IMSI Encryption Support

This chapter describes the following topics:

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	ePDG
Applicable Platform(s)	• ASR 5500 • VPC-DI • VPC-SI
Feature Default	Disabled - Configuration Required
Related Changes in This Release	Not applicable
Related Documentation	• *Command Line Interface Reference* • *ePDG Administration Guide* • *Statistics and Counters Reference*

Revision History

Revision Details	Release
First introduced.	21.6

Feature Description

During the IMSI Encryption scenario, UE sends encrypted IMSI to AAA server with EAP payload, and in IKE_AUTH payload to ePDG. All UEs send a common-identity in IDi payload due to which all the sessions were being processed on same IPSec Manager, which limited the capacity of ePDG to maximum sessions supported by one IPSec Manager. With this feature, ePDG supports distribution of sessions across all IPSec Managers. ePDG decodes and process the string “anonymous” or any mutually agreed value received in IDi payload in first IKE_AUTH request. ePDG receives real username with Mobile-Node Identifier AVP from AAA in Final Diameter-EAP-Answer. IMSI is extracted from it, and it is used to find any pre-existing session(s) present in the system and clean it. All the old calls from same IMSI will be deleted once authentication of new session is successful

Note Multi-PDN sessions are also treated as re-attach sessions. Any older Multi-PDN session will be deleted once new session’s authentication is successful.

Configuring ePDG IMSI Encryption Support

This section provides information on CLI commands available in support of this feature.

Configuring Common ID

Use the following configuration in Cytpto Template configuration mode to enable this feature.

```
configure
  context context_name
    crypto template template_name ikev2-dynamic
      ikev2-ikesa idi idi_value  { common-id | request-eap-identity }
       no ikev2-ikesa idi idi_value
      end
```

Notes:

- **ikev2-ikesa**: Configures the IKEv2 IKE Security Association parameters.
- **idi**: Configures the IKEv2 IKESA idi related parameters.
- *idi_value* : This is the Peer idi value to be used. This is a string of size 1 to 127.
- **common-id**: Configures the Common IDi(peer) session.
- **request-eap-identity**: Requests the EAP-Identity from peer.
- **no**: Disables the IKEv2 IKESA idi related parameters.

Monitoring and Troubleshooting

This section provides information on the show commands and bulk statistics available for the ePDG IMSI Encryption feature.

Show Commands and Outputs

This section provides information on show commands and their corresponding outputs for the ePDG IMSI Encryption Support feature.

show crypto template

The following new fields are added to the output of this command:

IKE SA IDi [peer]:

- anonymous@realm [Common-Id Session]

  It will increment once EAP-Identity request is sent to peer after receiving the configured IDi.

show crypto statistics ikev2

The following new fields are added to the output of this command:

- Common-Id Session Attempt:

  it will increment once the Configured IDi with common-id action is matched with Incoming session's IDi.
- Common-Id Session Success:

  It will increment once the Common-id session is successfully established.

show crypto ikev2-ikesa security-associations

The following new fields are added to the output of this command:

- Common ID Session

show subscribers full

The following new fields are added to the output of this command:

- Common ID Session

Bulk Statistics

The following bulk statistics are added in the System Schema in support of the ePDG IMSI Encryption Support feature.

- ikev2-auth-common-id-sess-attempt - Increment once the Configured IDi with common-id action is matched with Incoming session's IDi.
- ikev2-auth-common-id-sess-success - Increment once the Common-id session is successfully established.