IMSI Privacy on ePDG

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	ePDG
Applicable Platform(s)	VPC-DI
Feature Default	Disabled – Configuration Required
Related Documentation	• *Command Line Interface Reference* • *ePDG Administration Guide* • *Statistics and Counters Reference*

Revision History

Revision Details	**Release**

In this StarOS release, ePDG is enhanced to perform AUTH calculation based on the 'anonymous' or any other configured parameter received in the IDi payload. The existing support of performing AUTH calculation based on International Mobile Subscriber Identity (IMSI) shall be provided through the **imsi-privacy auth-imsi** CLI command.	2024.03.0
First introduced.	21.4

IMSI Privacy

The IMSI Privacy feature protects the exposure of IMSI to the untrusted ePDG and shares it over the wire only after the User Equipment (UE) has authenticated the ePDG.

By default, ePDG uses Peer IDi such as 'anonymous' or any other configured parameter for AUTH calculation instead of IMSI.

Limitation

The IMSI Privacy feature is not applicable for non-UICC (universal integrated circuit card) devices.

AUTH Calculation for IMSI Privacy

When the User Equipment (UE) sends an IKE-AUTH request to the evolved Packet Data Gateway (ePDG), the IKE-AUTH message includes the IDi payload. The ePDG decodes the IDi payload and compares it with the configured string in the ePDG to determine if the call flow is using IMSI privacy. If it is an IMSI privacy-based call flow, the ePDG then checks if auth-imsi is configured. The ePDG supports authentication (AUTH) calculation using two approaches:

- If auth-imsi is configured, authentication calculation will be based on the IMSI.
- If auth-imsi is not configured, authentication calculation will be based on the configured string.

How it Works

The following steps describe authenticaton process for IMSI-based AUTH Calculation.

Table 1: Procedure

Step	Description
1.	The UE sends IKE_SA_INIT Message.
2.	ePDG responds with IKE_SA_INIT_RSP Message.

Step	Description
3.	The UE sends the anonymous or configured value (in the IDi payload), APN (in the IDr payload), and CERTREQ information in this first message of the IKE_AUTH phase, and begins negotiation of child security associations. The UE omits the AUTH parameter in order to indicate to the ePDG that it wants to use EAP over IKEv2. The UE shall send the configuration payload (CFG_REQUEST) within the IKE_AUTH request message to obtain an IPv4 home IP Address and/or a Home Agent Address.
4.	ePDG decodes and processes the string anonymous or any configured value received in IDi payload in the IKE_AUTH request. In addition to the ePDG server certificate, the IKEv2 server initiates an EAP Identity request towards the IKEv2 client.
5	The IKEv2 client (UE) authenticates the server using the certificate and provides the IMSI in the EAP Identity response.
6	The ePDG sends the Authentication and Authorization Request message to the 3GPP AAA Server, containing the user identity and APN.
7.	The 3GPP AAA Server shall fetch the user profile and authentication vectors from HSS/HLR (if these parameters are not available in the 3GPP AAA Server). The 3GPP AAA Server shall lookup the IMSI of the authenticated user based on the received user identity (root NAI) and include the EAP-AKA as requested authentication method in the request sent to the HSS. The HSS shall then generate authentication vectors with AMF separation bit = 0 and send them back to the 3GPP AAA server. The 3GPP AAA Server checks in user's subscription if he/she is authorized for non-3GPP access. The counter of IKE SAs for that APN is stepped up. If the maximum number of IKE SAs for that APN is exceeded, the 3GPP AAA Server shall send an indication to the ePDG that established the oldest active IKE SA (it could be the same ePDG or a different one) to delete the oldest established IKE SA. The 3GPP AAA Server shall update accordingly the information of IKE SAs active for the APN. The 3GPP AAA Server initiates the authentication challenge. The user identity is not requested again.
8.	The ePDG responds with its identity, a certificate, and sends the AUTH parameter to protect the previous message it sent to the UE (in the IKE_SA_INIT exchange). It completes the negotiation of the child security associations if any. The EAP message received from the 3GPP AAA Server (EAP-Request/AKA-Challenge) is included in order to start the EAP procedure over IKEv2.
9.	The UE checks the authentication parameters and responds to the authentication challenge. The only payload (apart from the header) in the IKEv2 message is the EAP message.
10	The ePDG forwards the EAP-Response/AKA-Challenge message to the 3GPP AAA Server.
10a	The AAA checks, if the authentication response is correct.

