

## 9.1.2.6.3.3 Specific message contents

**Table 9.1.2.6.3.3-1: AUTHENTICATION REQUEST (step 3, Table 9.1.2.6.3.2-1)**

Derivation Path: 36.508, Table 4.7.2-7			
Information Element	Value/remark	Comment	Condition
Authentication parameter AUTN	Invalid MAC	SS shall calculate the correct MAC value as specified in TS 33.102 and use any different value, e.g. correct_MAC+5.	

**Table 9.1.2.6.3.3-2: AUTHENTICATION FAILURE (step 5, Table 9.1.2.6.3.2-1)**

Derivation Path: 36.508, Table 4.7.2-5			
Information Element	Value/remark	Comment	Condition
EMM cause	'0001 0100'B	MAC failure	
Authentication failure parameter	Not present		

**Table 9.1.2.6.3.3-3: AUTHENTICATION REQUEST (step 8, Table 9.1.2.6.3.2-1)**

Derivation Path: 36.508, Table 4.7.2-7			
Information Element	Value/remark	Comment	Condition
Authentication parameter AUTN	Valid MAC	SS shall calculate the correct MAC value as specified in TS 33.102, e.g. correct_MAC.	

## 9.1.3 Security mode control procedure

### 9.1.3.1 NAS security mode command accepted by the UE

#### 9.1.3.1.1 Test Purpose (TP)

(1)

```

with { successful completion of EPS authentication and key agreement (AKA) procedure }
ensure that {
  when { UE receives an integrity protected SECURITY MODE COMMAND message including replayed
security capabilities and IMEISV request }
  then { UE sends an integrity protected and ciphered SECURITY MODE COMPLETE message including
IMEISV and starts applying the NAS Security in both UL and DL }

```

(2)

```

with { NAS Security Activated and EPS Authentication and key agreement procedure is executed for new
Key generation}
ensure that {
  when { UE receives an integrity protected SECURITY MODE COMMAND message corresponding to NAS count
reset to zero including replayed security capabilities and IMEISV request }
  then { UE sends integrity protected and ciphered SECURITY MODE COMPLETE message [with NAS count
set to zero] including IMEISV and starts applying the NAS Security in both UL and DL }
}

```

#### 9.1.3.1.2 Conformance requirements

References: The conformance requirements covered in the current TC are specified in: TS 24.301 clause 4.4.3.1, 5.4.3.1, 5.4.3.2 and 5.4.3.3.

[TS 24.301, clause 4.4.3.1]

Each EPS NAS security context shall be associated with two separate counters NAS COUNT: one related to uplink NAS messages and one related to downlink NAS messages. The NAS COUNT counters use 24 bit internal

representation and are independently maintained by UE and MME. The NAS COUNT shall be constructed as a NAS sequence number (8 least significant bits) concatenated with a NAS overflow counter (16 most significant bits).

When NAS COUNT is input to NAS ciphering or NAS integrity algorithms it shall be considered to be a 32-bit entity which shall be constructed by padding the 24-bit internal representation with 8 zeros in the most significant bits.

During the handover from UTRAN/GERAN to E-UTRAN, if the mapped EPS security context is taken into use, the NAS COUNT values for this EPS security context shall be initialized to zero in the UE and the network for uplink and downlink NAS messages.

The NAS sequence number part of the NAS COUNT shall be exchanged between the UE and the MME as part of the NAS signalling. After each new or retransmitted outbound security protected NAS message, the sender shall increase the NAS COUNT number by one. Specifically, on the sender side, the NAS sequence number shall be increased by one, and if the result is zero (due to wrap around), the NAS overflow counter shall also be incremented by one (see subclause 4.4.3.5). The receiving side shall estimate the NAS COUNT used by the sending side. Specifically, if the estimated NAS sequence number wraps around, the NAS overflow counter shall be incremented by one.

[TS 24.301, clause 5.4.3.1]

The purpose of the NAS security mode control procedure is to take an EPS security context into use, and initialise and start NAS signalling security between the UE and the MME with the corresponding NAS keys and security algorithms.

[TS 24.301, clause 5.4.3.2]

The MME initiates the NAS security mode control procedure by sending a SECURITY MODE COMMAND message to the UE and starting timer T3460 (see example in figure 5.4.3.2.1).

If the security mode control procedure is initiated further to a successful execution of the authentication procedure, the MME shall use the reset downlink NAS COUNT to integrity protect the SECURITY MODE COMMAND message.

The MME shall send the SECURITY MODE COMMAND message unciphered, but shall integrity protect the message with the NAS integrity key based on  $K_{ASME}$  or mapped  $K'_{ASME}$  indicated by the eKSI included in the message. The MME shall set the security header type of the message to "integrity protected with new EPS security context".

...

