

Table 2-2 WLAN Offload Linux Android properties

S #	Android property	Value	Description	Default	Recommendation
1.	persist.data.iwlan.enable	TRUE/FALSE	This property is used to turn on IWLAN-specific functionality in Android if set to TRUE. If it is set to FALSE, WLAN Offload functionality is turned off on Linux Android.	FALSE	TRUE
2.	persist.data.iwlan.rekey	0 to 2^{32}-1	This property is used to set the ESP packet sequence number threshold value before an ESP rekey should be triggered.	2^{32}-1	2^{32}-1

2.3 WLAN Offload EFS configuration

2.3.1 Provisioning of PDN database file for MAPCON policies

This section discusses the provisioning of the PDN database (also known as PDN DB) via an EFS text file. The PDN DB needs to be provisioned in order to access the MAPCON functionality, thereby providing simultaneous access to the WLAN and the WWAN technologies.

The PDN DB file is an EFS file containing tokens and values associated with them. The EFS file format follows the standard Param_Name:Param_Val; rule. The Param_Name refers to the token name, and the Param_Val refers to the value/value list associated with the token Param_Name. Note that the tokens-value combinations end with a semicolon (;). Each new token is typically placed on a new line.

A token set comprises a list of two or more (up to a maximum of four) tokens for the PDN database file. The PDN database file can include multiple token sets, each token set typically associated with a particular APN name.

The PDN database file contains the following tokens (and associated values) in a single token set:

- PDN_APN_String – This is the token used to indicate the APN name associated with a PDN, for example, PDN_APN_String:internet.
- The PDN_APN_String token is mandatory and identifies a particular token set. It can take an array of characters of up to 100 bytes to represent an APN name. Some special values the PDN_APN_String token can incorporate are:
  - NULL – This indicates the NULL APN.
  - * – This is the identification of an implicit APN. In the absence of a default APN (default token details mentioned below), the implicit APN can be used as the default APN. Rules associated with the implicit APN token apply to all APNs that are not explicitly mentioned in the PDN DB file.
- Supported_RAT_Priority_List – This is the token that is used to indicate all the RATs the PDN with the above APN name can be associated with in ascending order of priority. There are currently three available values for RATs:
  - WWAN
  - WLAN_LB
  - IWLAN
- The supported RAT list is to be provisioned as a list of RATs (any combination of the above three values) in ascending order of priority separated by a comma (,), for example, Supported_RAT_Priority_List:WLAN_LB, WWAN, IWLAN.
- The Supported_RAT_Priority_List is a mandatory token and needs to be provisioned for every associated APN.
- Default – This is the token that is used to indicate whether a particular APN name specified in the PDN_APN_String token is the default APN for the carrier. It currently takes two values, TRUE or FALSE; default is TRUE.
- The default for a particular APN is not a mandatory token. The absence of the default token sets the default value to FALSE for the associated APN.
- If multiple APNs have the default token set to TRUE, the last APN to set its default token to TRUE is chosen to be the default APN per QTI's implementation. The default token values for all APNs prior to this are set to FALSE.

- Override_Type − Implementation of handoffs between the WLAN_S2b and the WWAN (LTE/eHRPD) technologies are as mentioned in *Mobility between 3GPP-Wireless Local Area Network (WLAN) Interworking and 3GPP Systems* (3GPP TS 23.327 (Rel 10)). However, Override_type provides a procedure to override the standards-based handoff behavior between the WLAN_S2b and the WWAN technologies for the associated APN. The Override_Type token takes three values:
  - API – An application can trigger handoffs from one technology to another explicitly by invoking an API provided by either QTI's QMI framework (for applications residing in the AP) or QTI's DSS API framework (for applications residing in the modem).
  - OPTION – Handoffs can be triggered based on a global option change on the Linux Android UI. This can be specified for certain APNs using OPTION as the value associated with the Override_Type token.
  - NONE – This has been defined just for completeness. If there is no Override_Type value associated with a particular APN, the user can explicitly set the value associated with Override_Type to NONE.
- Override_Type for a particular APN is not a mandatory token. The absence of the Override_Type token sets the default value for it to NONE for the associated APN.
- In short, the PDN DB file is made up of multiple such token sets. Each token set can be characterized as containing the following tokens:

```
PDN_APN_String: {name,NULL,*};
<compulsory, required to identify a token set>
Supported_RAT_Priority_List: {WWAN, IWLAN, WLAN_LB};
<compulsory>
Default: {TRUE, FALSE};
<optional, default value if absent set to FALSE>
Override_Type: {API, OPTION, NONE};
<optional, default value if absent set to NONE>
```

