



# Encryption and Integrity Protection

- [Feature Summary and Revision History, on page 1](#)
- [Feature Description, on page 1](#)
- [How it Works, on page 2](#)
- [Feature Configuration, on page 7](#)
- [OAM Support, on page 8](#)

## Feature Summary and Revision History

### Summary Data

*Table 1: Summary Data*

Applicable Product(s) or Functional Area	AMF
Applicable Platform(s)	SMI
Feature Default Setting	Enabled – Always-on
Related Documentation	Not Applicable

### Revision History

*Table 2: Revision History*

Revision Details	Release
First introduced.	2021.04.0

## Feature Description

The AMF supports the following encryption and integrity protection algorithms to enable encryption and integrity protection on the N1/N2 interface:

- NEA0/NIA0
- 128-NEA1/128-NIA1
- 128-NEA2/128-NIA2

## How it Works

This section describes how this feature works.

The UE Security Capability IE, received from the UE in Registration Request, is used by the network to indicate which security algorithms are supported by the UE for NAS security. The AMF creates a new security context for the UE and does the negotiation of encryption and integrity protection algorithms. These algorithms are configurable along with the priority of negotiation. The AMF compares the algorithms supported by the UE with configuration priority and selects the algorithms to be used for encryption and integrity protection. When integrity protection is disabled, ciphering is also auto-disabled.

In addition, the NasSubscriber database is a new database that stores the UE security context for both the AMF application and the protocol layer to access. The AMF application stores the derived keys and negotiated algorithms in the NasSubscriber database before sending the security mode command to the UE. The AMF protocol encodes the packets received from the AMF application and initiates the encryption and integrity protection based on the negotiated algorithm and the downlink Nas count.

The AMF extracts the security header from the packets to verify integrity protection in the uplink path. After verification, the AMF protocol deciphers the packets before sending it to the AMF application.

