# 9 USIM service handling

## 9.1 Access Point Name Control List handling

### 9.1.1 Access Point Name Control List handling for terminals supporting ACL

#### 9.1.1.1 Definition and applicability

This EFACL contains the list of allowed APNs (Access Point Names).When the APN Control List service is enabled, the ME shall check that the entire APN of any PDP context is listed in EFACL before requesting this PDP context activation from the network. If the APN is not present in EFACL, the ME shall not request the corresponding PDP context activation from the network.

#### 9.1.1.2 Conformance requirement

The terminal shall support the APN Control List service as defined in TS 31.102 [4], clauses 5.1.1.2 and 5.3.14.

Reference:

- TS 31.102 [4], clauses 4.2.8, 4.2.48, 5.1.1.2 and 5.3.14;

- TS 23.060 [25], clause 9.2.

#### 9.1.1.3 Test purpose

1) To verify that the terminal takes into account the status of the APN Control List service as indicated in EFUST and EFEST.

2) To verify that the terminal checks that the entire APN of any PDP context is listed in EFACL before requesting this PDP context activation from the network if the ACL service is enabled.

3) To verify that the terminal does not request the corresponding PDP context activation from the network if the ACL service is enabled and the APN is not present in EFACL.

#### 9.1.1.4 Method of test

##### 9.1.1.4.1 Initial conditions

The terminal is connected to the USIM Simulator and the (U)SS.

The default USIM is used with the following exceptions:

The APN Control List (ACL) shall be allocated and activated in the USIM Service Table and enabled in the Enabled Service Table.

EFACL shall be present with the following values:

**EFACL (Access Point Control List)**

Logically: Number of available bytes: 64

Number of APNs: 3

1st APN: test.test

2nd APN: 3gpp.test

3rd APN: 2gpp.test

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Byte: | B1 | B2 | B3 | B4 | B5 | B6 | B7 | B8 | B9 | B10 | B11 | B12 |
| Coding: | 03 | DD | 0A | 04 | 74 | 65 | 73 | 74 | 04 | 74 | 65 | 73 |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | B13 | B14 | B15 | B16 | B17 | B18 | B19 | B20 | B21 | B22 | B23 | B24 |
|  | 74 | DD | 0A | 04 | 33 | 67 | 70 | 70 | 04 | 74 | 65 | 73 |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | B25 | B26 | B27 | B28 | B29 | B30 | B31 | B32 | B33 | B34 | B35 | B36 |
|  | 74 | DD | 0A | 04 | 32 | 67 | 70 | 70 | 04 | 74 | 65 | 73 |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | B37 | B38 | … | B64 |  |  |  |  |  |  |  |  |
|  | 74 | FF | … | FF |  |  |  |  |  |  |  |  |

##### 9.1.1.4.2 Procedure

a) The terminal is switched on and the USIM application shall be activated.

b) The user shall request a PDP context activation to "1gpp.test".

c) The user shall request a PDP context activation to "3gpp.test".

d) The user shall deactivate the PDP context.

e) The user shall disable the APN Control List service. When prompted to enter PIN2, the user shall present the correct PIN2 value.

f) The user shall request a PDP context activation to "1gpp.test".

g) The user shall deactivate the PDP context and shall switch the terminal off and then switch on again.

h) The user shall enable the APN Control List service. When prompted to enter PIN2, the user shall present the correct PIN2 value.

i) The user shall request a PDP context activation to "1ppp.net".

j) The terminal is switched off and on.

k) The user shall add the APN "1ppp.net" to the APN Control List. When prompted to enter PIN2, the user shall present the correct PIN2 value.

l) The user shall request a PDP context activation to "1ppp.net".

m) The user shall deactivate the PDP context and switch off the terminal.

#### 9.1.1.5 Acceptance criteria

1) After step a) the terminal shall have activated the USIM application, shall have read the status of the ACL service in EFUST and EFEST and be in updated idle mode on the (U)SS.

2) The terminal shall have not requested a PDP context activation in step b).

3) After step c) the PDP context shall have been activated.

4) After step d) the PDP context shall have been deactivated.

5) After step e) the APN Control List service shall have been set to disabled in EFEST.

6) After step f) the PDP context shall have been activated.

7) After step g) the PDP context shall have been deactivated.

8) After step h) the APN Control List service shall have been set to enabled in EFEST.

9) The terminal shall not have requested a PDP context activation in step i).

10) After step k) the APN "1ppp.net" shall have been added to the APN Control List in EFACL.

11) After step l) the PDP context shall have been activated.

### 9.1.2 Network provided APN handling for terminals supporting ACL

#### 9.1.2.1 Definition and applicability

This EFACL contains the list of allowed APNs (Access Point Names).When the APN Control List service is enabled, the ME shall check that the entire APN of any PDP context is listed in EFACL before requesting this PDP context activation from the network. If the APN is not present in EFACL, the ME shall not request the corresponding PDP context activation from the network.

In the case that the APN Control List is enabled and no APN is indicated in the PDP context request, indicating that a network provided APN is to be used, then the ME shall only request the PDP context activation if "network provided APN" is contained within EFACL.

#### 9.1.2.2 Conformance requirement

The terminal shall support the APN Control List service as defined in TS 31.102 [4], clauses 5.1.1.2 and 5.3.14.

Reference:

- TS 31.102 [4], clauses 4.2.8, 4.2.48, 5.1.1.2 and 5.3.14;

- TS 23.060 [25], clause 9.2.

#### 9.1.2.3 Test purpose

1) To verify that if ACL is enabled and if no APN is indicated in the PDP context the terminal request the PDP context activation only if "network provided APN" is contained within EFACL.

2) To verify that the user is able to set an APN in EFACL entry to the value "network provided APN".

3) To verify that the minimum set of APN entries in EFACL is ensured when the user deletes APN entries.

#### 9.1.2.4 Method of test

##### 9.1.2.4.1 Initial conditions

The terminal is connected to the USIM Simulator and the (U)SS.

The default USIM is used with the following exceptions:

The APN Control List (ACL) shall be allocated and activated in the USIM Service Table and enabled in the Enabled Service Table.

EFACL shall be present with the following values:

**EFACL (Access Point Control List)**

Logically: Number of available bytes: 64

Number of APNs: 3

1st APN: test.test

2nd APN: 3gpp.test

3rd APN: 2gpp.test

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Byte: | B1 | B2 | B3 | B4 | B5 | B6 | B7 | B8 | B9 | B10 | B11 | B12 |
| Coding: | 03 | DD | 0A | 04 | 74 | 65 | 73 | 74 | 04 | 74 | 65 | 73 |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | B13 | B14 | B15 | B16 | B17 | B18 | B19 | B20 | B21 | B22 | B23 | B24 |
|  | 74 | DD | 0A | 04 | 33 | 67 | 70 | 70 | 04 | 74 | 65 | 73 |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | B25 | B26 | B27 | B28 | B29 | B30 | B31 | B32 | B33 | B34 | B35 | B36 |
|  | 74 | DD | 0A | 04 | 32 | 67 | 70 | 70 | 04 | 74 | 65 | 73 |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | B37 | B38 | … | B64 |  |  |  |  |  |  |  |  |
|  | 74 | FF | … | FF |  |  |  |  |  |  |  |  |

##### 9.1.2.4.2 Procedure

a) The terminal is switched on and the USIM application shall be activated.

b) The user shall add "network provided APN" to the APN Control List in EFACL by using an MMI dependent option in the terminal. When prompted to enter PIN2, the user shall present the correct PIN2 value.

c) The user shall request a PDP context activation to "3gpp.test".

d) The user shall deactivate the PDP context.

e) The user shall request a PDP context activation without indicating an APN.

f) The user shall deactivate the PDP context.

g) The user shall delete "network provided APN" from the APN Control List in EFACL by using an MMI dependent option in the terminal. When prompted to enter PIN2, the user shall present the correct PIN2 value.

h) The user shall request a PDP context activation to "3gpp.test".

i) The user shall deactivate the PDP context.

j) The user shall request a PDP context activation without indicating an APN.

k) The user shall try to delete all APNs from the APN Control List in EFACL by using an MMI dependent option in the terminal. When the terminal indicates that at least one APN entry shall remain, the user shall set this entry to "network provided APN". When prompted to enter PIN2, the user shall present the correct PIN2 value.

l) The user shall switch off the terminal.

#### 9.1.2.5 Acceptance criteria

1) After step a) the terminal shall have activated the USIM application, shall have read the status of the ACL service in EFUST and EFEST and be in updated idle mode on the (U)SS.

2) After step b) EFACL shall contain an entry for "network provided APN".

3) After step c) the PDP context shall have been activated.

4) After step d) the PDP context shall have been deactivated.

5) After step e) the PDP context shall have been activated.

6) After step f) the PDP context shall have been deactivated.

7) After step g) EFACL shall not contain an entry for "network provided APN".

8) After step h) the PDP context shall have been activated.

9) After step i) the PDP context shall have been deactivated.

10) The terminal shall have not requested a PDP context activation in step j).

11) After step k) EFACL shall contain one APN entry with the value "network provided APN" and the corresponding number of APNs in EFACL shall be 1.

### 9.1.3 Access Point Name Control List handling for terminals not supporting ACL

#### 9.1.3.1 Definition and applicability

This EFACL contains the list of allowed APNs (Access Point Names).When the APN Control List service is enabled, the ME shall check that the entire APN of any PDP context is listed in EFACL before requesting this PDP context activation from the network. If the APN is not present in EFACL, the ME shall not request the corresponding PDP context activation from the network.

If ACL is enabled, an ME which does not support ACL shall not send any APN to the network.

#### 9.1.3.2 Conformance requirement

An ME which does not support ACL shall not send any APN to the network if ACL is enabled.

Reference:

- TS 31.102 [4], 5.1.1.2.

#### 9.1.3.3 Test purpose

To verify that if ACL is enabled, an ME which does not support ACL, does not send any APN to the network to request a PDP context activation.9.1.3.4 Method of test

#### 9.1.3.4 Method of test

##### 9.1.3.4.1 Initial conditions

The terminal is connected to the USIM Simulator and the (U)SS.

The default USIM is used with the following exceptions:

The APN Control List (ACL) shall be allocated and activated in the USIM Service Table and enabled in the Enabled Service Table.

EFACL shall be present with the following values:

**EFACL (Access Point Control List)**

Logically: Number of available bytes: 64

Number of APNs: 3

1st APN: test.test

2nd APN: 3gpp.test

3rd APN: 2gpp.test

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Byte: | B1 | B2 | B3 | B4 | B5 | B6 | B7 | B8 | B9 | B10 | B11 | B12 |
| Coding: | 03 | DD | 0A | 04 | 74 | 65 | 73 | 74 | 04 | 74 | 65 | 73 |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | B13 | B14 | B15 | B16 | B17 | B18 | B19 | B20 | B21 | B22 | B23 | B24 |
|  | 74 | DD | 0A | 04 | 33 | 67 | 70 | 70 | 04 | 74 | 65 | 73 |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | B25 | B26 | B27 | B28 | B29 | B30 | B31 | B32 | B33 | B34 | B35 | B36 |
|  | 74 | DD | 0A | 04 | 32 | 67 | 70 | 70 | 04 | 74 | 65 | 73 |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | B37 | B38 | … | B64 |  |  |  |  |  |  |  |  |
|  | 74 | FF | … | FF |  |  |  |  |  |  |  |  |

##### 9.1.3.4.2 Procedure

a) The terminal is switched on and the USIM application shall be activated.

b) The user shall request a PDP context activation to "3gpp.test".

c) The terminal shall be switched off.

#### 9.1.3.5 Acceptance criteria

1) After step a) the terminal shall have activated the USIM application, shall have read the status of the ACL service in EFUST and EFEST and be in updated idle mode on the (U)SS.

2) The terminal shall not have sent any APN to the network in step b).

### 9.1.4 Access Point Name Control List handling for terminals supporting ACL connected to E-UTRAN/EPC

#### 9.1.4.1 Definition and applicability

This EFACL contains the list of allowed APNs (Access Point Names). If the APN Control List service is enabled and the ME is to provide an APN as part of attach for PDN connectivity, then the ME shall verify that the APN value is present in the EFACL and if it is not the ME shall not proceed with the attach procedure. If the APN Control List service is enabled and the ME does not indend to provide an APN as part of the attach for PDN connectivity and use a network provided APN, the ME shall not check if "network provided APN" is contained within EFACL.

There is 1:1 mapping between one PDP context and one EPS Bearer.

Some terminals might not support the enablement or the disablement of the APN Control List service or the modification of the APN Control List. In these cases, the test sequence below provides separate branches.

#### 9.1.4.2 Conformance requirement

The terminal shall support the APN Control List service as defined in TS 31.102 [4], clauses 5.1.1.2 and 5.3.14.

Reference:

- TS 31.102 [4], clauses 4.2.8, 4.2.48, 5.1.1.2 and 5.3.14;

- TS 23.060 [25], clause 9.2, 9.2.1A.

#### 9.1.4.3 Test purpose

1) To verify that the terminal takes into account the status of the APN Control List service as indicated in EFUST and EFEST.

2) To verify that the terminal checks that the entire APN of any EPS Bearer is listed in EFACL before requesting this EPS Bearer activation from the network if the ACL service is enabled.

3) To verify that the terminal does not request the corresponding EPS Bearer activation from the network if the ACL service is enabled and the APN is not present in EFACL.

4) To verify that the terminal does not check that the network provided APN is present in EFACL during the initial attach procedure.

#### 9.1.4.4 Method of test

##### 9.1.4.4.1 Initial conditions

The terminal is connected to the USIM Simulator and the E-USS.

The terminal is configured to use the network provided APN for the initial attach procedure.

The default E-UTRAN UICC is used with the following exceptions:

The APN Control List (ACL) shall be allocated and activated in the USIM Service Table and enabled in the Enabled Service Table.

EFACL shall be present with the following values:

**EFACL (Access Point Control List)**

Logically: Number of available bytes: 64

Number of APNs: 3

1st APN: test.test

2nd APN: 3gpp.test

3rd APN: 2gpp.test

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Byte: | B1 | B2 | B3 | B4 | B5 | B6 | B7 | B8 | B9 | B10 | B11 | B12 |
| Coding: | 03 | DD | 0A | 04 | 74 | 65 | 73 | 74 | 04 | 74 | 65 | 73 |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | B13 | B14 | B15 | B16 | B17 | B18 | B19 | B20 | B21 | B22 | B23 | B24 |
|  | 74 | DD | 0A | 04 | 33 | 67 | 70 | 70 | 04 | 74 | 65 | 73 |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | B25 | B26 | B27 | B28 | B29 | B30 | B31 | B32 | B33 | B34 | B35 | B36 |
|  | 74 | DD | 0A | 04 | 32 | 67 | 70 | 70 | 04 | 74 | 65 | 73 |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | B37 | B38 | … | B64 |  |  |  |  |  |  |  |  |
|  | 74 | FF | … | FF |  |  |  |  |  |  |  |  |

##### 9.1.4.4.2 Procedure

a) The terminal is switched on, the USIM application shall be activated and the terminal shall successfully attach the E-UTRAN.

b) The user shall request PDN connectivity to "1gpp.test".

c) The user shall request PDN connectivity to "3gpp.test".

d) The user shall deactivate the PDN connectivity to "3gpp.test".

e) If user interface does not have support to disable the APN Control List service, proceed to step l).

f) The user shall disable the APN Control List service. When prompted to enter PIN2, the user shall present the correct PIN2 value.

g) The user shall request PDN connectivity to "1gpp.test".

h) The user shall deactivate the PDN connectivity to "1gpp.test" and shall switch the terminal off and then switch on again.

i) The user shall enable the APN Control List service. When prompted to enter PIN2, the user shall present the correct PIN2 value.

j) The user shall request PDN connectivity to "1ppp.net".

k) The terminal is switched off and on.

l) If user interface does not have support to add APN to APN Control List, proceed to step p).

m) The user shall add the APN "1ppp.net" to the APN Control List. When prompted to enter PIN2, the user shall present the correct PIN2 value.

n) The user shall request PDN connectivity to "1ppp.net".

o) The user shall deactivate the PDN connectivity.

p) Switch off the terminal.

#### 9.1.4.5 Acceptance criteria

1) After step a) the terminal shall have activated the USIM application, shall have read the status of the ACL service in EFUST and EFEST and be in updated idle mode on the E-USS.

2) The terminal shall have not requested PDN connectivity in step b).

3) After step c) PDN connectivity shall have been activated.

4) After step d) PDN connectivity shall have been deactivated.

5) After step f) the APN Control List service shall have been set to disabled in EFEST.

6) After step g) PDN connectivity shall have been activated.

7) After step h) PDN connectivity shall have been deactivated.

8) After step i) the APN Control List service shall have been set to enabled in EFEST.

9) The terminal shall not have requested PDN connectivity in step j).

10) After step m) the APN "1ppp.net" shall have been added to the APN Control List in EFACL.

11) After step n) PDN connectivity shall have been activated.

12) After step o) PDN connectivity shall have been deactivated.

### 9.1.5 Void9.1.6 Void

## 9.2 Service Dialling Numbers handling

### 9.2.1 Definition and applicability

The Service Dialling Numbers feature allows for the storage of numbers related to services offered by the network operator/service provider in the SIM/USIM (e.g. customer care). The user can use these telephone numbers to make outgoing calls, but the access for updating of the numbers shall be under the control of the operator.

### 9.2.2 Conformance requirement

The terminal shall support the Service Dialling Numbers service as defined in TS 31.102 [4], clauses 4.2.8 and 4.2.29.

Reference:

- TS 31.102 [4], clauses 4.2.8, 4.2.29 and 4.2.31;

- TS 22.101 [11], clause A.23.

### 9.2.3 Test purpose

1) To verify that the terminal takes into account the status of the Service Dialling Numbers service as indicated in EFUST.

2) To verify that the user can use the Service Dialling Numbers to make outgoing calls.

3) To verify that the terminal is able to handle SDNs with an extended dialling number string.

4) To verify that the terminal is able to handle an empty alpha identifier in EFSDN.

5) To verify that the terminal is able to handle an alpha identifier of maximum length in EFSDN.

### 9.2.4 Method of test

#### 9.2.4.1 Initial conditions

The terminal is connected to the USIM Simulator and the (U)SS.

The default USIM is used with the following exceptions:

The Service Dialling Numbers (SDN) shall be allocated and activated in the USIM Service Table.

EFSDN shall be present with the following values:

**EFSDN (Service Dialling Numbers)**

Logically:

6 records, 1 record shall be empty. Unless otherwise stated, the SDN records shall not use extendend BCD numbers/SSC strings. Access to update EFSDN shall be granted by usage of ADM1 only.

Record 1: Length of alpha identifier: 241 characters;

Alpha identifier: "Hotline001122334455667788ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789abcdefghijklmnopqrstuvwxyz0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789abcdefghijklmnopqrstuvwxyz0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789abcdefghijklmnopqrstuvwxyz0123456789";

Length of BCD number: 5;

TON and NPI: Telephony and International;

Dialled number: "22223333";

CCP: 'FF';

Ext3: 'FF'.

Record 1:

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Coding: | B1 | B2 | B3 | B4 | B5 | B6 | B7 | B8 | B9 | B10 | B11 | … |
| Hex | 48 | 6F | 74 | 6C | 69 | 6E | 65 | 30 | 30 | 31 | … | … |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | B241 | B242 | B243 | B244 | B245 | B246 | B247 | B248 | B249 | B250 | B251 | B252 |
|  | 39 | 05 | 91 | 22 | 22 | 33 | 33 | FF | FF | FF | FF | FF |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | B253 | B254 | B255 |  |  |  |  |  |  |  |  |  |
|  | FF | FF | FF |  |  |  |  |  |  |  |  |  |

Record 2: Length of alpha identifier: 241 characters;

Alpha identifier: "Hotline002";

Length of BCD number: 5;

TON and NPI: Telephony and International;

Dialled number: "44554455";

CCI2: 'FF';

Ext3: 'FF'.

Record 2:

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Coding: | B1 | B2 | B3 | B4 | B5 | B6 | B7 | B8 | B9 | B10 | B11 | … |
| Hex | 48 | 6F | 74 | 6C | 69 | 6E | 65 | 30 | 30 | 32 | FF | … |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | B241 | B242 | B243 | B244 | B245 | B246 | B247 | B248 | B249 | B250 | B251 | B252 |
|  | FF | 05 | 91 | 44 | 55 | 44 | 55 | FF | FF | FF | FF | FF |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | B253 | B254 | B255 |  |  |  |  |  |  |  |  |  |
|  | FF | FF | FF |  |  |  |  |  |  |  |  |  |

Record 3: Length of alpha identifier: 241 characters;

Alpha identifier: "Hotline003";

Length of BCD number: 11;

TON and NPI: Telephony and International;

Dialled number: "01234567890123456789";

CCI2: 'FF';

Ext3: "01".

Record 3:

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Coding: | B1 | B2 | B3 | B4 | B5 | B6 | B7 | B8 | B9 | B10 | B11 | … |
| Hex | 48 | 6F | 74 | 6C | 69 | 6E | 65 | 30 | 30 | 33 | FF | … |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | B241 | B242 | B243 | B244 | B245 | B246 | B247 | B248 | B249 | B250 | B251 | B252 |
|  | FF | 0B | 91 | 10 | 32 | 54 | 76 | 98 | 10 | 32 | 54 | 76 |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | B253 | B254 | B255 |  |  |  |  |  |  |  |  |  |
|  | 98 | FF | 01 |  |  |  |  |  |  |  |  |  |

Record 4: Length of alpha identifier: 241 characters;

Alpha identifier: empty;

Length of BCD number: 03;

TON and NPI: Telephony and International;

Dialled number: "007";

CCI2: 'FF';

Ext3: 'FF'.

Record 4:

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Coding: | B1 | B2 | B3 | B4 | B5 | B6 | B7 | B8 | B9 | B10 | B11 | … |
| Hex | FF | FF | FF | FF | FF | FF | FF | FF | FF | FF | FF | … |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | B241 | B242 | B243 | B244 | B245 | B246 | B247 | B248 | B249 | B250 | B251 | B252 |
|  | FF | 03 | 91 | 00 | F7 | FF | FF | FF | FF | FF | FF | FF |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | B253 | B254 | B255 |  |  |  |  |  |  |  |  |  |
|  | FF | FF | FF |  |  |  |  |  |  |  |  |  |

Record 5: Length of alpha identifier: 241 characters;

Alpha identifier: empty;

Length of BCD number: 3;

TON and NPI: Telephony and International;

Dialled number: "008";

CCI2: 'FF';

Ext3: 'FF'.

Record 5:

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Coding: | B1 | B2 | B3 | B4 | B5 | B6 | B7 | B8 | B9 | B10 | B11 | … |
| Hex | FF | FF | FF | FF | FF | FF | FF | FF | FF | FF | FF | … |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | B241 | B242 | B243 | B244 | B245 | B246 | B247 | B248 | B249 | B250 | B251 | B252 |
|  | FF | 03 | 91 | 00 | F8 | FF | FF | FF | FF | FF | FF | FF |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | B253 | B254 | B255 |  |  |  |  |  |  |  |  |  |
|  | FF | FF | FF |  |  |  |  |  |  |  |  |  |

**EFEXT3 (Extension 3)**

Logically: 5 records, 4 records empty. Access to update EFEXT3 shall be granted by usage of ADM1 only.

Record 1: Record type: '02'

Extension data: "012345";

Identifier: 'FF'.

Record 1:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Coding: | B1 | B2 | B3 | B4 | B5 | B6 | B7 | B8 | B9 | B10 | B11 | B12 | B13 |  |
| Hex | 02 | 03 | 10 | 32 | 54 | FF | FF | FF | FF | FF | FF | FF | FF |  |

#### 9.2.4.2 Procedure

a) The terminal is switched on and the USIM application shall be activated.

b) The user shall use an MMI dependent procedure to set up a call to the dialling number associated with the alpha identifier "Hotline001122334455667788ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789abcdefghijklmnopqrstuvwxyz0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789abcdefghijklmnopqrstuvwxyz0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789abcdefghijklmnopqrstuvwxyz0123456789" in record 1 of EFSDN.

c) The user shall end the call.

d) The user shall use an MMI dependent procedure to set up a call to the dialling number associated with the "Hotline003" in record 3 of EFSDN.

e) The user shall end the call.

f) The user shall use an MMI dependent procedure to select and to set up a call to the dialling number "+007" stored in record 4 of EFSDN.

g) The user shall end the call and switch the terminal off.

### 9.2.5 Acceptance criteria

1) After step a) the terminal shall have activated the USIM application and shall have read the status of the SDN service in EFUST.

2) After step b) the terminal shall have read record 1 of EFSDN and a call to "+22223333" shall have been established.

3) After step c) the call shall have been terminated.

4) After step d) the terminal shall have read record 3 of EFSDN and record 1 of EFEXT1 and a call to "+01234567890123456789012345" shall have been established.

5) After step e) the call shall have been terminated.

6) After step f) the terminal shall have read record 4 of EFSDN and a call to "+007" shall have been established.

# 10 CSG list handling

## 10.1 CSG list handling for E-UTRA

### 10.1.1 Automatic CSG selection in E-UTRA with CSG list on USIM, success

#### 10.1.1.1 Definition and applicability

A Closed Subscriber Group identifies subscribers of an operator who are permitted to access one or more cells of the PLMN but which have restricted access (CSG cells). A CSG cell is part of the PLMN, broadcasting a CSG indication that is set to TRUE and a specific CSG identity. A CSG cell is accessible by the members of the closed subscriber group for that CSG identity. For a CSG cell, the UE shall check the broadcast CSG ID against the Allowed CSG list provided by NAS to check whether a CSG cell is suitable for the UE.

#### 10.1.1.2 Conformance requirement

When a UE in idle mode detects the presence of a permissible CSG cell (a CSG cell whose CSG identity is in the UE's permitted CSG list), the UE shall select the CSG cell.  
The ME shall read the allowed CSG IDs from EFACSGL in order to perform HNB selection procedures. The lists in EFACSGL shall take precedence over the list stored in the ME non-volatile memory.  
If the MS supports CSG, it is provisioned with a list of allowed CSG identities and associated PLMN identities from the USIM if the list is available in the USIM.

- TS 22.011 [6], clause 8.2.2.1;

- TS 31.102 [4], clauses 4.4.6.2 and 5.8.1;

- TS 23.122 [31], clause 3.1A.

#### 10.1.1.3 Test purpose

To verify that the ME only selects a CSG cell if the CSG IDs of the cell is found in the allowed CSG IDs from EFACSGL

#### 10.1.1.4 Method of test

##### 10.1.1.4.1 Initial conditions

For this test an E-USS is required.

The E-USS transmits on two cells, with the following network parameters:

- TAI (MCC/MNC/TAC): 246/081/0001.

- Access control: unrestricted.

- csg-Indication: TRUE

- csg-Identity: 05

- TAI (MCC/MNC/TAC): 246/081/0002.

- Access control: unrestricted.

- csg-Indication: TRUE

- csg-Identity: 04

The default E-UTRAN UICC is used.

The UICC is installed into the Terminal and the UE is set to automatic PLMN selection mode.

##### 10.1.1.4.2 Procedure

a) The UE is powered on.

b) After 2 minutes the E-USS stops all RF output for the first cell with TAI 246/081/0001 on the BCCH for a long enough period of time to cause a cell reselection procedure in the UE. The BCCH is changed to contain:

- csg-Identity: 03

The E-USS then resumes RF output on the BCCH.

c) After receipt of an *RRCConnectionRequest* from the UE on the E-UTRAN-cell related to the BCCH transmitting TAI 246/081/0001, the E-USS sends *RRCConnectionSetup* to the UE, followed by *RRCConnectionSetupComplete* sent by the UE to the E-USS.

d) During registration and after receipt of a *AttachRequest* from the UE, the E-USS initiates authentication, starts integrity by using the security procedure and sends *AttachAccept* with to the UE:

TAI (MCC/MNC/TAC): 246/081/ 0001

GUTI: "24608100010266436587"

e) After receipt of the *AttachComplete* during registration from the UE, the E-USS sends *RRCConnectionRelease to the UE.*

f) The UE is soft powered down.

#### 10.1.1.5 Acceptance criteria

1) After steps a) the terminal shall not attempt an Attach procedure.

2) After step b) the UE shall send an *RRCConnectionRequest* on the E-UTRAN-cell related to the BCCH transmitting TAI 246/081/0001 to the e-USS.

3) During step c) the terminal shall send *AttachRequest* to the E-USS.

4) After step d) the terminal shall respond with *AttachComplete* during registration.

5) After step e) the USIM shall contain the following values:

**EFEPSLOCI (EPS Information)**

Logically: GUTI: 24608100010266436587

Last visited registered TAI: 246/081/0001

EPS update status: updated

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Coding: | B1 | B2 | B3 | B4 | B5 | B6 | B7 | B8 | B9 | B10 | B11 |
| Hex | 0B | F6 | 42 | 16 | 80 | 00 | 01 | 02 | 66 | 43 | 65 |
|  | B12 | B13 | B14 | B15 | B16 | B17 | B18 |  |  |  |  |
|  | 87 | 42 | 16 | 80 | 00 | 01 | 00 |  |  |  |  |

### 10.1.2 Automatic CSG selection in E-UTRA with CSG list on USIM, removal of CSG ID from the USIM

#### 10.1.2.1 Definition and applicability

A Closed Subscriber Group identifies subscribers of an operator who are permitted to access one or more cells of the PLMN but which have restricted access (CSG cells). A CSG cell is part of the PLMN, broadcasting a CSG indication that is set to TRUE and a specific CSG identity. A CSG cell is accessible by the members of the closed subscriber group for that CSG identity. For a CSG cell, the UE shall check the broadcast CSG ID against the Allowed CSG list provided by NAS to check whether a CSG cell is suitable for the UE.

#### 10.1.2.2 Conformance requirement

When a UE in idle mode detects the presence of a permissible CSG cell (a CSG cell whose CSG identity is in the UE's permitted CSG list), the UE shall select the CSG cell.  
The ME shall read the allowed CSG IDs from EFACSGL in order to perform HNB selection procedures. The lists in EFACSGL shall take precedence over the list stored in the ME non-volatile memory.  
If the MS supports CSG, it is provisioned with a list of allowed CSG identities and associated PLMN identities from the USIM if the list is available in the USIM.

If the UE receives ATTACH REJECT with cause #25 (Not authorized for this CSG) with integrity protection, the UE shall remove the CSG ID of the cell where the UE has sent the ATTACH REQUEST message from the Allowed CSG list.

- TS 22.011 [6], clause 8.2.2.1;

- TS 31.102 [4], clauses 4.4.6.2 and 5.8.1;

- TS 23.122 [31], clause 3.1A.

- TS 24.301 [26], clause 5.5.1.2.5

#### 10.1.2.3 Test purpose

To verify that the ME removes the CSG ID from the Allowed CSG list in EFACSGL in case this CSG ID belongs to the cell where the ME has sent the ATTACH REQUEST message which was rejected with cause #25 by the E-USS.

#### 10.1.2.4 Method of test

##### 10.1.2.4.1 Initial conditions

For this test an E-USS is required.

The E-USS transmits on two cells, with the following network parameters:

- TAI (MCC/MNC/TAC): 246/081/0001.

- Access control: unrestricted.

- csg-Indication: TRUE

- csg-Identity: 03

- TAI (MCC/MNC/TAC): 246/081/0002.

- Access control: unrestricted.

- csg-Indication: TRUE

- csg-Identity: 04

The default E-UTRAN UICC is used.

The UICC is installed into the Terminal and the UE is set to automatic PLMN selection mode.

##### 10.1.2.4.2 Procedure

a) The UE is powered on.

b) After receipt of an *RRCConnectionRequest* from the UE on the E-UTRAN-cell related to the BCCH transmitting TAI 246/081/0001, the E-USS sends *RRCConnectionSetup* to the UE, followed by *RRCConnectionSetupComplete* sent by the UE to the E-USS.

c) During registration and after receipt of an *AttachRequest* from the UE, the E-USS initiates authentication, starts integrity by using the security procedure and sends *AttachReject* to the UE with cause #25 (Not authorized for this CSG) with integrity protection, followed by *RRCConnectionRelease.*

d) The UE is soft powered down.

#### 10.1.2.5 Acceptance criteria

1) After step a) the UE shall send an *RRCConnectionRequest* on the E-UTRAN-cell related to the BCCH transmitting TAI 246/081/0001 to the E-USS.

2) During step b) the terminal shall send *AttachRequest* to the E-USS.

3) After step c) the USIM shall contain the following values:

**EFEPSLOCI (EPS Information)**

Logically: GUTI: not checked

Last visited registered TAI: 246/081/0001

EPS update status: ROAMING NOT ALLOWED

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Coding: | B1 | B2 | B3 | B4 | B5 | B6 | B7 | B8 | B9 | B10 | B11 |
| Hex | xx | xx | xx | xx | xx | xx | xx | xx | xx | xx | xx |
|  | B12 | B13 | B14 | B15 | B16 | B17 | B18 |  |  |  |  |
|  | xx | 42 | 16 | 80 | xx | xx | 02 |  |  |  |  |

**EFACSGL (Allowed CSG Lists)**

Logically:

1st CSG list

PLMN: 246 081 (MCC MNC)

1st CSG list 1st CSG Type indication 02

1st CSG list 1st CSG HNB Name indication 02

1st CSG list 1st CSG CSG ID: 02 (27bit)

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Coding: | A0 | 0D | 80 | 03 | 42 | 16 | 80 | 81 | 06 | 02 |
|  | 02 | 00 | 00 | 00 | 5F |  |  |  |  |  |

2nd CSG list

PLMN: 244 081 (MCC MNC)

2nd CSG list 1st CSG Type indication 08

2nd CSG list 1st CSG HNB Name indication 08

2nd CSG list 1st CSG CSG ID: 08 (27bit)

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Coding: | A0 | 0D | 80 | 03 | 42 | 14 | 80 | 81 | 06 | 08 |
|  | 08 | 00 | 00 | 01 | 1F |  |  |  |  |  |

Note: the 1st and 2nd CSG list may be stored together or separately in any record in arbitrary order.

### 10.1.3 Manual CSG selection in E-UTRA with CSG list on USIM, success

#### 10.1.3.1 Definition and applicability

A Closed Subscriber Group identifies subscribers of an operator who are permitted to access one or more cells of the PLMN but which have restricted access (CSG cells). A CSG cell is part of the PLMN, broadcasting a CSG indication that is set to TRUE and a specific CSG identity. A CSG cell is accessible by the members of the closed subscriber group for that CSG identity. For a CSG cell, the UE shall check the broadcast CSG ID against the Allowed CSG list provided by NAS to check whether a CSG cell is suitable for the UE.

A UE supporting CSG selection selects CSG cell either automatically based on the list of allowed CSG identities or manually based on user selection of CSG on indication of list of available CSGs.

#### 10.1.3.2 Conformance requirement

The ME shall read the allowed CSG IDs from EFACSGL in order to perform HNB selection procedures. The lists in EFACSGL shall take precedence over the list stored in the ME non-volatile memory.  
In manual CSG selection mode, the ME indicates to the user the list of available CSGs in the currently selected PLMN. The list of CSGs presented to the user is not restricted by the allowed CSG list.  
If the MS supports CSG, it is provisioned with a list of allowed CSG identities and associated PLMN identities from the USIM if the list is available in the USIM.

If the UE supporting CSG selection has attempted manual CSG selection, the UE, when receiving the TRACKING AREA UPDATE ACCEPT message, shall check if the CSG ID of the cell where the UE has sent the TRACKING AREA UPDATE REQUEST message is contained in the Allowed CSG list. If not, the UE shall add that CSG ID to the

Allowed CSG list.

- TS 31.102 [4], clauses 4.4.6.2 and 5.8.1;

- TS 23.122 [31], clause 3.1A.

- TS 24.301 [26], clause 5.5.3.2.4

#### 10.1.3.3 Test purpose

To verify that the ME adds the CSG ID to the Allowed CSG list in EFACSGL in case this CSG ID belongs to the cell where the ME has sent the TRACKING AREA UPDATE REQUEST message which was accepted by the E-USS.

#### 10.1.3.4 Method of test

##### 10.1.3.4.1 Initial conditions

For this test an E-USS is required.

The E-USS transmits on two cells, with the following network parameters:

- TAI (MCC/MNC/TAC): 246/081/0001.

- Access control: unrestricted.

- csg-Indication: FALSE

- csg-Identity: not present

- TAI (MCC/MNC/TAC): 246/081/0002.

- Access control: unrestricted.

- csg-Indication: TRUE

- csg-Identity: 04

The default E-UTRAN UICC is used.

The UICC is installed into the Terminal and the UE is set to automatic PLMN selection mode.

