NAS Signaling Security

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	MME
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* • *MME Administration Guide* • *Statistics and Counters Reference*

Revision History

Important Revision history details are not provided for features introduced before releases 21.2 and N5.1.

Revision Details	Release
The support for EEA3 and EIA3 NAS encryption/integrity algorithms is added.	21.11.3
First introduced.	Pre 21.2

Feature Description

The Non-Access Stratum (NAS) Signaling Security feature provides integrity protection and encryption of NAS signaling. The MME works as the termination point in the network for ciphering/integrity protection of NAS signaling and handles the security key management.

The NAS security association is between the UE and the MME. The MME uses the NAS Security Mode Command procedure to securely deliver NAS signaling messages between the UE and MME.

The following two standardized algorithms are supported for the radio interface in the LTE network:

- EEA: EPS Encryption Algorithm
- EIA: EPS Integrity Algorithm

The first set of encryption and integrity algorithm, 128-EEA1 and 128-EIA1, is based on the stream cipher SNOW 3G, and inherited from the UMTS network. The second set, 128-EEA2 and 128-EIA2, is based on the block cipher AES (Advanced Encryption Standard). The third set, 128-EEA3 and 128-EIA3, is based on a core stream cipher algorithm named ZUC.

Configuring NAS Signaling Security

This section describes how to configure the NAS Signaling Security feature.

Configuring LTE Encryption Algorithm in Call Control Profile

Use the following configuration to configure the precedence for LTE encryption algorithms to use for security procedures in the call control profile.

```
configure
   call-control-profile profile_name
      encryption-algorithm-lte priority1 { 128-eea0 | 128-eea1 | 128-eea2
 | 128-eea3 } [ priority2 { 128-eea0 | 128-eea1 | 128-eea2 | 128-eea3 }
] [ priority3 { 128-eea0 | 128-eea1 | 128-eea2 | 128-eea3 } ] [ priority4
 { 128-eea0 | 128-eea1 | 128-eea2 | 128-eea3 } ]
      remove encryption-algorithm-lte
      end
```

NOTES:

- **call-control-profile** *profile_name*: Creates an instance of a call control profile. *profile_name* specifies the name of the call control profile as an alphanumeric string of 1 to 64 characters.
- **priority1**: Specifies the preference of encryption algorithm for security procedures on this call control profile as priority 1.

- **priority2**: Specifies the preference of encryption algorithm for security procedures on this call control profile as priority 2.
- **priority3**: Specifies the preference of encryption algorithm for security procedures on this call control profile as priority 3.
- **priority4**: Specifies the preference of encryption algorithm for security procedures on this call control profile as priority 4.
- **128-eea0**: Sets the Null ciphering algorithm (128-EEA0) for LTE encryption as the encryption algorithm for security procedures.
- **128-eea1**: Sets the SNOW 3G synchronous stream ciphering algorithm (128-EEA1) for LTE encryption as the encryption algorithm for security procedures.
- **128-eea2**: Sets the Advance Encryption Standard (AES) ciphering algorithm (128-EEA2) for LTE encryption as the encryption algorithm for security procedures.
- **128-eea3**: Sets the ZUC algorithm (128-EEA3) for LTE encryption as the encryption algorithm for security procedures.
- **remove**: Deletes the priorities definition from the call control profile configuration.
- All the priorities must be set or the definition is invalid. The command can be re-entered to change the priorities without removing the configuration.

Configuring LTE Encryption Algorithm in MME Service

Use the following configuration to configure the precedence for LTE encryption algorithms to use for security procedures in the MME service.

Caution When this command is executed, all the existing priority-to-algorithm mappings will be removed and the newly configured ones will be applicable for security procedures.

Caution Configuration of the same algorithm to multiple priorities is prohibited.

```
configure
   context context_name
     mme-service service_name
       encryption-algorithm-lte priority1 { 128-eea0 | 128-eea1 | 128-eea2
 | 128-eea3 } [ priority2 { 128-eea0 | 128-eea1 | 128-eea2 | 128-eea3 }
] [ priority3 { 128-eea0 | 128-eea1 | 128-eea2 | 128-eea3 } ] [ priority4
 { 128-eea0 | 128-eea1 | 128-eea2 | 128-eea3 } ]
        default encryption-algorithm-lte
        end
```

NOTES:

- **mme-service** *service_name*: Creates an MME service or configures an existing MME service in the current context. *service_name* specifies the name of the MME service as an alphanumeric string of 1 to 63 characters.