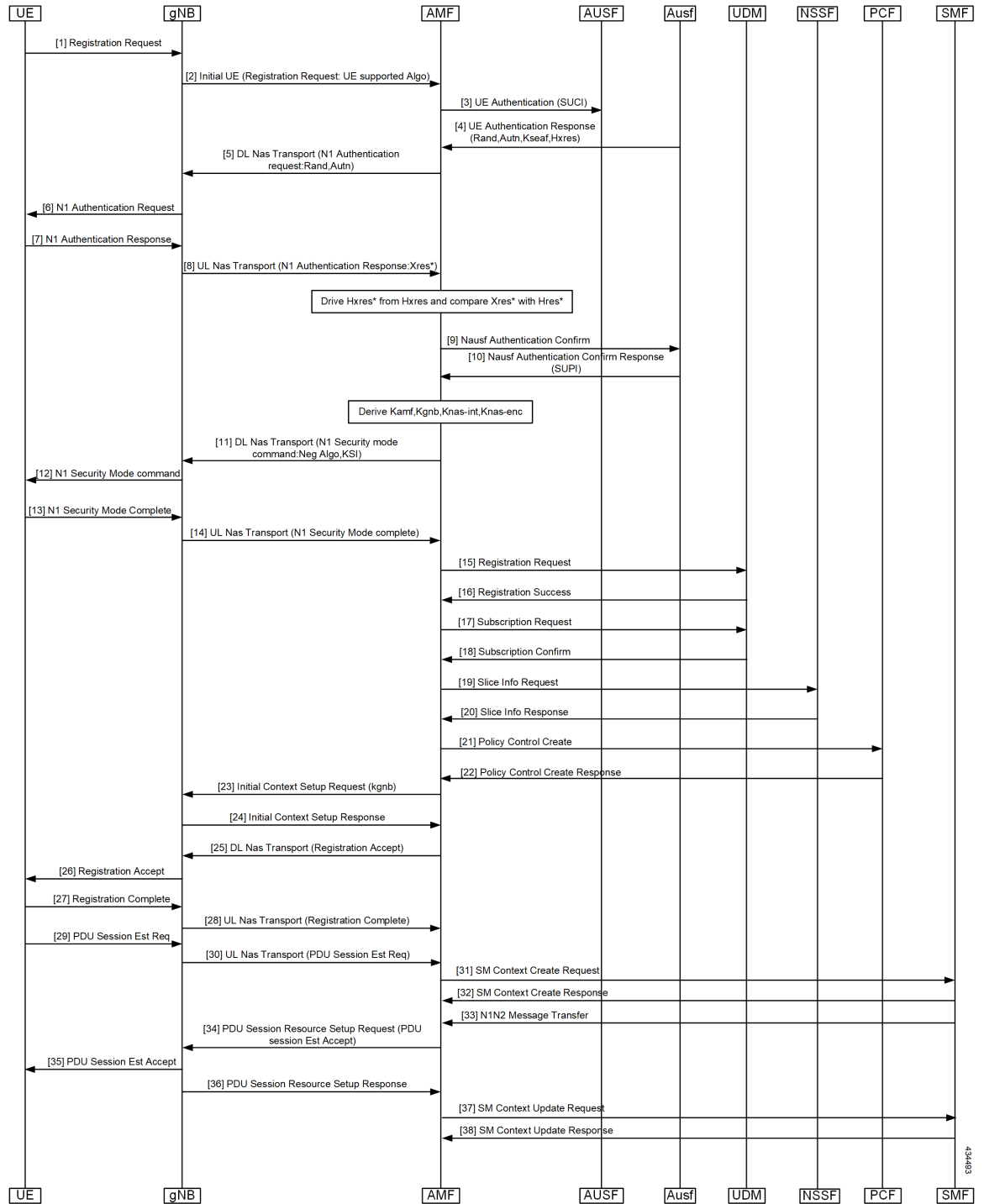
## Call Flows

This section describes the key call flows for this feature.

### UE Registration with Encryption/Integrity Protection Call Flow

The section describes the UE registration procedure with encryption/integrity protection call flow.

Figure 1: UE Registration with Encryption/Integrity Protection Call Flow



4-34437

Table 3: UE Registration with Encryption/Integrity Protection Call Flow Description

Step	Description
1	UE Registration with Encryption/Integrity Protection UE sends registration request to gNB.
2	gNB sends Initial UE Registration Request to AMF.
3	AMF sends UE Authentication (SUCI) to AUSF.
4	AUSF sends UE Authentication Response with Rand, Autn, Kseaf and Hxres information to AUSF.
5	AMF sends DL Nas Transport with N1 Authentication request with Rand and Autn to gNB.
6, 7	gNB sends N1 authentication request to UE and receives N1 Authentication Response from it.
8	gNB sends UL Nas Transport message N1 Authentication Response:Xres* to AMF.
9, 10	AMF derives HXres* from HXres and compares Xres* with Hres*. It sends Nausf authentication Confirm to AUSF and receives response with SUPI from it.
11	AMF derives Kamf, Kgnb, Knas-int and Knas-enc. It sends DL Nas Transport (N1 Security mode command:Neg Algo,KSI) to gNB.
12	gNB sends N1 Security mode command to UE.
13	UE sends N1 Security Mode Complete to gNB.
14	gNB sends UL Nas Transport (N1 Security Mode complete) to AMF.
15, 16	AMF sends Registration Request to UDM and receives Registration Success from it.
17, 18	AMF sends Subscription Request to UDM and receives Subscription Confirm from it.
19, 20	AMF sends Slice Info Request to NSSF and receives Slice Info Response from it.
21, 22	AMF sends Policy Control Create to PCF and receives Policy Control Create Response from it.
23, 24	AMF sends Initial Context Setup request (kgnb) to gNB and receives response from it.
25, 26	AMF sends DL Nas Transport (Registration Accept) message to gNB. gNB forwards it to UE.
27, 28	UE sends Registration Accept to gNB. gNB forwards this message in UL Nas Transport to AMF.
29, 30	UE sends PDU Session Establishment Request message to gNB. gNB forwards this message in UL Nas Transport to AMF.
31, 32	AMF sends SM context Create Request message to SMF and receives response from it.
33	SMF sends N1N2 Message Transfer message to AMF.
34	AMF sends PDU Session Resource setup request (PDU session Estb Accept) to gNB.
35, 36	gNB sends PDU Session Resource setup request to UE and receives PDU Session resource setup response from it.