Step	Description
11.	When all checks are successful, the 3GPP AAA Server sends the final Authentication and Authorization Answer (with a result code indicating success) including the relevant service authorization information, an EAP success and the key material to the ePDG. This key material shall consist of the MSK generated during the authentication process. When the SWm and SWd interfaces between ePDG and 3GPP AAA Server are implemented using Diameter, the MSK shall be encapsulated in the EAP-Master-Session-Key-AVP, as defined in RFC 4072.
12.	The MSK shall be used by the ePDG to generate the AUTH parameters in order to authenticate the IKE_SA_INIT phase messages, as specified for IKEv2 in RFC 4306. These two first messages had not been authenticated before as there was no key material available yet. According to RFC 4306 [3], the shared secret generated in an EAP exchange (the MSK), when used over IKEv2, shall be used to generated the AUTH parameters.
13.	The EAP Success/Failure message is forwarded to the UE over IKEv2.
14	The UE takes its own copy of the MSK as input to generate the AUTH parameter to authenticate the first IKE_SA_INIT message. The AUTH parameter is sent to the ePDG.
15	The ePDG checks the correctness of the AUTH parameter calculated based on: • IMSI - if **auth-imsi** is configured • amonymous or configured value - if **auth-imsi** is not configured
16	On successful authentication the ePDG selects the P-GW based on Node Selection options.The ePDG sends Create Session Request (IMSI, [MSISDN], Serving Network, RAT Type (WLAN), Indication Flags, Sender F-TEID for C-plane, APN, Selection Mode, PAA, APN-AMBR, Bearer Contexts, [Recovery], [Charging characteristics], [Additional Protocol Configuration Options (APCO)]), Private IE (P-CSCF, AP MAC address). Indication Flags shall have Dual Address Bearer Flag set if PDN Type is IPv4v6.Handover flag shall be set to Initial or Handover based on the presence of IP addresses in the IPv4/IPv6_Address configuration requests.Selection Mode shall be set to "MS or network provided APN, subscribed verified". The MSISDN, Charging characteristics, APN-AMBR and bearer QoS shall be provided on S2b interface by ePDG when these are received from AAA on SWm interface.The control plane TEID shall be per PDN connection and the user plane TEID shall be per bearer created.
17.	The P-GW allocates the requested IP address session and responds back to the ePDG with a Create Session Response (Cause, P-GW S2b Address C-plane, PAA, APN-AMBR, [Recovery], Bearer Contexts Created, [Additional Protocol Configuration Options (APCO)], Private IE (P-CSCF)) message.
18.	The ePDG calculates the AUTH parameter calculated based on IDr payload, which authenticates the second IKE_SA_INIT message.

Step	Description
19.	The ePDG sends the assigned Remote IP address in the configuration payload (CFG_REPLY).The AUTH parameter is sent to the UE together with the configuration payload, security associations and the rest of the IKEv2 parameters and the IKEv2 negotiation terminates.
20.	Router Advertisement will be sent for IPv6 address assignments, based on configuration. **Note** If the ePDG detects that an old IKE SA for that APN already exists, it will delete the IKE SA and send the UE an INFORMATIONAL exchange with a Delete payload in order to delete the old IKE SA in UE.

Configuring IMSI Privacy and AUTH Calculations

This section describes the configuration of IMSI Privacy and if Auth calculation is done based on the IMSI or 'anonymous' or configured value received in the IDi payload.

Configure IDi

You can use this task to match IDi from peer, which enables the ePDG to request the real identity using EAP-Identity Request.

Step 1 Specify a crypto template name to identify the Crypto template and IKEv2 Security Association parameter that are derived from this Crypto template.

crypto template *template_name* **ikev2-dynamic**

Example:

```
[local]EPDGCHASSIS# config
[local]EPDGCHASSIS(config)# context pdif
[pdif]EPDGCHASSIS(config-ctx)# crypto template boston ikev2-dynamic
[pdif]EPDGCHASSIS(cfg-crypto-tmpl-ikev2-tunnel)# ikev2-ikesa idi anonymous1@realm.com
request-eap-identity
[pdif]EPDGCHASSIS(cfg-crypto-tmpl-ikev2-tunnel)# end
```

Step 2 Specify the IDi value to match IDi from peer and request for EAP-Identity from peer. The *peer_idi_value* must be of size 1–127.