The MME shall include the replayed security capabilities of the UE (including the security capabilities with regard to NAS, RRC and UP (user plane) ciphering as well as NAS, RRC integrity, and other possible target network security capabilities, i.e. UTRAN/GERAN if UE included them in the message to network), the replayed nonce<sub>UE</sub> if the UE included it in the message to the network, the selected NAS ciphering and integrity algorithms and the Key Set Identifier (eKSI).

Additionally, the MME may request the UE to include its IMEISV in the SECURITY MODE COMPLETE message.

NOTE: The AS and NAS security capabilities will be the same, i.e. if the UE supports one algorithm for NAS it is also be supported for AS.

[TS 24.301, clause 5.4.3.3]

Upon receipt of the SECURITY MODE COMMAND message, the UE shall check whether the security mode command can be accepted or not. This is done by performing the integrity check of the message and by checking that the received UE security capabilities and the received nonce<sub>UE</sub> have not been altered compared to what the UE provided in the initial layer 3 message that triggered this procedure.

If the type of security context flag is set to "native security context" and if the KSI matches a valid native EPS security context held in the UE while the UE has a mapped EPS security context as the current security context, the UE shall take the native EPS security context into use. The UE shall store the native EPS security context, as specified in annex C.

If the security mode command can be accepted, the UE shall reset the uplink NAS COUNT and the UE shall take the new EPS security context into use when:

- a) the SECURITY MODE COMMAND message is received further to a successful execution of the authentication procedure; or

b) the type of security context flag is set to "mapped security context" in the NAS KSI IE included in the SECURITY MODE COMMAND message.

If the security mode command can be accepted and the eKSI was included in the SECURITY MODE COMMAND message, the UE shall send a SECURITY MODE COMPLETE message integrity protected with the selected NAS integrity algorithm and the NAS integrity key based on the  $K_{ASME}$  or mapped  $K'_{ASME}$  if the type of security context flag is set to "mapped security context" indicated by the eKSI. If the SECURITY MODE COMMAND message includes the type of security context flag set to "mapped security context" in the NAS KSI IE,  $nonce_{MME}$  and  $nonce_{UE}$ , the UE shall generate  $K'_{ASME}$  from both nonces as indicated in 3GPP TS 33.401 [19] and reset the downlink NAS COUNT to check whether the SECURITY MODE COMMAND can be accepted or not. The UE shall cipher the SECURITY MODE COMPLETE message with the selected NAS ciphering algorithm and the NAS ciphering key based on the  $K_{ASME}$  or mapped  $K'_{ASME}$  indicated by the eKSI. The UE shall set the security header type of the message to "integrity protected and ciphered with new EPS security context".

From this time onwards the UE shall cipher and integrity protect all NAS signalling messages with the selected NAS ciphering and NAS integrity algorithms.

If the MME indicated in the SECURITY MODE COMMAND message that the IMEISV is requested, the UE shall include its IMEISV in the SECURITY MODE COMPLETE message.

#### 9.1. 3.1.3 Test description

##### 9.1.3.1.3.1 Pre-test conditions

#### System Simulator:

- Cell A

#### Preamble:

- The UE is in state Switched OFF (state 1) according to [18].