To create a PDN database file in EFS, create a folder named "data" under the root directory in EFS. Create a text file titled pdn_policy_db.txt. Add token sets as appropriate in the file. A sample token set configuration is:

```
PDN_APN_String:admin;
Supported_RAT_Priority_List:IWLAN;

PDN_APN_String:ims;
Override_Type:API;
Supported_RAT_Priority_List:WWAN, IWLAN;
```

```
PDN_APN_String:internet;
Default:TRUE;
Override_Type:OPTION;
Supported_RAT_Priority_List:WLAN_LB, WWAN, IWLAN;

PDN_APN_String:*;
Supported_RAT_Priority_List:WWAN, IWLAN;
```

Sample pdn_policy_db.txt

A sample of the /data/pdn_policy_db.txt EFS file is as follows:

```
PDN_APN_String:admin;
Supported_RAT_Priority_List:WWAN;

PDN_APN_String:ims;
Override_Type:API;
Supported_RAT_Priority_List:WWAN, IWLAN;

PDN_APN_String:internet;
Default:TRUE;
Supported_RAT_Priority_List:WWAN;

PDN_APN_String:app;
Supported_RAT_Priority_List:WWAN, IWLAN;

PDN_APN_String:emergency;
Supported_RAT_Priority_List:WWAN;

PDN_APN_String:enterprise;
Supported_RAT_Priority_List:WWAN;

PDN_APN_String:*;
Supported_RAT_Priority_List:WWAN;
```

2.3.2 Provisioning of IWLAN S2b-specific EFS configuration

This section discusses the IWLAN S2b configuration file needed to provision IPSec IKEv2 connection parameters. When this file is provisioned, the configuration parameters shall be picked from this file. The list of parameters and parameter values are given in Table 2-3.

To configure the IWLAN S2b parameters in the EFS, create a text file named iwlan_s2b_config.txt under the /data directory in EFS.

- File contents should have the following format:
  - For a parameter that takes only a single value, the format should be <parameter_name>:<parameter_value>;
  - For a parameter that can take multiple values, the format should be <parameter_name>:<parameter_value_1>,<parameter_value_2>;
- Parameter name and value should be separated by a colon (:).
- Multiple parameter values should be separated by a comma (,).
- The last parameter value for each parameter should be followed by a semicolon (;).
- Some parameters in the EFS file are optional. If any of these parameters are not present, that parameter assumes the default value mentioned in Table 2-3.
- The parameters can be mentioned in any order.
- The <parameter_name> string should exactly match the entries listed in the first column of the table. These strings are not case-sensitive. In case of any typo, that parameter entry will not take effect. It will be treated as an invalid entry, and the default value for the parameter takes effect.
- The <parameter_value> string should exactly match the entries listed in the second column of the table. These strings are not case-sensitive. In case of any typo, that parameter entry will not take effect. It will be treated as an invalid entry, and the default value for the parameter takes effect.