Step	Description
37, 38	AMF sends SM Context Update Request to SMF and receives response from it.

## UE Access and Authentication Request Call Flow

The section describes the UE access and Authentication Request procedure call flow.

Figure 2: UE Access and Authentication Request Call Flow

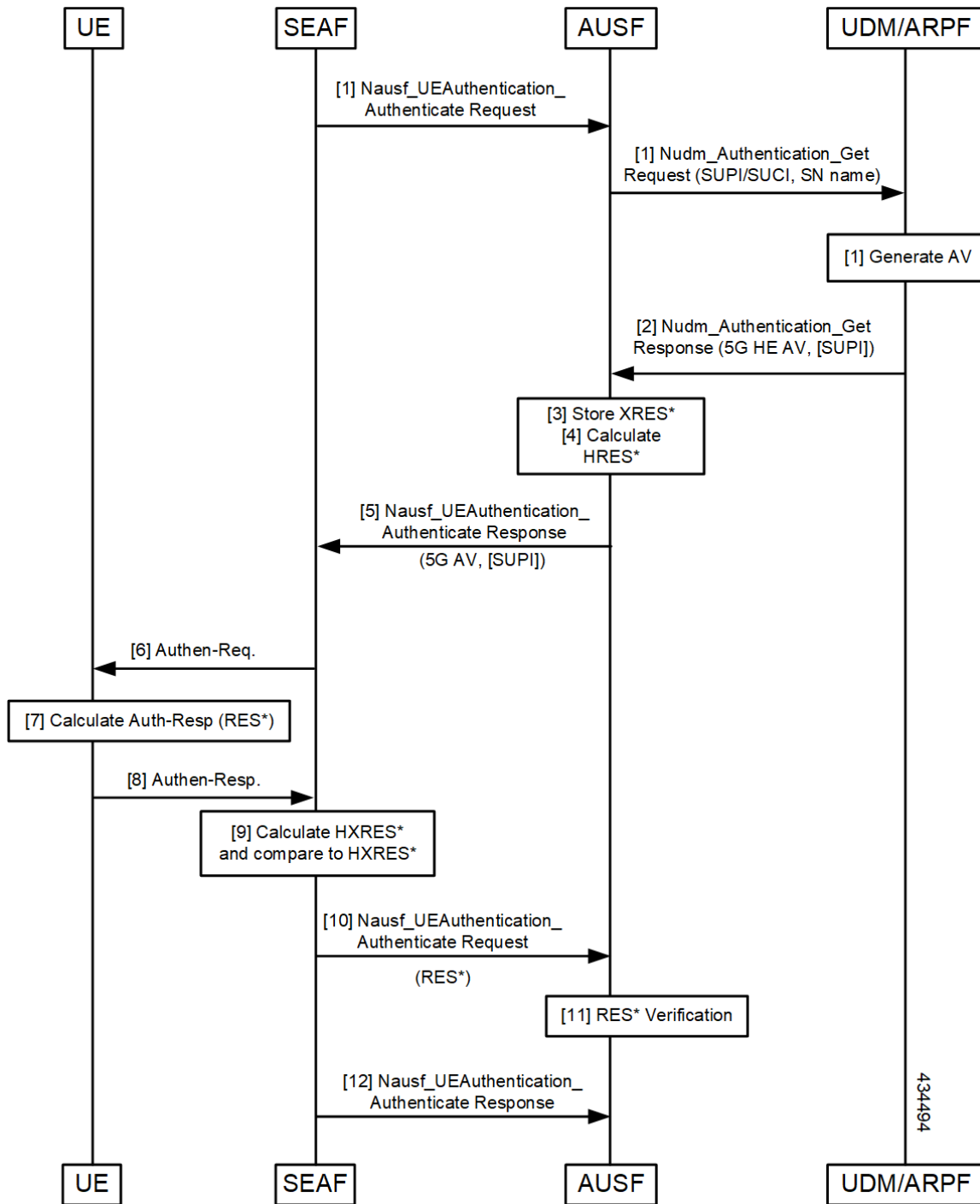


Table 4: UE Access and Authentication Request Call Flow Description

Step	Description
1	SEAF sends Nausf_UE_Authentication Request to AUSF. AUSF sends Nausf_UE_Authentication_Get Request with SUPI/SUCI and SN name to UDM/ARPF.
2	UDM/ARPF sends Nudm_Authentication_Get response to AUSF.
3, 4, 5	AUSF stores XRES and calculates HRES. It sends Nudm_Authentication_Get response to SEAF.
6	SEAF sends Authentication Response to UE.
7, 8	UE calculates Auth-Rsp and sends Authentcation response to SEAF.
9, 10	SEAF sends HXRES* and sends Nausf_UEAuthentication_Authenticate Request to AUSF.
11, 12	AUSF does RES* verification and sends Nausf_UEAuthentication_Authenticate Response to SEAF.

## Feature Configuration

This section describes how to configure AMF Cipherring Algorithm.

This feature is configured under the amf-global configuration.

The supi-policy is configured per subscriber or for a group of subscribers. It's done by associating the supi/supi-prefix with the supi policy. The operator policy name is configured under supi-policy and the call-control profile is configured under operator policy. Under call-control policy, authentication timer, retry, and security algorithms are configured.

To configure this feature, use the following configuration.

```

config
  amf-global
    call-control-policy call_control_policy_name
      timers t3560
        value time_value
        retry retry_value
      exit
    security-algo security_algo_priority
      cipherring-algo [5G-EA0 | 128-5G-EA1 | 128-5G-EA2]
      integrity-prot-algo [5G-IA0 | 128-5G-IA1 | 128-5G-IA2]
    exit
    operator-policy operator_policy_name
      ccp-name ccp_name
    exit
    supi-policy supi_policy_name
      operator-policy-name operator_policy_name
    end

```

### NOTES:

- **call-control-policy** *call\_control\_policy\_name*—Specify the call control policy name.

- **security-algo** *security\_algo\_priority*—Specify the priority of security algorithms. Its values are 1, 2, 3.