##### 10.1.3.4.2 Procedure

a) The UE is powered on.

b) After receipt of an *RRCConnectionRequest* from the UE on the E-UTRAN-cell related to the BCCH transmitting TAI 246/081/0001, the E-USS sends *RRCConnectionSetup* to the UE, followed by *RRCConnectionSetupComplete* sent by the UE to the E-USS.

c) During registration and after receipt of an *AttachRequest* from the UE, the E-USS initiates authentication, starts integrity by using the security procedure and sends *AttachAccept* with to the UE:

TAI (MCC/MNC/TAC): 246/081/ 0001

GUTI: "24608100010266345678"

d) After receipt of the *AttachComplete* during registration from the UE, the E-USS sends *RRCConnectionRelease*  to the UE.

e) The MMI of the UE is used to perform manual CSG selection. The UE shall indicate the availability of a cell with csg-Identity 04 for PLMN 246/081. The user shall select this cell by using the MMI.

f) After receipt of an *RRCConnectionRequest* from the UE on the E-UTRAN-cell related to the BCCH transmitting TAI 246/081/0002, the E-USS sends *RRCConnectionSetup* to the UE, followed by *RRCConnectionSetupComplete* sent by the UE to the E-USS.

g) During registration and after receipt of a *TrackingAreaUpdateRequest* from the UE, the E-USS initiates authentication, starts integrity by using the security procedure and sends *TrackingAreaUpdateAccept* with to the UE:

TAI (MCC/MNC/TAC): 246/081/ 0002

GUTI: "24608100010266436599"

h) After receipt of the *TrackingAreaUpdatComplete* during registration from the UE, the E-USS sends *RRCConnectionRelease* to the UE.

i) The UE is soft powered down.

#### 10.1.3.5 Acceptance criteria

1) After step b) the UE shall send an *RRCConnectionRequest* on the E-UTRAN-cell related to the BCCH transmitting TAI 246/081/0001 to the e-USS.

3) During step b) the terminal shall send *AttachRequest* to the E-USS.

4) After step c) the terminal shall respond with *AttachComplete* during registration.

5) During step e) the UE shall provide during the manual CSG selection the information for a cell with csg-Identity 04 for PLMN 246/081 to the user.

6) After step e) the UE shall send an *RRCConnectionRequest* on the E-UTRAN-cell related to the BCCH transmitting TAI 246/081/0002 to the e-USS.

7) During step f) the terminal shall send *TrackingAreaUpdateRequest* to the E-USS.

8) After step g) the terminal shall respond with *TrackingAreaUpdatComplete* during registration.

9) After step i) the USIM shall contain the following values:

**EFEPSLOCI (EPS Information)**

Logically: GUTI: 24608100010266436599

Last visited registered TAI: 246/081/0002

EPS update status: updated

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Coding: | B1 | B2 | B3 | B4 | B5 | B6 | B7 | B8 | B9 | B10 | B11 |
| Hex | 0B | F6 | 42 | 16 | 80 | 00 | 01 | 02 | 66 | 43 | 65 |
|  | B12 | B13 | B14 | B15 | B16 | B17 | B18 |  |  |  |  |
|  | 99 | 42 | 16 | 80 | 00 | 02 | 00 |  |  |  |  |

**EFACSGL (Allowed CSG Lists)**

Logically:

1st CSG list

PLMN: 246 081 (MCC MNC)

1st CSG list 1st CSG Type indication 02

1st CSG list 1st CSG HNB Name indication 02

1st CSG list 1st CSG CSG ID: 02 (27bit)

1st CSG list 2nd CSG Type indication 03

1st CSG list 2nd CSG HNB Name indication 03

1st CSG list 2nd CSG CSG ID: 03 (27bit)

1st CSG list 3rd CSG Type indication 'xx' (not checked)

1st CSG list 3rd CSG HNB Name indication 'xx' (not checked)

1st CSG list 3rd CSG CSG ID: 04 (27bit)

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Coding: | A0 | 1D | 80 | 03 | 42 | 16 | 80 | 81 | 06 | 02 |
|  | 02 | 00 | 00 | 00 | 5F | 81 | 06 | 03 | 03 | 00 |
|  | 00 | 00 | 7F | 81 | 06 | xx | xx | 00 | 00 | 00 |
|  | 9F |  |  |  |  |  |  |  |  |  |

2nd CSG list

PLMN: 244 081 (MCC MNC)

2nd CSG list 1st CSG Type indication 08

2nd CSG list 1st CSG HNB Name indication 08

2nd CSG list 1st CSG CSG ID: 08 (27bit)

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Coding: | A0 | 0D | 80 | 03 | 42 | 14 | 80 | 81 | 06 | 08 |
|  | 08 | 00 | 00 | 01 | 1F |  |  |  |  |  |

Note: The 1st and 2nd CSG list may be stored together or separately in any record in arbitrary order.  
 The CSG entries within each of the CSG lists are not sorted and may occur in arbitrary order.

### 10.1.4 Manual CSG selection in E-UTRA with CSG list on USIM, rejected

#### 10.1.4.1 Definition and applicability

A Closed Subscriber Group identifies subscribers of an operator who are permitted to access one or more cells of the PLMN but which have restricted access (CSG cells). A CSG cell is part of the PLMN, broadcasting a CSG indication that is set to TRUE and a specific CSG identity. A CSG cell is accessible by the members of the closed subscriber group for that CSG identity. For a CSG cell, the UE shall check the broadcast CSG ID against the Allowed CSG list provided by NAS to check whether a CSG cell is suitable for the UE.

A UE supporting CSG selection selects CSG cell either automatically based on the list of allowed CSG identities or manually based on user selection of CSG on indication of list of available CSGs.

#### 10.1.4.2 Conformance requirement

The ME shall read the allowed CSG IDs from EFACSGL in order to perform HNB selection procedures. The lists in EFACSGL shall take precedence over the list stored in the ME non-volatile memory.  
In manual CSG selection mode, the ME indicates to the user the list of available CSGs in the currently selected PLMN. The list of CSGs presented to the user is not restricted by the allowed CSG list.  
If the MS supports CSG, it is provisioned with a list of allowed CSG identities and associated PLMN identities from the USIM if the list is available in the USIM.

If the UE supporting CSG selection has attempted manual CSG selection, the UE, when receiving the TRACKING AREA UPDATE REJECT message with cause #25 (Not authorized for this CSG) with integrity protection, shall remove the CSG ID of the cell where the UE has sent the TRACKING AREA UPDATE REQUEST message if the CSG ID is contained in the Allowed CSG list.

- TS 31.102 [4], clauses 4.4.6.2 and 5.8.1;

- TS 23.122 [31], clause 3.1A.

- TS 24.301 [26], clause 5.5.3.2.5

#### 10.1.4.3 Test purpose

To verify that the ME does not add the CSG ID to the Allowed CSG list in EFACSGL in case this CSG ID belongs to the cell where the ME has sent the TRACKING AREA UPDATE REQUEST message which was rejected by the E-USS.

#### 10.1.4.4 Method of test

##### 10.1.4.4.1 Initial conditions

For this test an E-USS is required.

The E-USS transmits on two cells, with the following network parameters:

- TAI (MCC/MNC/TAC): 246/081/0001.

- Access control: unrestricted.

- csg-Indication: FALSE

- csg-Identity: not present

- TAI (MCC/MNC/TAC): 246/081/0002.

- Access control: unrestricted.

- csg-Indication: TRUE

- csg-Identity: 04

The default E-UTRAN UICC is used.

The UICC is installed into the Terminal and the UE is set to automatic PLMN selection mode.

##### 10.1.4.4.2 Procedure

a) The UE is powered on.

b) After receipt of an *RRCConnectionRequest* from the UE on the E-UTRAN-cell related to the BCCH transmitting TAI 246/081/0001, the E-USS sends *RRCConnectionSetup* to the UE, followed by *RRCConnectionSetupComplete* sent by the UE to the E-USS.

c) During registration and after receipt of a *AttachRequest* from the UE, the E-USS initiates authentication, starts integrity by using the security procedure and sends *AttachAccept* with to the UE:

TAI (MCC/MNC/TAC): 246/081/ 0001

GUTI: "24608100010266345678"

d) After receipt of the *AttachComplete* during registration from the UE, the E-USS sends *RRCConnectionRelease*, to the UE.

e) The MMI of the UE is used to perform manual CSG selection. The UE shall indicate the availability of a cell with csg-Identity 04 for PLMN 246/081. The user shall select this cell by using the MMI.

f) After receipt of an *RRCConnectionRequest* from the UE on the E-UTRAN-cell related to the BCCH transmitting TAI 246/081/0002, the E-USS sends *RRCConnectionSetup* to the UE, followed by *RRCConnectionSetupComplete* sent by the UE to the E-USS.

g) During registration and after receipt of an *TrackingAreaUpdateRequest* from the UE, the E-USS initiates authentication, starts integrity by using the security procedure and sends *TrackingAreaUpdateReject* to the UE with cause #25 (Not authorized for this CSG) with integrity protection, followed by *RRCConnectionRelease* to the UE.

h) The UE is soft powered down.

#### 10.1.4.5 Acceptance criteria

1) After step a) the UE shall send an *RRCConnectionRequest* on the E-UTRAN-cell related to the BCCH transmitting TAI 246/081/0001 to the E-USS.

3) During step b) the terminal shall send *AttachRequest* to the E-USS.

4) After step c) the terminal shall respond with *AttachComplete* during registration.

5.) During step e) the UE shall provide during the manual CSG selection the information for a cell with csg-Identity 04 for PLMN 246/081 to the user.

6) After step e) the UE shall send a RRCConnectionRequest on the E-UTRAN-cell related to the BCCH transmitting TAI 246/081/0002 to the E-USS.

7) During step f) the terminal shall send *TrackingAreaUpdateRequest* to the E-USS.

8) After step h) the USIM shall contain the following values:

**EFEPSLOCI (EPS Information)**

Logically: GUTI: not checked

Last visited registered TAI: 246/081/0001

EPS update status: ROAMING NOT ALLOWED

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Coding: | B1 | B2 | B3 | B4 | B5 | B6 | B7 | B8 | B9 | B10 | B11 |
| Hex | xx | xx | xx | xx | xx | xx | xx | xx | xx | xx | xx |
|  | B12 | B13 | B14 | B15 | B16 | B17 | B18 |  |  |  |  |
|  | xx | 42 | 16 | 80 | 00 | 01 | 02 |  |  |  |  |

**EFACSGL (Allowed CSG Lists)**

Content not changed, shall be the same as defined in clause 4.4.5.

### 10.1.5 CSG selection in E-UTRA with no CSG list on USIM, no IMSI change

#### 10.1.5.1 Definition and applicability

A Closed Subscriber Group identifies subscribers of an operator who are permitted to access one or more cells of the PLMN but which have restricted access (CSG cells). A CSG cell is part of the PLMN, broadcasting a CSG indication that is set to TRUE and a specific CSG identity. A CSG cell is accessible by the members of the closed subscriber group for that CSG identity. For a CSG cell, the UE shall check the broadcast CSG ID against the Allowed CSG list provided by NAS to check whether a CSG cell is suitable for the UE.

A UE supporting CSG selection selects CSG cell either automatically based on the list of allowed CSG identities or manually based on user selection of CSG on indication of list of available CSGs.

#### 10.1.5.2 Conformance requirement

In manual CSG selection mode, the ME indicates to the user the list of available CSGs in the currently selected PLMN. The list of CSGs presented to the user is not restricted by the allowed CSG list.  
If the MS supports CSG, it is provisioned with a list of allowed CSG identities and associated PLMN identities from the USIM if the list is available in the USIM.

If the UE supporting CSG selection has attempted manual CSG selection, the UE, when receiving the TRACKING AREA UPDATE ACCEPT message, shall check if the CSG ID of the cell where the UE has sent the TRACKING AREA UPDATE REQUEST message is contained in the Allowed CSG list. If not, the UE shall add that CSG ID to the Allowed CSG list.

If the corresponding file is not present on the USIM, these EMM parameters except allowed CSG list are stored in a non-volatile memory in the ME together with the IMSI from the USIM. The allowed CSG list is stored in a non-volatile memory in the ME if the UE supports CSG selection. These EMM parameters can only be used if the IMSI from the USIM matches the IMSI stored in the non-volatile memory; else the UE shall delete the EMM parameters.

- TS 31.102 [4], clauses 4.4.6.2 and 5.8.1;

- TS 23.122 [31], clause 3.1A.

- TS 24.301 [26], clause 5.5.3.2.4 and Annex C.

#### 10.1.5.3 Test purpose

To verify that the ME adds the CSG ID to the Allowed CSG list in a non-volatile memory in the ME together with the IMSI from the USIM in case this CSG ID belongs to the cell where the ME has sent the TRACKING AREA UPDATE REQUEST message which was accepted by the E-USS as the corresponding file is not present on the simulated USIM.

To verify that the ME still has this CSG ID stored in the Allowed CSG list available together with the IMSI after powered down and up in case the IMSI of the USIM has not changed.

To verify that the ME removes the CSG ID from the Allowed CSG list inside the terminal in case this CSG ID belongs to the cell where the ME has sent the ATTACH REQUEST message which was rejected with cause #25 by the E-USS.

#### 10.1.5.4 Method of test

##### 10.1.5.4.1 Initial conditions

For this test an E-USS is required.

The E-USS transmits on two cells, with the following network parameters:

- TAI (MCC/MNC/TAC): 246/081/0001.

- Access control: unrestricted.

- csg-Indication: FALSE

- csg-Identity: not present

- TAI (MCC/MNC/TAC): 246/081/0002.

- Access control: unrestricted.

- csg-Indication: TRUE

- csg-Identity: 04

The default UICC (without the service "Allowed CSG Lists and corresponding indications") is installed into the Terminal.

The ME shall not have csg-ID = 04 nor csg-ID=06 in the allowed CSG list stored in a non-volatile memory in the ME and the ME is set to automatic PLMN selection mode.

##### 10.1.5.4.2 Procedure

a) The UE is powered on.

b) After receipt of an *RRCConnectionRequest* from the UE on the E-UTRAN-cell related to the BCCH transmitting TAI 246/081/0001, the E-USS sends *RRCConnectionSetup* to the UE, followed by *RRCConnectionSetupComplete* sent by the UE to the E-USS.

c) During registration and after receipt of an *AttachRequest* from the UE, the E-USS initiates authentication, starts integrity by using the security procedure and sends *AttachAccept* with the following parameters to the UE:

TAI (MCC/MNC/TAC): 246/081/ 0001

GUTI: "24608100010266345678"

d) After receipt of the *AttachComplete* during registration from the UE, the E-USS sends *RRCConnectionRelease* to the UE.

e) The MMI of the UE is used to perform manual CSG selection. The UE shall indicate the availability of a cell with csg-Identity 04 for PLMN 246/081. The user shall select this cell by using the MMI.

f) After receipt of an *RRCConnectionRequest* from the UE on the E-UTRAN-cell related to the BCCH transmitting TAI 246/081/0002, the E-USS sends *RRCConnectionSetup* to the UE, followed by *RRCConnectionSetupComplete* sent by the UE to the E-USS.

g) During registration and after receipt of a *TrackingAreaUpdateRequest* from the UE, the E-USS initiates authentication, starts integrity by using the security procedure and sends *TrackingAreaUpdateAccept* with the following parameters to the UE:

TAI (MCC/MNC/TAC): 246/081/TACs: 0002

GUTI: "24608100010266345699"

h) After receipt of the *TrackingAreaUpdateComplete* during registration from the UE, the E-USS sends *RRCConnectionRelease* to the UE.

i) The UE is switched off and performs the *Detach* procedure.

j) The default UICC remains in use.

k) The E-USS shall change the BCCH for the cell transmitting TAI 246/081/0001 to the following network parameters:

- csg-Indication: TRUE

- csg-Identity: 06

l) The UE is powered on.

m) After receipt of an *RRCConnectionRequest* from the UE on the E-UTRAN-cell related to the BCCH transmitting TAI 246/081/0002, the E-USS sends *RRCConnectionSetup* to the UE, followed by *RRCConnectionSetupComplete* sent by the UE to the E-USS.

n) During registration and after receipt of an *AttachRequest* from the UE, the E-USS initiates authentication, starts integrity by using the security procedure and sends *AttachReject* to the UE with cause #25 (Not authorized for this CSG) with integrity protection, followed by *RRCConnectionRelease.*

o) The UE is soft powered down.

p) The default UICC remains in use.

q) The UE is powered on.

r) After 2 minutes the UE is soft powered down.

#### 10.1.5.5 Acceptance criteria

1) After step a) the UE shall send an *RRCConnectionRequest* on the E-UTRAN-cell related to the BCCH transmitting TAI 246/081/0001 to the E-USS.

3) During step b) the terminal shall send *AttachRequest* to the E-USS.

4) After step c) the terminal shall respond with *AttachComplete* during registration.

5) During step e) the UE shall provide during the manual CSG selection the information for a cell with csg-Identity 04 for PLMN 246/081 to the user.

6) After step e) the UE shall send an *RRCConnectionRequest* on the E-UTRAN-cell related to the BCCH transmitting TAI 246/081/0002 to the E-USS.

7) During step f) the terminal shall send *TrackingAreaUpdateRequest* to the E-USS.

8) After step g) the terminal shall respond with *TrackingAreaUpdateComplete* during registration.

9) After step l) the UE shall send an *RRCConnectionRequest* on the E-UTRAN-cell related to the BCCH transmitting TAI 246/081/0002 to the E-USS.

10) During step n) the terminal shall send *AttachRequest* to the E-USS.

10a) After step n) the terminal shall not try to register to the E-USS using the same CSG ID which was rejected in step n).

11) After step q) the terminal shall not try to register to the E-USS using the same CSG ID which was rejected in step n).

### 10.1.6 CSG selection in E-UTRA with no CSG list on USIM, with IMSI change

#### 10.1.6.1 Definition and applicability

A Closed Subscriber Group identifies subscribers of an operator who are permitted to access one or more cells of the PLMN but which have restricted access (CSG cells). A CSG cell is part of the PLMN, broadcasting a CSG indication that is set to TRUE and a specific CSG identity. A CSG cell is accessible by the members of the closed subscriber group for that CSG identity. For a CSG cell, the UE shall check the broadcast CSG ID against the Allowed CSG list provided by NAS to check whether a CSG cell is suitable for the UE.

A UE supporting CSG selection selects CSG cell either automatically based on the list of allowed CSG identities or manually based on user selection of CSG on indication of list of available CSGs.

#### 10.1.6.2 Conformance requirement

In manual CSG selection mode, the ME indicates to the user the list of available CSGs in the currently selected PLMN. The list of CSGs presented to the user is not restricted by the allowed CSG list..  
If the MS supports CSG, it is provisioned with a list of allowed CSG identities and associated PLMN identities from the USIM if the list is available in the USIM.

If the UE supporting CSG selection has attempted manual CSG selection, the UE, when receiving the TRACKING AREA UPDATE ACCEPT message, shall check if the CSG ID of the cell where the UE has sent the TRACKING AREA UPDATE REQUEST message is contained in the Allowed CSG list. If not, the UE shall add that CSG ID to the Allowed CSG list.

If the corresponding file is not present on the USIM, these EMM parameters except allowed CSG list are stored in a non-volatile memory in the ME together with the IMSI from the USIM. The allowed CSG list is stored in a non-volatile memory in the ME if the UE supports CSG selection. These EMM parameters can only be used if the IMSI from the USIM matches the IMSI stored in the non-volatile memory; else the UE shall delete the EMM parameters.

- TS 31.102 [4], clauses 4.4.6.2 and 5.8.1;

- TS 23.122 [31], clause 3.1A.

- TS 24.301 [26], clause 5.5.3.2.4 and Annex C.

#### 10.1.6.3 Test purpose

To verify that the ME adds the CSG ID to the Allowed CSG list in a non-volatile memory in the ME together with the IMSI from the USIM in case this CSG ID belongs to the cell where the ME has sent the TRACKING AREA UPDATE REQUEST message which was accepted by the E-USS as the corresponding file is not present on the simulated USIM.

To verify that the ME removes this CSG ID stored in the Allowed CSG list available together with the IMSI after powered down and up in case the IMSI of the USIM has changed.

#### 10.1.6.4 Method of test

##### 10.1.6.4.1 Initial conditions

For this test an E-USS is required.

The E-USS transmits on two cells, with the following network parameters:

- TAI (MCC/MNC/TAC): 246/081/0001.

- Access control: unrestricted.

- csg-Indication: FALSE

- csg-Identity: not present

- TAI (MCC/MNC/TAC): 246/081/0002.

- Access control: unrestricted.

- csg-Indication: TRUE

- csg-Identity: 04

The default UICC (without the service "Allowed CSG Lists and corresponding indications") is installed into the Terminal.

The ME shall not have csg-ID = 04 nor csg-ID=06 in the allowed CSG list stored in a non-volatile memory in the ME and the ME is set to automatic PLMN selection mode.

##### 10.1.6.4.2 Procedure

a) The UE is powered on.

b) After receipt of an *RRCConnectionRequest* from the UE on the E-UTRAN-cell related to the BCCH transmitting TAI 246/081/0001, the E-USS sends *RRCConnectionSetup* to the UE, followed by *RRCConnectionSetupComplete* sent by the UE to the E-USS.

c) During registration and after receipt of an *AttachRequest* from the UE, the E-USS initiates authentication, starts integrity by using the security procedure and sends *AttachAccept* with to the following parameters the UE:

TAI (MCC/MNC/TAC): 246/081/ 0001

GUTI: "24608100010266345678"

d) After receipt of the *AttachComplete* during registration from the UE, the E-USS sends *RRCConnectionRelease* to the UE.

e) The MMI of the UE is used to perform manual CSG selection. The UE shall indicate the availability of a cell with csg-Identity 04 for PLMN 246/081. The user shall select this cell by using the MMI.

f) After receipt of an *RRCConnectionRequest* from the UE on the E-UTRAN-cell related to the BCCH transmitting TAI 246/081/0002, the E-USS sends *RRCConnectionSetup* to the UE, followed by *RRCConnectionSetupComplete* sent by the UE to the E-USS.

g) During registration and after receipt of a *TrackingAreaUpdateRequest* from the UE, the E-USS may initiate authentication, may start integrity by using the security procedure and sends *TrackingAreaUpdateAccept* with the following parameters to the UE:

TAI (MCC/MNC/TAC): 246/081/ 0002

GUTI: "24608100010266345699"

h) After receipt of the *TrackingAreaUpdateComplete* during registration from the UE, the E-USS sends *RRCConnectionRelease* to the UE.

i) The UE is switched off and performs the *Detach* procedure.

j) A new UICC with the following configuration is activated:

The default UICC with the following exception: The IMSI is set to "246081222233333".

k) The E-USS shall change the BCCH for the cell transmitting TAI 246/081/0001 to the following network parameters:

- csg-Indication: TRUE

- csg-Identity: 06

l) The UE is powered on.

m) After 2 minutes the UE is soft powered down.

#### 10.1.6.5 Acceptance criteria

1) After step b) the UE shall send an *RRCConnectionRequest* on the E-UTRAN-cell related to the BCCH transmitting TAI 246/081/0001 to the e-USS.

3) During step b) the terminal shall send *AttachRequest* to the E-USS.

4) After step c) the terminal shall respond with *AttachComplete* during registration.

5) During step e) the UE shall provide during the manual CSG selection the information for a cell with csg-Identity 04 for PLMN 246/081 to the user.

6) After step e) the UE shall send an *RRCConnectionRequest* on the E-UTRAN-cell related to the BCCH transmitting TAI 246/081/0002 to the e-USS.

7) During step f) the terminal shall send *TrackingAreaUpdateRequest* to the E-USS.

8) After step g) the terminal shall respond with *TrackingAreaUpdateComplete* during registration.

9) After step l) the terminal shall not try to register to the E-USS.

### 10.1.7 Manual CSG selection without display restrictions in E-UTRA with ACSG list and OCSG list on USIM

#### 10.1.7.1 Definition and applicability

A Closed Subscriber Group identifies subscribers of an operator who are permitted to access one or more cells of the PLMN but which have restricted access (CSG cells). A CSG cell is part of the PLMN, broadcasting a CSG indication that is set to TRUE and a specific CSG identity. A CSG cell is accessible by the members of the closed subscriber group for that CSG identity. For a CSG cell, the UE shall check the broadcast CSG ID against the Allowed CSG list provided by NAS to check whether a CSG cell is suitable for the UE.

A UE supporting CSG selection selects a CSG cell either automatically based on the list of allowed CSG identities or manually based on user selection of CSG on indication of list of available CSGs.

*Editor's note: it is still being investigated whether the testing of Automatic CSG selection should be performed using a separate test case or an enhanced version of the Manual CSG selection test case.*

#### 10.1.7.2 Conformance requirement

The ME shall read the allowed CSG IDs from EFACSGL and EFOCSGL in order to perform HNB selection procedures. The lists in EFACSGL and EFOCSGL shall take precedence over the list stored in the ME non-volatile memory.  
  
If the MS supports CSG, it is provisioned with a list of allowed CSG identities and associated PLMN identities from the USIM if the list is available in the USIM.

If the UE supporting CSG selection has attempted manual CSG selection, the UE, when receiving the TRACKING AREA UPDATE ACCEPT message, shall check if the CSG ID of the cell where the UE has sent the TRACKING AREA UPDATE REQUEST message is contained in the Allowed CSG list. If not, the UE shall add that CSG ID to the Allowed CSG list EFACSGL.

By default, the UE shall display all available CSGs for any PLMN, unless the UE has been configured by the HPLMN,  
for a specific PLMN, to display only CSGs in the Operator CSG List that are available.

- TS 31.102 [4], clauses 4.2.18, 4.4.6.2, 4.4.6.5 and 5.8.1;

- TS 24.301 [26], clause 5.5.3.2.4

- TS 22.220 [34], clause 5.3.2 and 5.5.4

#### 10.1.7.3 Test purpose

To verify that the ME adds the CSG ID to the Allowed CSG list in EFACSGL in case this CSG ID belongs to the cell where the ME has sent the TRACKING AREA UPDATE REQUEST message which was accepted by the E-USS.  
During the manual CSG selection all available CSG ID shall be displayed without restrictions.

#### 10.1.7.4 Method of test

##### 10.1.7.4.1 Initial conditions

For this test an E-USS is required.

The E-USS transmits on two cells, with the following network parameters:

- TAI (MCC/MNC/TAC): 246/081/0001.

- Access control: unrestricted.

- csg-Indication: FALSE

- csg-Identity: not present

- TAI (MCC/MNC/TAC): 246/081/0002.

- Access control: unrestricted.

- csg-Indication: TRUE

- csg-Identity: 04

The default ACSGL/OCSGL E-UTRAN/EPC UICC is used.

The UICC is installed into the Terminal and the UE is set to automatic PLMN selection and manual CSG selection mode.

##### 10.1.7.4.2 Procedure

a) The UE is powered on.

b) After receipt of an *RRCConnectionRequest* from the UE on the E-UTRAN-cell related to the BCCH transmitting TAI 246/081/0001, the E-USS sends *RRCConnectionSetup* to the UE, followed by *RRCConnectionSetupComplete* sent by the UE to the E-USS.

c) During registration and after receipt of an *AttachRequest* from the UE, the E-USS initiates authentication, starts integrity by using the security procedure and sends *AttachAccept* with to the UE:

TAI (MCC/MNC/TAC): 246/081/ 0001

GUTI: "24608100010266345678"

d) After receipt of the *AttachComplete* during registration from the UE, the E-USS sends *RRCConnectionRelease*  to the UE.

e) The MMI of the UE is used to perform manual CSG selection. The UE shall indicate the availability of a cell with csg-Identity 04 for PLMN 246/081. The user shall select this cell by using the MMI.

f) After receipt of an *RRCConnectionRequest* from the UE on the E-UTRAN-cell related to the BCCH transmitting TAI 246/081/0002, the E-USS sends *RRCConnectionSetup* to the UE, followed by *RRCConnectionSetupComplete* sent by the UE to the E-USS.

g) During registration and after receipt of a *TrackingAreaUpdateRequest* from the UE, the E-USS initiates authentication, starts integrity by using the security procedure and sends *TrackingAreaUpdateAccept* with to the UE:

TAI (MCC/MNC/TAC): 246/081/ 0002

GUTI: "24608100010266436599"

h) After receipt of the *TrackingAreaUpdatComplete* during registration from the UE, the E-USS sends *RRCConnectionRelease* to the UE.

i) The UE is soft powered down.

#### 10.1.7.5 Acceptance criteria

1) After step b) the UE shall send an *RRCConnectionRequest* on the E-UTRAN-cell related to the BCCH transmitting TAI 246/081/0001 to the e-USS.

3) During step b) the terminal shall send *AttachRequest* to the E-USS.

4) After step c) the terminal shall respond with *AttachComplete* during registration.

5) During step e) the UE shall provide during the manual CSG selection the information for a cell with csg-Identity 04 for PLMN 246/081 to the user.

6) After step e) the UE shall send an *RRCConnectionRequest* on the E-UTRAN-cell related to the BCCH transmitting TAI 246/081/0002 to the E-USS.

7) During step f) the terminal shall send *TrackingAreaUpdateRequest* to the E-USS.

8) After step g) the terminal shall respond with *TrackingAreaUpdatComplete* during registration.

9) After step i) the USIM shall contain the following values:

**EFEPSLOCI (EPS Information)**

Logically: GUTI: 24608100010266436599

Last visited registered TAI: 246/081/0002

EPS update status: updated

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Coding: | B1 | B2 | B3 | B4 | B5 | B6 | B7 | B8 | B9 | B10 | B11 |
| Hex | 0B | F6 | 42 | 16 | 80 | 00 | 01 | 02 | 66 | 43 | 65 |
|  | B12 | B13 | B14 | B15 | B16 | B17 | B18 |  |  |  |  |
|  | 99 | 42 | 16 | 80 | 00 | 02 | 00 |  |  |  |  |

**EFACSGL (Allowed CSG Lists)**

Logically:

1st CSG list

PLMN: 246 081 (MCC MNC)

1st CSG list 1st CSG Type indication 02

1st CSG list 1st CSG HNB Name indication 02

1st CSG list 1st CSG CSG ID: 02 (27bit)

1st CSG list 2nd CSG Type indication 03

1st CSG list 2nd CSG HNB Name indication 03

1st CSG list 2nd CSG CSG ID: 03 (27bit)

1st CSG list 3rd CSG Type indication 'xx' (not checked)

1st CSG list 3rd CSG HNB Name indication 'xx' (not checked)

1st CSG list 3rd CSG CSG ID: 04 (27bit)

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Coding: | A0 | 1D | 80 | 03 | 42 | 16 | 80 | 81 | 06 | 02 |
|  | 02 | 00 | 00 | 00 | 5F | 81 | 06 | 03 | 03 | 00 |
|  | 00 | 00 | 7F | 81 | 06 | xx | xx | 00 | 00 | 00 |
|  | 9F |  |  |  |  |  |  |  |  |  |

2nd CSG list

PLMN: 244 081 (MCC MNC)

2nd CSG list 1st CSG Type indication 08

2nd CSG list 1st CSG HNB Name indication 08

2nd CSG list 1st CSG CSG ID: 08 (27bit)

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Coding: | A0 | 0D | 80 | 03 | 42 | 14 | 80 | 81 | 06 | 08 |
|  | 08 | 00 | 00 | 01 | 1F |  |  |  |  |  |

Note: The 1st and 2nd CSG list may be stored together or separately in any record in arbitrary order.

**EFOCSGL (Operator CSG Lists)**

Unchanged values as defined in 4.6.3

### 10.1.8 Manual CSG selection with display restrictions in E-UTRA with ACSG list and OCSG list on USIM

#### 10.1.8.1 Definition and applicability

A Closed Subscriber Group identifies subscribers of an operator who are permitted to access one or more cells of the PLMN but which have restricted access (CSG cells). A CSG cell is part of the PLMN, broadcasting a CSG indication that is set to TRUE and a specific CSG identity. A CSG cell is accessible by the members of the closed subscriber group for that CSG identity. For a CSG cell, the UE shall check the broadcast CSG ID against the Allowed CSG list provided by NAS to check whether a CSG cell is suitable for the UE.

A UE supporting CSG selection selects a CSG cell either automatically based on the list of allowed CSG identities or manually based on user selection of CSG on indication of list of available CSGs.

#### 10.1.8.2 Conformance requirement

The ME shall read the allowed CSG IDs from EFACSGL and EFOCSGL in order to perform HNB selection procedures. The lists in EFACSGL and EFOCSGL shall take precedence over the list stored in the ME non-volatile memory.  
  
If the MS supports CSG, it is provisioned with a list of allowed CSG identities and associated PLMN identities from the USIM if the list is available in the USIM.

If the UE supporting CSG selection has attempted manual CSG selection, the UE, when receiving the TRACKING AREA UPDATE ACCEPT message, shall check if the CSG ID of the cell where the UE has sent the TRACKING AREA UPDATE REQUEST message is contained in the Allowed CSG list. If not, the UE shall add that CSG ID to the Allowed CSG list EFACSGL.

By default, the UE shall display all available CSGs for any PLMN, unless the UE has been configured by the HPLMN,  
for a specific PLMN, to display only CSGs in the Operator CSG List that are available.

- TS 31.102 [4], clauses 4.2.18, 4.4.6.2, 4.4.6.5 and 5.8.1;

- TS 24.301 [26], clause 5.5.3.2.4

- TS 22.220 [34], clause 5.3.2 and 5.5.4

#### 10.1.8.3 Test purpose

To verify that the ME adds the CSG ID to the Allowed CSG list in EFACSGL in case this CSG ID belongs to the cell where the ME has sent the TRACKING AREA UPDATE REQUEST message which was accepted by the E-USS.  
During the manual CSG selection all available CSG ID shall be displayed with restrictions.

#### 10.1.8.4 Method of test

##### 10.1.8.4.1 Initial conditions

For this test an E-USS is required.

The E-USS transmits on two cells, with the following network parameters:

- TAI (MCC/MNC/TAC): 246/081/0001.

- Access control: unrestricted.

- csg-Indication: FALSE

- csg-Identity: not present

- TAI (MCC/MNC/TAC): 246/080/0002.

- Access control: unrestricted.

- csg-Indication: TRUE

- csg-Identity: 04

The default ACSGL/OCSGL E-UTRAN/EPC UICC is used except the following change:

**EFAD (Administrative Data)**

Logically: Normal operation + specific facilities

Ciphering indicator feature disabled

MNC: 3 digit  
For every PLMN not included in EF\_OCSGL or any PLMN for which a CSG display indicator tag is not present, only the available CSGs found in the Operator CSG list shall be displayed (B3)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Coding: | B1 | B2 | B3 | B4 |
| Hex | 01 | 00 | 02 | 03 |

The UICC is installed into the Terminal and the UE is set to automatic PLMN selection and manual CSG selection mode.

##### 10.1.8.4.2 Procedure

a) The UE is powered on.

b) After receipt of an *RRCConnectionRequest* from the UE on the E-UTRAN-cell related to the BCCH transmitting TAI 246/081/0001, the E-USS sends *RRCConnectionSetup* to the UE, followed by *RRCConnectionSetupComplete* sent by the UE to the E-USS.

c) During registration and after receipt of an *AttachRequest* from the UE, the E-USS initiates authentication, starts integrity by using the security procedure and sends *AttachAccept* with to the UE:

TAI (MCC/MNC/TAC): 246/081/ 0001

GUTI: "24608100010266345678"

d) After receipt of the *AttachComplete* during registration from the UE, the E-USS sends *RRCConnectionRelease*  to the UE.

e) The MMI of the UE is used to perform manual CSG selection. The UE shall not indicate the availability of a cell with csg-Identity 04 for PLMN 246/080, this shall be verified for 2 minutes.

f) The E-USS stops all RF output for the first cell with TAI 246/081/0001 on the BCCH. The BCCH is changed to contain:

- TAI (MCC/MNC/TAC): 246/081/0002

- csg-Indication: TRUE

- csg-Identity: 04

The E-USS then resumes RF output on the BCCH.

g) The MMI of the UE is used to perform manual CSG selection. The UE shall indicate the availability of a cell with csg-Identity 04 for PLMN 246/081. The user shall select this cell by using the MMI.

h) After receipt of an *RRCConnectionRequest* from the UE on the E-UTRAN-cell related to the BCCH transmitting TAI 246/081/0002, the E-USS sends *RRCConnectionSetup* to the UE, followed by *RRCConnectionSetupComplete* sent by the UE to the E-USS.

i) During registration and after receipt of a *TrackingAreaUpdateRequest* from the UE, the E-USS initiates authentication, starts integrity by using the security procedure and sends *TrackingAreaUpdateAccept* with to the UE:

TAI (MCC/MNC/TAC): 246/081/ 0002

GUTI: "24608100010266436599"

j) After receipt of the *TrackingAreaUpdatComplete* during registration from the UE, the E-USS sends *RRCConnectionRelease* to the UE.

k) The UE is soft powered down.