## 9.1.3.1.3.2 Test procedure sequence

Table 9.1.3.1.3.2-1: Main behaviour

St	Procedure	Message Sequence		TP	Verdict
		U - S	Message		
1	The UE is switched on.	-	-	-	-
2	The UE transmits an ATTACH REQUEST message including a PDN CONNECTIVITY REQUEST message.	-->	ATTACH REQUEST	-	-
3	The SS transmits an AUTHENTICATION REQUEST message to initiate the EPS authentication and AKA procedure.	<--	AUTHENTICATION REQUEST	-	-
4	The UE transmits an AUTHENTICATION RESPONSE message and establishes mutual authentication.	-->	AUTHENTICATION RESPONSE	-	-
5	The SS transmits a SECURITY MODE COMMAND message to activate NAS security. It is integrity protected and includes request to include IMEISV	<--	SECURITY MODE COMMAND	-	-
6	Check: Does the UE transmit a SECURITY MODE COMPLETE message and does it establish the initial security configuration?	-->	SECURITY MODE COMPLETE	1	P
-	EXCEPTION: Steps 6Aa1 to 6Aa2 describe behaviour that depends on UE configuration; the "lower case letter" identifies a step sequence that take place if the UE has ESM information which needs to be transferred.	-	-	-	-
6A a1	IF the UE sets the ESM information transfer flag in the last PDN CONNECTIVITY REQUEST message THEN the SS transmits an ESM INFORMATION REQUEST message to initiate exchange of protocol configuration options and/or APN.	<--	ESM INFORMATION REQUEST	-	-
6A a2	The UE transmits an ESM INFORMATION RESPONSE message to transfer protocol configuration options and/or APN.	-->	ESM INFORMATION RESPONSE	-	-
7	The SS transmits an ATTACH ACCEPT message. The ACTIVATE DEFAULT EPS BEARER CONTEXT REQUEST message is piggybacked in ATTACH ACCEPT message	<--	ATTACH ACCEPT	-	-
8	The UE transmits an ATTACH COMPLETE message including an ACTIVATE DEFAULT EPS BEARER CONTEXT ACCEPT message	-->	ATTACH COMPLETE	-	-
9	The SS Transmits an IDENTITY REQUEST message [Security protected]	<-	IDENTITY REQUEST	-	-
10	Check: Does the UE transmit an IDENTITY RESPONSE message [Security Protected]?	->	IDENTITY RESPONSE	1	P
11	The SS transmits an AUTHENTICATION REQUEST message to initiate the EPS authentication and AKA procedure for new key set generation.	<--	AUTHENTICATION REQUEST	-	-
12	The UE transmits an AUTHENTICATION RESPONSE message and establishes mutual authentication.	-->	AUTHENTICATION RESPONSE	-	-
13	SS resets UL and DL NAS Count to zero	-	-	-	-
14	The SS transmits a SECURITY MODE COMMAND message to activate NAS security. It is integrity protected and includes request to include IMEISV	<--	SECURITY MODE COMMAND	-	-
15	The UE transmits a NAS SECURITY MODE COMPLETE message and establishes the initial security configuration.	-->	SECURITY MODE COMPLETE	2	P
	Exception : Steps 16 and 17 are executed 100 times to check UE is applying security correctly				
16	The SS transmits an IDENTITY REQUEST message [Security protected]	<-	IDENTITY REQUEST	-	-

17	Check: Does the UE transmit an IDENTITY RESPONSE message [Security Protected]?	->	IDENTITY RESPONSE	2	P
----	--	----	-------------------	---	---

### 9.1.3.1.3.3 Specific message contents

**Table 9.1.3.1.3.3-1: SECURITY MODE COMMAND (Steps 5 and 14)**

Derivation path: 36.508 table 4.7.2-19			
Information Element	Value/Remark	Comment	Condition
IMEISV request	Present		

**Table 9.1.3.1.3.3-2: SECURITY MODE COMPLETE (Steps 6 and 15)**

Derivation path: 36.508 table 4.7.2-20			
Information Element	Value/Remark	Comment	Condition
IMEISV	Present		

## 9.1.3.2 NAS security mode command not accepted by the UE

### 9.1.3.2.1 Test Purpose (TP)

(1)

```
with { successful completion of EPS authentication and key agreement (AKA) procedure[ ]
ensure that {
  when { UE receives an integrity protected SECURITY MODE COMMAND message including not matching
replayed security capabilities}
  then { UE sends SECURITY MODE REJECT and does not start applying the NAS security in both UL and
DL}
}
```

### 9.1.3.2.2 Conformance requirements

References: The conformance requirements covered in the current TC are specified in: TS 24.301 clause 5.4.3.1, 5.4.3.2, 5.4.3.3 and 5.4.3.5.

[TS 24.301, clause 5.4.3.1]

The purpose of the NAS security mode control procedure is to take an EPS security context into use, and initialise and start NAS signalling security between the UE and the MME with the corresponding NAS keys and security algorithms.

[TS 24.301, clause 5.4.3.2]

The MME initiates the NAS security mode control procedure by sending a SECURITY MODE COMMAND message to the UE and starting timer T3460 (see example in figure 5.4.3.2.1).

If the security mode control procedure is initiated further to a successful execution of the authentication procedure, the MME shall use the reset downlink NAS COUNT to integrity protect the SECURITY MODE COMMAND message.

The MME shall send the SECURITY MODE COMMAND message unciphered, but shall integrity protect the message with the NAS integrity key based on  $K_{ASME}$  or mapped  $K'_{ASME}$  indicated by the eKSI included in the message. The MME shall set the security header type of the message to "integrity protected with new EPS security context".

...

The MME shall include the replayed security capabilities of the UE (including the security capabilities with regard to NAS, RRC and UP (user plane) ciphering as well as NAS, RRC integrity, and other possible target network security capabilities, i.e. UTRAN/GERAN if UE included them in the message to network), the replayed nonce<sub>UE</sub> if the UE included it in the message to the network, the selected NAS ciphering and integrity algorithms and the Key Set Identifier (eKSI).

Additionally, the MME may request the UE to include its IMEISV in the SECURITY MODE COMPLETE message.

NOTE: The AS and NAS security capabilities will be the same, i.e. if the UE supports one algorithm for NAS it is also be supported for AS.