

Evolved Packet Data Gateway Engineering Rules

This appendix provides ePDG (evolved Packet Data Gateway) engineering rules or guidelines that must be considered prior to configuring the system for your network deployment.

The following rules are covered in this appendix:

- IKEv2/IPSec Restrictions, on page 1
- X.509 Certificate (CERT) Restrictions, on page 2
- GTPv2 Restrictions, on page 2
- S2b Interface Rules, on page 3
- ePDG Service Rules, on page 3
- ePDG Subscriber Rules, on page 3

IKEv2/IPSec Restrictions

The following is a list of known restrictions for IKEv2 and IPSec:

- IKEv2 as per RFC 5996 is supported. IKEv1 is not supported.
- MOBIKE is not supported.
- Only one Child SA is supported.
- Each ePDG service must specify one crypto template.
- Per RFC 4306 and RFC 4718, the following known restrictions apply with respect to the payload and its order. Violations result in INVALID_SYNTAX being returned which is being enabled or disabled through a configuration CLI.
-
  - While RFC 4306 Section 2.19 specifies that the "CP payload MUST be inserted before the SA payload," the ePDG does not force strict ordering of this. The ePDG processes these payloads as long as the UE sends a CP payload anywhere inside the encryption data.
  - While RFC 4306 Section 2.23 specifies "The location of the payloads (Notify payloads of type NAT_DETECTION_SOURCE_IP and NAT_DETECTION_DESTINATION_IP) in the IKE_SA_INIT packets are just after the Ni and Nr payloads (before the optional CERTREQ payload)," the ePDG does not force strict ordering of this and still can process these NOTIFY payloads.
- ePDG egress processing will ensure that payloads are in order.
- As described above, when the ePDG receives IKEv2 messages, the ePDG does not enforce the payloads to be in order. However, when the ePDG sends the response or generates any IKEv2 messages, the ePDG will ensure that payloads are ordered according to RFC 4306.

- Traffic selector payloads from the UE support only traffic selectors by IP address range. In other words, the IP protocol ID must be 0. The start port must be 0 and the end port must be 65535. IP address range specification in the TSr payload is not supported.
- Only IKE and ESP protocol IDs are supported. AH is not supported.
- The IKE Protocol ID specification may not use the NONE algorithm for authentication or the ENCR_NULL algorithm for encryption as specified in Section 5 (Security Considerations) of RFC 4306.
- In ESP, ENCR_NULL encryption and NONE authentication cannot be simultaneously used.

X.509 Certificate (CERT) Restrictions

The following are known restrictions for the creation and use of X.509 CERT:

- The maximum size of a CERT configuration is 4096 bytes.
- The ePDG includes the CERT payload only in the first IKE_AUTH Response for the first authentication.
- If the ePDG receives the CERT-REQ payload when it is not configured to use certificate authentication and if the CRITICAL bit is set in the IKE_AUTH request, the ePDG will reject the exchange. If the ePDG receives the CERT-REQ payload when it is not configured to use certificate authentication and if the CRITICAL bit is not set, the ePDG ignores the payload and proceeds with the exchange to be authenticated using EAP.
- Only a single CERT payload is supported. While RFC 4306 mandates the support of up to four certificates, the ePDG service will support only one X.509 certificate per context. This is due to the size of an X.509 certificate. Inclusion of multiple certificates in a single IKE_AUTH may result in the IKE_AUTH message not being properly transmitted.

GTPv2 Restrictions

The following are known restrictions for the creation and use of GTPv2:

- The ePDG should not send Delete PDN connection set request message per 23.007 for the FQ-CSID failure.
- The ePDG does not support allowing the UE to have more than one PDN connection with one APN.
- The ePDG should not handle the delete PDN connection set request received from PGW, basically terminating all the sessions corresponding to the PGW FQ-CSID present in "delete PDN connection set request" message.
- The ePDG should not be allowed to send "Trace Activation/Deactivation" message to PGW for subscriber tracing when same is notified to ePDG on the SWm interface with presence of "Trace Information" AVP.
- The ePDG should not do any policy (QoS) enforcement, ePDG should only be doing the UL traffic QCI to DSCP mapping and marking. Downlink traffic marking shall be done at PGW and ePDG should not handle DSCP for same including the pass through mode marking. ePDG should be be communicating the static QoS profile received from the AAA to the PGW.
- The ePDG does not have CAC/Admission control functionality.
- The ePDG does not supports handling the piggy backed message as specified by 3GPP. ePDG does expects the separate create bearer request message post handling of create session request and response for the creation of dedicated bearer.

S2b Interface Rules

This section describes the engineering rules for the S2b interface for communications between the MAG (Mobility Access Gateway) service residing on the ePDG and the LMA (Local Mobility Anchor) service residing on the P-GW.

EGTP Service Rules

The following engineering rules apply to the S2b interface from the EGTP service residing on the ePDG:

- First GTPU service is defined and then eGTP service is defined with association of previously defined GTPU service and later on the eGTP service is associated with the ePDG service residing in same or different contex.
- An S2b interface is created once the IP address of a logical interface is bound to a eGTP and GTPU service.
- The eGTP and GTPU services must be configured within same egress context.
- The eGTP service must be associated with an ePDG service.
- **no gtpc path-failure detection-policy** CLI must be configured under eGTP service to avoid path failure detection action. When this configuration is used the ePDG does not cleans up session if the retransmission timeout has happened for the echo request sent by ePDG.

ePDG Service Rules

The following engineering rule applies to services configured within the system:

- A maximum of 256 services (regardless of type) can be configured per system.

ePDG Subscriber Rules

The following engineering rule applies to subscribers configured within the system:

- Default subscriber templates must be configured per ePDG service.