#### 10.1.8.5 Acceptance criteria

1) After step b) the UE shall send an *RRCConnectionRequest* on the E-UTRAN-cell related to the BCCH transmitting TAI 246/081/0001 to the E-USS.

2) During step b) the terminal shall send *AttachRequest* to the E-USS.

3) After step c) the terminal shall respond with *AttachComplete* during registration.

4) During step e) the UE shall not provide during the manual CSG selection the information for a cell with csg-Identity 04 for PLMN 246/080 to the user.

5) During step g) the UE shall provide during the manual CSG selection the information for a cell with csg-Identity 04 for PLMN 246/081 to the user.

6) After step h) the UE shall send an *RRCConnectionRequest* on the E-UTRAN-cell related to the BCCH transmitting TAI 246/081/0002 to the E-USS.

7) During step i) the terminal shall send *TrackingAreaUpdateRequest* to the E-USS.

8) After step j) the terminal shall respond with *TrackingAreaUpdatComplete* during registration.

9) After step k) the USIM shall contain the following values:

**EFEPSLOCI (EPS Information)**

Logically: GUTI: 24608100010266436599

Last visited registered TAI: 246/081/0002

EPS update status: updated

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Coding: | B1 | B2 | B3 | B4 | B5 | B6 | B7 | B8 | B9 | B10 | B11 |
| Hex | 0B | F6 | 42 | 16 | 80 | 00 | 01 | 02 | 66 | 43 | 65 |
|  | B12 | B13 | B14 | B15 | B16 | B17 | B18 |  |  |  |  |
|  | 99 | 42 | 16 | 80 | 00 | 02 | 00 |  |  |  |  |

**EFACSGL (Allowed CSG Lists)**

Logically:

1st CSG list

PLMN: 246 081 (MCC MNC)

1st CSG list 1st CSG Type indication 02

1st CSG list 1st CSG HNB Name indication 02

1st CSG list 1st CSG CSG ID: 02 (27bit)

1st CSG list 2nd CSG Type indication 03

1st CSG list 2nd CSG HNB Name indication 03

1st CSG list 2nd CSG CSG ID: 03 (27bit)

1st CSG list 3rd CSG Type indication 'xx' (not checked)

1st CSG list 3rd CSG HNB Name indication 'xx' (not checked)

1st CSG list 3rd CSG CSG ID: 04 (27bit)

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Coding: | A0 | 1D | 80 | 03 | 42 | 16 | 80 | 81 | 06 | 02 |
|  | 02 | 00 | 00 | 00 | 5F | 81 | 06 | 03 | 03 | 00 |
|  | 00 | 00 | 7F | 81 | 06 | xx | xx | 00 | 00 | 00 |
|  | 9F |  |  |  |  |  |  |  |  |  |

2nd CSG list

PLMN: 244 081 (MCC MNC)

2nd CSG list 1st CSG Type indication 08

2nd CSG list 1st CSG HNB Name indication 08

2nd CSG list 1st CSG CSG ID: 08 (27bit)

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Coding: | A0 | 0D | 80 | 03 | 42 | 14 | 80 | 81 | 06 | 08 |
|  | 08 | 00 | 00 | 01 | 1F |  |  |  |  |  |

Note: The 1st and 2nd CSG list may be stored together or separately in any record in arbitrary order.

**EFOCSGL (Operator CSG Lists)**

Unchanged values as defined in 4.6.3

## 10.2 CSG list handling for UTRA

### 10.2.1 Manual CSG selection without display restrictions in UTRA with ACSG list and OCSG list on USIM

#### 10.2.1.1 Definition and applicability

A Closed Subscriber Group identifies subscribers of an operator who are permitted to access one or more cells of the PLMN but which have restricted access (CSG cells). A CSG cell is part of the PLMN, broadcasting a CSG indication that is set to TRUE and a specific CSG identity. A CSG cell is accessible by the members of the closed subscriber group for that CSG identity. For a CSG cell, the UE shall check the broadcast CSG ID against the Allowed CSG list provided by NAS to check whether a CSG cell is suitable for the UE.

A UE supporting CSG selection selects a CSG cell either automatically based on the list of allowed CSG identities or manually based on user selection of CSG on indication of list of available CSGs.

*Editor's note: it is still being investigated whether the testing of Automatic CSG selection should be performed using a separate test case or an enhanced version of the Manual CSG selection test case.*

#### 10.2.1.2 Conformance requirement

The ME shall read the allowed CSG IDs from EFACSGL and EFOCSGL in order to perform HNB selection procedures. The lists in EFACSGL and EFOCSGL shall take precedence over the list stored in the ME non-volatile memory.  
  
If the MS supports CSG, it is provisioned with a list of allowed CSG identities and associated PLMN identities from the USIM if the list is available in the USIM.

If the UE supporting CSG selection has attempted manual CSG selection, the UE, when receiving the ROUTING AREA UPDATE ACCEPT message, shall check if the CSG ID of the cell where the UE has sent the ROUTING AREA UPDATE REQUEST message is contained in the Allowed CSG list. If not, the UE shall add that CSG ID to the Allowed CSG list EFACSGL.

By default, the UE shall display all available CSGs for any PLMN, unless the UE has been configured by the HPLMN,  
for a specific PLMN, to display only CSGs in the Operator CSG List that are available.

- TS 31.102 [4], clauses 4.2.18, 4.4.6.2, 4.4.6.5 and 5.8.1;

- TS 23.122 [31], clause 3.1A.

- TS 22.220 [34], clause 5.3.2 and 5.5.4

#### 10.2.1.3 Test purpose

To verify that the ME adds the CSG ID to the Allowed CSG list in EFACSGL in case this CSG ID belongs to the cell where the ME has sent the ROUTING AREA UPDATE REQUEST message which was accepted by the USS.  
During the manual CSG selection all available CSG ID shall be displayed without restrictions.

#### 10.2.1.4 Method of test

##### 10.2.1.4.1 Initial conditions

For this test an USS is required.

The USS transmits on two cells, with the following network parameters:

- RAI (MCC/MNC/LAC/RAC): 246/081/0001/01.

- Access control: unrestricted.

- csg-Indication: FALSE

- csg-Identity: not present

- RAI (MCC/MNC/LAC/RAC): 246/081/0002/02.

- Access control: unrestricted.

- csg-Indication: TRUE

- csg-Identity: 04

The default ACSGL/OCSGL E-UTRAN/EPC UICC is used.

The UICC is installed into the Terminal and the UE is set to automatic PLMN selection and manual CSG selection mode.

##### 10.2.1.4.2 Procedure

a) The UE is powered on.

b) After receipt of an *RRCConnectionRequest* from the UE on the UTRAN-cell related to the BCCH transmitting RAI 246/081/0001/01, the USS sends *RRCConnectionSetup* to the UE, followed by *RRCConnectionSetupComplete* sent by the UE to the USS.

c) During registration and after receipt of an *AttachRequest* from the UE, the USS initiates authentication, starts integrity by using the security procedure and sends *AttachAccept* to the UE:

RAI (MCC/MNC/LAC/RAC): 246/081/0001/01

P-TMSI "87512890"

d) After receipt of the *AttachComplete* during registration from the UE, the USS sends *RRCConnectionRelease* to the UE.

e) The MMI of the UE is used to perform manual CSG selection. The UE shall indicate the availability of a cell with csg-Identity 04 for PLMN 246/081. The user shall select this cell by using the MMI.

f) After receipt of an *RRCConnectionRequest* from the UE on the UTRAN-cell related to the BCCH transmitting RAI 246/081/0002/02, the USS sends *RRCConnectionSetup* to the UE, followed by *RRCConnectionSetupComplete* sent by the UE to the USS.

g) During registration and after receipt of a *RoutingAreaUpdateRequest* from the UE, the USS initiates authentication, starts integrity by using the security procedure and sends *RoutingAreaUpdateAccept* to the UE:

RAI (MCC/MNC/LAC/RAC): 246/081/0002/02

P-TMSI "34567890"

h) After receipt of the *RoutingAreaUpdateComplete* during registration from the UE, the USS sends *RRCConnectionRelease* to the UE.

i) The UE is soft powered down.

#### 10.2.1.5 Acceptance criteria

1) After step b) the UE shall send an *RRCConnectionRequest* on the UTRAN-cell related to the BCCH transmitting RAI 246/081/0001/01 to the USS.

3) During step c) the UE shall send *AttachRequest* to the USS.

4) After step c) the UE shall respond with *AttachComplete* during registration.

5) During step e) the UE shall provide during the manual CSG selection the information for a cell with csg-Identity 04 for PLMN 246/081 to the user.

6) After step e) the UE shall send an *RRCConnectionRequest* on the UTRAN-cell related to the BCCH transmitting RAI 246/081/0002/02 to the USS.

7) During step g) the UE shall send *RoutingAreaUpdateRequest* to the USS.

8) After step g) the UE shall respond with *RoutingAreaUpdateComplete* during registration.

9) After step i) the USIM shall contain the following values:

**EFPSLOCI (Location Information)**

Logically: RAI-MCC: 246

RAI-MNC: 081

RAI-LAC: 0002

RAI-RAC: 02

P-TMSI: "34567890"

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Coding: | B1 | B2 | B3 | B4 | B5 | B6 | B7 | B8 | B9 | B10 | B11 |
| Hex | 34 | 56 | 78 | 90 | xx | xx | xx | 42 | 16 | 80 | 00 |
|  |  |  |  |  |  |  |  |  |  |  |  |
| Coding: | B12 | B13 | B14 |  |  |  |  |  |  |  |  |
| Hex | 02 | 02 | 00 |  |  |  |  |  |  |  |  |

**EFACSGL (Allowed CSG Lists)**

Logically:

1st CSG list

PLMN: 246 081 (MCC MNC)

1st CSG list 1st CSG Type indication 02

1st CSG list 1st CSG HNB Name indication 02

1st CSG list 1st CSG CSG ID: 02 (27bit)

1st CSG list 2nd CSG Type indication 03

1st CSG list 2nd CSG HNB Name indication 03

1st CSG list 2nd CSG CSG ID: 03 (27bit)

1st CSG list 3rd CSG Type indication 'xx' (not checked)

1st CSG list 3rd CSG HNB Name indication 'xx' (not checked)

1st CSG list 3rd CSG CSG ID: 04 (27bit)

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Coding: | A0 | 1D | 80 | 03 | 42 | 16 | 80 | 81 | 06 | 02 |
|  | 02 | 00 | 00 | 00 | 5F | 81 | 06 | 03 | 03 | 00 |
|  | 00 | 00 | 7F | 81 | 06 | xx | xx | 00 | 00 | 00 |
|  | 9F |  |  |  |  |  |  |  |  |  |

2nd CSG list

PLMN: 244 081 (MCC MNC)

2nd CSG list 1st CSG Type indication 08

2nd CSG list 1st CSG HNB Name indication 08

2nd CSG list 1st CSG CSG ID: 08 (27bit)

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Coding: | A0 | 0D | 80 | 03 | 42 | 14 | 80 | 81 | 06 | 08 |
|  | 08 | 00 | 00 | 01 | 1F |  |  |  |  |  |

Note: The 1st and 2nd CSG list may be stored together or separately in any record in arbitrary order.

**EFOCSGL (Operator CSG Lists)**

Unchanged values as defined in 4.6.3

### 10.2.2 Manual CSG selection with display restrictions in UTRA with ACSG list and OCSG list on USIM

#### 10.2.2.1 Definition and applicability

A Closed Subscriber Group identifies subscribers of an operator who are permitted to access one or more cells of the PLMN but which have restricted access (CSG cells). A CSG cell is part of the PLMN, broadcasting a CSG indication that is set to TRUE and a specific CSG identity. A CSG cell is accessible by the members of the closed subscriber group for that CSG identity. For a CSG cell, the UE shall check the broadcast CSG ID against the Allowed CSG list provided by NAS to check whether a CSG cell is suitable for the UE.

A UE supporting CSG selection selects a CSG cell either automatically based on the list of allowed CSG identities or manually based on user selection of CSG on indication of list of available CSGs.

#### 10.2.2.2 Conformance requirement

The ME shall read the allowed CSG IDs from EFACSGL and EFOCSGL in order to perform HNB selection procedures. The lists in EFACSGL and EFOCSGL shall take precedence over the list stored in the ME non-volatile memory.  
  
If the MS supports CSG, it is provisioned with a list of allowed CSG identities and associated PLMN identities from the USIM if the list is available in the USIM.

If the UE supporting CSG selection has attempted manual CSG selection, the UE, when receiving the ROUTING AREA UPDATE ACCEPT message, shall check if the CSG ID of the cell where the UE has sent the ROUTING AREA UPDATE REQUEST message is contained in the Allowed CSG list. If not, the UE shall add that CSG ID to the Allowed CSG list EFACSGL.

By default, the UE shall display all available CSGs for any PLMN, unless the UE has been configured by the HPLMN,  
for a specific PLMN, to display only CSGs in the Operator CSG List that are available.

- TS 31.102 [4], clauses 4.2.18, 4.4.6.2, 4.4.6.5 and 5.8.1;

- TS 23.122 [31], clause 3.1A.

- TS 22.220 [34], clause 5.3.2 and 5.5.4

#### 10.2.2.3 Test purpose

To verify that the ME adds the CSG ID to the Allowed CSG list in EFACSGL in case this CSG ID belongs to the cell where the ME has sent the ROUTING AREA UPDATE REQUEST message which was accepted by the USS.  
During the manual CSG selection all available CSG ID shall be displayed with restrictions.

#### 10.2.2.4 Method of test

##### 10.2.2.4.1 Initial conditions

For this test an USS is required.

The USS transmits on two cells, with the following network parameters:

- RAI (MCC/MNC/LAC/RAC): 246/081/0001/01.

- Access control: unrestricted.

- csg-Indication: FALSE

- csg-Identity: not present

- RAI (MCC/MNC/LAC/RAC): 246/080/0002/02.

- Access control: unrestricted.

- csg-Indication: TRUE

- csg-Identity: 04

The default ACSGL/OCSGL E-UTRAN/EPC UICC is used except the following change:

**EF**AD **(Administrative Data)**

Logically: Normal operation + specific facilities

Ciphering indicator feature disabled

MNC: 3 digit  
For every PLMN not included in EF\_OCSGL or any PLMN for which a CSG display indicator tag is not present, only the available CSGs found in the Operator CSG list shall be displayed (B3)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Coding: | B1 | B2 | B3 | B4 |
| Hex | 01 | 00 | 02 | 03 |

.

The UICC is installed into the Terminal and the UE is set to automatic PLMN selection and manual CSG selection mode.

##### 10.2.2.4.2 Procedure

a) The UE is powered on.

b) After receipt of an *RRCConnectionRequest* from the UE on the UTRAN-cell related to the BCCH transmitting RAI 246/081/0001/01, the USS sends *RRCConnectionSetup* to the UE, followed by *RRCConnectionSetupComplete* sent by the UE to the USS.

c) During registration and after receipt of an *AttachRequest* from the UE, the USS initiates authentication, starts integrity by using the security procedure and sends *AttachAccept* with to the UE:

RAI (MCC/MNC/LAC/RAC): 246/081/0001/01

P-TMSI "87512890"

d) After receipt of the *AttachComplete* during registration from the UE, the USS sends *RRCConnectionRelease*  to the UE.

e) The MMI of the UE is used to perform manual CSG selection. The UE shall not indicate the availability of a cell with csg-Identity 04 for PLMN 246/080, this shall be verified for 2 minutes.

f) The USS stops all RF output for the first cell with RAI 246/081/0001/01 on the BCCH. The BCCH is changed to contain:

- RAI (MCC/MNC/LAC/RAC): 246/081/0002/02.

- csg-Indication: TRUE

- csg-Identity: 04

The USS then resumes RF output on the BCCH.

g) The MMI of the UE is used to perform manual CSG selection. The UE shall indicate the availability of a cell with csg-Identity 04 for PLMN 246/081. The user shall select this cell by using the MMI.

h) After receipt of an *RRCConnectionRequest* from the UE on the UTRAN-cell related to the BCCH transmitting RAI 246/081/0002/02, the USS sends *RRCConnectionSetup* to the UE, followed by *RRCConnectionSetupComplete* sent by the UE to the USS.

i) During registration and after receipt of a *RoutingAreaUpdateRequest* from the UE, the USS initiates authentication, starts integrity by using the security procedure and sends *RoutingAreaUpdateAccept* with to the UE:

RAI (MCC/MNC/TAC): 246/081/0002/02

P-TMSI "34567890"

j) After receipt of the *RoutingAreaUpdatComplete* during registration from the UE, the USS sends *RRCConnectionRelease* to the UE.

k) The UE is soft powered down.

#### 10.2.2.5 Acceptance criteria

1.) After step b) the UE shall send an *RRCConnectionRequest* on the UTRAN-cell related to the BCCH transmitting RAI 246/081/0001/01 to the USS.

3) During step c) the terminal shall send *AttachRequest* to the USS.

4) After step c) the terminal shall respond with *AttachComplete* during registration.

5) During step e) the UE shall not provide during the manual CSG selection the information for a cell with csg-Identity 04 for PLMN 246/080 to the user.

6) During step g) the UE shall provide during the manual CSG selection the information for a cell with csg-Identity 04 for PLMN 246/081 to the user.

6a) After step g) the UE shall send an *RRCConnectionRequest* on the UTRAN-cell related to the BCCH transmitting RAI 246/081/0002/02 to the USS.

7) During step i) the terminal shall send *RoutingAreaUpdateRequest* to the USS.

8) After step i) the terminal shall respond with *RoutingAreaUpdatComplete* during registration.

9) After step k) the USIM shall contain the following values:

**EFPSLOCI (Location Information)**

Logically: RAI-MCC: 246

RAI-MNC: 081

RAI-LAC: 0002

RAI-RAC: 02

P-TMSI: "34567890"

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Coding: | B1 | B2 | B3 | B4 | B5 | B6 | B7 | B8 | B9 | B10 | B11 |
| Hex | 34 | 56 | 78 | 90 | xx | xx | xx | 42 | 16 | 80 | 00 |
|  |  |  |  |  |  |  |  |  |  |  |  |
| Coding: | B12 | B13 | B14 |  |  |  |  |  |  |  |  |
| Hex | 02 | 02 | 00 |  |  |  |  |  |  |  |  |

**EFACSGL (Allowed CSG Lists)**

Logically:

1st CSG list

PLMN: 246 081 (MCC MNC)

1st CSG list 1st CSG Type indication 02

1st CSG list 1st CSG HNB Name indication 02

1st CSG list 1st CSG CSG ID: 02 (27bit)

1st CSG list 2nd CSG Type indication 03

1st CSG list 2nd CSG HNB Name indication 03

1st CSG list 2nd CSG CSG ID: 03 (27bit)

1st CSG list 3rd CSG Type indication 'xx' (not checked)

1st CSG list 3rd CSG HNB Name indication 'xx' (not checked)

1st CSG list 3rd CSG CSG ID: 04 (27bit)

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Coding: | A0 | 1D | 80 | 03 | 42 | 16 | 80 | 81 | 06 | 02 |
|  | 02 | 00 | 00 | 00 | 5F | 81 | 06 | 03 | 03 | 00 |
|  | 00 | 00 | 7F | 81 | 06 | xx | xx | 00 | 00 | 00 |
|  | 9F |  |  |  |  |  |  |  |  |  |

2nd CSG list

PLMN: 244 081 (MCC MNC)

2nd CSG list 1st CSG Type indication 08

2nd CSG list 1st CSG HNB Name indication 08

2nd CSG list 1st CSG CSG ID: 08 (27bit)

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Coding: | A0 | 0D | 80 | 03 | 42 | 14 | 80 | 81 | 06 | 08 |
|  | 08 | 00 | 00 | 01 | 1F |  |  |  |  |  |

Note: The 1st and 2nd CSG list may be stored together or separately in any record in arbitrary order.

**EFOCSGL (Operator CSG Lists)**

Unchanged values as defined in 4.6.3

### 10.2.3 Manual CSG selection in UTRA with CSG list on USIM, success

#### 10.2.3.1 Definition and applicability

A Closed Subscriber Group identifies subscribers of an operator who are permitted to access one or more cells of the PLMN but which have restricted access (CSG cells). A CSG cell is part of the PLMN, broadcasting a CSG indication that is set to TRUE and a specific CSG identity. A CSG cell is accessible by the members of the closed subscriber group for that CSG identity. For a CSG cell, the UE shall check the broadcast CSG ID against the Allowed CSG list provided by NAS to check whether a CSG cell is suitable for the UE.

A UE supporting CSG selection selects CSG cell either automatically based on the list of allowed CSG identities or manually based on user selection of CSG on indication of list of available CSGs.

*Editor's note: it is still being investigated whether the testing of both the unsuccessful Manual CSG selection and the Automatic CSG selection should be performed using a separate test case or an enhanced version of the Manual CSG selection test case.*

#### 10.2.3.2 Conformance requirement

The ME shall read the allowed CSG IDs from EFACSGL in order to perform HNB selection procedures. The lists in EFACSGL shall take precedence over the list stored in the ME non-volatile memory.  
In manual CSG selection mode, the ME indicates to the user the list of available CSGs in the currently selected PLMN. The list of CSGs presented to the user is not restricted by the allowed CSG list.  
If the MS supports CSG, it is provisioned with a list of allowed CSG identities and associated PLMN identities from the USIM if the list is available in the USIM.

If the UE supporting CSG selection has attempted manual CSG selection, the UE, when receiving the ROUTING AREA UPDATE ACCEPT message, shall check if the CSG ID of the cell where the UE has sent the ROUTING AREA UPDATE REQUEST message is contained in the Allowed CSG list. If not, the UE shall add that CSG ID to the Allowed CSG list.

- TS 31.102 [4], clauses 4.4.6.2 and 5.8.1;

- TS 23.122 [31], clause 3.1A.

- TS 24.008 [16], clause 4.7.5.1.3

#### 10.2.3.3 Test purpose

To verify that the ME adds the CSG ID to the Allowed CSG list in EFACSGL in case this CSG ID belongs to the cell where the ME has sent the ROUTING AREA UPDATE REQUEST message which was accepted by the USS.

#### 10.2.3.4 Method of test

##### 10.2.3.4.1 Initial conditions

For this test an USS is required.

The USS transmits on two cells, with the following network parameters:

- RAI (MCC/MNC/LAC/RAC): 246/081/0001/01.

- Access control: unrestricted.

- csg-Indication: FALSE

- csg-Identity: not present

- RAI (MCC/MNC/LAC/RAC): 246/081/0002/02.

- Access control: unrestricted.

- csg-Indication: TRUE

- csg-Identity: 04

The default E-UTRAN UICC is used.

The UICC is installed into the Terminal and the UE is set to automatic PLMN selection mode.

##### 10.2.3.4.2 Procedure

a) The UE is powered on.

b) After receipt of an *RRCConnectionRequest* from the UE on the UTRAN-cell related to the BCCH transmitting RAI 246/081/0001/01, the USS sends *RRCConnectionSetup* to the UE, followed by *RRCConnectionSetupComplete* sent by the UE to the USS.

c) During registration and after receipt of an *AttachRequest* from the UE, the USS initiates authentication, starts integrity by using the security procedure and sends *AttachAccept* with to the UE:

RAI (MCC/MNC/LAC/RAC): 246/081/0001/01

P-TMSI "87512890"

d) After receipt of the *AttachComplete* during registration from the UE, the USS sends *RRCConnectionRelease*  to the UE.

e) The MMI of the UE is used to perform manual CSG selection. The UE shall indicate the availability of a cell with csg-Identity 04 for PLMN 246/081. The user shall select this cell by using the MMI.

f) After receipt of an *RRCConnectionRequest* from the UE on the UTRAN-cell related to the BCCH transmitting RAI 246/081/0002/02, the USS sends *RRCConnectionSetup* to the UE, followed by *RRCConnectionSetupComplete* sent by the UE to the USS.

g) During registration and after receipt of a *RoutingAreaUpdateRequest* from the UE, the USS initiates authentication, starts integrity by using the security procedure and sends *RoutingAreaUpdateAccept* with to the UE:

RAI (MCC/MNC/LAC/RAC): 246/081/0002/02

P-TMSI "34567890"

h) After receipt of the *RoutingAreaUpdatComplete* during registration from the UE, the USS sends *RRCConnectionRelease* to the UE.

i) The UE is soft powered down.

#### 10.2.3.5 Acceptance criteria

1) After step a) the UE shall send an *RRCConnectionRequest* on the UTRAN-cell related to the BCCH transmitting RAI 246/081/0001/01 to the USS.

3) During step c) the terminal shall send *AttachRequest* to the USS.

4) After step c) the terminal shall respond with *AttachComplete* during registration.

5) During step e) the UE shall provide during the manual CSG selection the information for a cell with csg-Identity 04 for PLMN 246/081 to the user.

6) After step e) the UE shall send an *RRCConnectionRequest* on the UTRAN-cell related to the BCCH transmitting RAI 246/081/0002/02 to the USS.

7) During step g) the terminal shall send *RoutingAreaUpdateRequest* to the USS.

8) After step g) the terminal shall respond with *RoutingAreaUpdatComplete* during registration.

9) After step i) the USIM shall contain the following values:

**EFPSLOCI (Location Information)**

Logically: RAI-MCC: 246

RAI-MNC: 081

RAI-LAC: 0002

RAI-RAC: 02

P-TMSI: "34567890"

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Coding: | B1 | B2 | B3 | B4 | B5 | B6 | B7 | B8 | B9 | B10 | B11 |
| Hex | 34 | 56 | 78 | 90 | xx | xx | xx | 42 | 16 | 80 | 00 |
|  |  |  |  |  |  |  |  |  |  |  |  |
| Coding: | B12 | B13 | B14 |  |  |  |  |  |  |  |  |
| Hex | 02 | 02 | 00 |  |  |  |  |  |  |  |  |

**EFACSGL (Allowed CSG Lists)**

Logically:

1st CSG list

PLMN: 246 081 (MCC MNC)

1st CSG list 1st CSG Type indication 02

1st CSG list 1st CSG HNB Name indication 02

1st CSG list 1st CSG CSG ID: 02 (27bit)

1st CSG list 2nd CSG Type indication 03

1st CSG list 2nd CSG HNB Name indication 03

1st CSG list 2nd CSG CSG ID: 03 (27bit)

1st CSG list 3rd CSG Type indication 'xx'

1st CSG list 3rd CSG HNB Name indication 'xx'

1st CSG list 3rd CSG CSG ID: 04 (27bit)

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Coding: | A0 | 1D | 80 | 03 | 42 | 16 | 80 | 81 | 06 | 02 |
|  | 02 | 00 | 00 | 00 | 5F | 81 | 06 | 03 | 03 | 00 |
|  | 00 | 00 | 7F | 81 | 06 | xx | xx | 00 | 00 | 00 |
|  | 9F |  |  |  |  |  |  |  |  |  |

2nd CSG list

PLMN: 244 081 (MCC MNC)

2nd CSG list 1st CSG Type indication 08

2nd CSG list 1st CSG HNB Name indication 08

2nd CSG list 1st CSG CSG ID: 08 (27bit)

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Coding: | A0 | 0D | 80 | 03 | 42 | 14 | 80 | 81 | 06 | 08 |
|  | 08 | 00 | 00 | 01 | 1F |  |  |  |  |  |

Note: The 1st and 2nd CSG list may be stored together or separately in any record in arbitrary order.

# 11 NAS security context parameter handling

## 11.1 NAS security context parameter handling when service "EMM Information" is available

### 11.1.1 Definition and applicability

The security parameters for authentication, integrity protection and ciphering are tied together in an EPS security context and identified by a key set identifier for E-UTRAN (eKSI). The relationship between the security parameters is defined in 3GPP TS 33.401 [27].

The EPS security context parameters shall be stored on the USIM if the corresponding file is present. If the corresponding file is not present on the USIM, these EMM parameters except allowed CSG list are stored in a non-volatile memory in the ME together with the IMSI from the USIM.

The EFEPSNSC contains the EPS NAS Security context as defined in TS 33.401 [27]. This file shall contain only one record and shall be updated only when the requirements defined in TS 33.401 [27] are met.

### 11.1.2 Conformance requirement

EPS AKA is the authentication and key agreement procedure that shall be used over E-UTRAN.

Before security can be activated, the MME and the UE need to establish an EPS security context. Usually, the EPS security context is created as the result of an authentication procedure between MME and UE. The EPS security context parameters shall be stored on the USIM if the corresponding file is present, and shall be updated only when the requirements defined in TS 33.401 [27] are met. If the corresponding file is not present on the USIM, these EMM parameters except allowed CSG list are stored in a non-volatile memory in the ME together with the IMSI from the USIM.

- TS 24.301 [26], clause 4.4.2.1 and Annex C;

- TS 31.102 [4], clause 4.2.92;

- TS 33.401 [27], clause 6.1.1, 7.2.5.1 and 7.2.5.2.1.

### 11.1.3 Test purpose

To verify that the ME generates the EPS security context identified by a key set identifier for E-UTRAN (eKSI) and stores all inside EFEPSNSC if this EF is available and when the requirements defined in TS 33.401 [27] , clauses 7.2.5.1 and 7.2.5.2.1 are met.

### 11.1.4 Method of test

#### 11.1.4.1 Initial conditions

For this test an E-USS or a NB-SS is required.

The E-USS transmits on one cell, with the following network parameters:

- TAI (MCC/MNC/TAC): 246/081/0001.

- Access control: unrestricted.

The NB-SS transmits on one cell, with the following network parameters:

- TAI (MCC/MNC/TAC): 246/081/0001.

- Access control: unrestricted.

The default E-UTRAN UICC is used.

#### 11.1.4.2 Procedure

a) The UE is switched on.

b) After receipt of an *RRCConnectionRequest/RRCConnectionRequest-NB* from the UE the E-USS/NB-SS sends *RRCConnectionSetup/RRCConnectionSetup-NB* to the UE, followed by *RRCConnectionSetupComplete/RRCConnectionSetupComplete-NB* sent by the UE to the E-USS/NB-SS.

c) During registration and after receipt of an *AttachRequest* (included in the *RRCConnectionSetupComplete/RRCConnectionSetupComplete-NB*) from the UE, the E-USS/NB-SS initiates the EPS authentication and AKA procedure. The E-USS/NB-SS uses

eKSI: '00'

d) Afterwards the E-USS/NB-SS transmits a (NAS) *SecurityModeCommand* message to activate NAS security, and after receiving (NAS) *SecurityModeComplete* from the UE, the E-USS/NB-SS sends *AttachAccept* to the UE with:

TAI (MCC/MNC/TAC): 246/081/ 0001

GUTI: "24608100010266345678"

e) After receipt of the *AttachComplete* during registration from the UE, the E-USS/NB-SS sends *RRCConnectionRelease/RRCConnectionRelease-NB* to the UE.

f) The UE or the UE's radio interface is switched off to perform the DETACH procedure.

### 11.1.5 Acceptance criteria

1) After step a) the UE shall read EFUST and EFEPSNSC.

2) During step b) the UE shall indicate in the *AttachRequest* that no key is available.

3) During step c) the UE shall send the *AuthenticationResponse* message.

4) During step d) the UE shall send the (NAS) *SecurityModeComplete* message.

5) EFEPSNSC shall not be updated during steps c) to e), unless for invalidating the content of EFEPSNSC.

Note: Invalidation of EFEPSNSC is described in TS 31.102 [4], clause 4.2.92.

6) After step f) the UE shall send DETACH REQUEST to the E-USS/NB-SS.

7) After step f) EFEPSNSC shall contain:

**EFEPSNSC (EPS NAS Security Context)**

Logically: Key Set Identifier KSIASME: '00'

ASME Key (KSIASME): 32 byte key, value not checked

Uplink NAS count: any value

Downlink NAS count: any value

Identifiers of selected NAS any value  
integrity and encryption  
algorithm

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Coding: | B1 | B2 | B3 | B4 | B5 | B6 | B7 | B8 | … | … | … | Bxx |
| Hex | A0 | xx | 80 | 01 | 00 | 81 | xx | xx | … | … | … | xx |

## 11.2 NAS security context parameter handling when service "EMM Information" is not available, no IMSI change

### 11.2.1 Definition and applicability

The security parameters for authentication, integrity protection and ciphering are tied together in an EPS security context and identified by a key set identifier for E-UTRAN (eKSI). The relationship between the security parameters is defined in 3GPP TS 33.401 [27].

The EPS security context parameters shall be stored on the USIM if the corresponding file is present. If the corresponding file is not present on the USIM, these EMM parameters except allowed CSG list are stored in a non-volatile memory in the ME together with the IMSI from the USIM.

The EFEPSNSC contains the EPS NAS Security context as defined in TS 33.401 [27]. This file shall contain only one record.

### 11.2.2 Conformance requirement

EPS AKA is the authentication and key agreement procedure that shall be used over E-UTRAN.

Before security can be activated, the MME and the UE need to establish an EPS security context. Usually, the EPS security context is created as the result of an authentication procedure between MME and UE. The EPS security context parameters shall be stored on the USIM if the corresponding file is present. If the corresponding file is not present on the USIM, these EMM parameters except allowed CSG list are stored in a non-volatile memory in the ME together with the IMSI from the USIM.

These EMM parameters can only be used if the IMSI from the USIM matches the IMSI stored in the non-volatile memory; else the UE shall delete the EMM parameters.

- TS 24.301 [26], clause 4.4.2.1 and Annex C;

- TS 31.102 [4], clause 4.2.92;

- TS 33.401 [27], clause 6.1.1.

### 11.2.3 Test purpose

To verify that the ME generates the EPS security context identified by a key set identifier for E-UTRAN (eKSI) and stores all inside a non-volatile memory in the ME as EMM information is not available on the USIM. During the test the IMSI on the USIM remains unchanged.

### 11.2.4 Method of test

#### 11.2.4.1 Initial conditions

For this test an E-USS or a NB-SS is required.

The E-USS transmits on one cell, with the following network parameters:

- TAI (MCC/MNC/TAC): 246/081/0001.

- Access control: unrestricted.

The NB-SS transmits on one cell, with the following network parameters:

- TAI (MCC/MNC/TAC): 246/081/0001.

- Access control: unrestricted.

The default UICC (without the service "EMM Information") is installed into the Terminal.

#### 11.2.4.2 Procedure

a) The UE is switched on.

b) After receipt of an *RRCConnectionRequest/RRCConnectionRequest-NB* from the UE the E-USS/NB-SS sends *RRCConnectionSetup/RRCConnectionSetup-NB* to the UE, followed by *RRCConnectionSetupComplete/ RRCConnectionSetupComplete-NB* sent by the UE to the E-USS/NB-SS.

c) During registration and after receipt of an *AttachRequest* (included in the *RRCConnectionSetupComplete/RRCConnectionSetupComplete-NB*) from the UE, the E-USS/NB-SS initiates the EPS authentication and AKA procedure. The E-USS/NB-SS uses

eKSI: 00

d) Afterwards the E-USS/NB-SS transmits a (NAS) *SecurityModeCommand* message to activate NAS security, and after receiving (NAS) *SecurityModeComplete* from the UE, the E-USS/NB-SS sends *AttachAccept* to the UE with:

TAI (MCC/MNC/TAC): 246/081/0001

GUTI: "24608100010266345678"

e) After receipt of the *AttachComplete* during registration from the UE, the E-USS/NB-SS sends *RRCConnectionRelease/ RRCConnectionRelease-NB* to the UE.

f) The UE is switched off and performs the *Detach* procedure.

g) The default UICC remains in use.

h) The Terminal is switched on.

i) After receipt of an *RRCConnectionRequest/RRCConnectionRequest-NB* from the UE the E-USS/NB-SS sends *RRCConnectionSetup/RRCConnectionSetup-NB* to the UE, followed by *RRCConnectionSetupComplete/RRCConnectionSetupComplete-NB* sent by the UE to the E-USS/NB-SS.

j) During registration and after receipt of an *AttachRequest* (included in the *RRCConnectionSetupComplete/RRCConnectionSetupComplete-NB*) from the UE, E-USS/NB-SS transmits a (NAS) *SecurityModeCommand* message to activate NAS security using the last known KASME, and after receiving (NAS) *SecurityModeComplete* from the UE, the E-USS/NB-SS sends *AttachAccept* to the UE with:

TAI (MCC/MNC/TAC): 246/081/0001

GUTI: "24608100010266345619"

k) After receipt of the *AttachComplete* during registration from the UE, the E-USS/NB-SS sends *RRCConnectionRelease/RRCConnectionRelease-NB* to the UE.

### 11.2.5 Acceptance criteria

1) After step a) the UE shall read EFUST.

