ePDG IMSI Privacy Support

This chapter describes the ePDG IMSI Privacy Support feature.

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.	21.4

Feature Description

The IMSI Privacy feature protects the exposure of IMSI to the untrusted ePDG and shares it only after it has authenticated the ePDG.

How it Works

1. ePDG decodes and processes the string anonymous or any configured value received in IDi payload in IKE_AUTH request.
2. ePDG then responds with IKE AUTH response which includes the ePDG server certificate along with the authentication payload.
3. The client can be configured to send a CERTREQ in the IKE AUTH request if required. In addition to the ePDG server certificate, the IKEv2 server initiates an EAP Identity request towards the IKEv2 client.
4. The IKEv2 client authenticates the server using the certificate and provides the IMSI in the EAP Identity response.
5. The same EAP Payload (EAP response) will be forwarded to AAA with the first Diameter EAP Request. Rest of the call flow for ePDG remains the same.

Configuring IMSI Privacy Support

This section describes the configuration of IMSI Privacy.

Configuring IDI

Use the following configuration to match IDI from peer which enables the ePDG to request the real identity using EAP-Identity Request.

```
configure
  context context_name
    crypto template template_name ikev2-dynamic
      ikev2-ikesa idi peer_idi_value request-eap-identity
      no ikev2-ikesa idi peer_idi_value
      end
```

Notes:

- **crypto template** *template_name*: Configures the context level name to be used to identify the Crypto Template. *template_name* is string of size 1 to 104.
- **ikev2-dynamic**: Configures the parameters for IKEv2 Security Associations derived from this Crypto Template.
- **idi** *peer_idi_value*: Specifies the IDI related configuration. *peer_idi_value* is a string of size 1 to 127.
- **request-eap-identity**: Requests EAP-Identity from peer.

- **no**: Disables the peer IDI value.

Monitoring and Troubleshooting

This section provides information on how to monitor and troubleshoot the IMSI Privacy feature.

Show Commands and Outputs

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

show crypto statistics ikev2

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

- EAP-Identity Req Sent

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

  It will increment when any of the configured IDi is received from peer.