Example file:

```
#iwlan_s2b_config.txt
epdg_fqdn:wireless.epdg.com;
epdg_ipv4_address:10.20.30.40;
natt_enabled:TRUE;
natt_keep_alive_timer_sec:60;
ikev2_sa_rekey_timer_soft_sec:3000;
ikev2_sa_rekey_timer_hard_sec:3600;
ikev2_retransmit_timer_sec:2;
ikev2_max_retries:3;
ikev2_dpd_timer_sec:120;
esp_max_tunnel_timer_sec:300;
esp_rekey_timer_soft_sec:1500;
esp_rekey_timer_hard_sec:1800;
cert_req_enabled:FALSE;
ikev2_self_id_type:ID_RFC822_ADDR_MAC;
ikev2_peer_id_type:ID_KEY_ID;
ke_payload_enabled:FALSE;
pcscfv4_attr_type_val:16389;
pcscfv6_attr_type_val:16390;
pcscfv6_with_prefix_len:TRUE;
ikev2_dh_group_list:2,5,14;
ikev2_eap_fra_pseudo_enabled:FALSE;
pdn_throttle_timer_values_sec:0,0,60,120,480,900;
ikev2_encr_algo_list:2,3,12;
ikev2_aes_cbc_encr_key_size_list:128,256;
ikev2_aes_ctr_encr_key_size_list:128,256;
ikev2_hash_algo_list:1,2,5;
ikev2_prf_algo_list2,4;
esp_encr_algo_list:2,3,12;
esp_aes_cbc_encr_key_size_list:128,256;
esp_aes_ctr_encr_key_size_list:128,256;
esp_auth_algo_list:1,2,5;
configured_ike_port:4500;
ikev2_eap_reauth_realm_enabled:FALSE;
static_fqdn_enabled:TRUE;
epdg_plmn_list:123456;
epdg_fqdn_validation_enabled:FALSE;
```

Table 2-3 provides a list of all parameters that can be configured in the iwlan_s2b_config.txt file along with a description of each parameter, the possible range, and default values that will be used if the parameter is not provisioned in the file. Column 2 of Table 2-3 mentions whether the parameter is mandatory. If a mandatory parameter is not present, the IWLAN S2b call will not be allowed.

NOTE: All fields in Table 2-3 are subject to change or deletion.

Table 2-3 IWLAN S2b configuration parameter names and description

Parameter name	Mandatory	Value range	Default value	Description	Applicable modem PLs
epdg_fqdn	Yes	1 to 100 characters	NA	Stores the ePDG FQDN to be used in the DNS query to retrieve the ePDG server's IP address.	All
epdg_ipv4_address	No	0.0.0.0 to 255.255.255.255	NA	Stores the static ePDG IP address if the ePDG has an IPv4 address.	All
natt_enabled	No	TRUE, FALSE	TRUE	Flag to indicate whether NATTraversal support is enabled; that is, NAT detection and UDP encapsulation of ESP packets.	All
natt_keep_alive_timer_sec	No	0 to 2^{32}-1	60	Time in seconds after which the UE shall send NATT keep-alive messages.	All
ikev2_sa_rekey_timer_soft_sec	No	0 to 2^{32}-1	3000	Time in seconds after which the UE shall start an IKE SA rekey procedure.	All
ikev2_sa_rekey_timer_hard_sec	No	0 to 2^{32}-1	3600	Time in seconds after which the UE shall tear down IKE SA if rekey procedure has not succeeded.	All
ikev2_retransmit_timer_sec	No	0 to 2^{32}-1	2	Time in seconds after which the UE shall retransmit an IKEv2 packet if it does not receive a response.	All

Parameter name	Mandatory	Value range	Default value	Description	Applicable modem PLs
ikev2_max_retries	No	0 to 2^{32}-1	3	Maximum number of times a UE shall retransmit an IKEv2 packet if it does not receive a response.	All
ikev2_dpd_timer_sec	No	0 to 2^{32}-1	120	Time period in seconds after which the UE shall perform the DPD.	All
esp_max_tunnel_timer_sec	No	0 to 2^{32}-1	300	Maximum time in seconds for tunnel setup.	All
esp_rekey_timer_soft_sec	No	0 to 2^{32}-1	1500	Time in seconds after which the UE shall start an ESP SA rekey procedure.	All
esp_rekey_timer_hard_sec	No	0 to 2^{32}-1	1800	Time in seconds after which the UE shall tear down an ESP SA if a rekey procedure has not succeeded.	All
cert_req_enabled	No	TRUE, FALSE	FALSE	Used to determine if certificates are used to authenticate the ePDG server during tunnel establishment procedures.	All
ikev2_self_id_type	No	ID_RFC822_ ADDR ID_RFC822_ ADDR_MAC	ID_RFC822_ADDR_MAC	Specifies the format of the IDi that should be used in the IKEv2 authentication message(s): ▪ ID_RFC822_ADDR is the 3GPP standard IDi format. ▪ ID_RFC822_ADDR_MAC is the ID_RFC822_ADDR-based IDi format with inclusion of the AP's MAC address.	All