2) During step c) the UE shall send the *AuthenticationResponse* message.

3) During step d) the UE shall send the (NAS) *SecurityModeComplete* message.

4) During step j) the UE shall indicate in the *AttachRequest* eKSI as 00.

5) During step j) the UE shall send the (NAS) *SecurityModeComplete* message.

6) During step k) the UE shall send the *AttachComplete* message.

## 11.3 NAS security context parameter handling when service "EMM Information" is not available, IMSI changed

### 11.3.1 Definition and applicability

The security parameters for authentication, integrity protection and ciphering are tied together in an EPS security context and identified by a key set identifier for E-UTRAN (eKSI). The relationship between the security parameters is defined in 3GPP TS 33.401 [27].

The EPS security context parameters shall be stored on the USIM if the corresponding file is present. If the corresponding file is not present on the USIM, these EMM parameters except allowed CSG list are stored in a non-volatile memory in the ME together with the IMSI from the USIM.

The EFEPSNSC contains the EPS NAS Security context as defined in TS 33.401 [27]. This file shall contain only one record.

### 11.3.2 Conformance requirement

EPS AKA is the authentication and key agreement procedure that shall be used over E-UTRAN.

Before security can be activated, the MME and the UE need to establish an EPS security context. Usually, the EPS security context is created as the result of an authentication procedure between MME and UE. The EPS security context parameters shall be stored on the USIM if the corresponding file is present. If the corresponding file is not present on the USIM, these EMM parameters except allowed CSG list are stored in a non-volatile memory in the ME together with the IMSI from the USIM.

These EMM parameters can only be used if the IMSI from the USIM matches the IMSI stored in the non-volatile memory; else the UE shall delete the EMM parameters.

- TS 24.301 [26], clause 4.4.2.1 and Annex C;

- TS 31.102 [4], clause 4.2.92;

- TS 33.401 [27], clause 6.1.1.

### 11.3.3 Test purpose

1) To verify that the ME generates the EPS security context identified by a key set identifier for E-UTRAN (eKSI) and stores all inside a non-volatile memory in the ME as EMM information is not available on the USIM.

2) To verify that UE deletes existing EMM parameters from the ME's non-volatile memory in case a different IMSI is activated.

### 11.3.4 Method of test

#### 11.3.4.1 Initial conditions

For this test an E-USS or NB-SS is required.

The E-USS transmits on one cell, with the following network parameters:

- TAI (MCC/MNC/TAC): 246/081/0001.

- Access control: unrestricted.

The NB-SS transmits on one cell, with the following network parameters:

- TAI (MCC/MNC/TAC): 246/081/0001.

- Access control: unrestricted.

The default UICC (without the service "EMM Information") is installed into the Terminal.

#### 11.3.4.2 Procedure

a) The UE is switched on.

b) After receipt of an *RRCConnectionRequest/RRCConnectionRequest-NB* from the UE the E-USS/NB-SS sends *RRCConnectionSetup/RRCConnectionSetup-NB* to the UE, followed by *RRCConnectionSetupComplete/RRCConnectionSetupComplete-NB* sent by the UE to the E-USS/NB-SS.

c) During registration and after receipt of an *AttachRequest* (included in the *RRCConnectionSetupComplete/RRCConnectionSetupComplete-NB*) from the UE, the E-USS/NB-SS initiates the EPS authentication and AKA procedure. The E-USS/NB-SS uses

eKSI: 00

d) Afterwards the E-USS/NB-SS transmits a (NAS) *SecurityModeCommand* message to activate NAS security, and after receiving (NAS) *SecurityModeComplete* from the UE, the E-USS/NB-SS sends *AttachAccept* to the UE with:

TAI (MCC/MNC/TAC): 246/081/0001

GUTI: "24608100010266345678"

e) After receipt of the *AttachComplete* during registration from the UE, the E-USS/NB-SS sends *RRCConnectionRelease/RRCConnectionRelease-NB* to the UE.

f) The UE is switched off and performs the *Detach* procedure.

g) A new UICC with the following configuration is activated:

The default UICC with the following exception: The IMSI is set to "246081222233333".

h) The Terminal is switched on.

i) After receipt of an *RRCConnectionRequest/RRCConnectionRequest-NB* from the UE the E-USS/NB-SS sends *RRCConnectionSetup/RRCConnectionSetup-NB* to the UE, followed by *RRCConnectionSetupComplete/RRCConnectionSetupComplete-NB* sent by the UE to the E-USS/NB-SS.

j) During registration and after receipt of an *AttachRequest* (included in the *RRCConnectionSetupComplete/RRCConnectionSetupComplete-NB*) from the UE, E-USS/NB-SS transmits a (NAS) *SecurityModeCommand* message to activate NAS security using the last known KASME.

k) The UE responds with (NAS) *SecurityModeReject*.

l) The E-USS/NB-SS sends *RRCConnectionRelease/RRCConnectionRelease-NB* to the UE.

### 11.3.5 Acceptance criteria

1) After step a) the UE shall read EFUST.

2) During step c) the UE shall send the *AuthenticationResponse* message.

3) During step d) the UE shall send the (NAS) *SecurityModeComplete* message.

4) During step j) the UE shall indicate in the *AttachRequest* that no key is available.

5) After step j) the UE shall send the (NAS) *SecurityModeReject* message.

## 11.4 EPS NAS Security Context Storage

### 11.4.1 Definition and applicability

The security parameters for authentication, integrity protection and ciphering are tied together in an EPS security context and identified by a key set identifier for E-UTRAN (eKSI). The relationship between the security parameters is defined in 3GPP TS 33.401 [27].

The EPS security context parameters shall be stored on the USIM if the corresponding file is present. If the corresponding file is not present on the USIM, these EMM parameters except allowed CSG list are stored in a non-volatile memory in the ME together with the IMSI from the USIM.

The EFEPSNSC contains the EPS NAS Security context as defined in TS 33.401 [27]. This file shall contain only one record and shall be updated only when the requirements defined in TS 33.401 [27] are met.

### 11.4.2 Conformance requirement

EPS AKA is the authentication and key agreement procedure that shall be used over E-UTRAN.

Before security can be activated, the MME and the UE need to establish an EPS security context. Usually, the EPS security context is created as the result of an authentication procedure between MME and UE. The EPS security context parameters shall be stored on the USIM if the corresponding file is present, and shall be updated only when the requirements defined in TS 33.401 [27] are met.

- TS 24.301 [26], clause 4.4.2.1 and Annex C;

- TS 31.102 [4], clause 4.2.92 and 5.2.28;

- TS 33.401 [27], clause 6.1.1, 7.2.5.2, 7.2.6.1 and 7.2.6.3.

### 11.4.3 Test purpose

The update of EPS NAS security context shall be according to the rules and procedures specified in TS 33.401 [27], clause 6.1.1, 7.2.5.2, 7.2.6.1 and 7.2.6.3.

### 11.4.4 Method of test

#### 11.4.4.1 Initial conditions

For this test an E-USS or a NB-SS is required.

The E-USS transmits on one cell, with the following network parameters:

- TAI (MCC/MNC/TAC): 246/081/0001.

- Access control: unrestricted.

The NB-SS transmits on one cell, with the following network parameters:

- TAI (MCC/MNC/TAC): 246/081/0001.

- Access control: unrestricted.

The default E-UTRAN UICC is used.

#### 11.4.4.2 Procedure

a) The UE is switched on.

b) After receipt of an *RRCConnectionRequest/RRCConnectionRequest-NB* from the UE the E-USS/NB-SS sends *RRCConnectionSetup/RRCConnectionSetup-NB* to the UE, followed by *RRCConnectionSetupComplete/RRCConnectionSetupComplete-NB* sent by the UE to the E-USS/NB-SS.

c) The E-USS/NB-SS receives an *AttachRequest* (included in the *RRCConnectionSetupComplete/RRCConnectionSetupComplete-NB*) from the UE.

d) The E-USS/NB-SS initiates the EPS authentication and AKA procedure. The E-USS/NB-SS uses

eKSI: '00'

e) Afterwards the E-USS/NB-SS transmits a (NAS) *SecurityModeCommand* message to activate NAS security, and after receiving (NAS) *SecurityModeComplete* from the UE, the E-USS/NB-SS sends *AttachAccept* to the UE with:

TAI (MCC/MNC/TAC): 246/081/0001

GUTI: "24608100010266345678"

f) After receipt of the *AttachComplete* during registration from the UE, the E-USS/NB-SS sends *RRCConnectionRelease/RRCConnectionRelease-NB*, to the UE.

g) The E-USS/NB-SS sends *Paging/Paging-NB* to the UE using the S-TMSI.

- for WB-S1: with CN domain indicator set to ''PS''.with CN domain indicator set to ''PS''.

h) After receipt of a *RRCConnectionRequest/RRCConnectionRequest-NB* message from the UE, the E-USS/NB-SS sends *RRCConnectionSetup/RRCConnectionSetup-NB* message to the UE, followed by *RRCConnectionSetupComplete/RRCConnectionSetupComplete*-*NB* sent by the UE to the E-USS/NB-SS.

i) The UE sends:

- for WB-S1: *EMM Service Request* followed by the activation of AS security by the E-USS and the Dedicated EPS bearer.

- for NB-IoT: *Control Plane* *Service Request*, the NB-SS sends a *Service Accept*.

j) The following is checked:

- for WB-S1: After keeping the Dedicated EPS Bearer active for 5 seconds, the E-USS sends *RRCConnectionRelease* to the UE.

- for NB-IoT: After keeping the Default EPS Bearer active for 5 seconds, the NB-SS sends *RRCConnectionRelease-NB* to the UE.

### 11.4.5 Acceptance criteria

1) After step a) the UE shall read EFUST and EFEPSNSC.

2) After step a) and before step d) the UE shall either keep the content of EFEPSNSC as specified in the initial conditions or invalidate the content of EFEPSNSC as described in TS 31.102 [4], clause 4.2.92.

3) During step d) the UE shall send the *AuthenticationResponse* message.

4) During step e) the UE shall send the (NAS) *SecurityModeComplete* message.

5) After step f) the UE shall have entered idle mode.

6) After step i) the UE shall have

- for WB-S1: a Dedicated EPS bearer established.

- for NB-IoT: a Default bearer established.

7) During steps d), e), f), g), h), i) and j) the UE shall not update EFEPSNSC.

# 12 Non Access Stratum (NAS) Configuration parameter handling

## 12.1 EFNASCONFIG – NAS signaling priority handling

### 12.1.1 Definition and applicability

If the UE is configured for NAS signalling priority (see 3GPP TS 24.368 [36], 3GPP TS 31.102 [4]), the UE shall indicate this by including the Device properties IE in the appropriate NAS message and setting the low priority indicator to "MS is configured to NAS signalling low priority". This NAS signalling low priority indication can be used by the network for NAS level mobility management congestion control on a per core network node basis and APN based congestion control.

The test case is covered in TS 34.123-1 [38] clauses 9.4.3.7, 9.4.5.5, 11.1.1.3, 11.1.1.4, 11.1.3.4, 11.2.2.3, 12.4.1.1e and 12.4.3.2a. Refer to CR #0229 for details.

### 12.1.2 Void

### 12.1.3 Void

### 12.1.4 Void

### 12.1.5 Void

## 12.2 EFNASCONFIG – NMO I Network Mode of Operation I handling

### 12.2.1 Definition and applicability

The behaviour of the UE with respect to NMO I is determined by the combination of PS domain specific system information IE and the setting of the parameter "NMO\_I\_Behaviour" in the NAS configuration Management Object as specified in 3GPP TS 24.368 [36] or in USIM file NASCONFIG as specified in 3GPP TS 31.102 [4].

The test case is covered in TS 34.123-1 [38] clause 12.2.2.3a. Refer to CR #0230 for details.

### 12.2.2 Void

### 12.2.3 Void

### 12.2.4 Void

### 12.2.5 Void

## 12.3 EFNASCONFIG – Attach with IMSI handling

### 12.3.1 Definition and applicability

The AttachWithIMSI leaf indicates whether attach with IMSI is performed when moving to a non-equivalent PLMN as specified in 3GPP TS 24.008 [16] and 3GPP TS 24.301 [26].

The test case is covered in TS 34.123-1 [38] clause 12.2.1.1a. Refer to CR #0224 for details.

### 12.3.2 Void

### 12.3.3 Void

### 12.3.4 Void

### 12.3.5 Void

## 12.4 EFNASCONFIG – Verifying Minimum Periodic Search Timer

### 12.4.1 Definition and applicability

The MinimumPeriodicSearchTimer leaf gives a minimum value in minutes for the timer T controlling the periodic search for higher prioritized PLMNs as specified in 3GPP TS 23.122 [31].

If the MS is configured for Fast First Higher Priority PLMN search and the MinimumPeriodicSearchTimer is configured as specified in 3GPP TS 24.368 [36] or 3GPP TS 31.102 [4], the MS shall not use a value for T that is less than the MinimumPeriodicSearchTimer.

The test case is covered in TS 34.123-1 [38] clauses 9.4.5.4 and 9.4.5.4.7. Refer to CR #0228 for details.

### 12.4.2 Void

### 12.4.3 Void

### 12.4.4 Void

### 12.4.5 Void

## 12.5 EFNASCONFIG – Extended access barring handling

### 12.5.1 Definition and applicability

Extended Access Barring (EAB) is a mechanism to control Mobile Originating access attempts from UEs that are configures for EAB in order to prevent overload for the access network and/or the core network. In congestion situations, the operator can restrict access from UEs configured for EAB while permitting access from other UEs.

The ExtendedAccessBarring leaf indicates whether the extended access barring is applicable for the UE as specified in 3GPP TS 24.008 [16] and 3GPP TS 24.301 [26].

The test case is covered in TS 34.123-1 [38] clauses 8.1.1.20, 9.4.11, 12.2.1.16 and 12.4.1.9. Refer to CR #0226 for details.

### 12.5.2 Void

### 12.5.3 Void

### 12.5.4 Void

### 12.5.5 Void

## 12.6 EFNASCONFIG – Verifying Timer T3245 Behaviour

### 12.6.1 Definition and applicability

For an MS that is configured to use timer T3245 (see 3GPP TS 24.368 [36] or 3GPP TS 31.102 [4]) and when the MS adds a PLMN identity to the "forbidden PLMN list" or the "forbidden PLMNs for GPRS service" list or sets the SIM/USIM as invalid for non-GPRS services or GPRS services or both, and timer T3245 is not running, the MS shall start timer T3245 with a random value, uniformly drawn from the range between 12h and 24h.

Upon expiry of the timer T3245, the MS shall erase the "forbidden PLMN list" and the "forbidden PLMNs for GPRS service" list and set the SIM/USIM to valid for non-GPRS services and GPRS services.

### 12.6.2 Conformance requirement

For NAS configuration parameter by USIM, the UE shall check and apply the setting present in EFNASCONFIG for "Timer T3245 Behaviour".

Reference:

- TS 31.102 [4], clauses 4.2.94, 5.2.29

- TS 24.368 [36], clause 5.7.

- TS 24.008 [16], clause 4.1.1.6

### 12.6.3 Test purpose

1) To verify that the UE reads the NAS configuration stored on the USIM.

2) To verify that the UE applies the USIM stored NAS configuration correctly to connect to the USS.

3) To verify that the UE erase the "forbidden PLMN list" and the "forbidden PLMNs for GPRS service" list upon expiry of the timer T3245.

### 12.6.4 Method of test

#### 12.6.4.1 Initial conditions

a) The USS transmits on the BCCH, with the following network parameters:

- Attach/detach: disabled.

- LAI (MCC/MNC/LAC): 234/005/0001.

- RAI (MCC/MNC/LAC/RAC): 234/005/0001/05

- Access control: unrestricted.

b) The default Non Access Stratum Configuration UICC is installed into the Terminal with the following exception:

**EFFPLMN (Forbidden PLMNs)**

Logically: PLMN1: empty

PLMN2: empty

PLMN3: empty

PLMN4: empty

PLMN5: empty

PLMN6: empty

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Coding: | B1 | B2 | B3 | B4 | B5 | B6 | B7 | B8 | B9 | B10 | B11 | B12 |
| Hex | FF | FF | FF | FF | FF | FF | FF | FF | FF | FF | FF | FF |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
| Coding: | B13 | B14 | B15 | B16 | B17 | B18 |  |  |  |  |  |  |
| Hex | FF | FF | FF | FF | FF | FF |  |  |  |  |  |  |

**EFNASCONFIG (Non Access Stratum Configuration):**

Logically:

NAS signalling priority value: Reserved (NAS signalling low priority is not used)

NMO I Behaviour value: "NMO I, Network Mode of Operation I" indication is not used

Attach with IMSI value: attach with IMSI is performed when moving to a non-equivalent PLMN

Minimum Periodic Search Timer value: 00

Extended access barring value: extended access barring is not applied for the UE

Timer T3245 Behaviour value: T3245 is used

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Coding: | B1 | B2 | B3 | B4 | B5 | B6 | B7 | B8 | B9 | B10 | B11 |
| Hex | 80 | 01 | 00 | 81 | 00 | 00 | 82 | 01 | 00 | 83 | 01 |
|  |  |  |  |  |  |  |  |  |  |  |  |
| Coding: | B12 | B13 | B14 | B15 | B16 | B17 | B18 |  |  |  |  |
| Hex | 00 | 84 | 01 | 00 | 85 | 01 | 01 |  |  |  |  |

#### 12.6.4.2 Procedure

a) The UE is powered on.

b) Depending on which domain the UE is going to be registered on, the UE attempts to perform CS, PS or CS/PS registration to the USS.

c) After receipt of a *LOCATION UPDATING REJECT* and/or *ATTACH REJECT* message during registration with the cause "PLMN not allowed" the Terminal shall update the EF FPLMN in the USIM. T3245 will start.

d) After the expiry of timer T3245, the terminal shall establish the RRC connection again.

e) Depending on which domain the UE is going to be registered on, the UE performs CS, PS or CS/PS registration to the USS.

f) The UE is powered down.

### 12.6.5 Acceptance criteria

a) After power on in step a) the UE shall reads EFNASCONFIG

b) The UE shall update EFFPLMN in step c) as following:

**EFFPLMN (Forbidden PLMNs)**

Logically: PLMN1: 234 005 (MCC MNC)

PLMN2: empty

PLMN3: empty

PLMN4: empty

PLMN5: empty

PLMN6: empty

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Coding: | B1 | B2 | B3 | B4 | B5 | B6 | B7 | B8 | B9 | B10 | B11 | B12 |
| Hex | 32 | 54 | 00 | FF | FF | FF | FF | FF | FF | FF | FF | FF |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
| Coding: | B13 | B14 | B15 | B16 | B17 | B18 |  |  |  |  |  |  |
| Hex | FF | FF | FF | FF | FF | FF |  |  |  |  |  |  |

c) The UE shall update EFFPLMN in step e) as following:

**EFFPLMN (Forbidden PLMNs)**

Logically: PLMN1: empty

PLMN2: empty

PLMN3: empty

PLMN4: empty

PLMN5: empty

PLMN6: empty

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Coding: | B1 | B2 | B3 | B4 | B5 | B6 | B7 | B8 | B9 | B10 | B11 | B12 |
| Hex | FF | FF | FF | FF | FF | FF | FF | FF | FF | FF | FF | FF |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
| Coding: | B13 | B14 | B15 | B16 | B17 | B18 |  |  |  |  |  |  |
| Hex | FF | FF | FF | FF | FF | FF |  |  |  |  |  |  |

## 12.7 EFNASCONFIG – Override NAS signalling low priority

### 12.7.1 Definition and applicability

The "Override NAS signalling low priority" indicates whether the UE can override the NAS Signalling Priority configuration in the NAS message as specified in 3GPP TS 24.008 [16] and 3GPP TS 24.301 [26].

### 12.7.2 Conformance requirement

For NAS configuration parameter by USIM, the UE shall check and apply correctly the setting present in EFNASCONFIG for "Override NAS signalling low priority" to connect to the network.

References:

- TS 31.102 [4], clauses 4.2.94, 5.2.29

- TS 24.368 [36], clause 5.9.

- TS 24.008 [16], clause 1.8, 6.1.3.1.3.2, 6.1.3.12, 4.7.13.5

- TS 23.060 [25], clause 5.3.13.6.

### 12.7.3 Test purpose

1) To verify that the UE reads the NAS configuration stored on the USIM.

2) To verify that the UE applies the USIM stored NAS configuration correctly to connect to the USS.

### 12.7.4 Method of test

#### 12.7.4.1 Initial conditions

a) The USS transmits on the BCCH, with the following network parameters:

- Attach/detach: disabled.

- LAI (MCC/MNC/LAC): 246/081/0001.

- RAI (MCC/MNC/LAC/RAC): 246/081/0001/05.

- Access control: unrestricted.

b) The default Non Access Stratum Configuration UICC is installed into the Terminal with the following exception:

**EFNASCONFIG (Non Access Stratum Configuration)**

Logically:

NAS signalling priority value: NAS signalling low priority

NMO I Behaviour value: "NMO I, Network Mode of Operation I" indication is not used

Attach with IMSI value: normal behaviour is applied

Minimum Periodic Search Timer value: 00

Extended access barring value: extended access barring is applied for the UE

Timer T3245 Behaviour value: T3245 not used

Override NAS signalling low priority: Indicates that the UE can override the NAS signalling low priority indicator

Override Extended access barring: Indicates that the UE can override extended access barring

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Coding: | B1 | B2 | B3 | B4 | B5 | B6 | B7 | B8 | B9 | B10 | B11 |
| Hex | 80 | 01 | 01 | 81 | 01 | 00 | 82 | 01 | 00 | 83 | 01 |
| Coding: | B12 | B13 | B14 | B15 | B16 | B17 | B18 | B19 | B20 | B21 | B22 |
| Hex | 00 | 84 | 01 | 01 | 85 | 01 | 00 | 86 | 01 | 01 | 87 |
| Coding: | B23 | B24 |  |  |  |  |  |  |  |  |  |
| Hex | 01 | 01 |  |  |  |  |  |  |  |  |  |

#### 12.7.4.2 Procedure

a) The UE is powered on where the UICC is configured as defined in b) in the initial conditions.

b) The user requests activation of a PDP context. After receipt of *ACTIVATE PDP CONTEXT REQUEST* from the UE, the USS sends *ACTIVATE PDP CONTEXT REJECT* to the UE indicating:

- SM cause value # 26: insufficient resources;

- Back-off timer T3396: 1 minute

c) Before timer T3396 expires, the users request activation of a PDP context, the UE sends *ACTIVATE PDP CONTEXT REQUEST*, the USS sends *ACTIVATE PDP CONTEXT ACCEPT* to the UE.

d) The UE is powered down.

### 12.7.5 Acceptance criteria

a) After power on in step a) the UE shall read EFNASCONFIG

b) In step b) the UE shall set in *ACTIVATE PDP CONTEXT REQUEST* message the low priority indicator to "MS is configured for NAS signalling low priority" in the device properties.

c) In step c) the UE shall send *ACTIVATE PDP CONTEXT REQUEST* message where the low priority indicator is set to "MS is not configured for NAS signalling low priority" in the device properties.

## 12.8 EFNASCONFIG – Override Extended access barring

### 12.8.1 Definition and applicability

The "Override Extended Access Barring" indicates whether the UE can override "Extended Access Barring" configured to extended access barring.

The handling of extended access barring for the UE when the Override Extended Access Barring is used is specified in 3GPP TS 24.008 [16] and 3GPP TS 24.301 [26].

### 12.8.2 Conformance requirement

For NAS configuration parameter by USIM, the UE shall check and apply correctly the setting present in EFNASCONFIG for "Override Extended Access Barring" to connect to the network.

References:

- TS 31.102 [4], clauses 4.2.94, 5.2.29

- TS 24.368 [36], clause 5.10.

- TS 23.060 [25], clause 5.3.13.6.

- TS 23.401 [37], clause 4.3.17.2, 4.3.17.4

- TS 22.011 [6], clause 4.3.4.1.

### 12.8.3 Test purpose

1) To verify that the UE reads the NAS configuration stored on the USIM.

2) To verify that the UE applies the USIM stored NAS configuration correctly to connect to the USS.

3) To verify that the UE overrides "Extended Access Barring" when the Override Extended Access Barring is used

### 12.8.4 Method of test

#### 12.8.4.1 Initial conditions

a) The USS transmits on the BCCH, with the following network parameters:

- Attach/detach: disabled.

- LAI (MCC/MNC/LAC): 246/081/0001.

- RAI (MCC/MNC/LAC/RAC): 246/081/0001/05.

- Access control: unrestricted.

- SYSTEM INFORMATION BLOCK TYPE 21:

EAB Authorization Mask: 0010000000 (Mobile stations configured for EAB and a member of Access Class 7 are barred)

EAB Subcategory (2 bit): 00 (The EAB Authorization mask is applicable to all mobile stations configured for EAB.)

b) The default Non Access Stratum Configuration UICC is installed into the Terminal with the following exception:

**EFNASCONFIG (Non Access Stratum Configuration)**

Logically:

NAS signalling priority value: Reserved (NAS signalling low priority is not used)

NMO I Behaviour value: "NMO I, Network Mode of Operation I" indication is not used

Attach with IMSI value: normal behaviour is applied

Minimum Periodic Search Timer value: 00

Extended access barring value: extended access barring is applied for the UE

Timer T3245 Behaviour value: T3245 not used

Override NAS signalling low priority: Indicates that the UE can override the NAS signalling low priority indicator

Override Extended access barring: Indicates that the UE can override extended access barring

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Coding: | B1 | B2 | B3 | B4 | B5 | B6 | B7 | B8 | B9 | B10 | B11 |
| Hex | 80 | 01 | 00 | 81 | 01 | 00 | 82 | 01 | 00 | 83 | 01 |
| Coding: | B12 | B13 | B14 | B15 | B16 | B17 | B18 | B19 | B20 | B21 | B22 |
| Hex | 00 | 84 | 01 | 01 | 85 | 01 | 00 | 86 | 01 | 01 | 87 |
| Coding: | B23 | B24 |  |  |  |  |  |  |  |  |  |
| Hex | 01 | 01 |  |  |  |  |  |  |  |  |  |

#### 12.8.4.2 Procedure

a) The UE shall be powered on where the UICC is configured as defined in b) in the initial conditions and the USS transmits of the BCCH as defined inside the initial conditions.

b) User request activate a PDP context. The UE sends *ACTIVATE PDP CONTEXT REQUEST*, the USS sends *ACTIVATE PDP CONTEXT ACCEPT* to the UE.

c) The UE is powered down

### 12.8.5 Acceptance criteria

a) After power on in step a) the UE shall reads EFNASCONFIG

b) In step b) the UE shall send *ACTIVATE PDP CONTEXT REQUEST* message to the USS.

## 12.9 EFNASCONFIG – Fast First Higher Priority PLMN Search

### 12.9.1 Definition and applicability

The "Fast First Higher Priority PLMN Search" indicates whether the UE performs the first search for a higher priority PLMN after at least 2 minutes and at most T minutes upon entering a VPLMN as specified in 3GPP TS 23.122 [31].

### 12.9.2 Conformance requirement

For NAS configuration parameter by USIM, the UE shall check and apply correctly the setting present in EFNASCONFIG for "Fast First Higher Priority PLMN Search" to connect to the network.

References:

- TS 31.102 [4], clauses 4.2.94, 5.2.29

- TS 24.368 [36], clause 5.10a.

- TS 23.122 [31], clause 4.4.3.3.1

### 12.9.3 Test purpose

1) To verify that the UE reads the NAS configuration stored on the USIM.

2) To verify that the UE applies the USIM stored NAS configuration correctly to connect to the USS.

3) To verify that the UE performs first search for higher priority PLMN according to "Fast First Higher Priority PLMN Search" configuration when this parameter is present and used.

### 12.9.4 Method of test

#### 12.9.4.1 Initial conditions

a) The USS transmits on BCCH, with the following network parameters:

- Attach/detach: disabled.

- LAI (MCC/MNC/LAC): 244/009/0001.

- RAI (MCC/MNC/LAC/RAC): 244/009/0001/05

- Access control: unrestricted.

b) After the registration of UE the USS transmits on a second BCCH, with the following network parameters:

- Attach/detach: disabled.

- LAI (MCC/MNC/LAC): 244/081/0001.

- RAI (MCC/MNC/LAC/RAC): 244/081/0001/05

- Access control: unrestricted.

c) The default Non Access Stratum Configuration UICC is installed into the Terminal with the following exception:

**EFHPPLMN (Higher Priority PLMN Search period)**

Logically: set to 6 minutes

|  |  |
| --- | --- |
| Coding: | B1 |
| Hex | 01 |

**EFNASCONFIG (Non Access Stratum Configuration)**

Logically:

NAS signalling priority value: Reserved (NAS signalling low priority is not used)

NMO I Behaviour value: "NMO I, Network Mode of Operation I" indication is not used

Attach with IMSI value: normal behaviour is applied

Minimum Periodic Search Timer value: 00

Extended access barring value: extended access barring is not applied for the UE

Timer T3245 Behaviour value: T3245 not used

Override NAS signalling low priority: Indicates that the UE cannot override the NAS signalling low priority indicator

Override Extended access barring: Indicates that the UE cannot override extended access barring

Fast First Higher Priority PLMN Search: Indicates that the Fast First Higher Priority PLMN Search is enabled

EUTRA Disabling Allowed For EMM

Cause15: disabled

SM\_RetryWaitTime: E0

SM\_RetryAtRATChange: UE is allowed to retry the corresponding ESM procedure in S1 mode if an SM procedure was rejected in A/Gb or Iu mode, and to retry the corresponding SM procedure in A/Gb or Iu mode if an ESM procedure was rejected in S1 mode.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Coding: | B1 | B2 | B3 | B4 | B5 | B6 | B7 | B8 | B9 | B10 | B11 |
| Hex | 80 | 01 | 00 | 81 | 01 | 00 | 82 | 01 | 00 | 83 | 01 |
| Coding: | B12 | B13 | B14 | B15 | B16 | B17 | B18 | B19 | B20 | B21 | B22 |
| Hex | 00 | 84 | 01 | 00 | 85 | 01 | 00 | 86 | 01 | 00 | 87 |
| Coding: | B23 | B24 | B25 | B26 | B27 | B28 | B29 | B30 | B31 | B32 | B33 |
| Hex | 01 | 00 | 88 | 01 | 01 | 89 | 01 | 00 | 8A | 01 | E0 |
| Coding: | B34 | B35 | B36 |  |  |  |  |  |  |  |  |
| Hex | 8B | 01 | 00 |  |  |  |  |  |  |  |  |

#### 12.9.4.2 Procedure

a) The UE shall be powered on where the UICC is configured as defined in b) in the initial conditions and the USS starts to transmit on the first BCCH with the MMC/MNC 246/009.

b) Depending on which domain the UE is going to be registered on, the UE performs CS, PS or CS/PS registration to the USS.

c) The USS starts to send on the second BCCH with the MCC/MNC 244/081.

d) Depending on which domain the UE is going to be registered on, the UE performs CS, PS or CS/PS registration to the USS on the cell related to the BCCH transmitting MCC/MNC 244/081.

e) The UE is powered down.

### 12.9.5 Acceptance criteria

a) After power on in step a) the UE shall read EFNASCONFIG

b) The UE shall perform step d) after 2 - 6 minutes.

## 12.10 EFNASCONFIG – E-UTRA Disabling Allowed for EMM cause #15

### 12.10.1 Definition and applicability

The "EUTRA Disabling Allowed For EMM Cause #15" indicates whether the UE is allowed to disable the E-UTRA capability when it receives the Extended EMM cause IE with value "E-UTRAN not allowed" as described in 3GPP TS 24.301 [26].

### 12.10.2 Conformance requirement

For NAS configuration parameter by USIM, the UE shall check and apply the setting present in EFNASCONFIG for "EUTRA Disabling Allowed For EMM Cause #15" to connect to the network.

References:

- TS 31.102 [4], clauses 4.2.94, 5.2.29

- TS 24.368 [36], clause 5.10b.

- TS 24.301 [26], clause 4.5, 5.5.1.2.5

### 12.10.3 Test purpose

1) To verify that the UE reads the NAS configuration stored on the USIM.

2) To verify that the UE applies the USIM stored NAS configuration correctly to connect to the USS

3) To verify that the UE shall disable the E-UTRA capability and search for a suitable cell in GERAN or UTRAN radio access technology upon ATTACH REJECT reception that include both EMM cause #15 "no suitable cells in tracking area" and an Extended EMM cause IE with value "E-UTRAN not allowed" if " EUTRA Disabling Allowed For EMM Cause #15" is present and enabled in the UE.

### 12.10.4 Method of test

#### 12.10.4.1 Initial conditions

a) For this test both a UTRAN USS and an E-UTRAN E-USS is needed.

The E-USS transmits on the BCCH, with the following network parameters:

- TAI (MCC/MNC/TAC): 244/003/0001.

- Access control: unrestricted.

At step c) the E-USS transmits on the BCCH, with the following network parameters:

- TAI (MCC/MNC/TAC): 244/003/0002.

- Access control: unrestricted.

At step c) the USS transmits on BCCH, with the following network parameters:

- Attach/detach: disabled.

- LAI (MCC/MNC/LAC): 244/003/0003.

- Access control: unrestricted.

The UICC is installed into the Terminal and the UE is set to automatic PLMN selection mode.

b) The default Non Access Stratum Configuration of E-UTRAN/EPC UICC is installed into the Terminal with the following exception:

**EFNASCONFIG (Non Access Stratum Configuration)**

Logically:

NAS signalling priority value: Reserved (NAS signalling low priority is not used)

NMO I Behaviour value: "NMO I, Network Mode of Operation I" indication is not used

Attach with IMSI value: normal behaviour is applied

Minimum Periodic Search Timer value: 00

Extended access barring value: extended access barring is not applied for the UE

Timer T3245 Behaviour value: T3245 not used

Override NAS signalling low priority: Indicates that the UE cannot override the NAS signalling low priority indicator

Override Extended access barring: Indicates that the UE cannot override extended access barring

Fast First Higher Priority PLMN Search: Indicates that the Fast First Higher Priority PLMN Search is enabled

EUTRA Disabling Allowed For EMM

Cause15: enabled

SM\_RetryWaitTime: E0

SM\_RetryAtRATChange: UE is allowed to retry the corresponding ESM procedure in S1 mode if an SM procedure was rejected in A/Gb or Iu mode, and to retry the corresponding SM procedure in A/Gb or Iu mode if an ESM procedure was rejected in S1 mode.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Coding: | B1 | B2 | B3 | B4 | B5 | B6 | B7 | B8 | B9 | B10 | B11 |
| Hex | 80 | 01 | 00 | 81 | 01 | 00 | 82 | 01 | 00 | 83 | 01 |
| Coding: | B12 | B13 | B14 | B15 | B16 | B17 | B18 | B19 | B20 | B21 | B22 |
| Hex | 00 | 84 | 01 | 00 | 85 | 01 | 00 | 86 | 01 | 00 | 87 |
| Coding: | B23 | B24 | B25 | B26 | B27 | B28 | B29 | B30 | B31 | B32 | B33 |
| Hex | 01 | 00 | 88 | 01 | 00 | 89 | 01 | 01 | 8A | 01 | E0 |
| Coding: | B34 | B35 | B36 |  |  |  |  |  |  |  |  |
| Hex | 8B | 01 | 00 |  |  |  |  |  |  |  |  |

#### 12.10.4.2 Procedure

a) The UE shall be powered on where the UICC is configured as defined in b) in the initial conditions and the E-USS starts to send only on the BCCH with the MCC/MNC 244/003.

b) After receipt of *AttachRequest* from the UE, the E-USS sends *Attach Reject* message with:

- EMM cause set to #15: "No suitable cells in tracking area",

- Extended EMM cause IE: "E-UTRAN not allowed"

c) The E-USS starts to send on the BCCH with MCC/MNC 244/003 and the USS starts to send on the BCCH with MCC/MNC 244/003.

d) After receipt of an *RRCConnectionRequest* from the UE, the USS sends *RRCConnectionSetup* to the UE, followed by *RRCConnectionSetupComplete* sent by the UE to the USS.

e) The UE is powered down.

### 12.10.5 Acceptance criteria

a) After power on in step a) the UE shall read EFNASCONFIG

b) In step d) the UE shall send a *RRCConnectionRequest* on the UTRAN-cell related to the BCCH transmitting MCC/MNC 244/003 to the USS.

## 12.11 EFNASCONFIG – SM\_RetryWaitTime

### 12.11.1 Definition and applicability

The "SM\_RetryWaitTime" indicates a configured UE retry wait time value applicable when in HPLMN or EHPLMN (see 3GPP TS 23.122 [31]) for controlling the UE session management retry behaviour when prior session management request was rejected by the network with cause value #8, #27, #32, #33 as specified in 3GPP TS 24.008 [16] and 3GPP TS 24.301 [26].