- **priority1**: Specifies the preference of encryption algorithm for security procedures on this MME service as priority 1.
- **priority2**: Specifies the preference of encryption algorithm for security procedures on this MME service as priority 2.
- **priority3**: Specifies the preference of encryption algorithm for security procedures on this MME service as priority 3.
- **priority4**: Specifies the preference of encryption algorithm for security procedures on this MME service as priority 4.
- **128-eea0**: Sets the Null ciphering algorithm (128-EEA0) for LTE encryption as the encryption algorithm for security procedures.
- **128-eea1**: Sets the SNOW 3G synchronous stream ciphering algorithm (128-EEA1) for LTE encryption as the encryption algorithm for security procedures.
- **128-eea2**: Sets the Advance Encryption Standard (AES) ciphering algorithm (128-EEA2) for LTE encryption as the encryption algorithm for security procedures.
- **128-eea3**: Sets the ZUC algorithm (128-EEA3) for LTE encryption as the encryption algorithm for security procedures.
- **default**: Sets the default LTE encryption algorithm for security procedures with configured priority value. The lowest value has the highest preference.

  The default configuration of LTE encryption algorithm is:

  - priority1 with 128-eea0 encryption algorithm
  - priority2 with 128-eea1 encryption algorithm
  - priority3 with 128-eea2 encryption algorithm

Configuring LTE Integrity Algorithm in Call Control Profile

Use the following configuration to configure the precedence of LTE integrity algorithms to use for security procedures in the call control profile.

```
configure
   call-control-profile profile_name
      integrity-algorithm-lte priority1 { 128-eia0 | 128-eia1 | 128-eia2
| 128-eia3 } [ priority2 { 128-eia0 | 128-eia1 | 128-eia2 | 128-eia3 } ]
 [ priority3 { 128-eia0 | 128-eia1 | 128-eia2 | 128-eia3 } ] [ priority4
 { 128-eia0 | 128-eia1 | 128-eia2 | 128-eia3 } ]
      remove integrity-algorithm-lte
      end
```

NOTES:

- **call-control-profile** *profile_name*: Creates an instance of a call control profile. *profile_name* specifies the name of the call control profile as an alphanumeric string of 1 to 64 characters.
- **priority1**: Specifies the preference of integrity algorithm for security procedures on this call control profile as priority 1.

- **priority2**: Specifies the preference of integrity algorithm for security procedures on this call control profile as priority 2.
- **priority3**: Specifies the preference of integrity algorithm for security procedures on this call control profile as priority 3.
- **priority4**: Specifies the preference of integrity algorithm for security procedures on this call control profile as priority 4.
- **128-eia0**: Sets the Null ciphering algorithm (128-EIA0) for LTE integrity as the integrity algorithm for security procedures.
- **128-eia1**: Sets the SNOW 3G synchronous stream ciphering algorithm (128-EIA1) for LTE integrity as the integrity algorithm for security procedures.
- **128-eia2**: Sets the Advance Encryption Standard (AES) ciphering algorithm (128-EIA2) for LTE integrity as the integrity algorithm for security procedures.
- **128-eia3**: Sets the ZUC algorithm (128-EIA3) for LTE integrity as the integrity algorithm for security procedures.
- **remove**: Deletes the priorities definition from the call control profile configuration.
- All the priorities must be set or the definition is invalid. The command can be re-entered to change the priorities without removing the configuration.

Configuring LTE Integrity Algorithm in MME Service

Use the following configuration to configure the precedence of LTE integrity algorithms to use for security procedures in the MME service.

By default, the integrity algorithm is enabled on MME service and cannot be disabled.

Caution When this command is executed, all the existing priority-to-algorithm mappings will be removed and the newly configured ones will be applicable for security procedures.

Caution Configuration of the same algorithm to multiple priorities is prohibited.

```
configure
   context context_name
      mme-service service_name
        integrity-algorithm-lte priority1 { 128-eia0 | 128-eia1 | 128-eia2
 | 128-eia3 } [ priority2 { 128-eia0 | 128-eia1 | 128-eia2 | 128-eia3 }
] [ priority3 { 128-eia0 | 128-eia1 | 128-eia2 | 128-eia3 } ] [ priority4
 { 128-eia0 | 128-eia1 | 128-eia2 | 128-eia3 } ]
        default integrity-algorithm-lte
        end
```

NOTES:

- **mme-service** *service_name*: Creates an MME service or configures an existing MME service in the current context. *service_name* specifies the name of the MME service as an alphanumeric string of 1 to 63 characters.
- **priority1**: Specifies the preference of integrity algorithm for security procedures on this MME service as priority 1.
- **priority2**: Specifies the preference of integrity algorithm for security procedures on this MME service as priority 2.
- **priority3**: Specifies the preference of integrity algorithm for security procedures on this MME service as priority 3.
- **priority4**: Specifies the preference of integrity algorithm for security procedures on this MME service as priority 4.
- **128-eia0**: Sets the Null ciphering algorithm (128-EIA0) for LTE integrity as the integrity algorithm for security procedures.
- **128-eia1**: Sets the SNOW 3G synchronous stream ciphering algorithm (128-EIA1) for LTE integrity as the integrity algorithm for security procedures.
- **128-eia2**: Sets the Advance Encryption Standard (AES) ciphering algorithm (128-EIA2) for LTE integrity as the integrity algorithm for security procedures.
- **128-eia3**: Sets the ZUC algorithm (128-EIA3) for LTE integrity as the integrity algorithm for security procedures.
- **default**: Removes the preconfigured integrity algorithm and sets the default LTE integrity algorithm for security procedures. The default configuration of LTE integrity algorithm is:

  The default configuration of LTE integrity algorithm is:

  - priority1 with 128-eia0 integrity algorithm
  - priority2 with 128-eia1 integrity algorithm
  - priority3 with 128-eia2 integrity algorithm

Monitoring and Troubleshooting

This section provides information regarding show commands available to monitor and troubleshoot the NAS Signaling Security feature.

Show Commands and Outputs

This section provides information regarding show commands and their outputs in support of the NAS Signaling Security feature.

show call-control-profile full all

The output of this command includes the following fields:

- Order of Preference for Integrity Algorithm is — The integrity algorithm that receives the first priority.

- Order of Preference for Encryption Algorithm is — The encryption algorithm that receives the first priority.
- Order of Preference for Gprs Ciphering Algorithm is — The GPRS ciphering algorithm that receives the first priority.
- Order of Preference for LTE(MME) Encryption Algorithm is — Displays the configured priorities and the LTE encryption algorithm applied for security procedures.
- Order of Preference for LTE(MME) Integrity Algorithm is — Displays the configured priorities and the LTE integrity algorithm applied for security procedures.

show mme-service all

The output of this command includes the following fields:

- Encryption Algorithms — Displays the priority and the encryption algorithm applied for security procedures through the MME service.
  - **Priority**: The priority set for the applied encryption algorithm. The least value has the highest preference.

    In releases prior to 21.11.3: Possible priority values are between 1 to 3.

    In 21.11.3 and later releases: Possible priority values are between 1 to 4.
  - **Algorithm**: The applied encryption algorithm. Possible algorithms are:
    - **128-eea0**: Null ciphering algorithm (128-EEA0) for LTE encryption as the encryption algorithm for security procedures. This is the default encryption algorithm applicable for security procedures.
    - **128-eea1**: SNOW 3G synchronous stream ciphering algorithm (128-EEA1) for LTE encryption as the encryption algorithm for security procedures.
    - **128-eea2**: Advance Encryption Standard (AES) ciphering algorithm (128-EEA2) for LTE encryption as the encryption algorithm for security procedures.
    - **128-eea3**: ZUC algorithm (128-EEA3) for LTE encryption as the encryption algorithm for security procedures.

- Integrity Algorithms — Displays the priority and the integrity algorithm applied for security procedures through the MME service.
  - **Priority**: The priority set for the applied integrity algorithm. The least value has the highest preference.

    In releases prior to 21.11.3: Possible priority values are between 1 to 3.

    In 21.11.3 and later releases: Possible priority values are between 1 to 4.
  - **Algorithm**: The applied encryption algorithm. Possible algorithms are:
    - **128-eia0**: Null ciphering algorithm (128-EIA0) for LTE integrity as the integrity algorithm for security procedures.
    - **128-eia1**: SNOW 3G synchronous stream ciphering algorithm (128-EIA1) for LTE integrity as the integrity algorithm for security procedures.

- **128-eia2**: Advance Encryption Standard (AES) ciphering algorithm (128-EIA2) for LTE encryption as the integrity algorithm for security procedures. This is the default encryption algorithm applicable for security procedures.
- **128-eia3**: ZUC algorithm (128-EIA3) for LTE integrity as the integrity algorithm for security procedures.