ikev2-ikesa idi *peer_idi_value* **request-eap-identity**

Example:

```
[local]EPDGCHASSIS# config
[local]EPDGCHASSIS(config)# context pdif
[pdif]EPDGCHASSIS(config-ctx)# crypto template boston ikev2-dynamic
[pdif]EPDGCHASSIS(cfg-crypto-tmpl-ikev2-tunnel)# ikev2-ikesa idi anonymous1@realm.com
request-eap-identity
[pdif]EPDGCHASSIS(cfg-crypto-tmpl-ikev2-tunnel)# end
```

Step 3 (Optional) Disable the peer IDi value.

no ikev2-ikesa idi *peer_idi_value*

Example:

```
[local]EPDGCHASSIS# config
[local]EPDGCHASSIS(config)# context pdif
[pdif]EPDGCHASSIS(config-ctx)# crypto template boston ikev2-dynamic
[pdif]EPDGCHASSIS(cfg-crypto-tmpl-ikev2-tunnel)# no  ikev2-ikesa idi anonymous1@realm.com
[pdif]EPDGCHASSIS(cfg-crypto-tmpl-ikev2-tunnel)# end
```

Enable Use of IMSI for AUTH Calculation

Use this task to enable ePDG to use IMSI for AUTH calculation on the Context Configuration mode when the IMSI Privacy feature is used.

Also, verify whether the IMSI based AUTH calculation is enabled on the ePDG using the .**show configuration** and **show crypto template** coomands.

Step 1 Specify a crypto template name to identify the Crypto template and IKEv2 Security Association parameter that are derived from this Crypto template.

crypto template *template_name* **ikev2-dynamic**

Example:

```
[local]EPDGCHASSIS# config
[local]EPDGCHASSIS(config)# context pdif
[pdif]EPDGCHASSIS(config-ctx)# crypto template boston ikev2-dynamic
[pdif]EPDGCHASSIS(cfg-crypto-tmpl-ikev2-tunnel)# ikev2-ikesa imsi-privacy auth-imsi
[pdif]EPDGCHASSIS(cfg-crypto-tmpl-ikev2-tunnel)# end
[
```

Step 2 Enable ePDG to use IMSI for AUTH calculation with IMSI Privacy related parameters.

ikev2-ikesa imsi-privacy auth-imsi

Example:

```
[local]EPDGCHASSIS# config
[local]EPDGCHASSIS(config)# context pdif
[pdif]EPDGCHASSIS(config-ctx)# crypto template boston ikev2-dynamic
[pdif]EPDGCHASSIS(cfg-crypto-tmpl-ikev2-tunnel)# ikev2-ikesa imsi-privacy auth-imsi
[pdif]EPDGCHASSIS(cfg-crypto-tmpl-ikev2-tunnel)# end
```

Step 3 Verify whether the IMSI based AUTH calculation is enabled on the ePDG.

a) Use the **show configuration** command to verify if the IMSI Privacy AUTH calculation enabled with auth-imsi.

Example:

```
show configuration
crypto template boston ikev2-dynamic
authentication remote eap-profile eapl
ikev2-ikesa transform-set list ikesa-boston  ikev2-ikesa rekey
   payload foo-saO match childsa match any
    ipsec transform-set list tselsa-boston
    rekey keepalive
    #exit
     ikev2-ikesa policy error-notification.
     ikev2-ikesa imsi-privacy auth-imsi
     iKev2-iKesa Keepaiive-user-activity
     allow-custom-fqdn-idr
  #exit
```

b) Use the **show crypto template** command to verify if a certain crypto template has the IMSI or IMSI Privacy string configured for AUTH calculation and if the IKE SA IDi value is defined.

Example:

```
[local]EPDGCHASSIS# context pdif
[pdif]EPDGCHASSIS# show crypto template
Map Name: boston
Map status: Incomplete
Crypto Map Type: IPSEC IKEv2 Template
IKE SA Transform 1/1
  Transform Set: ikesa-boston
    Encryption Cipher: aes-cbc-128 Encryption Accel: AES-NI Pseudo Random Function: shal
    Hashed Message Authentication Code: shal—96 HMAC Accel: None Diffie-Hellman Group: 2 IKE SA
Rekey:
Enabled
IKE SA User Activity Keepalive: Enabled IKE SA Setup Timer: 120 [Default]
IKE SA Backoff Timer per Notify Msg Type:
   No APN Subscription: 3600 sec [Default]
   Network Failure : 3600 sec [Default]
IKE SA Max Retransmission Count : 5 [Default]
IKE SA Max Retransmission Timeout: 500 [Default] IKE SA Ignore Rekeying request: Disabled IKE SA
 Cert Sign: PKCS 1.5 [Default]
IKE SA Use CDP: Disabled IKE SA Mobike: Disabled
IKE SA RFC5996 Notification: Disabled
IKE SA Ignore Notify Protocol ID: None [Default]
IKE SA DSCP Value: 0x0 [Default]
IKE SA IDi [Peer]: Disabled
imsi-privacy used Id for AUTH calculation : imsi
```

You have successfully configured IMSI based AUTH calculation under the Crypto template configuration mode.