SM\_RetryWaitTime shall be coded in the same format as the value part of GPRS Timer 3 IE as specified in Table 10.5.163a/3GPP TS 24.008 [16] converted into a decimal value.

### 12.11.2 Conformance requirement

For NAS configuration parameter by USIM, the UE shall check and apply the setting present in EFNASCONFIG for "SM\_RetryWaitTime" to connect to the network.

Reference:

- TS 31.102 [4], clauses 4.2.94, 5.2.29

- TS 24.368 [36], clause 5.10c.

- TS 24.008 [16], clauses 6.1.3.1.3.3, 10.5.7.4a.

### 12.11.3 Test purpose

1) To verify that the UE reads the NAS configuration stored on the USIM.

2) To verify that the UE applies the USIM stored NAS configuration correctly to connect to the USS.

3) To verify that the UE behaves as described in TS 24.008 [16] clause 6.1.3.1.3.3, using the default value of 12 minutes for the back-off timer when the SM Retry Timer value is not configured.

4) To verify that the UE behaves as described in TS 24.008 [16] clause 6.1.3.1.3.3, using the configured SM Retry Timer value as back-off timer value.

### 12.11.4 Method of test

#### 12.11.4.1 Initial conditions

a) The USS transmits on BCCH, with the following network parameters:

- Attach/detach: disabled.

- LAI (MCC/MNC/LAC): 246/081/0001.

- RAI (MCC/MNC/LAC/RAC): 246/081/0001/05.

- Access control: unrestricted.

b) The default Non Access Stratum Configuration UICC is installed into the Terminal with the following exception:

**EFNASCONFIG (Non Access Stratum Configuration)**

Logically:

NAS signalling priority value: Reserved (NAS signalling low priority is not used)

NMO I Behaviour value: "NMO I, Network Mode of Operation I" indication is not used

Attach with IMSI value: normal behaviour is applied

Minimum Periodic Search Timer value: 00

Extended access barring value: extended access barring is not applied for the UE

Timer T3245 Behaviour value: T3245 not used

Override NAS signalling low priority: Indicates that the UE cannot override the NAS signalling low priority indicator

Override Extended access barring: Indicates that the UE cannot override extended access barring

Fast First Higher Priority PLMN Search: Indicates that the Fast First Higher Priority PLMN Search is not enabled

EUTRA Disabling Allowed For EMM

Cause15: disabled

SM\_RetryWaitTime: 60 seconds

SM\_RetryAtRATChange: UE is allowed to retry the corresponding ESM procedure in S1 mode if an SM procedure was rejected in A/Gb or Iu mode, and to retry the corresponding SM procedure in A/Gb or Iu mode if an ESM procedure was rejected in S1 mode.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Coding: | B1 | B2 | B3 | B4 | B5 | B6 | B7 | B8 | B9 | B10 | B11 |
| Hex | 80 | 01 | 00 | 81 | 01 | 00 | 82 | 01 | 00 | 83 | 01 |
| Coding: | B12 | B13 | B14 | B15 | B16 | B17 | B18 | B19 | B20 | B21 | B22 |
| Hex | 00 | 84 | 01 | 00 | 85 | 01 | 00 | 86 | 01 | 00 | 87 |
| Coding: | B23 | B24 | B25 | B26 | B27 | B28 | B29 | B30 | B31 | B32 | B33 |
| Hex | 01 | 00 | 88 | 01 | 00 | 89 | 01 | 00 | 8A | 01 | 7E |
| Coding: | B34 | B35 | B36 |  |  |  |  |  |  |  |  |
| Hex | 8B | 01 | 00 |  |  |  |  |  |  |  |  |

#### 12.11.4.2 Procedure

a) The UE is powered on where the UICC is configured as defined in b) in the initial conditions.

b) User request activate a PDP context. After receipt of *ACTIVATE PDP CONTEXT REQUEST* from the UE, the USS sends *ACTIVATE PDP CONTEXT REJECT* to the UE indicating:

- SM cause value #8: operator determined barring;

c) User request activate a PDP context and the UE sends *ACTIVATE PDP CONTEXT REQUEST*, the USS sends *ACTIVATE PDP CONTEXT ACCEPT* to the UE.

d) The UE is powered down.

### 12.11.5 Acceptance criteria

a) After power on in step a) the UE shall read EFNASCONFIG

b) In step c) the UE shall send *ACTIVATE PDP CONTEXT REQUEST* message after the SM\_RetryWaitTime of 1 minute has expired.

## 12.12 EFNASCONFIG – SM\_RetryAtRATChange

### 12.12.1 Definition and applicability

The "SM\_RetryAtRATChange" indicates the UE's retry behaviour when in HPLMN or EHPLMN (see 3GPP TS 23.122 [31]) after inter-system change between S1 mode and A/Gb or Iu mode as specified in 3GPP TS 24.008 [16] and 3GPP TS 24.301 [26].

### 12.12.2 Conformance requirement

Editor's note: this clause is for future study.

### 12.12.3 Test purpose

Editor's note: this clause is for future study.

### 12.12.4 Method of test

Editor's note: this clause is for future study.

### 12.12.5 Acceptance criteria

Editor's note: this clause is for future study.

# 13 UICC interface during PSM

## 13.1 UICC interface in PSM handling for E-UTRAN – No UICC deactivation in PSM

### 13.1.1 Definition and applicability

PSM is intended for UEs that are expecting only infrequent mobile originating and terminating services and that can accept a corresponding latency in the mobile terminating communication. In order to reduce power consumption while in PSM, and only in case the PIN of the USIM is disabled, the ME may optionally deactivate the UICC after entering the PSM.

### 13.1.2 Conformance requirement

In order to reduce power consumption while the ME is in PSM, and only in case the PIN of the USIM is disabled, the ME may optionally deactivate the UICC (as specified in clause 6A.1 of 3GPP TS 31.101 [39]) after entering the PSM.

Reference:

- TS 31.102 [4], clause 5.1.10;

- TS 24.301 [26], clauses 5.3.5 and 5.3.11.

- TS 31.101 [39], clause 6A.1.

### 13.1.3 Test purpose

1) To verify that UE does not deactivate the UICC in case the PIN for the USIM is enabled and verified.

### 13.1.4 Method of test

#### 13.1.4.1 Initial conditions

The UE is configured to use Power Saving Mode.

The UE is configured to use the timer T3324 set to T3324\_V.

The E-USS transmits on the BCCH, with the following network parameters:

- TAI (MCC/MNC/TAC): 246/081/0001.

- Access control: unrestricted.

The NB-SS transmits on the BCCH, with the following network parameters:

- TAI (MCC/MNC/TAC): 246/081/0001.

- Access control: unrestricted.

The default E-UTRAN UICC is used with the following exceptions:

EFUMPC (UICC Maximum Power Consumption)

Logically:

UICC maximum power consumption: 60 mA

Operator defined time out (T\_OP): 5 seconds

Additional information: UICC does not require increased idle current

UICC does not support the UICC suspension procedure

Byte 4 and byte 5: RFU

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Byte: | B1 | B2 | B3 | B4 | B5 |
| Coding: | 3C | 05 | 00 | 00 | 00 |

The PIN of the USIM is enabled and verified

#### 13.1.4.2 Procedure

a) The UE is switched on.

b) The UE requests RRC Connection and transmits an *ATTACH REQUEST* message to the E-USS/NB-SS including T3324 set to T3324\_V.

c) The E-USS/NB-SS sends the *ATTACH ACCEPT* message contains T3324 set to T3324\_V and T3412 set to T3412\_V.. It shall not contain the eDRX parameters

d) After receipt of the *AttachComplete* during registration from the UE, the E-USS/NB-SS sends *RRCConnectionRelease/RRCConnectionRelease-NB*, to the UE.

e) After the T3412 timer expires the UE sends *TRACKING AREA UPDATE REQUEST*

f) The E-USS/NB-SS sends *TRACKING AREA UPDATE ACCEPT*.

g) The UE is switched off.

### 13.1.5 Acceptance criteria

1) After step c) the UE shall not deactivate the UICC or send SUSPEND UICC command.

## 13.2 UICC interface in PSM handling for E-UTRAN – PSM not accepted by E-USS/NB-SS

### 13.2.1 Definition and applicability

PSM is intended for UEs that are expecting only infrequent mobile originating and terminating services and that can accept a corresponding latency in the mobile terminating communication. In order to reduce power consumption while in PSM, and only in case the PIN of the USIM is disabled, the ME may optionally deactivate the UICC after entering the PSM.

### 13.2.2 Conformance requirement

In order to reduce power consumption while the ME is in PSM, and only in case the PIN of the USIM is disabled, the ME may optionally deactivate the UICC (as specified in clause 6A.1 of 3GPP TS 31.101 [39]) after entering the PSM.

Reference:

- TS 31.102 [4], clause 5.1.10;

- TS 24.301 [26], clauses 5.3.5 and 5.3.11.

- TS 31.101 [39] in clause 6A.1.

### 13.2.3 Test purpose

1) To verify that UE does not deactivate the UICC in case the network is not supporting/accepting PSM.

### 13.2.4 Method of test

#### 13.2.4.1 Initial conditions

The UE is configured to use Power Saving Mode.

The UE is configured to use the timer T3324 set to T3324\_V.

The E-USS transmits on the BCCH, with the following network parameters:

- TAI (MCC/MNC/TAC): 246/081/0001.

- Access control: unrestricted.

The NB-SS transmits on the BCCH, with the following network parameters:

- TAI (MCC/MNC/TAC): 246/081/0001.

- Access control: unrestricted.

The default E-UTRAN UICC is installed into the Terminal.

The PIN of the USIM is disabled.

#### 13.2.4.2 Procedure

a) The UE is switched on.

b) The UE requests RRC Connection and transmits an *ATTACH REQUEST* message to the E-USS/NB-SS including T3324 set to T3324\_V.

c) The E-USS/NB-SS sends the *ATTACH ACCEPT* message contains a T3324 set to "deactivated". It shall not contain the eDRX parameters.

d) After receipt of the *AttachComplete* during registration from the UE, the E-USS/NB-SS sends *RRCConnectionRelease/RRCConnectionRelease-NB*, to the UE

e) After the time period T3324\_V has passed, the E-USS/NB-SS transmits *Paging/Paging-NB* to the UE using the S-TMSI.

f) After receipt of *RRCConnectionRequest/RRCConnectionRequest-NB* message from the UE, the E-USS/NB-SS sends *RRCConnectionSetup/RRCConnectionSetup-NB* message to the UE, followed by *RRCConnectionSetupComplete/RRCConnectionSetupComplete*-*NB* sent by the UE to the E-USS/NB-SS.

g) The terminal sends *Service Request*, the E-USS/NB-SS sends *SERVICE ACCEPT* followed by *RRCConnectionRelease/RRCConnectionRelease-NB* to the UE.

h) The UE is switched off.

### 13.2.5 Acceptance criteria

1) After step c) the UE shall not deactivate the UICC.

## 13.3 UICC interface in PSM handling for E-UTRAN – UICC deactivation in PSM

### 13.3.1 Definition and applicability

PSM is intended for UEs that are expecting only infrequent mobile originating and terminating services and that can accept a corresponding latency in the mobile terminating communication. In order to reduce power consumption while in PSM, and only in case the PIN of the USIM is disabled, the ME may optionally deactivate the UICC after entering the PSM.

### 13.3.2 Conformance requirement

In order to reduce power consumption while the ME is in PSM, and only in case the PIN of the USIM is disabled, the ME may optionally deactivate the UICC (as specified in clause 6A.1 of 3GPP TS 31.101 [39]) after entering the PSM.

In this case, the ME shall perform these steps before it can leave the PSM:

- re-activate the UICC (as specified in clause 6A.1 of 3GPP TS 31.101 [39]),

- re-initialize the USIM (as specified in clause 5.1.1 [4]), with the exception of re-reading EFs that are not required for the verification of the USIM,

- take appropriate steps to verify that the same USIM is used.

Verification shall include at least the check of the content of the following EFs: EFICCID, EFIMSI and EFLOCI, and/or EFPSLOCI and/or EFEPSLOCI (depending on which of these specific EFs containing LOCI the ME used prior to entering PSM)

Reference:

- TS 31.102 [4], clause 5.1.10;

- TS 24.301 [26], clauses 5.3.5 and 5.3.11.

- TS 31.101 [39] in clause 6A.1.

### 13.3.3 Test purpose

1) To verify that when the UE enters PSM it deactivates the UICC in case the PIN for the USIM is disabled.

2) To verify that UE when it leaves the PSM performs the following steps:

- re-activates the UICC;

- re-initializes the USIM;

- verifies the following EFs: EFICCID, EFIMSI, and EFEPSLOCI.

### 13.3.4 Method of test

#### 13.3.4.1 Initial conditions

The UE is configured to use Power Saving Mode.

The UE is configured to use the timer T3324 set to T3324\_V.

The E-USS transmits on the BCCH, with the following network parameters:

- TAI (MCC/MNC/TAC): 246/081/0001.

- Access control: unrestricted.

The NB-SS transmits on the BCCH, with the following network parameters:

- TAI (MCC/MNC/TAC): 246/081/0001.

- Access control: unrestricted.

The default E-UTRAN UICC is installed into the Terminal.

The PIN of the USIM is disabled.

#### 13.3.4.2 Procedure

a) The UE is switched on.

b) The UE requests RRC Connection and transmits an *ATTACH REQUEST* message to the E-USS/NB-SS including T3324 set to T3324\_V.

c) The E-USS/NB-SS sends the *ATTACH ACCEPT* message contains T3324 set to T3324\_V and T3412 set to T3412\_V. It shall not contain the eDRX parameters.

d) After receipt of the *AttachComplete* during registration from the UE, the E-USS/NB-SS sends *RRCConnectionRelease/RRCConnectionRelease-NB*, to the UE.

e) After the T3412 timer expires the UE sends *TRACKING AREA UPDATE REQUEST*.

f) The E-USS/NB-SS sends *TRACKING AREA UPDATE ACCEPT*.

g) The UE is switched off.

### 13.3.5 Acceptance criteria

1) After step d) and the expiration of T3324 timer, the UE deactivates the UICC.

2) After step e) the UE leaves the PSM and re-activates the UICC, re-initializes the USIM and verifies the following EFs: EFICCID, EFIMSI and EFEPSLOCI.

## 13.4 UICC interface in PSM for E-UTRAN – SUSPEND UICC

### 13.4.1 Definition and applicability

PSM is intended for UEs that are expecting only infrequent mobile originating and terminating services and that can accept a corresponding latency in the mobile terminating communication. If the UICC supports the UICC suspension mechanism (SUSPEND UICC command), the ME may suspend the UICC after entering the PSM. In this case, the ME shall successfully resume the UICC before it can leave the PSM.

### 13.4.2 Conformance requirement

If the UICC supports the UICC suspension mechanism (SUSPEND UICC command), the ME may suspend the UICC after entering the PSM. In this case, the ME shall successfully resume the UICC before it can leave the PSM.

Reference:

- TS 31.102 [4], clause 5.1.10;

- TS 24.301 [26], clauses 5.3.5, 5.3.11 and 5.5.1.2.2.

- TS 31.101 [39] in clause 11.1.22.

13.4.3 Test purpose

1) To verify that after reading EFUMPC and entering the PSM the ME sends a SUSPEND UICC command to the UICC in case the UICC indicates the support of the SUSPEND UICC command.

2) To verify that the ME resumes the UICC before it can leave the PSM.

### 13.4.4 Method of test

#### 13.4.4.1 Initial conditions

The ME is configured to use Power Saving Mode.

The ME is configured to use the timer T3324 set to T3324\_V.

The E-USS transmits on the BCCH, with the following network parameters:

- TAI (MCC/MNC/TAC): 246/081/0001.

- Access control: unrestricted.

The NB-SS transmits on the BCCH, with the following network parameters:

- TAI (MCC/MNC/TAC): 246/081/0001.

- Access control: unrestricted.

The default E-UTRAN UICC is used with the following exceptions:

**EFUMPC**

Logically:

UICC maximum power consumption: 60 mA

Operator defined time out (T\_OP): 5 seconds

Additional information:

UICC does not require increased idle current

UICC supports the UICC suspension procedure

Byte 4 and byte 5: RFU

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Coding | B1 | B2 | B3 | B4 | B5 |
| Hex | 3C | 05 | 02 | 00 | 00 |

The PIN of the USIM is enabled and verified.

#### 13.4.4.2 Procedure

a) The UE is switched on.

b) The UE requests RRC Connection and transmits an *ATTACH REQUEST* message to the E-USS/NB-SS including T3324 set to T3324\_V.

c) The E-USS/NB-SS sends the *ATTACH ACCEPT* message contains T3324 set to T3324\_V and T3412 set to T3412\_V. It shall not contain the eDRX parameters.

d) After receipt of the AttachComplete during registration from the UE, the E-USS/NB-SS sends RRCConnectionRelease/RRCConnectionRelease-NB, to the UE.

e) The ME sends SUSPEND UICC command to the UICC indicating "Minimum duration of the suspension proposed by the terminal" and the "Maximum duration of the suspension proposed by the terminal".

f) The UICC returns a maximum suspension duration in the range proposed by the ME, Resume token and SW 9000.

g) After the T3412 timer expires the UE sends *TRACKING AREA UPDATE REQUEST*

h) The E-USS/NB-SS sends *TRACKING AREA UPDATE ACCEPT*.

i) The UE is switched off.

NOTE: For testing purposes, and to not extend the test execution time the maximum suspension duration returned by the UICC shall be equal to the minimum duration of the suspension proposed by the terminal.

### 13.4.5 Acceptance criteria

1) After step a) the ME reads EFUMPC to verify that the SUSPEND UICC command is supported.

2) After step e) the ME deactivates the UICC as specified in 3GPP TS 31.101 [39].

3) After step g) the ME leaves the PSM and resumes the UICC.

# 14 UICC interface during eDRX

## 14.1 UICC interface during eDRX for E-UTRAN – eDRX is not supported by the UICC

### 14.1.1 Definition and applicability

In order to reduce power consumption when the UE uses extended idle mode DRX cycle, the UE may optionally deactivate the UICC during the extended idle mode DRX cycle.

### 14.1.2 Conformance requirement

In case the UICC does not support the UICC suspension mechanism, the PIN of the USIM is disabled and deactivation of UICC is authorized in EFAD, the UE may optionally deactivate the UICC (as specified in clause 6A.1 of 3GPP TS 31.101 [39]) during the extended idle mode DRX cycle.

Reference:

- TS 31.102 [4], clause 5.1.11;

- TS 24.301 [26], clauses 5.3.12.

- TS 23.401 [37], clause 5.13a.

- TS 31.101 [39] in clause 6A.1.

### 14.1.3 Test purpose

1) To verify that UE does not deactivate the UICC in case the ME is not authorized to modify the polling interval and/or disable the UICC interface during extended DRX cycle in EFAD in USIM.

### 14.1.4 Method of test

#### 14.1.4.1 Initial conditions

The UE is configured to request the use of eDRX (in the ATTACH REQUEST and TRACKING AREA UPDATE messages).

The E-USS transmits on the BCCH, with the following network parameters:

- TAI (MCC/MNC/TAC): 246/081/0001.

- Access control: unrestricted.

The NB-SS transmits on the BCCH, with the following network parameters:

- TAI (MCC/MNC/TAC): 246/081/0001.

- Access control: unrestricted.

The default E-UTRAN UICC is used with the following exceptions:

EFUMPC (UICC Maximum Power Consumption)

Logically:

UICC maximum power consumption: 60 mA

Operator defined time out (T\_OP): 5 seconds

Additional information: UICC does not require increased idle current

UICC does not support the UICC suspension procedure

Byte 4 and byte 5: RFU

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Byte: | B1 | B2 | B3 | B4 | B5 |
| Coding: | 3C | 05 | 00 | 00 | 00 |

The PIN of the USIM is enabled and verified.

#### 14.1.4.2 Procedure

a) The UE is switched on.

b) The UE requests RRC Connection and transmits an *ATTACH REQUEST* message to the E-USS/NB-SS including eDRX parameters.

c) The E-USS/NB-SS sends the *ATTACH ACCEPT* message containing eDRX set to eDRX\_V and PTW set to PTW\_V. If ATTACH REQUEST in step b) above also contains T3324, the ATTACH ACCEPT message shall contain T3324 set to "deactivated". If ATTACH REQUEST in step b) does not contain T3324, the ATTACH ACCEPT message shall not contain T3324.

d) After receipt of the *AttachComplete* during registration from the UE, the E-USS/NB-SS sends *RRCConnectionRelease/RRCConnectionRelease-NB*, to the UE.

e) The E-USS/NB-SS transmits *Paging/Paging-NB* to the UE using the S-TMSI in a valid paging occasion within the PTW of the paging Hyperframes as per Idle eDRX.

f) After receipt of *RRCConnectionRequest/RRCConnectionRequest-NB* message from the UE, the E-USS/NB-SS sends *RRCConnectionSetup/RRCConnectionSetup-NB* message to the UE, followed by *RRCConnectionSetupComplete/RRCConnectionSetupComplete*-*NB* sent by the UE to the E-USS/NB-SS.

g) The terminal sends *Service Request,* the E-USS/NB-SS sends *SERVICE ACCEPT* followed by *RRCConnectionRelease/RRCConnectionRelease-*NB to the UE.

h) The UE is switched off.

### 14.1.5 Acceptance criteria

1) After step d) the UE shall not deactivate the UICC or send SUSPEND UICC command.

## 14.2 UICC interface during eDRX for E-UTRAN – eDRX is not accepted by E-USS/NB-SS

### 14.2.1 Definition and applicability

In order to reduce power consumption when the UE uses extended idle mode DRX cycle, the UE may optionally deactivate the UICC during the extended idle mode DRX cycle.

### 14.2.2 Conformance requirement

In case the UICC does not support the UICC suspension mechanism, the PIN of the USIM is disabled and deactivation of UICC is authorized in EFAD, the UE may optionally deactivate the UICC (as specified in clause 6A.1 of 3GPP TS 31.101 [39]) during the extended idle mode DRX cycle.

Reference:

- 3GPP TS 31.102 [4], clause 5.1.11;

- TS 24.301 [26], clauses 5.3.12.

- TS 23.401 [37], clause 5.13a

- 3GPP TS 31.101 [39] in clause 6A.1.

### 14.2.3 Test purpose

1) To verify that UE does not deactivate the UICC in case extended DRX cycle is not supported by the network.

### 14.2.4 Method of test

#### 14.2.4.1 Initial conditions

The UE is configured to request the use of eDRX (in the ATTACH REQUEST and TRACKING AREA UPDATE messages).

The E-USS transmits on the BCCH, with the following network parameters:

- TAI (MCC/MNC/TAC): 246/081/0001.

- Access control: unrestricted.

The NB-SS transmits on the BCCH, with the following network parameters:

- TAI (MCC/MNC/TAC): 246/081/0001.

- Access control: unrestricted.

The default E-UTRAN UICC is installed into the Terminal with following exception:

EFAD (Administrative Data)

Logically: Normal operation + specific facilities;

Ciphering indicator feature disabled;

CSG Display Control: for every PLMN not included in EF\_OCSGL, or for which a CSG display indicator tag is not present, all available CSGs can be displayed without any restriction;

ProSe services for Public Safety: the ME is not authorized for ProSe services for Public Safety usage without contacting the ProSe Function;

Extended DRX cycle: the ME is authorized to modify the polling interval and/or disable the UICC interface during extended DRX cycle;

Length of MNC in the IMSI: 3.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Coding:** | **B1** | **B2** | **B3** | **B4** |
| Hex | 01 | 00 | 08 | 03 |

The PIN of the USIM is disabled.

14.2.4.2 Procedure

a) The UE is switched on.

b) The UE requests RRC Connection and transmits an *ATTACH REQUEST* message to the E-USS/NB-SS including eDRX parameters:

c) The E-USS/NB-SS sends the *ATTACH ACCEPT* message where the eDRX parameters are not present. If ATTACH REQUEST in step b) above also contains T3324, the ATTACH ACCEPT message shall contain T3324 set to "deactivated". If ATTACH REQUEST in step b) does not contain T3324, the ATTACH ACCEPT message shall not contain T3324.

d) After receipt of the *AttachComplete* during registration from the UE, the E-USS/NB-SS sends *RRCConnectionRelease/RRCConnectionRelease-NB*, to the UE.

e) E-USS/NB-SS transmits *Paging/Paging-NB* to the UE in a valid paging occasion as per normal DRX

f) After receipt of *RRCConnectionRequest/RRCConnectionRequest-NB* message from the UE, the E-USS/NB-SS sends *RRCConnectionSetup/RRCConnectionSetup-NB* message to the UE, followed by *RRCConnectionSetupComplete/RRCConnectionSetupComplete*-*NB* sent by the UE to the E-USS/NB-SS.

g) The terminal sends *Service Request,* the E-USS/NB-SS sends *SERVICE ACCEPT* followed by *RRCConnectionRelease/RRCConnectionRelease-*NB to the UE

h) The UE is switched off.

### 14.2.5 Acceptance criteria

1) After step d) the UE shall not deactivate the UICC.

## 14.3 UICC interface during eDRX for E-UTRAN – UICC deactivation during eDRX

### 14.3.1 Definition and applicability

In order to reduce power consumption when the UE uses extended idle mode DRX cycle, the UE may optionally deactivate the UICC during the extended idle mode DRX cycle.

In this case, the UE shall re-activate the UICC, re-initialize the USIM and take appropriate steps to verify that the same USIM is used, before the end of the extended idle mode DRX cycle or before any other transmission to the network

### 14.3.2 Conformance requirement

In case the UICC does not support the UICC suspension mechanism, the PIN of the USIM is disabled and deactivation of UICC is authorized in EFAD, the UE may optionally deactivate the UICC (as specified in clause 6A.1 of 3GPP TS 31.101 [39]) during the extended idle mode DRX cycle.

In this case, the UE shall re-activate the UICC (as specified in clause 6A.1 of 3GPP TS 31.101 [39]), re-initialize the USIM (as specified in clause 5.1.1 from [4]) and take appropriate steps to verify that the same USIM is used, before the end of the extended idle mode DRX cycle or before any other transmission to the network.

Verification shall include at least the check of the content of the following EFs: EFICCID, EFIMSI and EFLOCI, and/or EFPSLOCI and/or EFEPSLOCI (depending on which of these specific EFs containing LOCI the ME used prior to entering PSM).

Reference:

- 3GPP TS 31.102 [4], clause 5.1.11;

- TS 24.301 [26], clauses 5.3.12.

- TS 23.401 [37], clause 5.13a

- 3GPP TS 31.101 [39] in clause 6A.1.

### 14.3.3 Test purpose

1) To verify that UE does not deactivate the UICC in case the ME is not authorized to modify the polling interval and/or disable the UICC interface during extended DRX cycle in EFAD in USIM.

2) To verifies that UE when it leaves the PSM performs the following steps:

- re-activates the UICC.

- re-initializes the USIM

- verifies the following EFs: EFICCID, EFIMSI and EFEPSLOCI.

### 14.3.4 Method of test

#### 14.3.4.1 Initial conditions

The UE is configured to request the use of eDRX (in the ATTACH REQUEST and TRACKING AREA UPDATE messages).

The E-USS transmits on the BCCH, with the following network parameters:

- TAI (MCC/MNC/TAC): 246/081/0001.

- Access control: unrestricted.

The NB-SS transmits on the BCCH, with the following network parameters:

- TAI (MCC/MNC/TAC): 246/081/0001.

- Access control: unrestricted.

The default E-UTRAN UICC is installed into the Terminal with following exception:

EFAD (Administrative Data)

Logically: Normal operation + specific facilities;

Ciphering indicator feature disabled;

CSG Display Control: for every PLMN not included in EF\_OCSGL, or for which a CSG display indicator tag is not present, all available CSGs can be displayed without any restriction;

ProSe services for Public Safety: the ME is not authorized for ProSe services for Public Safety usage without contacting the ProSe Function;

Extended DRX cycle: the ME is authorized to modify the polling interval and/or disable the UICC interface during extended DRX cycle;

Length of MNC in the IMSI: 3.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Coding:** | **B1** | **B2** | **B3** | **B4** |
| Hex | 01 | 00 | 08 | 03 |

The PIN of the USIM is disabled.

#### 14.3.4.2 Procedure

a) The UE is switched on.

b) The UE requests RRC Connection and transmits an *ATTACH REQUEST* message to the E-USS/NB-SS including eDRX parameters:

c) The E-USS/NB-SS sends the *ATTACH ACCEPT* message containing eDRX set to eDRX\_V and PTW set to PTW\_V. If ATTACH REQUEST in step b) above also contains T3324, the ATTACH ACCEPT message shall contain T3324 set to "deactivated". If ATTACH REQUEST in step b) does not contain T3324, the ATTACH ACCEPT message shall not contain T3324.

d) After receipt of the *AttachComplete* during registration from the UE, the E-USS/NB-SS sends *RRCConnectionRelease/RRCConnectionRelease-NB*, to the UE.

e) The E-USS/NB-SS transmits *Paging/Paging-NB* to the UE using the S-TMSI in a valid paging occasion within the PTW of the paging Hyperframes as per Idle eDRX.

f) After receipt of a *RRCConnectionRequest/RRCConnectionRequest-NB* message from the UE, the E-USS/NB-SS sends *RRCConnectionSetup/RRCConnectionSetup-NB* message to the UE, followed by *RRCConnectionSetupComplete/RRCConnectionSetupComplete*-*NB* sent by the UE to the E-USS/NB-SS.

g) The terminal sends *Service Request*, the E-USS/NB-SS sends *SERVICE ACCEPT* followed by *RRCConnectionRelease/RRCConnectionRelease-NB* to the UE.

h) The UE is switched off.

### 14.3.5 Acceptance criteria

1) After step d) the UE the UE deactivates the UICC.

2) After step e) the UE shall re-activate the UICC, re-initialize the USIM and verify the following EFs: EFICCID, EFIMSI and EFEPSLOCI

## 14.4 UICC interface during eDRX for E-UTRAN– SUSPEND UICC

### 14.4.1 Definition and applicability

In order to reduce power consumption when the UE uses extended idle mode DRX cycle, as defined in 3GPP TS 24.301 [26], in case the UICC supports the UICC suspension mechanism (SUSPEND UICC command), the ME may suspend the UICC during the extended idle mode DRX cycle. In this case, the ME shall resume the UICC successfully before the end of the extended idle mode DRX cycle or before any other transmission to the network.

### 14.4.2 Conformance requirement

In case the UICC supports the UICC suspension mechanism (SUSPEND UICC command), the ME may suspend the UICC during the extended idle mode DRX cycle. In this case, the ME shall resume the UICC successfully before the end of the extended idle mode DRX cycle or before any other transmission to the network.

Reference:

- 3GPP TS 31.102 [4], clause 5.1.11;

- TS 24.301 [26], clauses 5.3.12.

- TS 23.401 [37], clause 5.13a.

- 3GPP TS 31.101 [39] in clauses 6A.1 and 11.1.22.

### 14.4.3 Test purpose

1) To verify that UE does not send SUSPEND UICC command to the UICC in case the UICC does not indicates the support of SUSPEND UICC command in EFUMPC during the extended idle mode DRX cycle

2) To verify that UE sends SUSPEND UICC command to the UICC in case the UICC indicates the support of SUSPEND UICC command in EFUMPC during the extended idle mode DRX cycle.

3) To verify that UE resumes the UICC before the end of the extended idle mode DRX cycle or before any other transmission to the network.

### 14.4.4 Method of test

#### 14.4.4.1 Initial conditions

The UE is configured to request the use of eDRX (in the ATTACH REQUEST and TRACKING AREA UPDATE messages).

The E-USS transmits on the BCCH, with the following network parameters:

- TAI (MCC/MNC/TAC): 246/081/0001.

- Access control: unrestricted.

The NB-SS transmits on the BCCH, with the following network parameters:

- TAI (MCC/MNC/TAC): 246/081/0001.

- Access control: unrestricted.

The default E-UTRAN UICC is used with the following exceptions:

EFUMPC (UICC Maximum Power Consumption)

Logically:

UICC maximum power consumption: 60 mA

Operator defined time out (T\_OP): 5 seconds

Additional information: UICC does not require increased idle current

UICC supports the UICC suspension procedure

Byte 4 and byte 5: RFU

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Byte: | B1 | B2 | B3 | B4 | B5 |
| Coding: | 3C | 05 | 02 | 00 | 00 |

EFAD (Administrative Data)

Logically: Normal operation + specific facilities;

Ciphering indicator feature disabled;

CSG Display Control: for every PLMN not included in EF\_OCSGL, or for which a CSG display indicator tag is not present, all available CSGs can be displayed without any restriction;

ProSe services for Public Safety: the ME is not authorized for ProSe services for Public Safety usage without contacting the ProSe Function;

Extended DRX cycle: the ME is authorized to modify the polling interval and/or disable the UICC interface during extended DRX cycle;

Length of MNC in the IMSI: 3.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Coding:** | **B1** | **B2** | **B3** | **B4** |
| Hex | 01 | 00 | 08 | 03 |

The PIN of the USIM is enabled and verified.

#### 14.4.4.2 Procedure

a) The UE is switched on.

b) The UE requests RRC Connection and transmits an *ATTACH REQUEST* message to the E-USS/NB-SS including eDRX parameters:

c) The E-USS/NB-SS sends the *ATTACH ACCEPT* message containing eDRX set to eDRX\_V and PTW set to PTW\_V. If ATTACH REQUEST in step b) above also contains T3324, the ATTACH ACCEPT message shall contain T3324 set to "deactivated". If ATTACH REQUEST in step b) does not contain T3324, the ATTACH ACCEPT message shall not contain T3324.

d) After receipt of the *AttachComplete* during registration from the UE, the E-USS/NB-SS sends *RRCConnectionRelease/RRCConnectionRelease-NB*, to the UE.

e) The UE sends SUSPEND UICC command to the UICC indicating "Minimum duration of the suspension proposed by the terminal" and the "Maximum duration of the suspension proposed by the terminal".

f) The UICC returns Maximum duration of the "suspension negotiated by the UICC" = "Minimum duration of the suspension proposed by the terminal", Resume token and SW 9000.

g) The E-USS/NB-SS transmits *Paging/Paging-NB* to the UE using the S-TMSI in a valid paging occasion within the PTW of the paging Hyperframes as per Idle eDRX.

h) After receipt of *RRCConnectionRequest/RRCConnectionRequest-NB* message from the UE, the E-USS/NB-SS sends *RRCConnectionSetup/RRCConnectionSetup-NB* message to the UE, followed by *RRCConnectionSetupComplete/RRCConnectionSetupComplete*-*NB* sent by the UE to the E-USS/NB-SS.

i) The terminal sends *Service Request*, the E-USS/NB-SS sends *SERVICE ACCEPT* followed by *RRCConnectionRelease/RRCConnectionRelease-NB* to the UE.

j) The UE is switched off.

### 14.4.5 Acceptance criteria

1) After step f) the UE deactivates the UICC as specified in 3GPP TS 31.101 [39].

2) After step g) the UE resumes the UICC.

# 15 Authentication procedure and NAS security context handling for 5G

## 15.1 Authentication procedure for EAP-AKA'

### 15.1.1 Authentication procedure for EAP-AKA' - Authentication is successful

#### 15.1.1.1 Definition and applicability

The purpose of the primary authentication and key agreement procedure is to enable mutual authentication between the UE and the network and to provide keying material that can be used between the UE and network in subsequent security procedures. The UE and the AMF shall support the EAP based primary authentication and key agreement procedure.

In order to initiate the EAP based primary authentication and key agreement procedure using EAP-AKA', the AUSF shall send an EAP message IE with EAP-request/AKA'-challenge message in the *AUTHENTICATION REQUEST* message.

The 5G NAS security context parameters from a full native 5G NAS security context shall be stored on the USIM if the corresponding file is present on the USIM as specified in 3GPP TS 31.102 [4]. If the corresponding file is not present on the USIM, this 5GMM parameters is stored in a non-volatile memory in the ME together with the SUPI from the USIM.

The EF5GS3GPPNSC contains the 5GS 3GPP access NAS security context as defined in 3GPP TS 24.501 [42], consisting of KAMF with the associated key set identifier, the UE security capabilities, and the uplink and downlink NAS COUNT values. This file shall contain one record.

The EF5GAUTHKEYS contains KAUSF and KSEAF that are generated on the ME using CK and IK as part of AKA procedures as described in 3GPP TS 33.501 [41].

#### 15.1.1.2 Conformance requirement

1) The UE shall support the EAP based primary authentication and key agreement procedure.

2) The ME shall forward the RAND and AUTN received in EAP message IE with EAP-request/AKA'-challenge within the *AUTHENTICATION REQUEST* message to the USIM.