- **ciphering-algo** [5G-EA0 | 128-5G-EA1 | 128-5G-EA2]—Specify the Ciphering algorithm to use.
- **integrity-prot-algo** [5G-IA0 | 128-5G-IA1 | 128-5G-IA2]—Specify the Integrity protocol algorithm to use.
- **operator-policy** *operator\_policy\_name*—Specify the operator policy name.
- **supi-policy** *supi\_policy\_name*—Specify the SUPI policy name. SUPI policy name is the number which represents PLMN ID.

Example: `amf-global supi-policy 223556 operator-policy-name local`

## Configuration Example

The following is an example configuration.

```
config
  amf-global
    call-control-policy local
      timers t3560
      value 10
      retry 3
    security-algo 1
      ciphering-algo 128-5G-EA1
      ciphering-algo 128-5G-EA1
    exit
  operator-policy local
    ccp-name local
  exit
  supi-policy 123
    operator-policy-name local
  end
```

## OAM Support

This section describes operations, administration, and maintenance support for this feature.

## Bulk Statistics Support

The following statistics are supported for this feature.

### **amf\_nas\_security\_algos\_total**

Description: Captures the integrity and confidentiality algorithms that are used in AMF for processing the NAS messages and failure or errors that are associated with the security algorithms.

Labels:

- Label: `algos_lang`  
Label Description: The language type as go or c.
- Label: `algos_type`



Label Description: The algorithm type. Example: 128-5G-EA1

- Label: message\_direction

Label Description: The message direction as inbound or outbound.

- Label: message\_type

Label Description: The message type.

- Label: reason

Label Description: The reason for the failure.

- Label: status

Label Description: The status as success or failure.

### **amf\_nas\_security\_algos\_seconds\_total**

Description: Captures the time spent processing the security algorithms.

Labels:

- Label: algos\_lang

Label Description: The language type as go or c.

- Label: algos\_type

Label Description: The algorithm type. Example: 128-5G-EA1

- Label: message\_direction

Label Description: The message direction as inbound or outbound.

- Label: message\_type

Label Description: The message type.

- Label: reason

Label Description: The reason for the failure.

- Label: status

Label Description: The status as success or failure.

