Identity Procedure on Authentication Failure

- Feature Description, on page 1
- How It Works, on page 2
- Configuring Performance of Identity Procedure, on page 3
- Monitoring and Troubleshooting the Performance of Identity Procedure for Authentication Failure, on page 4

Feature Description

Performing Identity Procedure in response to authentication failures results in fewer subscribers losing network connectivity due to Authentication Rejects. In the network, authentication rejects due to authentication failures such as Sync failure, GSM authentication unacceptable, and MAC failure, cause loss of network connectivity to subscribers. Often uthentication failure is due to incorrectly sent authentication vectors, which could be due to a P-TMSI (Packet Temporary Mobile Subscriber Identity) collision in the network.

Authentication Failures

GSM Authentication Unacceptable

When a 3G MS/UE attaches and sends a RAU Request with P-TMSI identity, this means that this subscriber:

- was registered in the SGSN,
- received this P-TMSI identity from the SGSN,
- left the SGSN, and
- has returned to this SGSN.
- And in the time between leaving and returning, another subscriber, a 2G subscriber, has registered with this SGSN and has the same P-TMSI.

The SGSN tries to authenticate the returning 3G subscriber with the authentication vectors of the 2G subscriber. This causes the MS/UE to send authentication failure with cause "GSM authentication unacceptable" because the SGSN has sent RAND from the 2G subscriber when the 3G subscriber's MS/UE was expecting quintets.

MAC Failure

When a 2G MS sends a RAU Request (new SGSN RAU) with a P-TMSI identity, the SGSN tries to authenticate the new 2G subscriber with the authentication vectors of a different 2G subscriber. In this scenario, it appears as if IMSI-PTMSI collision occurs within the SGSN or it is due to the peer-SGSN sending vectors of another

subscriber or an incorrect IMSI in the Context Response. This results in authentication failure with cause "MAC failure".

Identity Procedure

In most cases, these forms of authentication failure can be resolved by the subscriber restarting their device - if the subscriber knows to try this.

MAC Failure

The SGSN supports performing an Identity Procedure on receiving MAC Failure in 3G and on MAC Failure during 2G Attach.

Beginning with release 19.2, the SGSN also supports performing Identity Procedure on MAC Failure in 2G New-ISRAU.

If the SGSN gets MAC failure for the first time from an MS/UE, the SGSN sends an SGSN-Context-ACK Failure message to the peer-SGSN and starts an Identity Procedure.

1. Once the SGSN receives the IMSI from the MS/UE in an Identity Response, if the IMSI is different from the IMSI received from the peer-SGSN then the SGSN will authenticate by fetching vectors from the HLR.
2. Next the SGSN tries to get the context from the peer-SGSN by initiating a new Context Request, including the IMSI obtained from the MS/UE, and the MS/UE validated flag is set.
3. The SGSN proceeds with the call.

If the IMSI is not found in the peer-SGSN, the SGSN sends RAU Reject with cause "MS Identity Cannot Be Derived by the Network". In accordance with the 3GPP specification, the MS/UE tries to register again using its IMSI.

GSM Authentication Unacceptable

Beginning with Release 19.2, the SGSN performs Identity Procedure on receiving GSM Authentication Unacceptable failure for 3G Attach, for 3G New-ISRAU, for 3G Intra-RAU, and for Inter-RAT.

If the SGSN gets the correct IMSI in the Identity Response, then the SGSN will try to authenticate the MS/UE again using the vectors from the HLR. If the authentication fails again, the SGSN send Authentication Reject to the MS/UE.

How It Works

3GPP specification TS 24.008, section 4.3.2.6 (c) suggest that "Upon the first receipt of an AUTHENTICATION FAILURE message from the MS with reject cause "MAC failure" or "GSM authentication unacceptable", the network may initiate the identification procedure. This is to allow the network to obtain the IMSI from the MS. When the SGSN receives authentication failure message with cause as GSM authentication unacceptable or MAC failure from a 3G/2G subscriber respectively, it will start identity procedure and authenticate the subscriber with vectors fetched using IMSI. This will avoid network loss to subscribers due to such PTMSI collision cases.

With Release 19.2, the SGSN performs Identity Procedure in accordance with 3GPP recommendations, as detailed below.

GSM Authentication Unacceptable

Scenarios:

- 3G Attach Request from a UE with P-TMSI (with the same P-TMSI the SGSN gave to a 2G subscriber now registered in the SGSN)
- 3G New-ISRAU with a P-TMSI

In the above scenarios, if authentication fails due to cause "GSM authentication unacceptable", then the SGSN performs the identity procedure and authenticates using vectors from the HLR.

In the case of a 3G Intra-RAU or Inter-RAT, if the arriving MS/UE is a different subscriber than the already registered one, then the SGSN rejects the RAU with cause "MS Identity Cannot be Derived by the Network", so the UE will use the IMSI at the next Attach.

MAC Failure in 2G

The SGSN will perform identity procedure if MAC failure is received for any of the following scenario:

- 2G Atach Request from a UE with P-TMSI (with a P-TMSI given to a different 2G subscriber now registered in the SGSN).
- 2G New-ISRAU with a P-TMSI

Configuring Performance of Identity Procedure

The default behavior of the SGSN is to perform identity procedure when authentication failures occur. The configuration noted below, allows the operator to disable or to re-enable the SGSN's default behavior.

With Release 19.2, the default behavior has been extended to enable the SGSN to initiate the identity procedure on receiving authentication failures with either cause "MAC Failure" or cause "GSM Authentication Failure".

The following command sequence configures the SGSN so that performance of the identity procedure upon receipt of an authentication failure is disabled:

```
config
  context context_name
    sgsn-service sgsn_srvc_name
      no gmm perform-identity-on-auth-failure
      end
```

Notes:

- If the default behavior has been disabled with the command sequence noted above, then to re-enable performance of the identity procedure upon receipt of an authentication failure, re-enter the sequence but do not include the **no** prefix with the **gmm perform-identity-on-auth-failure**command.

Verifying the Configuration

To determine the current configuration for this feature, issue the following command sequence in the Exec mode.

```
show sgsn-service name sgsn_srvc_name
```

The output generated by this command will include the following information field with either a 'Disabled' or 'Enabled' value :

```
GMM-Perform-Identity-After-Auth  :  Disabled
```

Monitoring and Troubleshooting the Performance of Identity Procedure for Authentication Failure

show gmm-sm statistics verbose

Statistics are available which track of the number of IMSI Identity Requests triggered in response to authentication failures noted in this chapter.

The **show gmm-sm statistics verbose** command from the Exec mode will generate an output that includes the following:

```
IMSI-Identity-Req triggered due to auth failures:
  3G-GSM Auth Unacc:       0           2G-MAC failure:      0
  3G-MAC failure:          0
```

show gmm-sm statistics

The number of IMSI identity requests initiated by the SGSN are captured in the following counter:

```
Total-IMSI-Identity-Req
```