3) The ME shall return the EAP message IE with EAP-response/AKA'-challenge in *AUTHENTICATION RESPONSE* message.

4) As a result of successful authentication procedure and upon receipt of the EAP Success message, the 5G NAS security context parameters shall be stored on the USIM if the corresponding file is present on the USIM when entering state 5GMM-DEREGISTERED.

5) If service n°122 is "available", the ME shall store KAMF with the associated key set identifier, the UE security capabilities, and the uplink and downlink NAS COUNT values in EF5GS3GPPNSC on the USIM.

6) If service n°123 is "available", the ME shall store the KAUSF and KSEAF in EF5GAUTHKEYS on the USIM.

Reference:

- 3GPP TS 31.102 [4], clauses 4.4.11.3, 4.4.11.4 and 4.4.11.6;

- 3GPP TS 33.501 [41], clause 6.1.3.1;

- 3GPP TS 24.501 [42], clause 5.4.1.2 and Annex C.

#### 15.1.1.3 Test purpose

1) To verify that the ME forwards the RAND and AUTN received in EAP-request/AKA'-challenge within EAP message IE to the USIM.

2) To verify that the ME returns the EAP message IE with EAP-response/AKA'-challenge in *AUTHENTICATION RESPONSE* message indicating the response calculated in the USIM (RES).

3) To verify that the ME stores 5G NAS security context parameters, consisting of KAMF with the associated key set identifier in EF5GS3GPPNSC on the USIM if service n°122 is "available".

4) To verify that the ME stores the KAUSF and KSEAF in EF5GAUTHKEYS on the USIM if service n°123 is "available".

#### 15.1.1.4 Method of test

##### 15.1.1.4.1 Initial conditions

The NG-SS transmits on the BCCH, with the following network parameters:

- TAI (MCC/MNC/TAC): 244/083/000001.

- Access control: unrestricted.

The default 5G-NR UICC is used and the UICC is installed into the ME and the UE is powered on.

##### 15.1.1.4.2 Procedure

a) Bring up Cell A and the UE is switched on.

b) Upon reception of an *RRCSetupRequest* message from the UE, NG-SS transmits an *RRCSetup* message to the UE followed by reception of an *RRCSetupComplete* message from the UE.

c) After receipt of a *REGISTRATION REQUEST* message from the UE during registration, the NG-SS initiates the EAP-AKA' authentication procedure and sends EAP message IE with EAP-request/AKA'-challenge message in the *AUTHENTICATION REQUEST* message and it uses:

ngKSI:

NAS key set identifier: '000'

TSC: '0'

EAP message: EAP-request/AKA'-challenge

d) Using the EAP-request/AKA'-challenge data received in *AUTHENTICATION REQUEST* message the ME passes the RAND and AUTN to the USIM.

e) The UE shall return the EAP message IE with EAP-response/AKA'-challenge in *AUTHENTICATION RESPONSE* message.

f) After reception of *AUTHENTICATION RESPONSE* message from the UE, the NG-SS sends EAP-success in *SECURITY MODE COMMAND* message, the UE sends a *SECURITY MODE COMPLETE* message.

g) The NG-SS sends a *REGISTRATION ACCEPT* message.

5G-GUTI: 24408300010266436587

TAI: 42 34 80 00 00 01

h) The UE sends a *REGISTRATION COMPLETE* message.

i) The UE is switched off or the UE's radio interface is switched off to perform the *DEREGISTRATION* procedure.

#### 15.1.1.5 Acceptance criteria

1) After step a) the ME shall read EFUST, EF5GS3GPPNSC and EF5GAUTHKEYS.

2) During step c) the UE shall indicate within the *REGISTRATION REQUEST* for the NAS key set identifier that no key is available.

3) In step d) the ME forwards the RAND and AUTN received in EAP message IE with EAP-request/AKA'-challenge message to the USIM.

4) In step e) the ME shall send *AUTHENTICATION RESPONSE* message with EAP message IE with EAP-response/AKA'-challenge containing the response calculated in the USIM (RES):

- Authentication response message identity: '0101 0111’

- Authentication response parameter: 4 – 16 octets RES value calculated according to 3GPP TS 24.501 [42]

5) In step f) the UE shall send *SECURITY MODE COMPLETE* message.

6) After step f) the ME updates EF5GAUTHKEYS as shown below.

**EF5GAUTHKEYS (5G authentication keys)**

Logically:

KAUSF: 32 bytes, value not checked

KSEAF:32 bytes, value not checked

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Coding:** | **B1** | **B2** | **B3** | **Bx** | **Bx+1** | **Bx+2** | **Bx+3** | **..** | **Bxx** |
| Hex | 80 | L1 | Xx | .. | 81 | L2 | xx | .. | xx |

7) After step i) the ME updates EF5GS3GPPNSC as shown below.

**EF5GS3GPPNSC (5GS 3GPP Access NAS Security Context)**

Logically:

5GS NAS Security Context:

ngKSI: 00

KAMF:32 bytes, value not checked

Uplink NAS count: any value

Downlink NAS count: any value

Identifiers of selected NAS integrity  
and encryption algorithms: any value

Identifiers of selected EPS NAS  
integrity and encryption algorithms  
for use after mobility to EPS: any value

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Coding:** | **B1** | **B2** | **B3** | **B4** | **B5** | **B6** | **B7** | **B8** | **B9** | **Bx** |
| Hex | A0 | XX | 80 | 01 | 00 | 81 | xx | xx | … | xx |

### 15.1A.1 Authentication procedure for EAP-AKA' - Authentication is Successful

#### 15.1A.1.1 Definition and applicability

The purpose of the primary authentication and key agreement procedure is to enable mutual authentication between the UE and the network and to provide keying material that can be used between the UE and network in subsequent security procedures. The UE and the AMF shall support the EAP based primary authentication and key agreement procedure.

In order to initiate the EAP based primary authentication and key agreement procedure using EAP-AKA', the AUSF shall send an EAP message IE with EAP-request/AKA'-challenge message in the *AUTHENTICATION REQUEST* message.

The 5G NAS security context parameters from a full native 5G NAS security context shall be stored on the USIM if the corresponding file is present on the USIM as specified in 3GPP TS 31.102 [4]. If the corresponding file is not present on the USIM, this 5GMM parameters is stored in a non-volatile memory in the ME together with the SUPI from the USIM.

The EF5GS3GPPNSC contains the 5GS 3GPP access NAS security context as defined in 3GPP TS 24.501 [42], consisting of KAMF with the associated key set identifier, the UE security capabilities, and the uplink and downlink NAS COUNT values. This file shall contain one record.

The EF5GAUTHKEYS contains KAUSF and KSEAF that are generated on the ME using CK and IK as part of AKA procedures as described in 3GPP TS 33.501 [41]. If service n°133 is "available" in EFUST, the EF5GAUTHKEYS also contains SOR counter and UE parameter update counter associated with the key KAUSF as described in 3GPP TS 33.501 [41] and 3GPP TS 31.102 [4].

#### 15.1A.1.2 Conformance requirement

1) The UE shall support the EAP based primary authentication and key agreement procedure.

2) The ME shall forward the RAND and AUTN received in EAP message IE with EAP-request/AKA'-challenge within the *AUTHENTICATION REQUEST* message to the USIM.

3) The ME shall return the EAP message IE with EAP-response/AKA'-challenge in *AUTHENTICATION RESPONSE* message.

4) As a result of successful authentication procedure and upon receipt of the EAP Success message, the 5G NAS security context parameters shall be stored on the USIM if the corresponding file is present on the USIM when entering state 5GMM-DEREGISTERED.

5) With service n°122 "available", the ME shall store KAMF with the associated key set identifier, the UE security capabilities, and the uplink and downlink NAS COUNT values in EF5GS3GPPNSC on the USIM.

6) With service n°123 "available" and service n°133 "available" the ME shall store the KAUSF, KSEAF for 3GPP access, KSEAF for non-3GPP access, SOR counter and UE parameter update counter in the EF5GAUTHKEYS on the USIM.

Reference:

- TS 31.102 [4], clauses 4.4.11.3, 4.4.11.4 and 4.4.11.6;

- TS 33.501 [41], clause 6.1.3.1;

- TS 24.501 [42], clause 5.4.1.2 and Annex C.

#### 15.1A.1.3 Test purpose

1) To verify that the ME forwards the RAND and AUTN received in EAP-request/AKA'-challenge within EAP message IE to the USIM.

2) To verify that the ME returns the EAP message IE with EAP-response/AKA'-challenge in *AUTHENTICATION RESPONSE* message indicating the response calculated in the USIM (RES).

3) To verify that the ME stores 5G NAS security context parameters, consisting of KAMF with the associated key set identifier in EF5GS3GPPNSC on the USIM where service n°122 is "available".

4) To verify that the ME stores the KAUSF, KSEAF for 3GPP access, KSEAF for non-3GPP access, SOR counter and UE parameter update in the EF5GAUTHKEYS on the USIM where service n°123 is "available" and service n°133 is "available".

#### 15.1A.1.4 Method of test

##### 15.1A.1.4.1 Initial conditions

The NG-SS transmits on the BCCH, with the following network parameters:

- TAI (MCC/MNC/TAC): 244/083/000001.

- Access control: unrestricted.

The 5G-NR UICC - support of Rel-16 features is used and the UICC is installed into the ME and the UE is powered on.

##### 15.1A.1.4.2 Procedure

a) Bring up Cell A and the UE is switched on.

b) Upon reception of an *RRCSetupRequest* message from the UE, NG-SS transmits an *RRCSetup* message to the UE followed by reception of an *RRCSetupComplete* message from the UE.

c) After receipt of a *REGISTRATION REQUEST* message from the UE during registration, the NG-SS initiates the EAP-AKA' authentication procedure and sends EAP message IE with EAP-request/AKA'-challenge message in the *AUTHENTICATION REQUEST* message and it uses:

ngKSI:

NAS key set identifier: '000'

TSC: '0'

EAP message: EAP-request/AKA'-challenge

d) Using the EAP-request/AKA'-challenge data received in *AUTHENTICATION REQUEST* message the ME passes the RAND and AUTN to the USIM.

e) The UE shall return the EAP message IE with EAP-response/AKA'-challenge in *AUTHENTICATION RESPONSE* message.

f) After reception of *AUTHENTICATION RESPONSE* message from the UE, the NG-SS sends EAP-success in *SECURITY MODE COMMAND* message, the UE sends a *SECURITY MODE COMPLETE* message.

g) The NG-SS sends a *REGISTRATION ACCEPT* message.

5G-GUTI: 24408300010266436587

TAI: 42 34 80 00 00 01

h) The UE sends a *REGISTRATION COMPLETE* message.

i) The UE is switched off or the UE's radio interface is switched off to perform the *DEREGISTRATION* procedure.

#### 15.1A.1.5 Acceptance criteria

1) After step a) the ME shall read EFUST, EF5GS3GPPNSC and EF5GAUTHKEYS.

2) During step c) the UE shall indicate within the *REGISTRATION REQUEST* for the NAS key set identifier that no key is available.

3) In step d) the ME forwards the RAND and AUTN received in EAP message IE with EAP-request/AKA'-challenge message to the USIM.

4) In step e) the ME shall send *AUTHENTICATION RESPONSE* message with EAP message IE with EAP-response/AKA'-challenge containing the response calculated in the USIM (RES):

- Authentication response message identity: '0101 0111’

- Authentication response parameter: 4 – 16 octets RES value calculated according to 3GPP TS 24.501 [42]

5) In step f) the UE shall send *SECURITY MODE COMPLETE* message.

6) After step f) the ME updates EF5GAUTHKEYS as shown below.

**EF5GAUTHKEYS (5G authentication keys)**

Logically:

KAUSF: 32 bytes, value not checked

KSEAF for 3GPP access:32 bytes, value not checked

KSEAF for non-3GPP access:32 bytes, all values set to 'FF'

SOR counter: 2 bytes, value not checked

UE parameter update counter: 2 bytes, value not checked

Coding:

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Byte** | **B1** | **B2** | **B3** | **..** | **B35** | **B36** | **B37** | **..** |
| Hex | 80 | 20 | xx | xx | 81 | 20 | xx | xx |
|  | **B69** | **B70** | **B71** | **..** | **B103** | **B104** | **B105** | **B106** |
|  | 82 | 20 | FF | FF | 83 | 02 | xx | xx |
|  | **B107** | **B108** | **B109** | **B110** |
|  | 84 | 02 | xx | xx |

7) After step i) the ME updates EF5GS3GPPNSC as shown below.

**EF5GS3GPPNSC (5GS 3GPP Access NAS Security Context)**

Logically:

5GS NAS Security Context:

ngKSI: 00

KAMF:32 bytes, value not checked

Uplink NAS count: any value

Downlink NAS count: any value

Identifiers of selected NAS integrity  
and encryption algorithms: any value

Identifiers of selected EPS NAS  
integrity and encryption algorithms  
for use after mobility to EPS: any value

Coding:

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Byte** | **B1** | **B2** | **B3** | **B4** | **B5** | **B6** | **B7** | **B8** | **B9** | **Bx** |
| Hex | A0 | xx | 80 | 01 | 00 | 81 | xx | xx | … | xx |

### 15.1.2 Authentication procedure for EAP-AKA' – Authentication is successful - GSM UICC

#### 15.1.2.1 Definition and applicability

The purpose of the primary authentication and key agreement procedure is to enable mutual authentication between the UE and the network and to provide keying material that can be used between the UE and network in subsequent security procedures. The UE and the AMF shall support the EAP based primary authentication and key agreement procedure.

The 5G NAS security context parameters from a full native 5G NAS security context shall be stored on the USIM if the corresponding file is present on the USIM as specified in 3GPP TS 31.102 [4]. If the corresponding file is not present on the USIM, this 5GMM parameters is stored in a non-volatile memory in the ME together with the SUPI from the USIM.

During the authentication procedure if the USIM computes a Kc (i.e. GPRS Kc) from CK and IK using conversion function c3 as described in 3GPP TS 33.102 [45], and sends it to the ME, then the ME shall ignore such GPRS Kc and not store the GPRS Kc on USIM or in ME.

#### 15.1.2.2 Conformance requirement

1) The ME shall ignore the GPRS Kc and not store the GPRS Kc on USIM or in ME if the USIM computes a Kc (i.e. GPRS Kc) from CK and IK using conversion function c3 as described in TS 33.102 [45].

2) If Service n°122 and Service n°123 are not available on the USIM, the 5GS 3GPP access NAS security context parameters and the 5G authentication keys shall be stored in the non-volatile memory of the ME.

Reference:

- 3GPP TS 33.501 [41], clause 6.1.3.1;

- 3GPP TS 24.501 [42], clause 5.4.1.2 and Annex C.

#### 15.1.2.3 Test purpose

1) To verify that the ME will ignore the GPRS Kc and will not store the GPRS Kc on USIM or in ME when the USIM computes a Kc (i.e. GPRS Kc) from CK and IK.

2) To verify that the ME stores the 5GS 3GPP access NAS security context parameters and the 5G authentication keys inside the ME non-volatile memory when Service n°122 and Service n°123 are not available on the USIM.

#### 15.1.2.4 Method of test

##### 15.1.2.4.1 Initial conditions

The NG-SS transmits on the BCCH, with the following network parameters:

- TAI (MCC/MNC/TAC): 244/083/000001.

- Access control: unrestricted.

The default UICC is used and installed into the ME.

##### 15.1.2.4.2 Procedure

a) Bring up Cell A and the UE is switched on.

b) The UE sends REGISTRATION REQUEST to NG-SS. Further NG-SS responds with REGISTRATION REJECT (cause: Roaming not allowed in this tracking area), and then UE is switched off.

c) The UE is switched on.

d) Upon reception of an *RRCSetupRequest* message from the UE, NG-SS transmits an *RRCSetup* message to the UE followed by reception of an *RRCSetupComplete* message from the UE.

e) After receipt of a *REGISTRATION REQUEST* message from the UE during registration, the NG-SS initiates the EAP-AKA' authentication procedure and sends EAP message IE with EAP-request/AKA'-challenge message in the *AUTHENTICATION REQUEST* message, uses:

ngKSI:

NAS key set identifier: '000'

TSC: '0'

EAP message: EAP-request/AKA'-challenge

f) Using the 5G authentication challenge data received in *AUTHENTICATION REQUEST* message the ME passes the RAND and AUTN to the USIM, the USIM calculates the response parameter KC (i.e. GPRS Kc) from CK and IK using conversion function c3.

g) After the reception of *AUTHENTICATION RESPONSE* message from the UE, the NG-SS sends a *SECURITY MODE COMMAND* message. The UE sends a *SECURITY MODE COMPLETE* message.

h) The NG-SS sends a *REGISTRATION ACCEPT* message.

5G-GUTI: 24408300010266436587

i) The UE sends a *REGISTRATION COMPLETE* message.

j) The UE is switched off or the UE's radio interface is switched off to perform the *DEREGISTRATION* procedure, then the NG-SS sends the RRCRelease message.

k) The UE is switched on.

l) The UE sends *REGISTRATION REQUEST* message in protected mode using the last calculated KAMF, indicates the 5GS mobile identity information element type "5G-GUTI"

m)The NG-SS sends *REGISTRATION ACCEPT* to the UE.

n) The UE sends a *REGISTRATION COMPLETE* message.

o) The UE is switched off or the UE's radio interface is switched off to perform the *DEREGISTRATION* procedure.

#### 15.1.2.5 Acceptance criteria

1) After step c) the ME shall read EFUST

2) During step e) the UE shall indicate in the *REGISTRATION REQUEST* that no key is available for the NAS key set identifier.

3) In step f) the ME forwards the RAND and AUTN received in *AUTHENTICATION REQUEST* message to the USIM.

4) In step g) the ME shall send *AUTHENTICATION RESPONSE* message contains:

- Authentication response message identity: '0101 0111’

- Authentication response parameter: 16 octets RES value calculated according to 3GPP TS 24.501 [42]

5) During steps g) to i) the ME does not store GPRS Kc on the USIM.

6) In step l) the UE shall indicate in the protected mode *REGISTRATION REQUEST* that NAS key set identifier is set to '000' and TSC is set to '0' and uses the 5GS mobile identity information element type "5G-GUTI" with value:

5G-GUTI: 24408300010266436587.

### 15.1.3 Authentication procedure for EAP-AKA' – AUTN fails on the USIM

#### 15.1.3.1 Definition and applicability

The purpose of the primary authentication and key agreement procedure is to enable mutual authentication between the UE and the network and to provide keying material that can be used between the UE and network in subsequent security procedures. The UE and the AMF shall support the EAP based primary authentication and key agreement procedure.

At receipt of the RAND and AUTN, the USIM shall verify the freshness of the AV' by checking whether AUTN can be accepted as described in 3GPP TS 33.102 [45]. If so, the USIM computes a response RES. The USIM shall return RES, CK, IK to the ME. The ME shall derive CK' and IK'. If the verification of the AUTN fails on the USIM, then the USIM and ME shall proceed as described in clause 6.1.3.3 in 3GPP TS 33.501 [41].

#### 15.1.3.2 Conformance requirement

1) The ME shall forward the RAND and AUTN received in the EAP message IE with EAP-request/AKA'-challenge in the *AUTHENTICATION REQUEST* message to the USIM.

2) If the verification of the AUTN fails on the USIM, then the USIM and ME shall proceed as described in clause 6.1.3.3 in 3GPP TS 33.501 [41].

3) The ME shall return the EAP-Response/AKA-Synchronization-Failure, when the sequence number in the AUTN parameter is incorrect as described in clause 9.6 of RFC 4187 [47].

Reference:

- 3GPP TS 33.501 [41], clause 6.1.3.1 and 6.1.3.3;

- 3GPP TS 24.501 [42], clauses 5.4.1.2.2.1.

- RFC 4187 [47], clause 9.6.

#### 15.1.3.3 Test purpose

1) To verify that the ME forwards the RAND and AUTN received in EAP-request/AKA'-challenge message to the USIM.

2) To verify that the ME returns the EAP-Response/AKA-Synchronization-Failure if the verification of AUTN failed on the USIM due to a synchronisation failure.

#### 15.1.3.4 Method of test

##### 15.1.3.4.1 Initial conditions

The NG-SS transmits on the BCCH, with the following network parameters:

- TAI (MCC/MNC/TAC): 244/083/000001.

- Access control: unrestricted.

The default 5G-NR UICC is used and installed into the ME and the UE is powered on.

##### 15.1.3.4.2 Procedure

a) Bring up Cell A and the UE is switched on.

b) Upon reception of an *RRCSetupRequest* message from the UE, NG-SS transmits an *RRCSetup* message to the UE followed by reception of an *RRCSetupComplete* message from the UE.

c) After receipt of a *REGISTRATION REQUEST* message from the UE during registration, the NG-SS initiates the EAP-AKA' authentication procedure and sends EAP message IE with EAP-request/AKA'-challenge message in the *AUTHENTICATION REQUEST* message contains:

ngKSI:

NAS key set identifier: '000'

TSC: '0'

EAP message: EAP-request/AKA'-challenge

d) Using the EAP-request/AKA'-challenge data received in *AUTHENTICATION REQUEST* message the ME pass the RAND and AUTN to the USIM and starts the timer T3520.

e) The UICC returns AUTS parameter to the ME indicating that the verification of AUTN failed due to a synchronisation failure.

f) The UE transmits the *AUTHENTICATION RESPONSE* messageincluding the EAP-response/AKA'-synchronization-failure message and stops the timer T3520, the NG-SS sends an *AUTHENTICATION REQUEST* message.

g) After the reception of *AUTHENTICATION REQUEST* message from the NG-SS, the ME forwards the received RAND, AUTN to the UICC.

h) After reception of *AUTHENTICATION RESPONSE* message from the UE, the NG-SS sends a *SECURITY MODE COMMAND* message, the UE sends a *SECURITY MODE COMPLETE* message

i) Upon reception of *REGISTRATION ACCEPT* message with a new 5G-GUTI, the UE sends a *REGISTRATION COMPLETE* message.

#### 15.1.3.5 Acceptance criteria

1. In step d) the ME forwards the RAND and AUTN received in *AUTHENTICATION REQUEST* message to the USIM.

2. In step f) the UE sends *AUTHENTICATION RESPONSE* message, including the AT AUTS attribute.

3. After step h) ME shall send *AUTHENTICATION RESPONSE* message contains the response calculated in the USIM (RES).

### 15.1.4 Authentication procedure for EAP-AKA' - after SUPI is changed

#### 15.1.4.1 Definition and applicability

The purpose of the primary authentication and key agreement procedure is to enable mutual authentication between the UE and the network and to provide keying material that can be used between the UE and network in subsequent security procedures. The UE and the AMF shall support the EAP based primary authentication and key agreement procedure.

The 5G NAS security context parameters from a full native 5G NAS security context shall be stored on the USIM if the corresponding file is present on the USIM as specified in 3GPP TS 31.102 [4]. If the corresponding file is not present on the USIM, this 5GMM parameters is stored in a non-volatile memory in the ME together with the SUPI from the USIM. These 5GMM parameters can only be used if the SUPI from the USIM matches the SUPI stored in the non-volatile memory; else the UE shall delete the 5GMM parameters.

#### 15.1.4.2 Conformance requirement

1) The UE shall support the EAP based primary authentication and key agreement procedure.

2) The 5G NAS security context parameters shall be stored on the USIM or in a non-volatile memory in the ME together with the SUPI from the USIM.

3) The UE shall delete the 5GMM parameters if the SUPI from the USIM does not match the SUPI stored in the non-volatile memory.

Reference:

- 3GPP TS 33.501 [41], clause 6.1.3.1;

- 3GPP TS 24.501 [42], clauses 5.4.1.2 and Annex C.

#### 15.1.4.3 Test purpose

1) To verify that the UE generates the 5G NAS security context parameters and stores them inside the non-volatile memory in the ME together with the SUPI from the USIM.

2) To verify that the UE rejects the SECURITY MODE COMMAND with the existing 5G NAS security context parameters if the SUPI is changed.

#### 15.1.4.4 Method of test

15.1.4.4.1 Initial conditions

The NG-SS transmits on the BCCH, with the following network parameters:

- TAI (MCC/MNC/TAC): 244/083/000001.

- Access control: unrestricted.

The default 5G-NR UICC is used with the following exception and installed into the ME.

**EFUST (USIM Service Table)**

Logically:

5GS Mobility Management Information not available

5G Security Parameters not available

|  |  |  |  |
| --- | --- | --- | --- |
| Byte: | B1 | … | B16 |
| Binary: | … | xxx0 100x |

##### 15.1.4.4.2 Procedure

a) Bring up Cell A and the UE is switched on with default IMSI.

b) The UE sends REGISTRATION REQUEST to NG-SS. Further NG-SS responds with REGISTRATION REJECT (cause: Roaming not allowed in this tracking area), and then UE is switched off.

c) The UE is switched on, with IMSI set as 246081685533963.

d) The UE sends REGISTRATION REQUEST to NG-SS. Further NG-SS responds REGISTRATION REJECT (cause: Roaming not allowed in this tracking area), and then UE is switched off.

e) The UE is switched on with default IMSI.

f) Upon reception of an *RRCSetupRequest* message from the UE, NG-SS transmits an *RRCSetup* message to the UE followed by reception of an *RRCSetupComplete* message from the UE.

g) After receipt of a *REGISTRATION REQUEST* message from the UE during registration, the NG-SS initiates the EAP-AKA' authentication procedure and sends EAP message IE with EAP-request/AKA'-challenge message in the *AUTHENTICATION REQUEST* message, uses:

ngKSI:

NAS key set identifier: '000'

TSC: '0'

EAP message: EAP-request/AKA'-challenge

h) After receipt of *AUTHENTICATION RESPONSE* message from the UE, the NG-SS sends a *SECURITY MODE COMMAND* message, then the UE sends a *SECURITY MODE COMPLETE* message.

i) The NG-SS sends a *REGISTRATION ACCEPT* message.

5G-GUTI: 24408300010266436587

TAI: 42 34 80 00 00 01

j) The UE sends a *REGISTRATION COMPLETE* message.

k) The UE is switched off or the UE's radio interface is switched off to perform the *DEREGISTRATION* procedure.

l) Change the UICC configuration (by setting the IMSI to 246081685533963), then switch the UE on.

m) After the receipt of *REGISTRATION REQUEST* message from the UE during registration, the NG-SS performs *AUTHENTICATION* procedure and transmits a *SECURITY MODE COMMAND* message using the last calculated KAMF (at step 'g’) indicated by the ngKSI to activate NAS security.

n) The UE is switched off.

15.1.4.5 Acceptance criteria

1) In step h) the UE sends a SECURITY MODE COMPLETE message.

2) In step m) the UE shall not use the 5G-GUTI or the Last visited registered TAI parameters in the REGISTRATION REQUEST message, instead it shall use SUCI as 5GS mobile identity IE.

3) During step m) the UE shall indicate within the REGISTRATION REQUEST for the NAS key set identifier that no key is available.

4) After step m) and before step n) the UE sends SECURITY MODE REJECT message.

## 15.2 Authentication procedure for 5G AKA

15.2.1 Authentication procedure for 5G AKA - Authentication is successful

15.2.1.1 Definition and applicability

The purpose of the 5G AKA based primary authentication and key agreement procedure is to provide mutual authentication between the UE and the network and to agree on the keys KAUSF, KSEAF and KAMF. The UE and the AMF shall support the 5G AKA based primary authentication and key agreement procedure.

The 5G NAS security context parameters from a full native 5G NAS security context shall be stored on the USIM if the corresponding file is present on the USIM as specified in 3GPP TS 31.102 [4]. If the corresponding file is not present on the USIM, this 5GMM parameters is stored in a non-volatile memory in the ME together with the SUPI from the USIM.

The EF5GS3GPPNSC contains the 5GS 3GPP access NAS security context as defined in 3GPP TS 24.501 [42], consisting of KAMF with the associated key set identifier, the UE security capabilities, and the uplink and downlink NAS COUNT values. This file shall contain one record.

The EF5GAUTHKEYS contains KAUSF and KSEAF that are generated on the ME using CK and IK as part of AKA procedures as described in TS 33.501[41]

15.2.1.2 Conformance requirement

1) The UE shall support the 5G AKA based primary authentication and key agreement procedure.

2) The ME shall forward the RAND and AUTN received in *AUTHENTICATION REQUEST* message to the USIM.

3) The ME shall compute RES\* from RES according to Annex A.4 TS 33.501[41] and return it in *AUTHENTICATION RESPONSE* message.

4) As a result of successful authentication procedure if service n°122 is "available", the 5G NAS security context parameters shall be stored on the USIM.

5) If service n°123 is "available", the ME shall store the KAUSF and KSEAF in EF5GAUTHKEYS on the USIM.

Reference:

- TS 31.102 [4], clauses 4.4.11.3, 4.4.11.4 and 4.4.11.6;

- 3GPP TS 33.501 [41], clause 6.1.3.2;

- 3GPP TS 24.501 [42], clause 5.4.1.3 and Annex C.

15.2.1.3 Test purpose

1) To verify that the ME forwards the RAND and AUTN received in 5G authentication challenge data within *AUTHENTICATION REQUEST* message to the USIM.

2) To verify that the ME sends *AUTHENTICATION RESPONSE* message contains the calculated RES\* in response to *AUTHENTICATION REQUEST* message.

3) To verify that the ME stores 5G NAS security context parameters when entering state 5GMM-DEREGISTERED, consisting of KAMF with the associated key set identifier in EF5GS3GPPNSC on the USIM if service n°122 is "available".

4) To verify that the ME stores the KAUSF and KSEAF in EF5GAUTHKEYS on the USIM if service n°123 is "available".

#### 15.2.1.4 Method of test

##### 15.2.1.4.1 Initial conditions

The NG-SS transmits on the BCCH, with the following network parameters:

- TAI (MCC/MNC/TAC): 244/083/000001.

- Access control: unrestricted.

The default 5G-NR UICC is and the UICC is installed into the ME.

15.2.1.4.2 Procedure

a) Bring up Cell A and the UE is switched on.

b) Upon reception of an *RRCSetupRequest* message from the UE, NG-SS transmits an RRCSetup message to the UE followed by reception of an *RRCSetupComplete* message from the UE.

c) After receipt of a REGISTRATION REQUEST message from the UE during registration, the UE, NG-SS initiates the 5G AKA authentication procedure and sends 5G AKA-Challenge message in the AUTHENTICATION REQUEST message, uses:

ngKSI:

NAS key set identifier: '000'

TSC: '0'

Authentication parameter RAND (5G authentication challenge): 128 bits value

Authentication parameter AUTN (5G Authentication challenge). 128 bits value

d) Using the 5G authentication challenge data received in *AUTHENTICATION REQUEST* message the ME pass the RAND and AUTN to the USIM.

e) Upon reception of *AUTHENTICATION RESPONSE* message from the UE, the NG-SS sends a *SECURITY MODE COMMAND* message. The UE sends a *SECURITY MODE COMPLETE* message.

f) The NG-SS sends a *REGISTRATION ACCEPT* message.

5G-GUTI: 24408300010266436587

TAI: 42 34 80 00 00 01

g) The UE sends a *REGISTRATION COMPLETE* message.

h) The UE is switched off or the UE's radio interface is switched off to perform the *DEREGISTRATION* procedure.

15.2.1.5 Acceptance criteria

1) After step a) the ME shall read EFUST, EF5GS3GPPNSC and EF5GAUTHKEYS.

2) During step c) the UE shall indicate within the *REGISTRATION REQUEST* for the NAS key set identifier that no key is available.

3) In step d) the ME forwards the RAND and AUTN received in *AUTHENTICATION REQUEST* message to the USIM.

4) During step e) the UE sends an *AUTHENTICATION RESPONSE* message contains:

Authentication response parameter: 16 octets RES\* value calculated according to 3GPP TS 24.501 [42]

5) In step e) the UE shall send *SECURITY MODE COMPLETE* message.

6) After step e) the ME updates EF5GAUTHKEYS as shown below.

**EF5GAUTHKEYS (5G authentication keys)**

Logically:

KAUSF: value not checked

KSEAF:value not checked

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Coding:** | **B1** | **B2** | **B3** | **Bx** | **Bx+1** | **Bx+2** | **Bx+3** | **..** | **Bxx** |
| Hex | 80 | L1 | xx | .. | 81 | L2 | xx | .. | xx |

7) After step h) the ME updates EF5GS3GPPNSC as shown below.

**EF5GS3GPPNSC (5GS 3GPP Access NAS Security Context)**

Logically:

5GS NAS Security Context:

ngKSI: 00

KAMF:value not checked

Uplink NAS count: any value

Downlink NAS count: any value

Identifiers of selected NAS integrity  
and encryption algorithms: any value

Identifiers of selected EPS NAS  
integrity and encryption algorithms  
for use after mobility to EPS: any value

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Coding:** | **B1** | **B2** | **B3** | **B4** | **B5** | **B6** | **B7** | **B8** | **B9** | **Bx** |
| Hex | A0 | xx | 80 | 01 | 00 | 81 | xx | xx | … | xx |

15.2A.1 Authentication procedure for 5G AKA - Authentication is successful

15.2A.1.1 Definition and applicability

The purpose of the 5G AKA based primary authentication and key agreement procedure is to provide mutual authentication between the UE and the network and to agree on the keys KAUSF, KSEAF and KAMF. The UE and the AMF shall support the 5G AKA based primary authentication and key agreement procedure.

The 5G NAS security context parameters from a full native 5G NAS security context shall be stored on the USIM if the corresponding file is present on the USIM as specified in 3GPP TS 31.102 [4]. If the corresponding file is not present on the USIM, this 5GMM parameters is stored in a non-volatile memory in the ME together with the SUPI from the USIM.

The EF5GS3GPPNSC contains the 5GS 3GPP access NAS security context as defined in 3GPP TS 24.501 [42], consisting of KAMF with the associated key set identifier, the UE security capabilities, and the uplink and downlink NAS COUNT values. This file shall contain one record.

The EF5GAUTHKEYS contains KAUSF and KSEAF that are generated on the ME using CK and IK as part of AKA procedures as described in 3GPP TS 33.501 [41]. If service n°133 is "available" in EFUST, the EF5GAUTHKEYS also contains SOR counter and UE parameter update counter associated with the key KAUSF as described in 3GPP TS 33.501 [41] and 3GPP TS 31.102 [4].

15.2A.1.2 Conformance requirement

1) The UE shall support the 5G AKA based primary authentication and key agreement procedure.

2) The ME shall forward the RAND and AUTN received in *AUTHENTICATION REQUEST* message to the USIM.

3) The ME shall compute RES\* from RES according to 3GPP TS 33.501 [41], Annex A.4 and return it in *AUTHENTICATION RESPONSE* message.

4) As a result of successful authentication procedure the 5G NAS security context parameters shall be stored on the USIM where service n°122 is "available".

5) The ME shall store the KAUSF, KSEAF for 3GPP access, KSEAF for non-3GPP access, SOR counter and UE parameter update counter in the EF5GAUTHKEYS on the USIM where service n°123 and service n°133 are "available".

Reference:

- TS 31.102 [4], clauses 4.4.11.3, 4.4.11.4 and 4.4.11.6;

- TS 33.501 [41], clause 6.1.3.2;

- TS 24.501 [42], clause 5.4.1.3 and Annex C.

15.2A.1.3 Test purpose

1) To verify that the ME forwards the RAND and AUTN received in 5G authentication challenge data within *AUTHENTICATION REQUEST* message to the USIM.

2) To verify that the ME sends *AUTHENTICATION RESPONSE* message contains the calculated RES\* in response to *AUTHENTICATION REQUEST* message.

3) To verify that the ME stores 5G NAS security context parameters when entering state 5GMM-DEREGISTERED, consisting of KAMF with the associated key set identifier in EF5GS3GPPNSC on the USIM where service n°122 is "available".

4) To verify that the ME stores the KAUSF, KSEAF for 3GPP access, KSEAF for non-3GPP access, SOR counter and UE parameter update in EF5GAUTHKEYS on the USIM where service n°123 is "available" and service n°133 is "available".

#### 15.2A.1.4 Method of test

##### 15.2A.1.4.1 Initial conditions

The NG-SS transmits on the BCCH, with the following network parameters:

- TAI (MCC/MNC/TAC): 244/083/000001.

- Access control: unrestricted.

The 5G-NR UICC - support of Rel-16 features is used and the UICC is installed into the ME.