Parameter name	Mandatory	Value range	Default value	Description	Applicable modem PLs
ikev2_peer_id_type	No	ID_FQDN ID_KEY_ID	ID_KEY_ID	Specifies the format of the IDr that should be used in the IKEv2 authentication message(s).	All
ke_payload_enabled	No	TRUE, FALSE	TRUE	Used to determine if the KE payload should be sent during UE-initiated ESP SA rekey.	All
pcscfv4_attr_type_val	No	16384-32767	16389	Specifies the PCSCF v4 attribute type value used in the IKEv2 exchange.	DI.4.0+ DPM.2.0 BO
pcscfv6_attr_type_val	No	16384-32767	16390	Specifies the PCSCF v6 attribute type value used in the IKEv2 exchange.	DI.4.0+ DPM.2.0 BO
pcscfv6_with_prefix_len	No	TRUE, FALSE	TRUE	Used to determine the accepted length of the PCSCF v6 address; TRUE indicates 17 bytes, FALSE indicates 16 bytes.	All
ikev2_dh_group_list	No	{2,5,14}	2, 5, 14	Specifies the DH group types that are supported by the UE; the first type listed will be used in the initial IKE exchange.	DI.3.0 BO
epdg_call_setup_timer_sec	No	0 to 2^{32}-1	40	Maximum time in seconds for complete call bring-up establishment.	DI.4.0.x, BO Deprecated in DPM/BO.2.5
ikev2_eap_fra_pseudo_ enabled	No	TRUE, FALSE	FALSE	Used to determine if the UE will support EAP-AKA fast reauthentication during IKEv2 authentication.	BO

Parameter name	Mandatory	Value range	Default value	Description	Applicable modem PLs
pdn_throttle_timer_values_sec	No	{0,1,2,…, 2^{32}-1} Max list size=6	0,0,60+*r*,120,480,900	Specifies the series of timers to be used for throttling a PDN; the final value in the list will be used for subsequent failures after the list is exhausted.	DPM.2.0 BO
ikev2_encr_algo_list	No	{0,1,2,…, 2^{32}-1} Max list size=8	2-ENCR_DES 3-ENCR_3DES 12-ENCR_AES_CBC	Specifies the supported IKEv2 encryption algorithms Invalid algorithm enumerations will be ignored.	DPM.2.0 BO
ikev2_aes_cbc_encr_key_size_list	No	{0,1,2,…, 2^{32}-1} Max list size=8	128, 256	If 12 (ENCR_AES_CBC) is specificed in the ikev2_encr_algo_list, this parameter will specify the length of the AES CBC encryption: 128 and/or 256. Invalid encryption key sizes will be ignored.	DPM.2.0 BO
ikev2_aes_ctr_encr_key_size_list	No	{0,1,2,…, 2^{32}-1} Max list size=8	128, 256	If 13 (ENCR_AES_CTR) is specificed in ikev2_encr_algo_list, this parameter will specify the length of the AES CTR encryption: 128 and/or 256. Invalid encryption key sizes will be ignored.	DPM.2.0 BO
ikev2_hash_algo_list	No	{0,1,2,…, 2^{32}-1} Max list size=8	1-AUTH_HMAC_MD5_96 2-AUTH_HMAC_SHA1_96 5-AUTH_AES_XCBC_96	Specifies the supported IKEv2 authentication algorithms. Invalid algorithm enumerations will be ignored.	DPM.2.0 BO