Disable Use of IMSI for AUTH Calculation

Use this task to revert to the default behavior of IKESA using the configured IDi parameters, which is used for AUTH calculation when IMSI Privacy feature is used.

View the IMSI Privacy AUTH calculation disabled using the **show configuration** and **show crypto template** commands.

Step 1 Specify a crypto template name to identify the Crypto template and IKEv2 Security Association parameter that are derived from this Crypto template.

crypto template *template_name* **ikev2-dynamic**

Example:

```
[local]EPDGCHASSIS# config
[local]EPDGCHASSIS(config)#  context pdif
[pdif]EPDGCHASSIS(config-ctx)# crypto template boston ikev2-dynamic
[pdif]EPDGCHASSIS(cfg-crypto-tmpl-ikev2-tunnel)# no ikev2-ikesa imsi-privacy auth-imsi
[pdif]EPDGCHASSIS(cfg-crypto-tmpl-ikev2-tunnel)# end
```

Step 2 Disable IMSI based AUTH calculation.

no ikev2-ikesa imsi-privacy auth-imsi

Example:

```
[local]EPDGCHASSIS# config
[local]EPDGCHASSIS(config)#  context pdif
[pdif]EPDGCHASSIS(config-ctx)# crypto template boston ikev2-dynamic
[pdif]EPDGCHASSIS(cfg-crypto-tmpl-ikev2-tunnel)# no ikev2-ikesa imsi-privacy auth-imsi
[pdif]EPDGCHASSIS(cfg-crypto-tmpl-ikev2-tunnel)# end
```

Step 3 Verify whether the IMSI based AUTH calculation is disabled on the ePDG using **show configuration** and **show crypto template** CLI commands.

a) Using **show configuration** command:

Example:

```
crypto template boston ikev2-dynamic
authentication remote eap-profile eapl ikev2-ikesa transform-set list ikesa-boston ikev2-ikesa
rekey
payload foo-saO match childsa match any
ipsec transform-set list tselsa-boston     reley keepalive
#exit
ikev2-ikesa policy error-notification
ikev2-ikesa keepalive-nspr-activity
ikev2-ikesa idi anonymousl@realm.com request-eap-identity allow-custom-tqdn-idr
#exit
```

b) Using **show crypto template** command:

Example:

```
[pdif]EPDGCHASSIS# show crypto template
Map Name: boston
Map status: Incomplete
Crypto Map Type: IPSEC IKEv2 Template
IKE SA Transform 1/1
Transform Set: ikesa-boston
 Encryption Cipher: aes-cbc-128
 Encryption Accel: AES-NI
 Pseudo Random Function: shal
 Hashed Message Authentication Code: shal-96
 HMAC Accel: None
 Diffie—Heilman Group: 2 IKE SA Rekey: Enabled
IKE SA User Activity Keepalive: Enabled
IKE SA Setup Timer: 120 [Default]
IKE SA Backoff Timer per Notify Msg Type:
  No APN Subscription: 3600 sec [Default]
  Network Failure : 3600 sec [Default]
IKE SA Max Retransmission Count: 5 [Default]
IKE SA Max Retransmission Timeout: 500 [Default] IKE SA Ignore Rekeying request: Disabled IKE SA
 Cert Sign: PKCS 1.5 [Default]
IKE SA Use CDP: Disabled
IKE SA Mobike: Disabled
IKE SA RFC5996 Notification: Disabled
IKE SA Ignore Notify Protocol ID: None [Default]
IKE SA DSCP Value: 0x0 [Default]
IKE SA IDi [Peer]:
  anonymousl@realm.com [Request EAP-Identity]
imsi-privacy used Id for AUTH calculation: configured-string
```

You have successfully disabled IMSI based AUTH calculation.

Monitoring and Troubleshooting

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.