15.2A.1.4.2 Procedure

a) Bring up Cell A and the UE is switched on.

b) Upon reception of an *RRCSetupRequest* message from the UE, NG-SS transmits an RRCSetup message to the UE followed by reception of an *RRCSetupComplete* message from the UE.

c) After receipt of a REGISTRATION REQUEST message from the UE during registration, the UE, NG-SS initiates the 5G AKA authentication procedure and sends 5G AKA-Challenge message in the AUTHENTICATION REQUEST message, uses:

ngKSI:

NAS key set identifier: '000'

TSC: '0'

Authentication parameter RAND (5G authentication challenge): 128 bits value

Authentication parameter AUTN (5G Authentication challenge). 128 bits value

d) Using the 5G authentication challenge data received in *AUTHENTICATION REQUEST* message the ME pass the RAND and AUTN to the USIM.

e) Upon reception of *AUTHENTICATION RESPONSE* message from the UE, the NG-SS sends a *SECURITY MODE COMMAND* message. The UE sends a *SECURITY MODE COMPLETE* message.

f) The NG-SS sends a *REGISTRATION ACCEPT* message.

5G-GUTI: 24408300010266436587

TAI: 42 34 80 00 00 01

g) The UE sends a *REGISTRATION COMPLETE* message.

h) The UE is switched off or the UE's radio interface is switched off to perform the *DEREGISTRATION* procedure.

15.2A.1.5 Acceptance criteria

1) After step a) the ME shall read EFUST, EF5GS3GPPNSC and EF5GAUTHKEYS.

2) During step c) the UE shall indicate within the *REGISTRATION REQUEST* for the NAS key set identifier that no key is available.

3) In step d) the ME forwards the RAND and AUTN received in *AUTHENTICATION REQUEST* message to the USIM.

4) During step e) the UE sends an *AUTHENTICATION RESPONSE* message contains:

Authentication response parameter: 16 octets RES\* value calculated according to 3GPP TS 24.501 [42]

5) In step e) the UE shall send *SECURITY MODE COMPLETE* message.

6) After step e) the ME updates the EF5GAUTHKEYS as shown below.

**EF5GAUTHKEYS (5G authentication keys)**

Logically:

KAUSF: 32 bytes, value not checked

KSEAF for 3GPP access:32 bytes, value not checked

KSEAF for non-3GPP access:32 bytes, all values set to 'FF'

SOR counter: 2 bytes, value not checked

UE parameter update counter: 2 bytes, value not checked

Coding:

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Byte** | **B1** | **B2** | **B3** | **..** | **B35** | **B36** | **B37** | **..** |
| Hex | 80 | 20 | xx | xx | 81 | 20 | xx | xx |
|  | **B69** | **B70** | **B71** | **..** | **B103** | **B104** | **B105** | **B106** |
|  | 82 | 20 | FF | FF | 83 | 02 | xx | xx |
|  | **B107** | **B108** | **B109** | **B110** |
|  | 84 | 02 | xx | xx |

7) After step h) the ME updates EF5GS3GPPNSC as shown below.

**EF5GS3GPPNSC (5GS 3GPP Access NAS Security Context)**

Logically:

5GS NAS Security Context:

ngKSI: 00

KAMF:value not checked

Uplink NAS count: any value

Downlink NAS count: any value

Identifiers of selected NAS integrity  
and encryption algorithms: any value

Identifiers of selected EPS NAS  
integrity and encryption algorithms  
for use after mobility to EPS: any value

Coding:

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Byte** | **B1** | **B2** | **B3** | **B4** | **B5** | **B6** | **B7** | **B8** | **B9** | **Bx** |
| Hex | A0 | xx | 80 | 01 | 00 | 81 | xx | xx | … | xx |

### 15.2A.2 Authentication procedure for 5G AKA – Authentication is successful - GSM UICC

#### 15.2A.2.1 Definition and applicability

The purpose of the 5G AKA based primary authentication and key agreement procedure is to provide mutual authentication between the UE and the network and to agree on the keys KAUSF, KSEAF and KAMF. The UE and the AMF shall support the 5G AKA based primary authentication and key agreement procedure.

The 5G NAS security context parameters from a full native 5G NAS security context shall be stored on the USIM if the corresponding file is present on the USIM as specified in 3GPP TS 31.102 [4]. If the corresponding file is not present on the USIM, this 5GMM parameters is stored in a non-volatile memory in the ME together with the SUPI from the USIM.

During the authentication procedure if the USIM computes a Kc (i.e. GPRS Kc) from CK and IK using conversion function c3 as described in 3GPP TS  33.102 [45], and sends it to the ME, then the ME shall ignore such GPRS Kc and not store the GPRS Kc on USIM or in ME.

#### 15.2A.2.2 Conformance requirement

1) The ME shall ignore the GPRS Kc and not store the GPRS Kc on USIM or in ME if the USIM computes a Kc (i.e. GPRS Kc) from CK and IK using conversion function c3 as described in 3GPP TS 33.102 [45].

2) If Service n°122 and Service n°123 are not available on the USIM, the 5GS 3GPP access NAS security context parameters and the 5G authentication keys shall be stored in the non-volatile memory of the ME.

Reference:

- 3GPP TS 33.501 [41], clause 6.1.3.1;

- 3GPP TS 24.501 [42], clause 5.4.1.2 and Annex C.

#### 15.2A.2.3 Test purpose

1) To verify that the ME will ignore the GPRS Kc and will not store the GPRS Kc on USIM or in ME when the USIM computes a Kc (i.e. GPRS Kc) from CK and IK.

2) To verify that the ME stores the 5GS 3GPP access NAS security context parameters, the 5G authentication keys, SOR counter and UE parameter update inside the ME non-volatile memory when Service n°122 and Service n°123 and Serivce n°133 are not available on the USIM.

#### 15.2A.2.4 Method of test

##### 15.2A.2.4.1 Initial conditions

The NR-SS transmits on the BCCH, with the following network parameters:

- TAI (MCC/MNC/TAC): 244/083/000001.

- Access control: unrestricted.

The default UICC is used and installed into the ME.

##### 15.2A.2.4.2 Procedure

a) Bring up Cell A and the UE is switched on.

b) The UE sends REGISTRATION REQUEST to NG-SS. Further NG-SS responds with REGISTRATION REJECT (cause: Roaming not allowed in this tracking area), and then UE is switched off.

c) The UE is switched on.

d) Upon reception of an *RRCSetupRequest* message from the UE, NG-SS transmits an RRCSetup message to the UE followed by reception of an *RRCSetupComplete* message from the UE.

e) After receipt of a *REGISTRATION REQUEST* message from the UE during registration, the NG-SS initiates the 5G AKA authentication procedure and sends 5G-AKA-Challenge message in the *AUTHENTICATION REQUEST* message, uses:

ngKSI:

NAS key set identifier: '000'

TSC: '0'

Authentication parameter RAND (5G authentication challenge): 128 bits value

Authentication parameter AUTN (5G Authentication challenge). 128 bits value

f) Using the 5G authentication challenge data received in *AUTHENTICATION REQUEST* message the ME pass the RAND and AUTN to the USIM, the USIM calculates the response parameter KC (i.e. GPRS Kc) from CK and IK using conversion function c3.

g) Upon reception of *AUTHENTICATION RESPONSE* message from the UE, the NG-SS sends a *SECURITY MODE COMMAND* message. The UE sends a *SECURITY MODE COMPLETE* message.

h) The NG-SS sends a REGISTRATION ACCEPT message contains:

5G-GUTI: 24408300010266436587

TAI: 42 34 80 00 00 01

i) The UE sends a *REGISTRATION COMPLETE* message.

j) The UE is switched off or the UE's radio interface is switched off to perform the *DEREGISTRATION* procedure, then the NG-SS sends the RRCRelease message.

k) The UE is switched on.

l) The UE sends *REGISTRATION REQUEST* message in protected mode using the last calculated KAMF, indicates the 5GS mobile identity information element type "5G-GUTI"

m) The NG-SS sends *REGISTRATION ACCEPT* to the UE with:

5G-GUTI: 24408300010266436555

TAI: 42 34 80 00 00 01

n) The UE sends a *REGISTRATION COMPLETE* message.

o) The UE is switched off or the UE's radio interface is switched off to perform the *DEREGISTRATION* procedure.

#### 15.2A.2.5 Acceptance criteria

1) After step c) the ME shall read EFUST.

2) During step e) the UE shall indicate within the *REGISTRATION REQUEST* for the NAS key set identifier that no key is available.

3) In step f) the ME forwards the RAND and AUTN received in *AUTHENTICATION REQUEST* message to the USIM.

4) During step g) the UE sends an *AUTHENTICATION RESPONSE* message contains:

Authentication response parameter: 16 octets RES\* value calculated according to 3GPP TS 24.501 [42].

5) During steps g) to i) the ME does not store GPRS Kc, SOR counter, or UE parameter update counter on the USIM.

6) In step l) the UE shall indicate in protected mode the *REGISTRATION REQUEST* that NAS key set identifier is set to '000' and TSC is set to '0' and uses the 5GS mobile identity information element type "5G-GUTI" with value:

5G-GUTI: 24408300010266436587.

### 15.2.2 Authentication procedure for 5G AKA – Authentication is successful - GSM UICC

#### 15.2.2.1 Definition and applicability

The purpose of the 5G AKA based primary authentication and key agreement procedure is to provide mutual authentication between the UE and the network and to agree on the keys KAUSF, KSEAF and KAMF. The UE and the AMF shall support the 5G AKA based primary authentication and key agreement procedure.

The 5G NAS security context parameters from a full native 5G NAS security context shall be stored on the USIM if the corresponding file is present on the USIM as specified in 3GPP TS 31.102 [4]. If the corresponding file is not present on the USIM, this 5GMM parameters is stored in a non-volatile memory in the ME together with the SUPI from the USIM.

During the authentication procedure if the USIM computes a Kc (i.e. GPRS Kc) from CK and IK using conversion function c3 as described in TS 33.102 [45], and sends it to the ME, then the ME shall ignore such GPRS Kc and not store the GPRS Kc on USIM or in ME.

#### 15.2.2.2 Conformance requirement

1) The ME shall ignore the GPRS Kc and not store the GPRS Kc on USIM or in ME if the USIM computes a Kc (i.e. GPRS Kc) from CK and IK using conversion function c3 as described in TS 33.102 [45].

2) If Service n°122 and Service n°123 are not available on the USIM, the 5GS 3GPP access NAS security context parameters and the 5G authentication keys shall be stored in the non-volatile memory of the ME.

Reference:

- 3GPP TS 33.501 [41], clause 6.1.3.1;

- 3GPP TS 24.501 [42], clause 5.4.1.2 and Annex C.

#### 15.2.2.3 Test purpose

1) To verify that the ME will ignore the GPRS Kc and will not store the GPRS Kc on USIM or in ME when the USIM computes a Kc (i.e. GPRS Kc) from CK and IK.

2) To verify that the ME stores the 5GS 3GPP access NAS security context parameters and the 5G authentication keys inside the ME non-volatile memory when Service n°122 and Service n°123 are not available on the USIM.

#### 15.2.2.4 Method of test

##### 15.2.2.4.1 Initial conditions

The NR-SS transmits on the BCCH, with the following network parameters:

- TAI (MCC/MNC/TAC): 244/083/000001.

- Access control: unrestricted.

The default UICC is used and installed into the ME.

##### 15.2.2.4.2 Procedure

a) Bring up Cell A and the UE is switched on.

b) The UE sends REGISTRATION REQUEST to NG-SS. Further NG-SS responds with REGISTRATION REJECT (cause: Roaming not allowed in this tracking area), and then UE is switched off.

c) The UE is switched on.

d) Upon reception of an *RRCSetupRequest* message from the UE, NG-SS transmits an RRCSetup message to the UE followed by reception of an *RRCSetupComplete* message from the UE.

e) After receipt of a *REGISTRATION REQUEST* message from the UE during registration, the NG-SS initiates the 5G AKA authentication procedure and sends 5G-AKA-Challenge message in the *AUTHENTICATION REQUEST* message, uses:

ngKSI:

NAS key set identifier: '000'

TSC: '0'

Authentication parameter RAND (5G authentication challenge): 128 bits value

Authentication parameter AUTN (5G Authentication challenge). 128 bits value

f) Using the 5G authentication challenge data received in *AUTHENTICATION REQUEST* message the ME pass the RAND and AUTN to the USIM, the USIM calculates the response parameter KC (i.e. GPRS Kc) from CK and IK using conversion function c3.

g) Upon reception of *AUTHENTICATION RESPONSE* message from the UE, the NG-SS sends a *SECURITY MODE COMMAND* message. The UE sends a *SECURITY MODE COMPLETE* message.

h) The NG-SS sends a REGISTRATION ACCEPT message contains:

5G-GUTI: 24408300010266436587

TAI: 42 34 80 00 00 01

i) The UE sends a *REGISTRATION COMPLETE* message.

j) The UE is switched off or the UE's radio interface is switched off to perform the *DEREGISTRATION* procedure, then the NG-SS sends the RRCRelease message.

k) he UE is switched on.

l) The UE sends *REGISTRATION REQUEST* message in protected mode using the last calculated KAMF, indicates the 5GS mobile identity information element type "5G-GUTI"

m) The NG-SS sends *REGISTRATION ACCEPT* to the UE with:

5G-GUTI: 24408300010266436555

TAI: 42 34 80 00 00 01

n) The UE sends a *REGISTRATION COMPLETE* message.

o) The UE is switched off or the UE's radio interface is switched off to perform the *DEREGISTRATION* procedure.

#### 15.2.2.5 Acceptance criteria

1) After step c) the ME shall read EFUST.

2) During step e) the UE shall indicate within the *REGISTRATION REQUEST* for the NAS key set identifier that no key is available.

3) In step f) the ME forwards the RAND and AUTN received in *AUTHENTICATION REQUEST* message to the USIM.

4) During step g) the UE sends an *AUTHENTICATION RESPONSE* message contains:

Authentication response parameter: 16 octets RES\* value calculated according to 3GPP TS 24.501 [42].

5) During steps g) to i) the ME does not store GPRS Kc on the USIM.

6) In step l) the UE shall indicate in protected mode the *REGISTRATION REQUEST* that NAS key set identifier is set to '000' and TSC is set to '0' and uses the 5GS mobile identity information element type "5G-GUTI" with value:

5G-GUTI: 24408300010266436587.

### 15.2.3 Authentication procedure 5G AKA – AUTN fails on the USIM

#### 15.2.3.1 Definition and applicability

The purpose of the primary authentication and key agreement procedure is to enable mutual authentication between the UE and the network and to provide keying material that can be used between the UE and network in subsequent security procedures. The UE and the AMF shall support the EAP based primary authentication and key agreement procedure.

At receipt of the RAND and AUTN, the USIM shall verify the freshness of the AV' by checking whether AUTN can be accepted as described in TS 33.102 [45]. If so, the USIM computes a response RES. The USIM shall return RES, CK, IK to the ME. If the verification of the AUTN fails on the USIM, then the USIM and ME shall proceed as described in clause 6.1.3. 3 in 3GPP TS 33.501 [41].

#### 15.2.3.2 Conformance requirement

1) The ME shall forward the RAND and AUTN received in 5G authentication challenge data within *AUTHENTICATION REQUEST* message*.*

2) If the verification of the AUTN fails on the USIM, then the USIM and ME shall proceed as described in clause 6.1.3. 3 in 3GPP TS 33.501 [41].

3) The ME shall return Synchronization-Failure of AUTH in the *AUTHENTICATION FAILURE* message.

Reference:

- 3GPP TS 33.501 [41], clause 6.1.3.2 and 6.1.3.3;

- 3GPP TS 24.501 [42], clause 5.4.1.3.7

#### 15.2.3.3 Test purpose

1) To verify that the ME forwards the RAND and AUTN received in the 5G authentication challenge message to the USIM.

2) To verify that the ME returns the Synchronization-Failure in the *AUTHENTICATION FAILURE* message if the verification of AUTN failed on the USIM due to a synchronisation failure.

#### 15.2.3.4 Method of test

##### 15.2.3.4.1 Initial conditions

The NG-SS transmits on the BCCH, with the following network parameters:

- TAI (MCC/MNC/TAC): 244/083/000001.

- Access control: unrestricted.

The default 5G-NR UICC is used and installed into the ME.

##### 15.2.3.4.2 Procedure

a) Bring up Cell A and the UE is switched on.

b) Upon reception of an *RRCSetupRequest* message from the UE, NG-SS transmits an *RRCSetup* message to the UE followed by reception of an *RRCSetupComplete* message from the UE.

c) After reception of a *REGISTRATION REQUEST* message from the UE during registration, the NG-SS initiates the 5G AK' authentication procedure and sends 5G AKA challenge data in the *AUTHENTICATION REQUEST* message contains:

ngKSI:

NAS key set identifier: '000'

TSC: '0'

Authentication parameter RAND (5G Authentication challenge): 128 bits value

Authentication parameter AUTN (5G Authentication challenge): 128 bits value

d) Using the data received in *AUTHENTICATION REQUEST* message the ME passes the RAND and AUTN to the USIM.

e) The UICC returns AUTS parameter to the ME indicating that the verification of AUTN failed due to a synchronisation failure.

f) The UE transmits the *AUTHENTICATION FAILURE* messageand starts the timer T3520, the NG-SS sends an *AUTHENTICATION REQUEST* message.

g) After the reception of *AUTHENTICATION REQUEST* message from the NG-SS, the ME forwards the received RAND, AUTN to the UICC and stops the timer T3520.

h) After reception of *AUTHENTICATION RESPONSE* message from the UE, the NG-SS sends a *SECURITY MODE COMMAND* message, the UE sends a *SECURITY MODE COMPLETE* message

i) Upon reception of *REGISTRATION ACCEPT* message with a new 5G-GUTI, the UE sends a *REGISTRATION COMPLETE* message.

#### 15.2.3.5 Acceptance criteria

1) In step d) the ME forwards the RAND and AUTN received in *AUTHENTICATION REQUEST* message to the USIM.

2) In step f) the UE sends *AUTHENTICATION FAILURE* message indicating:

5GMM cause: #21 "Synch failure"

Authentication Failure parameter: AUTS (see 3GPP TS 33.102 [45]

3) In step g) after the reception of *AUTHENTICATION REQUEST* message the UE shall stop the timer T3520.

4) In step h) ME shall send *AUTHENTICATION RESPONSE* message containing the response calculated in the USIM (RES).

### 15.2.4 Authentication procedure for 5G AKA - after SUPI is changed

#### 15.2.4.1 Definition and applicability

The purpose of the 5G AKA based primary authentication and key agreement procedure is to provide mutual authentication between the UE and the network and to agree on the keys KAUSF, KSEAF and KAMF. The UE and the AMF shall support the 5G AKA based primary authentication and key agreement procedure.

The 5G NAS security context parameters from a full native 5G NAS security context shall be stored on the USIM if the corresponding file is present on the USIM as specified in 3GPP TS 31.102 [4]. If the corresponding file is not present on the USIM, this 5GMM parameters is stored in a non-volatile memory in the ME together with the SUPI from the USIM. These 5GMM parameters can only be used if the SUPI from the USIM matches the SUPI stored in the non-volatile memory; else the UE shall delete the 5GMM parameters.

#### 15.2.4.2 Conformance requirement

1) The UE shall support the 5G AKA based primary authentication and key agreement procedure.

2) The 5G NAS security context parameters shall be stored on the USIM if the corresponding file is present on the USIM, else the 5GMM parameters shall be stored in the non-volatile memory in the ME together with the SUPI from the USIM.

3) The UE shall delete the 5GMM parameters if the SUPI from the USIM does not match the SUPI stored in the non-volatile memory.

Reference:

- 3GPP TS 33.501 [41], clause 6.1.3.2;

- 3GPP TS 24.501 [42], clauses 5.4.1.3, Annex C.

#### 15.2.4.3 Test purpose

1) To verify that the UE generates the 5G NAS security context parameters and stores them inside the non-volatile memory in the ME together with the SUPI from the USIM.

2) To verify that the UE rejects the SECURITY MODE COMMAND with the existing 5G NAS security context parameters if the SUPI is changed.

#### 15.2.4.4 Method of test

##### 15.2.4.4.1 Initial conditions

The NG-SS transmits on the BCCH, with the following network parameters:

- TAI (MCC/MNC/TAC): 244/083/000001.

- Access control: unrestricted.

The default 5G-NR UICC is used with the following exceptions and installed into the ME.

**EFUST (USIM Service Table)**

Logically:

5GS Mobility Management Information not available

5G Security Parameters not available

|  |  |  |  |
| --- | --- | --- | --- |
| Byte: | B1 | … | B16 |
| Binary: | … | xxx0 100x |

##### 15.2.4.4.2 Procedure

a) Bring up Cell A and the UE is switched on with default IMSI.

b) The UE sends REGISTRATION REQUEST to NG-SS. Further NG-SS responds with REGISTRATION REJECT (cause: Roaming not allowed in this tracking area), and then UE is switched off.

c) The UE is switched on, with IMSI set as 246081685533963.

d) The UE sends REGISTRATION REQUEST to NG-SS. Further NG-SS responds REGISTRATION REJECT (cause: Roaming not allowed in this tracking area), and then UE is switched off.

e) The UE is switched on with default IMSI.

f) Upon reception of an *RRCSetupRequest* message from the UE, NG-SS transmits an RRCSetup message to the UE followed by reception of an *RRCSetupComplete* message from the UE.

g) After receipt of a *REGISTRATION REQUEST* message from the UE during registration, the NG-SS initiates the 5G AKA authentication procedure and sends 5G AKA challenge message in the *AUTHENTICATION REQUEST* message, uses:

ngKSI:

NAS key set identifier: '000'

TSC: '0'

Authentication parameter RAND (5G Authentication challenge): 128 bits value

Authentication parameter AUTN (5G Authentication challenge). 128 bits value

h) After reception of *AUTHENTICATION RESPONSE* message from the UE, the NG-SS sends a *SECURITY MODE COMMAND* message, then the UE sends a *SECURITY MODE COMPLETE* message.

i) The NG-SS sends a *REGISTRATION ACCEPT* message.

5G-GUTI: 24408300010266436587

TAI: 42 34 80 00 00 01

j) The UE sends a *REGISTRATION COMPLETE* message.

k) The UE is switched off or the UE's radio interface is switched off to perform the *DEREGISTRATION* procedure, then the NG-SS sends *RRCRelease* message.

l) Change the UICC configuration (by setting the IMSI to 246081685533963), then switch the ME on.

m) After the receipt of *REGISTRATION REQUEST* message from the UE during registration, the NG-SS performs *AUTHENTICATION* procedure and transmits a *SECURITY MODE COMMAND* message using the last calculated KAMF (at step 'g’) indicated by the ngKSI to activate NAS security.

n) The UE is switched off.

#### 15.2.4.5 Acceptance criteria

1) In step h) the UE sends a SECURITY MODE COMPLETE message.

2) In step m) the UE shall not use the 5G-GUTI or the Last visited registered TAI parameters in the REGISTRATION REQUEST message, instead it shall use SUCI as 5GS mobile identity IE.

3) During step m) the UE shall indicate within the REGISTRATION REQUEST for the NAS key set identifier that no key is available.

4) After step m) and before step n) the UE sends SECURITY MODE REJECT message.

15.2.5 Authentication procedure for registrations on 3GPP access, 5G AKA - Authentication successful in different PLMNs

15.2.5.1 Definition and applicability

The purpose of the 5G AKA based primary authentication and key agreement procedure is to provide mutual authentication between the UE and the network and to agree on the keys KAUSF, KSEAF and KAMF. The UE and the AMF shall support the 5G AKA based primary authentication and key agreement procedure.

If the UE supports multiple records of NAS security context storage for multiple registration, the UE shall store the previously current 5G NAS security context in the second 5G security context of that access (see 3GPP TS 31.102 [4]) and store the new 5G security context in the first 5G security context, when the UE activates the new 5G security context for a different PLMN over that access but the previously current 5G NAS security context is associated with the 5G-GUTI of the other access.

If the previously current 5G NAS security context is not associated with the 5G-GUTI of the other access (e.g. UE uses only 3GPP access) the second record will not be used.

The EF5GS3GPPNSC contains the 5GS 3GPP access NAS security context as defined in 3GPP TS 24.501 [42], consisting of KAMF with the associated key set identifier, the UE security capabilities, and the uplink and downlink NAS COUNT values. This file shall contain two records if service n°136 is "available".

The EF5GAUTHKEYS contains KAUSF and KSEAF that are generated on the ME using CK and IK as part of AKA procedures as described in 3GPP TS 33.501 [41]. If service n°133 is also "available" in EFUST, the EF5GAUTHKEYS also contains SOR counter and UE parameter update counter associated with the key KAUSF as described in 3GPP TS 33.501 [41] and 3GPP TS 31.102 [4].

#### 15.2.5.2 Conformance requirement

1) The UE shall support the 5G AKA based primary authentication and key agreement procedure.

2) The ME shall forward the RAND and AUTN received in AUTHENTICATION REQUESTmessage to the USIM.

3) The ME shall compute RES\* from RES according to Annex A.4 3GPP TS 33.501 [41] and return it in AUTHENTICATION RESPONSE message.

4) As a result of the first successful authentication procedure in a PLMN (PLMN 1 over 3GPP access), the 5G 3GPP access NAS security context parameters shall be stored on the USIM in the first record of the EF5GS3GPPNSC.

5) As a result of the second successful authentication procedure in another (second) PLMN (PLMN 2 over 3GPP access), and the previously current 5G NAS security context is not associated with the 5G-GUTI of the other access the 5G 3GPP access NAS security context parameters of the PLMN 2 shall be stored on the USIM in the first record of the EF5GS3GPPNSC sincethe previously current 5G NAS security context is not associated with the 5G-GUTI of the other access.

6) The 5G 3GPP access NAS security context parameters of PLMN 1 will be overwritten with the 5G 3GPP access NAS security context parameters of the PLMN 2.The second record of the EF5GS3GPPNSC is not used.

Reference:

- 3GPP TS 31.102 [4], clauses 4.4.11.2, 4.4.11.3, 4.4.11.4, 4.4.11.5 and 4.4.11.6;

- 3GPP TS 33.501 [41], clause 6.1.3.2 and 6.3.2;

- 3GPP TS 24.501 [42], clause 4.4.2.1, 4.4.2.5, 5.4.1.3 and Annex C.

15.2.5.3 Test purpose

1) To verify that the ME forwards the RAND and AUTN received in 5G authentication challenge data from the first PLMN to the USIM within the *AUTHENTICATION REQUEST* message.

2) To verify that the ME sends *AUTHENTICATION RESPONSE* message contains the calculated RES\* in response to *AUTHENTICATION REQUEST* message.

3) To verify that the ME stores 5G 3GPP access NAS security context parameters when entering state 5GMM-DEREGISTERED, consisting of KAMF with the associated key set identifier in the first record of the EF5GS3GPPNSC on the USIM. as service n°122 is "available".

4) To verify that ME forwards the RAND and AUTN received in 5G authentication challenge data from the second PLMN to the USIM within the *AUTHENTICATION REQUEST* message.

5) To verify that the ME sends *AUTHENTICATION RESPONSE* message contains the calculated RES\* in response to *AUTHENTICATION REQUEST* message.

6) To verify that the ME stores (overwrites) 5G 3GPP access NAS security context parameters of the second PLMN (PLMN 2) when entering state 5GMM-DEREGISTERED, consisting of KAMF with the associated key set identifier in the same first record of the EF5GS3GPPNSC on the USIM.

#### 15.2.5.4 Method of test

##### 15.2.5.4.1 Initial conditions

The NG-SS transmits on the BCCH, with the following network parameters:

Cell A –TAI (MCC/MNC/TAC): 244/083/000001.

- CellIdentity: "000000001"

Access control: unrestricted.

Cell B -TAI (MCC/MNC/TAC): 244/084/000001.

- CellIdentity: "000000001"

Access control: unrestricted.

The 5G-NR UICC - support of Rel-16 features is used and the UICC is installed into the ME.

##### 15.2.5.4.2 Procedure

a) Bring up Cell A and the UE is switched on.

b) Upon reception of an *RRCSetupRequest* message from the UE, NG-SS transmits an RRCSetup message to the UE followed by reception of an *RRCSetupComplete* message from the UE.

c) After receipt of a REGISTRATION REQUEST message from the UE during registration, the UE, NG-SS initiates the 5G AKA authentication procedure and sends 5G AKA-Challenge message in the AUTHENTICATION REQUEST message, uses:

ngKSI:

NAS key set identifier: '000'

TSC: '0'

Authentication parameter RAND (5G authentication challenge): 128 bits value

Authentication parameter AUTN (5G Authentication challenge). 128 bits value

d) Using the 5G authentication challenge data received in AUTHENTICATION REQUEST message the ME pass the RAND and AUTN to the USIM.

e) Upon reception of AUTHENTICATION RESPONSE message from the UE, the NG-SS sends a SECURITY MODE COMMAND message. The UE sends a SECURITY MODE COMPLETE message.

f) The NG-SS sends a REGISTRATION ACCEPT message.

5G-GUTI: 24408300010266436587

TAI: 42 34 80 00 00 01

g) The UE sends a REGISTRATION COMPLETE message.

h) The UE is powered down.

i) Bring down Cell A and bring up Cell B.

j) The UE is powered on. The UE reads the first record of the 5G 3GPP NAS security context from the USIM to construct a REGISTRATION REQUEST message. Upon reception of an *RRCSetupRequest* message from the UE, NG-SS transmits an RRCSetup message to the UE followed by reception of an *RRCSetupComplete* message from the UE.

k) After receipt of a REGISTRATION REQUEST message from the UE during registration, the UE, NG-SS initiates the 5G AKA authentication procedure and sends 5G AKA-Challenge message in the AUTHENTICATION REQUEST message, uses:

ngKSI:

NAS key set identifier: '001'

TSC: '0'

Authentication parameter RAND (5G authentication challenge): 128 bits value

Authentication parameter AUTN (5G Authentication challenge). 128 bits value

l) Using the 5G authentication challenge data received in AUTHENTICATION REQUEST message the ME pass the RAND and AUTN to the USIM.

m) Upon reception of AUTHENTICATION RESPONSE message from the UE, the NG-SS sends a SECURITY MODE COMMAND message. The UE sends a SECURITY MODE COMPLETE message.

n) The NG-SS sends a REGISTRATION ACCEPT message.

5G-GUTI: 24408400010266436587

TAI: 42 34 80 00 00 01

o) The UE sends a REGISTRATION COMPLETE message.

p) The UE is switched off or the UE's radio interface is switched off to perform the deregistration procedure.

#### 15.2.5.5 Acceptance criteria

1) After step a) the ME shall read EFUST, EF5GS3GPPNSC and EF5GAUTHKEYS.

2) During step c) the UE shall indicate within the REGISTRATION REQUEST for the NAS key set identifier that no key is available.

3) In step d) the ME forwards the RAND and AUTN received in AUTHENTICATION REQUEST message to the USIM.

4) During step e) the UE sends an AUTHENTICATION RESPONSE message contains:

Authentication response parameter: 16 octets RES\* value calculated according to 3GPP TS 24.501 [42]

5) In step e) the UE shall send SECURITY MODE COMPLETE message.

6) After step e) the ME updates the EF5GAUTHKEYS as shown below.

**EF5GAUTHKEYS (5G authentication keys)**

Logically:

KAUSF: 32 bytes, value not checked

KSEAF for 3GPP access:32 bytes, value not checked

KSEAF for non-3GPP access:32 bytes, all values set to 'FF'

SOR counter: 2 bytes, value not checked

UE parameter update counter: 2 bytes, value not checked

Coding:

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Byte** | **B1** | **B2** | **B3** | **..** | **B35** | **B36** | **B37** | **..** |
| Hex | 80 | 20 | xx | xx | 81 | 20 | xx | xx |
|  | **B69** | **B70** | **B71** | **..** | **B103** | **B104** | **B105** | **B106** |
|  | 82 | 20 | FF | FF | 83 | 02 | xx | xx |
|  | **B107** | **B108** | **B109** | **B110** |
|  | 84 | 02 | xx | xx |

7) After step h) the ME updates EF5GS3GPPNSC as shown below.

**EF5GS3GPPNSC (5GS 3GPP Access NAS Security Context)**

Logically:

5GS NAS Security Context first record:

ngKSI: 000

KAMF:value not checked

Uplink NAS count: any value

Downlink NAS count: any value

Identifiers of selected NAS integrity  
and encryption algorithms: any value

Identifiers of selected EPS NAS  
integrity and encryption algorithms  
for use after mobility to EPS: any value

Coding:

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Byte** | **B1** | **B2** | **B3** | **B4** | **B5** | **B6** | **B7** | **B8** | **B9** | **Bx** |
| Hex | A0 | xx | 80 | 01 | 00 | 81 | xx | xx | … | xx |

5GS NAS Security Context second record:

ngKSI: 007 (no key available)

KAMF:value not checked

Uplink NAS count: any value

Downlink NAS count: any value

Identifiers of selected NAS integrity  
and encryption algorithms: any value

Identifiers of selected EPS NAS  
integrity and encryption algorithms  
for use after mobility to EPS: any value

PLMN: any value

Coding:

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Byte** | **B1** | **B2** | **B3** | **B4** | **B5** | **B6** | **B7** | **B8** | **B9** | **Bx** |
| Hex | A0 | xx | 80 | 01 | 07 | 81 | xx | xx | … | xx |

8) During step j) the ME shall read EFUST, EFLOCI, EF5GS3GPPNSC and EF5GAUTHKEYS. The UE shall indicate within the REGISTRATION REQUEST for the NAS key set identifier the value '000'.

9) In step k) the ME forwards the RAND and AUTN received in AUTHENTICATION REQUEST message to the USIM.

10) During step m) the UE sends an AUTHENTICATION RESPONSE message contains:

Authentication response parameter: 16 octets RES\* value calculated according to 3GPP TS 24.501 [42]

11) In step m) the UE shall send SECURITY MODE COMPLETE message.

12) After step m) as service n°133 is "available", the ME updates the EF5GAUTHKEYS as shown below.

**EF5GAUTHKEYS (5G authentication keys)**

Logically:

KAUSF: 32 bytes, value not checked

KSEAF for 3GPP access:32 bytes, value not checked

KSEAF for non-3GPP access:32 bytes, all values set to 'FF'

SOR counter: 2 bytes, value not checked

UE parameter update counter: 2 bytes, value not checked

Coding:

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Byte** | **B1** | **B2** | **B3** | **..** | **B35** | **B36** | **B37** | **..** |
| Hex | 80 | 20 | xx | xx | 81 | 20 | xx | xx |
|  | **B69** | **B70** | **B71** | **..** | **B103** | **B104** | **B105** | **B106** |
|  | 82 | 20 | FF | FF | 83 | 02 | xx | xx |
|  | **B107** | **B108** | **B109** | **B110** |
|  | 84 | 02 | xx | xx |

13) After step p) the ME updates EF5GS3GPPNSC as shown below.

**EF5GS3GPPNSC (5GS 3GPP Access NAS Security Context)**

Logically:

5GS NAS Security Context first record

ngKSI: 001

KAMF:value not checked

Uplink NAS count: any value

Downlink NAS count: any value

Identifiers of selected NAS integrity  
and encryption algorithms: any value

Identifiers of selected EPS NAS  
integrity and encryption algorithms  
for use after mobility to EPS: any value

Coding:

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Byte** | **B1** | **B2** | **B3** | **B4** | **B5** | **B6** | **B7** | **B8** | **B9** | **Bx** |
| Hex | A0 | xx | 80 | 01 | 01 | 81 | xx | xx | … | xx |

5GS NAS Security Context second record:

ngKSI: 007 (no key available)

KAMF:value not checked

Uplink NAS count: any value

Downlink NAS count: any value

Identifiers of selected NAS integrity  
and encryption algorithms: any value

Identifiers of selected EPS NAS  
integrity and encryption algorithms  
for use after mobility to EPS: any value

PLMN: any value

Coding:

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Byte** | **B1** | **B2** | **B3** | **B4** | **B5** | **B6** | **B7** | **B8** | **B9** | **Bx** |
| Hex | A0 | xx | 80 | 01 | 07 | 81 | xx | xx | … | xx |

## 15.3 Authentication procedure for 5G AKA over non-3GPP access via N3IWF

15.3.1 Authentication procedure for 5G AKA over non-3GPP access, Authentication is successful

15.3.1.1 Definition and applicability

The purpose of the 5G AKA based primary authentication and key agreement procedure is to provide mutual authentication between the UE and the network and to agree on the keys KAUSF, KSEAF and KAMF. The UE and the AMF shall support the 5G AKA based primary authentication and key agreement procedure.

The Authentication server function (AUSF) shall handle authentication requests for both, 3GPP access and non-3GPP access.

The primary authentication and key agreement procedures shall bind the KSEAF to the serving network. This serving network authentication shall be provided to the UE irrespective of the access network technology, so it applies to both 3GPP and non-3GPP access networks.

A UE authenticated to 5G network via an untrusted non-3GPP access network uses a vendor-specific EAP method 'EAP-5G' between the UE and the N3IWF and is utilized for encapsulating NAS messages.