Parameter name	Mandatory	Value range	Default value	Description	Applicable modem PLs
ikev2_prf_algo_list	No	{0,1,2,…, 2^{32}-1} Max list size=8	2-PRF_HMAC_SHA1 4-PRF_AES128_XCBC	Specifies the supported IKEv2 PRF algorithms. Invalid algorithm enumerations will be ignored.	DPM.2.0 BO
esp_encr_algo_list	No	{0,1,2,…, 2^{32}-1} Max list size=8	2-ENCR_DES 3-ENCR_3DES 12-ENCR_AES_CBC	Specifies the supported ESP encryption algorithms. Invalid algorithm enumerations will be ignored.	DPM.2.0 BO
esp_aes_cbc_encr_key_size_list	No	{0,1,2,…, 2^{32}-1} Max list size=8	128, 256	If 12 (ENCR_AES_CBC) is specificed in the ikev2_encr_algo_list, this parameter will specify the length of the AES CBC encryption: 128 and/or 256. Invalid encryption key sizes will be ignored.	DPM.2.0 BO
esp_aes_ctr_encr_key_size_list	No	{0,1,2,…, 2^{32}-1} Max list size=8	128, 256	If 13 (ENCR_AES_CTR) is specificed in ikev2_encr_algo_list, this parameter will specify the length of the AES CTR encryption: 128 and/or 256. Invalid encryption key sizes will be ignored.	DPM.2.0 BO
esp_auth_algo_list	No	{0,1,2,…, 2^{32}-1} Max list size=8	1-AUTH_HMAC_MD5_96 2-AUTH_HMAC_SHA1_96 5-AUTH_AES_XCBC_96	Specifies the supported ESP authentication algorithms Invalid algorithm enumerations will be ignored.	DPM.2.0 BO

Parameter name	Mandatory	Value range	Default value	Description	Applicable modem PLs
configured_ike_port	No	4500	Not set	Enables the UE to send/receive IKE packets on either port 4500 This property is used exclusively for WP targets.	DPM.2.0 BO
ikev2_eap_reauth_realm_ enabled	No	TRUE, FALSE	FALSE	When set to TRUE, the UE will append a realm to the EAP reauthentication identity if realm is not provided by the EAP server. Must enable the ikev2_eap_fra_pseudo_ enabled parameter before this item will take effect. <reauth_id>@<realm>	BO
static_fqdn_enabled	No	TRUE, FALSE	TRUE	When set to TRUE, the UE will use only the static string provided in epdg_fqdn for EPDG FQDN resolution. When set to FALSE, the UE will dynamically create the EPDG FQDN string using PLMN information. The static FQDN provisioned will be used only as a fallback if the DNS query for dynamic FQDN resolution fails. The string that is constructed will be in the following format: epdg.epc.mnc<MNC>. mcc<MCC>.pub.3gppnet work.org	BO.2.5

Parameter name	Mandatory	Value range	Default value	Description	Applicable modem PLs
epdg_plmn_list	No	5 or 6 digit comma-separated PLMN values. Max list size = 40	-	This list will be used when static_fqdn_enabled is set to FALSE. The UE will dynamically create EPDG FQDN strings based on 3GPP PLMN standards using the PLMN list provisioned. PLMN format is MCCMNC For example, for 123456, 123 will be the MCC and 456 will be the MNC, and for 12345, 123 will be the MCC and 045 will be the MNC.	BO.2.5
epdg_fqdn_validation_enabled	No	TRUE,FALSE	FALSE	Used to determine if the EPDG FQDN should be validated against the subjectAltName in the certificate received from the server.	BO.2.5

NOTE: For IKEv2 and ESP encryption, authentication, and PRF list values, see *Internet Key Exchange Protocol Version 2 (IKEv2)* (IETF RFC 5996).

Sample iwlan_s2b_config.txt

A sample of the /data/ iwlan_s2b_config.txt EFS file is as follows:

```
epdg_fqdn: wireless.epdg.com;
ke_payload_enabled:FALSE;
```

2.4 Keep-alive manager file

The keep-alive manager configuration is required to maintain LTE connectivity when an attempt is made to hand over the attach PDN for LTE from LTE to IWLAN (resulting in a potential loss of LTE connectivity).

The configuration parameter is a clear EFS text file named ds_eps_kamgr_pdn.txt. This file specifies the keep-alive manager (KAMGR) PDN profile ID and KAMGR retry timer values. This file should be placed under the EFS directory /data.

The EFS file format follows the standard Param_Name:Param_Val; rule. Param_Name refers to the token name, and Param_Val refers to the value/value list associated with the token Param_Name. Note that the tokens-value combinations end with a semicolon (;). Each new token is typically placed on a new line.

The EFS file contains the tokens (and associated values) listed in Table 2-4.

Table 2-4 KAMGR configurable parameter names and description

Parameter name	Mandatory	Value range	Default value	Description
PROFILE_ID	Yes	0 to 2^{16}-1	NA	Profile number of the PDN to be kept alive; the most preferred system for the APN associated with the keep-alive PDN should be WWAN in its MAPCON policy.
TIMER_VAL	No	See Table 2-5	500:500:10000:2	Values used in the keep-alive manager retry mechanism; see Table 2-5 for details.

The value list for TIMER_VAL is given in Table 2-5.

Table 2-5 TIMER_VAL description

Timer_Val values	Value range	Default value	Description
First value	0 to 2^{32}-1	500 (ms)	Default timer – Timer value to be used on first retry attempt.
Second value	0 to 2^{32}-1	500 (ms)	Incremental timer – Timer increment added on subsequent retries.
Third value	0 to 2^{32}-1	10000 (ms)	Maximum timer value – Used after retry threshold has reached.
Fourth value	0 to 2^{8}-1	2	Maximum no. of retries – Retries attempted after PDN is torn down by network before maximum timer takes effect.

The token names in the file are not case-sensitive, for example, PROFILE_ID and profile_id are treated the same.

The parameter TIMER_VAL need not be present. If TIMER_VAL is not present, the default value list will be used. See the file format samples below:

Sample file 1:

profile_id:2;

timer_val:500:600:20000:2;

Sample file 2:

profile_id:2;

Sample iwlan_s2b_config.txt

A sample of the /data/ iwlan_s2b_config.txt EFS file is as follows:

```
epdg_fqdn: wireless.epdg.com;
ke_payload_enabled:FALSE;
```

A References

A.1 Related documents

Documents	
Qualcomm Technologies, Inc.	
Data Services API Interface Specification	80-V6415-1
Standards	
Mobility between 3GPP-Wireless Local Area Network (WLAN) Interworking and 3GPP Systems	3GPP TS 23.327 (Rel 10)
3GPP Systems to Wireless Local Area Network (WLAN) Interworking; System Description	3GPP TS 23.234 (Rel 10)
3GPP System to Wireless Local Area Network (WLAN) Interworking; WLAN User Equipment (WLAN UE) to Network Protocols	3GPP TS 24.234 (Rel 10)
3G Security; Wireless Local Area Network (WLAN) Interworking Security	3GPP TS 33.234 (Rel 10)
Access to the 3GPP Evolved Packet Core (EPC) via non-3GPP Access Networks	3GPP TS 24.302 (Rel 10)
Architecture Enhancements for non-3GPP Accesses	3GPP TS 23.402 (Rel 10)
Policy and Charging Control Architecture	3GPP TS 23.203 (Rel 10)
Internet Key Exchange Protocol Version 2 (IKEv2)	IETF RFC 5996
Security Architecture for the Internet Protocol	IETF RFC 4301
IP Encapsulating Security Payload (ESP)	IETF RFC 4303
UDP Encapsulation of IPsec ESP Packets	IETF RFC 3948
Extensible Authentication Protocol (EAP)	IETF RFC 3748
Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)	IETF RFC 4187
Proxy Mobile IPv6	IETF RFC 5213
Generic Routing Encapsulation (GRE) Key Option for Proxy Mobile IPv6	IETF RFC 5845
Mobile IPv6 Support for Dual Stack Hosts and Routers (DSMIPv6)	IETF RFC 5555

A.2 Acronyms and terms

Term	Definition
IWLAN_S2b	WLAN offload over S2b/ePDG
KAMGR	keep-alive manager