KN3IWF is a key derived by ME and AMF from KAMF for the non-3GPP access. The N3IWF shall use KN3IWF as the key MSK for IKEv2 between UE and N3IWF in the procedures for untrusted non-3GPP access. This key KN3IWF and the IPsec SA cryptographic keys are taken into use with the establishment of IPsec Security Association (SA) between the UE and the N3IWF.

N3IWF sends an EAP-Success/EAP-5G to the UE to complete the EAP session and the IPsec SA is established between the UE and N3IWF by using the N3IWF key KN3IWF

The 5G NAS security context parameters from a full native 5G NAS security context shall be stored on the USIM if the corresponding file EF5GSN3GPPNSC is present on the USIM as specified in 3GPP TS 31.102 [4]. If the corresponding file is not present on the USIM, this 5GMM parameters is stored in a non-volatile memory in the ME together with the SUPI from the USIM.

The EF5GSN3GPPNSC contains the 5GS 3GPP access NAS security context as defined in 3GPP TS 24.501 [42], consisting of KAMF with the associated key set identifier, the UE security capabilities, and the uplink and downlink NAS COUNT values. This file shall contain two records for handling multiple registrations.

The EF5GAUTHKEYS contains KAUSF and KSEAF (separate keys for 3GPP access and non-3GPP access) that are generated on the ME using CK and IK as part of AKA procedures as described in TS 33.501[41]

15.3.1.2 Conformance requirement

1) The UE shall use vendor-specific EAP method 'EAP-5G' between the UE and the N3IWF and is utilized for encapsulating NAS messages

2) The UE shall support the 5G AKA based primary authentication and key agreement procedure using IKE\_AUTH exchange.

3) The ME shall forward the RAND and AUTN received in *AUTHENTICATION REQUEST* message to the USIM.

4) The ME shall compute RES\* from RES according to Annex A.4 TS 33.501[41] and return it in *AUTHENTICATION RESPONSE* message.

5) As a result of successful authentication procedure IPSec SA is established and, the 5G NAS security context parameters stored on the USIM (upon power down or DEREGISTARTION).

6) The ME shall store the KAUSF and KSEAF for 3GPP access and KSEAF for non-3GPP access in EF5GAUTHKEYS on the USIM.

Reference:

- TS 31.102 [4], clauses 4.4.11.3, 4.4.11.4 and 4.4.11.6;

- TS 33.501 [41], clauses 6.1.1.3, 6.1.3.2, 7.2.1;

- TS 24.501 [42], clause 5.4.1.3 and Annex C.

15.3.1.3 Test purpose

1) To verify that ME starts 'EAP-5G' (EAP Response/5G-NAS) between the UE and the N3IWF and is utilized for encapsulating NAS messages.

2) To verify that the ME forwards the RAND and AUTN upon receiving 5G authentication challenge data within *AUTHENTICATION REQUEST* message [EAP Request/5G-NAS/AKA Challenge] to the USIM.

2) To verify that the ME sends *AUTHENTICATION RESPONSE* message [EAP Response/5G-NAS/AKA Challenge] contains the calculated RES\* in response to *AUTHENTICATION REQUEST* message.

3) To verify that ME sends [EAP Response/5G-NAS/Security Mode Complete] and received EAP-Success from N3IWF to confirm IPSec SA is established.

4) To verify that the ME stores 5G NAS security context parameters when entering state 5GMM-DEREGISTERED, consisting of KAMF with the associated key set identifier in EF5GSN3GPPNSC on the USIM.

5) To verify that the ME stores the KAUSF and KSEAF for 3GPP access and KSEAF for non-3GPP access in EF5GAUTHKEYS on the USIM.

#### 15.3.1.4 Method of test

##### 15.3.1.4.1 Initial conditions

The NG-SS WLAN Cell Aw and UE are configured as in clause 4.y. Cell Aw and the N3IWF are in the PLMN 246/081.

The 5G-NR UICC– support of Rel-16 features as defied in clause 4.11 is used and the UICC is installed into the ME.

##### 15.3.1.4.2 Procedure

1. Bring up WLAN AP Cell Aw and the UE is switched on.
2. UE connects to the untrusted non-3GPP access using the WLAN AP. UE associates with the WLAN AP and obtains the local IP address.
3. UE selects the N3IWF and obtains its IP address.
4. The UE establishes an IPsec tunnel as per the IKEv2 protocol as defined in TS 23.502 [xx] clause 4.12.2.2 figure 4.12.2.2-1.
5. The NG-SS transmit EAP-Request/5G-Start.
6. The UE transmits EAP-Response/5G-NAS with NAS PDU [REGISTRATION REQUEST] message.
7. The NG-SS transmits an EAP-Request/5G-NAS with NAS PDU [AUTHENTICATION REQUEST] message including EAP/5G AKA Challenge.

ngKSI:

NAS key set identifier: '000'

TSC: '0'

Authentication parameter RAND (5G authentication challenge): 128 bits value

Authentication parameter AUTN (5G Authentication challenge). 128 bits value

1. Using the 5G authentication challenge data received in AUTHENTICATION REQUEST message the ME pass the RAND and AUTN to the USIM.
2. The UE transmits an EAP-Response/5G-NAS [AUTHENTICATION RESPONSE] message including EAP/5G AKA Challenge with the response received from the USIM.
3. Upon reception of AUTHENTICATION RESPONSE message from the UE, The NG-SS transmits an EAP-Request/5G-NAS with NAS PDU a [SECURITY MODE COMMAND] message including EAP-Success.
4. The UE transmits EAP-Response/5G-NAS with NAS PDU [SECURITY MODE COMPLETE] message.
5. The NG-SS transmits EAP-Success and the IPSec SA is established.
6. The NG-SS transmits a REGISTRATION ACCEPT message over IPSec SA.

5G-GUTI: 24408300010266436587

TAI: 42 34 80 00 00 01

1. The UE transmits a REGISTRATION COMPLETE message over IPSec SA.
2. The UE is switched off or the UE's radio interface is switched off to perform the DEREGISTRATION procedure.

15.3.1.5 Acceptance criteria

1) After step a) the ME shall read EFUST, EF5GSN3GPPNSC, and EF5GAUTHKEYS.

2) During step f) the UE shall transmit EAP-Response/5G-NAS with NAS PDU [REGISTRATION REQUEST] message and the UE shall indicate within the REGISTRATION REQUEST for the NAS key set identifier that no key is available.

3) In step h) the ME forwards the RAND and AUTN received in AUTHENTICATION REQUEST message to the USIM.

4) During step i) the UE sends an AUTHENTICATION RESPONSE message contains:

Authentication response parameter: 16 octets RES\* value calculated according to 3GPP TS 24.501 [42]

5) In step k) the UE shall send SECURITY MODE COMPLETE message.

6) In step l) UE receives EAP-Success to confirm IPSec SA is established.

7) After step m) the ME updates the EF5GAUTHKEYS as shown below.

**EF5GAUTHKEYS (5G authentication keys)**

Logically:

KAUSF: 32 bytes, value not checked

KSEAF for 3GPP access: 32 bytes, all values set to 'FF'

KSEAF for non-3GPP access: 32 bytes,value not checked

SOR counter: 2 bytes, all values set to 'FF'

UE parameter update counter: 2 bytes, all values set to 'FF'

Coding:

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Byte** | **B1** | **B2** | **B3** | **..** | **B35** | **B36** | **B37** | **..** |
| Hex | 80 | 20 | xx | xx | 81 | 20 | FF | FF |
|  | **B69** | **B70** | **B71** | **..** | **B103** | **B104** | **B105** | **B106** |
|  | 82 | 20 | xx | xx | 83 | 02 | FF | FF |
|  | **B107** | **B108** | **B109** | **B110** |
|  | 84 | 02 | FF | FF |

7) After step o) the ME updates EF5GSN3GPPNSC as shown below.

**EF5GSN3GPPNSC (5GS non-3GPP Access NAS Security Context)**

Logically:

5GS NAS Security Context first record:

ngKSI: 000

KAMF:any value

Uplink NAS count: any value

Downlink NAS count: any value

Identifiers of selected NAS integrity  
and encryption algorithms: any value

Identifiers of selected EPS NAS  
integrity and encryption algorithms  
for use after mobility to EPS: any value

Coding:

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Byte** | **B1** | **B2** | **B3** | **B4** | **B5** | **B6** | **B7** | **B8** | **B9** | **Bx** |
| Hex | A0 | xx | 80 | 01 | 00 | 81 | xx | xx | … | xx |

5GS NAS Security Context second record:

ngKSI: 007 (no key available)

KAMF: invalid

Uplink NAS count: invalid

Downlink NAS count: invalid

Identifiers of selected NAS integrity  
and encryption algorithms: invalid

Identifiers of selected EPS NAS  
integrity and encryption algorithms  
for use after mobility to EPS: invalid

PLMN: invalid

Coding:

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Byte** | **B1** | **B2** | **B3** | **B4** | **B5** | **B6** | **B7** | **B8** | **B9** | **Bx** |
| Hex | A0 | xx | 80 | 07 | 00 | 81 | FF | FF | … | FF |

\*\*\*\* Next Change \*\*\*\*

## 15.4 5G AKA Authentication procedure for Multiple registration over 3GPP access and non-3GPP access

15.4.1 5G AKA Authentication is successful in the same PLMN over 3GPP access and non-3GPP access

15.4.1.1 Definition and applicability

The purpose of the 5G AKA based primary authentication and key agreement procedure is to provide mutual authentication between the UE and the network and to agree on the keys KAUSF, KSEAF and KAMF. The UE and the AMF shall support the 5G AKA based primary authentication and key agreement procedure.

The Authentication server function (AUSF) shall handle authentication requests for both, 3GPP access and non-3GPP access.

There are two cases where the UE can be multiple registered in different PLMN's serving networks or in the same PLMN's serving networks. When the UE is registered in a serving network over two types of access (e.g. 3GPP and non-3GPP), then the UE has two active NAS connections with the same AMF. A common 5G NAS security context is created during the registration procedure over the first access type.

Keys for more than one security context can be derived from the KSEAF without the need of a new authentication run. A concrete example of this is that an authentication run over a 3GPP access network can also provide keys to establish security between the UE and a N3IWF used in untrusted non-3GPP access.

The AMF may decide to skip a new authentication run in case there is an available 5G security context for this UE by means of 5G-GUTI, e.g. when the UE successfully registered to 3GPP access. If the UE registers to the same AMF via non-3GPP access, the AMF can decide not to run a new authentication if it has an available security context to use. In this case, the UE shall directly take into use the available common 5G NAS security context and use it to protect the registration over the non-3GPP access.

The primary authentication and key agreement procedures shall bind the KSEAF to the serving network. This serving network authentication shall be provided to the UE irrespective of the access network technology, so it applies to both 3GPP and non-3GPP access networks.

If the UE supports multiple records of NAS security context storage for multiple registration, the UE shall replace the previously current 5G NAS security context stored in the first 5G security context of that access with the new 5G security context (taken into use through a security mode control procedure), when the UE activates the new 5G security context for the same PLMN and access.

The EF5GAUTHKEYS contains KAUSF and KSEAF (keys for 3GPP access and non-3GPP access both) that are generated on the ME using CK and IK as part of AKA procedures as described in TS 33.501[41].

15.4.1.2 Conformance requirement

For 3GPP Access:

1. The UE shall support the 5G AKA based primary authentication and key agreement procedure.
2. The ME shall forward the RAND and AUTN received in *AUTHENTICATION REQUEST* message to the USIM.

The ME shall compute RES\* from RES according to TS 33.501[41]

15.4.1.3 Test purpose

For 3GPP access:

1) To verify that the ME forwards the RAND and AUTN received in 5G authentication challenge data within *AUTHENTICATION REQUEST* message to the USIM.

2) To verify that the ME sends *AUTHENTICATION RESPONSE* message contains the calculated RES\* in response to *AUTHENTICATION REQUEST* message.

3) To verify that the ME stores 5G NAS security context parameters when entering state 5GMM‑DEREGISTERED, consisting of KAMF with the associated key set identifier and NAS COUNTs in the record 1 of EF5GS3GPPNSC on the USIM.

4) To verify that the ME stores the KAUSF and KSEAF for 3GPP access in EF5GAUTHKEYS on the USIM.

For non-3GPP access:

1. To verify that ME starts 'EAP-5G' (EAP Response/5G-NAS) between the UE and the N3IWF and is utilized for encapsulating NAS messages.
2. To verify that ME transmits EAP-Response/5G-NAS with NAS PDU [REGISTRATION REQUEST] message protected, and integrity is verified successfully.
3. To verify that ME receives EAP-Success from N3IWF and IPSec SA is established.
4. To verify that the ME stores 5G NAS security context parameters when entering state 5GMM‑DEREGISTERED, consisting of KAMF with the associated key set identifier and NAS COUNTs in the record 1 of EF5GSN3GPPNSC on the USIM.
5. To verify that the ME stores the KSEAF for non-3GPP access in EF5GAUTHKEYS on the USIM.

#### 15.4.1.4 Method of test

##### 15.4.1.4.1 Initial conditions

For 3GPP access:

The NG-SS Cell A transmits on the BCCH, with the following network parameters:

- TAI (MCC/MNC/TAC): 244/083/000001.

- Access control: unrestricted.

For non-3GPP access:

The NG-SS WLAN Cell Aw and UE are configured as in clause 4y. Cell Aw and N3IWF are in the PLMN 244/083.

The 5G-NR UICC – support of Rel-16 features as defied in clause 4.11 is used and the UICC is installed into the ME.

##### 15.4.1.4.2 Procedure

For 3GPP access, PLMN-A:

1. Bring up Cell A and the UE is switched on.
2. Upon reception of an RRCSetupRequest message from the UE, NG-SS transmits an RRCSetup message to the UE followed by reception of an RRCSetupComplete message from the UE.
3. After receipt of a REGISTRATION REQUEST message from the UE during registration, the UE, NG-SS initiates the 5G AKA authentication procedure and sends 5G AKA-Challenge message in the AUTHENTICATION REQUEST message, uses:

ngKSI:

NAS key set identifier: '000'

TSC: '0'

Authentication parameter RAND (5G authentication challenge): 128 bits value

Authentication parameter AUTN (5G Authentication challenge). 128 bits value

1. Using the 5G authentication challenge data received in AUTHENTICATION REQUEST message the ME pass the RAND and AUTN to the USIM.
2. Upon reception of AUTHENTICATION RESPONSE message from the UE, the NG-SS sends a SECURITY MODE COMMAND message. The UE sends a SECURITY MODE COMPLETE message.
3. The NG-SS sends a REGISTRATION ACCEPT message.

5G-GUTI: 24408300010266436587

TAI: 42 34 80 00 00 01

1. The UE sends a REGISTRATION COMPLETE message.

For non-3GPP access, PLMN-A:

1. Bring up WLAN AP Cell Aw.
2. UE connects to the untrusted non-3GPP access using the WLAN AP. UE associates with the WLAN AP and obtains the local IP address.
3. UE selects the N3IWF and obtains its IP address.
4. The UE establishes an IPsec tunnel as per the IKEv2 protocol as defined in TS 23.502 [xx] clause 4.12.2.2 figure 4.12.2.2-1.
5. The NG-SS transmit EAP-Request/5G-Start.
6. The UE transmits EAP-Response/5G-NAS with NAS PDU [REGISTRATION REQUEST] message protected.
7. The NG-SS transmits EAP-Success and the IPSec SA is established.
8. The NG-SS transmits a REGISTRATION ACCEPT message over IPSec SA.

5G-GUTI: 24408300010266436587

TAI: 42 34 80 00 00 01

1. The UE transmits a REGISTRATION COMPLETE message over IPSec SA.
2. The UE is switched off or the UE's radio interface is switched off to perform the DEREGISTRATION procedure.

15.4.1.5 Acceptance criteria

1) After step a) the ME shall read EFUST, EF5GS3GPPNSC, EF5GSN3GPPNSC, and EF5GAUTHKEYS.

2) During step c) the UE shall indicate within the *REGISTRATION REQUEST* for the NAS key set identifier that no key is available.

3) In step d) the ME forwards the RAND and AUTN received in *AUTHENTICATION REQUEST* message to the USIM.

4) During step e) the UE sends an *AUTHENTICATION RESPONSE* message contains:

Authentication response parameter: 16 octets RES\* value calculated according to TS 24.501 [42]

5) In step e) the UE shall send *SECURITY MODE COMPLETE* message.

6) During step m) the UE transmits EAP-Response/5G-NAS with NAS PDU [REGISTRATION REQUEST] message protected and NG-SS verifies Integrity successfully.

7) In step n) UE receives EAP-Success to confirm IPSec SA is established.

8) After step q) the ME updates the EF5GAUTHKEYS as shown below.

**EF5GAUTHKEYS (5G authentication keys)**

Logically:

KAUSF: 32 bytes, value not checked

KSEAF (for 3GPP access): 32 bytes, value not checked

KSEAF (for non-3GPP access): 32 bytes, value not checked

SOR counter: 2 bytes, invalid

UE parameter update counter: 2 bytes, invalid

Coding:

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Byte** | **B1** | **B2** | **B3** | **..** | **B35** | **B36** | **B37** | **..** |
| Hex | 80 | 20 | xx | xx | 81 | 20 | FF | FF |
|  | **B69** | **B70** | **B71** | **..** | **B103** | **B104** | **B105** | **B106** |
|  | 82 | 20 | xx | xx | 83 | 02 | FF | FF |
|  | **B107** | **B108** | **B109** | **B110** |
|  | 84 | 02 | FF | FF |

9) After step q) the ME updates EF5GS3GPPNSC and EF5GSN3GPPNSC as shown below.

**EF5GS3GPPNSC (5GS 3GPP Access NAS Security Context)**

Logically:

5GS NAS Security Context first record:

ngKSI: 000

KAMF:any value

Uplink NAS count: any value

Downlink NAS count: any value

Identifiers of selected NAS integrity  
and encryption algorithms: any value

Identifiers of selected EPS NAS  
integrity and encryption algorithms  
for use after mobility to EPS: any value

Coding:

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Byte** | **B1** | **B2** | **B3** | **B4** | **B5** | **B6** | **B7** | **B8** | **B9** | **Bx** |
| Hex | A0 | xx | 80 | 01 | 00 | 81 | xx | xx | … | xx |

5GS NAS Security Context second record:

ngKSI: 007 (no key available)

KAMF: invalid

Uplink NAS count: invalid

Downlink NAS count: invalid

Identifiers of selected NAS integrity  
and encryption algorithms: invalid

Identifiers of selected EPS NAS  
integrity and encryption algorithms  
for use after mobility to EPS: invalid

PLMN: invalid

Coding:

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Byte** | **B1** | **B2** | **B3** | **B4** | **B5** | **B6** | **B7** | **B8** | **B9** | **Bx** |
| Hex | A0 | xx | 80 | 01 | 07 | 81 | FF | FF | … | FF |

**EF5GSN3GPPNSC (5GS non-3GPP Access NAS Security Context)**

Logically:

5GS NAS Security Context first record:

ngKSI: same as in EF5GS3GPPNSC

KAMF:same as in EF5GS3GPPNSC

Uplink NAS count: any value

Downlink NAS count: any value

Identifiers of selected NAS integrity  
and encryption algorithms: same as in EF5GS3GPPNSC

Identifiers of selected EPS NAS  
integrity and encryption algorithms  
for use after mobility to EPS: same as in EF5GS3GPPNSC

Coding:

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Byte** | **B1** | **B2** | **B3** | **B4** | **B5** | **B6** | **B7** | **B8** | **B9** | **Bx** |
| Hex | A0 | xx | 80 | 01 | 00 | 81 | xx | xx | … | xx |

5GS NAS Security Context second record:

ngKSI: 007 (no key available)

KAMF:invalid

Uplink NAS count: invalid

Downlink NAS count: invalid

Identifiers of selected NAS integrity  
and encryption algorithms: invalid

Identifiers of selected EPS NAS  
integrity and encryption algorithms  
for use after mobility to EPS: invalid

PLMN: invalid

Coding:

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Byte** | **B1** | **B2** | **B3** | **B4** | **B5** | **B6** | **B7** | **B8** | **B9** | **Bx** |
| Hex | A0 | xx | 80 | 01 | 07 | 81 | FF | FF | … | FF |

15.4.2 5G AKA Authentication is successful in the same PLMN over 3GPP access and non-3GPP access, and then 3GPP access on a different PLMN

15.4.2.1 Definition and applicability

The purpose of the 5G AKA based primary authentication and key agreement procedure is to provide mutual authentication between the UE and the network and to agree on the keys KAUSF, KSEAF and KAMF. The UE and the AMF shall support the 5G AKA based primary authentication and key agreement procedure.

The Authentication server function (AUSF) shall handle authentication requests for both, 3GPP access and non-3GPP access.

There are two cases where the UE can be multiple registered in different PLMN's serving networks or in the same PLMN's serving networks. When the UE is registered in a serving network over two types of access (e.g. 3GPP and non-3GPP), then the UE has two active NAS connections with the same AMF. A common 5G NAS security context is created during the registration procedure over the first access type.

Keys for more than one security context can be derived from the KSEAF without the need of a new authentication run. A concrete example of this is that an authentication run over a 3GPP access network can also provide keys to establish security between the UE and a N3IWF used in untrusted non-3GPP access.

The AMF may decide to skip a new authentication run in case there is an available 5G security context for this UE by means of 5G-GUTI, e.g. when the UE successfully registered to 3GPP access. If the UE registers to the same AMF via non-3GPP access, the AMF can decide not to run a new authentication if it has an available security context to use. In this case, the UE shall directly take into use the available common 5G NAS security context and use it to protect the registration over the non-3GPP access.

The primary authentication and key agreement procedures shall bind the KSEAF to the serving network. This serving network authentication shall be provided to the UE irrespective of the access network technology, so it applies to both 3GPP and non-3GPP access networks.

If the UE supports multiple records of NAS security context storage for multiple registration, the UE shall replace the previously current 5G NAS security context stored in the first 5G security context of that access with the new 5G security context (taken into use through a security mode control procedure), when the UE activates the new 5G security context for the same PLMN and access; or

store the previously current 5G NAS security context in the second 5G security context of that access (see TS 31.102 [22]) and store the new 5G security context (taken into use through a security mode control procedure) in the first 5G security context, when the UE activates the new 5G security context for a different PLMN over that access but the previously current 5G NAS security context is associated with the 5G-GUTI of the other access;

The EF5GAUTHKEYS contains KAUSF and KSEAF (keys for 3GPP access and non-3GPP access both) that are generated on the ME using CK and IK as part of AKA procedures as described in TS 33.501[41].

15.4.2.2 Conformance requirement

For 3GPP Access, PLMN A:

1. The UE shall support the 5G AKA based primary authentication and key agreement procedure.
2. The ME shall forward the RAND and AUTN received in *AUTHENTICATION REQUEST* message to the USIM.
3. The ME shall compute RES\* from RES according to TS 33.501[41], Annex A.4 and return it in *AUTHENTICATION RESPONSE* message.
4. As a result of successful authentication procedure, the 5G NAS security context parameters shall be stored on the record 1 of USIM EF5SG3GPPNSC upon power off or DEREGISTRATION.
5. The ME shall store the KAUSF and KSEAF for 3GPP access in EF5GAUTHKEYS on the USIM

For non-3GPP access, PLMN A:

1. The UE shall use vendor-specific EAP method 'EAP-5G' between the UE and the N3IWF and is utilized for encapsulating NAS messages.
2. The UE transmits EAP-Response/5G-NAS with NAS PDU [REGISTRATION REQUEST] message protected using the common NAS security context (generated during 3GPP access Authentication) and the NAS COUNTs as 0.
3. As a result of successful Integrity verification, IPSec SA is established and the 5G NAS security context parameters shall be stored on the record 1 of USIM EF5SGN3GPPNSC (upon power down or DEREGISTARTION).
4. The ME shall store the KSEAF for non-3GPP access in EF5GAUTHKEYS on the USIM.

For 3GPP Access, PLMN B:

1. The UE shall support the 5G AKA based primary authentication and key agreement procedure for 3GPP access on a new PLMN.
2. As a result of successful authentication procedure, the 5G NAS security context parameters for PLMN B shall be stored on the record 1 of USIM EF5SG3GPPNSC, and 5G NAS security context parameters for PLMN A shall be stored on the record 2 of USIM EF5SG3GPPNSC upon power off or DEREGISTRATION.
3. The ME shall store the KAUSF and KSEAF for 3GPP access on PLMN B in EF5GAUTHKEYS on the USIM

Reference:

- TS 31.102 [4], clauses 4.4.11.3, 4.4.11.4, 4.4.11.6 and Annex O;

- TS 33.501 [41], clauses 6.1.1.3, 6.1.3.2, 7.2.1, 6.3.2.2, 6.4.2.2

- TS 24.501 [42], clauses 4.4.2.1, 5.4.1.3 and Annex C.

15.4.2.3 Test purpose

For 3GPP access, PLMN A:

1. To verify that the ME forwards the RAND and AUTN received in 5G authentication challenge data within *AUTHENTICATION REQUEST* message to the USIM.
2. To verify that the ME sends *AUTHENTICATION RESPONSE* message contains the calculated RES\* in response to *AUTHENTICATION REQUEST* message.
3. To verify that the ME stores 5G NAS security context parameters when entering state 5GMM-DEREGISTERED, consisting of KAMF with the associated key set identifier and NAS COUNTs in the record 1 of EF5GS3GPPNSC on the USIM.
4. To verify that the ME stores the KAUSF and KSEAF for 3GPP access in EF5GAUTHKEYS on the USIM.

For non-3GPP access, PLMN A:

1. To verify that ME starts 'EAP-5G' (EAP Response/5G-NAS) between the UE and the N3IWF and is utilized for encapsulating NAS messages.
2. To verify that ME transmits EAP-Response/5G-NAS with NAS PDU [REGISTRATION REQUEST] message protected, and integrity is verified successfully.
3. To verify that ME receives EAP-Success from N3IWF and IPSec SA is established.
4. To verify that the ME stores 5G NAS security context parameters when entering state 5GMM-DEREGISTERED, consisting of KAMF with the associated key set identifier and NAS COUNTs in the record 1 of EF5GSN3GPPNSC on the USIM.
5. To verify that the ME stores the KSEAF for non-3GPP access in EF5GAUTHKEYS on the USIM.

For 3GPP access, PLMN B:

1. To verify that the ME forwards the RAND and AUTN received in 5G authentication challenge data within AUTHENTICATION REQUEST message received from the PLMN-B to the USIM.
2. To verify that the ME sends AUTHENTICATION RESPONSE message contains the calculated RES\* in response to AUTHENTICATION REQUEST message.
3. To verify that when ME entering state 5GMM-DEREGISTERED, it replaces the data in record 1 of EF5GS3GPPNSC with 5G NAS security context parameters, consisting of KAMF with the associated key set identifier and NAS COUNTs for PLMN-B, and stores the 5G NAS security context parameters of PLMN-A that was in record 1 along with PLMN identity of the PLMN-A on to the second record of EF5GS3GPPNSC.
4. To verify that the ME stores the KAUSF and KSEAF for 3GPP access in EF5GAUTHKEYS on the USIM

#### 15.4.2.4 Method of test

##### 15.4.2.4.1 Initial conditions

For 3GPP access:

The NG-SS transmits on the BCCH, with the following network parameters:

Cell A –TAI (MCC/MNC/TAC): 244/083/000001.

- CellIdentity: "000000001"

Access control: unrestricted.

Cell B -TAI (MCC/MNC/TAC): 244/084/000001.

- CellIdentity: "000000001"

Access control: unrestricted.

For non-3GPP access:

The NG-SS WLAN Cell Aw and UE are configured as in clause 4y. Cell Aw and N3IWF are in the PLMN 244/083.

The default 5G-NR UICC as defied in clause 4.11 is used and the UICC is installed into the ME.

##### 15.4.2.4.2 Procedure

For 3GPP access, PLMN-A:

1. Bring up Cell A and the UE is switched on.
2. Upon reception of an RRCSetupRequest message from the UE, NG-SS transmits an RRCSetup message to the UE followed by reception of an RRCSetupComplete message from the UE.
3. After receipt of a REGISTRATION REQUEST message from the UE during registration, the UE, NG-SS initiates the 5G AKA authentication procedure and sends 5G AKA-Challenge message in the AUTHENTICATION REQUEST message, uses:

ngKSI:

NAS key set identifier: '000'

TSC: '0'

Authentication parameter RAND (5G authentication challenge): 128 bits value

Authentication parameter AUTN (5G Authentication challenge). 128 bits value

1. Using the 5G authentication challenge data received in AUTHENTICATION REQUEST message the ME pass the RAND and AUTN to the USIM.
2. Upon reception of AUTHENTICATION RESPONSE message from the UE, the NG-SS sends a SECURITY MODE COMMAND message. The UE sends a SECURITY MODE COMPLETE message.
3. The NG-SS sends a REGISTRATION ACCEPT message.

5G-GUTI: 24408300010266436587

TAI: 42 34 80 00 00 01

1. The UE sends a REGISTRATION COMPLETE message.

For non-3GPP access, PLMN-A:

1. Bring up WLAN AP Cell Aw.
2. UE connects to the untrusted non-3GPP access using the WLAN AP. UE associates with the WLAN AP and obtains the local IP address.
3. UE selects the N3IWF and obtains its IP address.
4. The UE establishes an IPsec tunnel as per the IKEv2 protocol as defined in TS 23.502 [xx] clause 4.12.2.2 figure 4.12.2.2-1.
5. The NG-SS transmit EAP-Request/5G-Start.
6. The UE transmits EAP-Response/5G-NAS with NAS PDU [REGISTRATION REQUEST] message protected.
7. The NG-SS transmits EAP-Success and the IPSec SA is established.
8. The NG-SS transmits a REGISTRATION ACCEPT message over IPSec SA.

5G-GUTI: 24408300010266436587

TAI: 42 34 80 00 00 01

1. The UE transmits a REGISTRATION COMPLETE message over IPSec SA.

For 3GPP access, PLMN-B:

1. Turn off Cell A and bring up Cell B.
2. After receipt of a REGISTRATION REQUEST message from the UE during registration, the UE, NG-SS initiates the 5G AKA authentication procedure and sends 5G AKA-Challenge message in the AUTHENTICATION REQUEST message, uses:

ngKSI:

NAS key set identifier: '001'

TSC: '0'

Authentication parameter RAND (5G authentication challenge): 128 bits value

Authentication parameter AUTN (5G Authentication challenge). 128 bits value

1. Using the 5G authentication challenge data received in AUTHENTICATION REQUEST message the ME pass the RAND and AUTN to the USIM.
2. Upon reception of AUTHENTICATION RESPONSE message from the UE, the NG-SS sends a SECURITY MODE COMMAND message. The UE sends a SECURITY MODE COMPLETE message.
3. The NG-SS sends a REGISTRATION ACCEPT message.

5G-GUTI: 24408400010266436587

TAI: 42 44 80 00 00 01

1. The UE sends a REGISTRATION COMPLETE message.
2. The UE is switched off or the UE's radio interface is switched off to perform the DEREGISTRATION procedure.

15.4.2.5 Acceptance criteria

1. After step a) the ME shall read EFUST, EF5GS3GPPNSC, EF5GSN3GPPNSC, and EF5GAUTHKEYS
2. During step c) the UE shall indicate within the *REGISTRATION REQUEST* for the NAS key set identifier that no key is available.
3. In step d) the ME forwards the RAND and AUTN received in *AUTHENTICATION REQUEST* message to the USIM.
4. During step e) the UE sends an *AUTHENTICATION RESPONSE* message contains:

Authentication response parameter: 16 octets RES\* value calculated according to TS 24.501 [42]

1. In step e) the UE shall send *SECURITY MODE COMPLETE* message.
2. During step m) the UE transmits EAP-Response/5G-NAS with NAS PDU [REGISTRATION REQUEST] message protected and NG-SS verifies Integrity successfully.
3. In step n) UE receives EAP-Success to confirm IPSec SA is established.
4. In step r) UE initiates REGISTARTION REQUEST over 3GPP access on the new PLMN.
5. In step s) the ME forwards the RAND and AUTN received in *AUTHENTICATION REQUEST* message to the USIM.
6. During step t) the UE sends an *AUTHENTICATION RESPONSE* message contains:

Authentication response parameter: 16 octets RES\* value calculated according to TS 24.501 [42]

and, the UE shall send *SECURITY MODE COMPLETE* message.

1. After step v), the ME updates the EF5GAUTHKEYS as shown below.

**EF5GAUTHKEYS (5G authentication keys)**

Logically:

KAUSF: 32 bytes, any value

KSEAF (for 3GPP access): 32 bytes, any value

KSEAF (for non-3GPP access): 32 bytes, any value

SOR counter: 2 bytes, invalid

UE parameter update counter: 2 bytes, invalid

Coding:

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Byte** | **B1** | **B2** | **B3** | **..** | **B35** | **B36** | **B37** | **..** |
| Hex | 80 | 20 | xx | xx | 81 | 20 | xx | xx |
|  | **B69** | **B70** | **B71** | **..** | **B103** | **B104** | **B105** | **B106** |
|  | 82 | 20 | xx | xx | 83 | 02 | FF | FF |
|  | **B107** | **B108** | **B109** | **B110** |
|  | 84 | 02 | FF | FF |

9) After step w) the ME updates EF5GS3GPPNSC and EF5GSN3GPPNSC as shown below.

**EF5GS3GPPNSC (5GS 3GPP Access NAS Security Context)**

Logically:

5GS NAS Security Context first record:

ngKSI: 001

KAMF:any value

Uplink NAS count: any value

Downlink NAS count: any value

Identifiers of selected NAS integrity  
and encryption algorithms: any value

Identifiers of selected EPS NAS  
integrity and encryption algorithms  
for use after mobility to EPS: any value

Coding:

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Byte** | **B1** | **B2** | **B3** | **B4** | **B5** | **B6** | **B7** | **B8** | **B9** | **Bx** |
| Hex | A0 | xx | 80 | 01 | 00 | 81 | xx | xx | … | xx |

5GS NAS Security Context second record:

ngKSI: 000

KAMF:any value

Uplink NAS count: any value

Downlink NAS count: any value

Identifiers of selected NAS integrity  
and encryption algorithms: any value

Identifiers of selected EPS NAS  
integrity and encryption algorithms  
for use after mobility to EPS: any value

PLMN: 244/083

Coding:

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Byte** | **B1** | **B2** | **B3** | **B4** | **B5** | **B6** | **B7** | **B8** | **…** | **B58** |
| Hex | A0 | xx | 80 | 01 | 00 | 81 | xx | xx | … | 86 |
|  | **B59** | **B60** | **B61** |
|  | 42 | 34 | 80 |

**EF5GSN3GPPNSC (5GS non-3GPP Access NAS Security Context)**

Logically:

5GS NAS Security Context first record:

ngKSI: 000

KAMF:same as in record 2 of EF5GS3GPPNSC

Uplink NAS count: any value

Downlink NAS count: any value

Identifiers of selected NAS integrity  
and encryption algorithms: same as in EF5GS3GPPNSC

Identifiers of selected EPS NAS  
integrity and encryption algorithms  
for use after mobility to EPS: same as in EF5GS3GPPNSC

Coding:

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Byte** | **B1** | **B2** | **B3** | **B4** | **B5** | **B6** | **B7** | **B8** | **B9** | **Bx** |
| Hex | A0 | xx | 80 | 01 | 00 | 81 | xx | xx | … | xx |

5GS NAS Security Context second record:

ngKSI: 007 (no key available)

KAMF: invalid

Uplink NAS count: invalid

Downlink NAS count: invalid

Identifiers of selected NAS integrity  
and encryption algorithms: invalid

Identifiers of selected EPS NAS  
integrity and encryption algorithms  
for use after mobility to EPS: invalid

PLMN: invalid

Coding:

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Byte** | **B1** | **B2** | **B3** | **B4** | **B5** | **B6** | **B7** | **B8** | **B9** | **Bx** |
| Hex | A0 | xx | 80 | 01 | 07 | 81 | FF | FF | … | FF |

# 16 UE Route Selection Policy (URSP) procedure

## 16.1 Pre-configured URSP rules

### 16.1.1 Support for URSP by USIM

#### 16.1.1.1 Definition and applicability

As specified in 3GPP TS 24.526 [50], if the UE has no signalled URSP, and the UE has pre-configured URSPs configured in both the USIM and the ME, then the UE shall use the pre-configured URSP in the USIM.

As specified in 3GPP TS 31.102 [4], the EFURSP in the USIM contains UE Route Selection Policies per PLMN and shall be taken into account by the ME if EFUST service ° 132 "Support for URSP by USIM" is available.

#### 16.1.1.2 Conformance requirement

1) The UE shall support the URSP procedure.

2) The URSP rules shall be read from USIM if service n°132 is "available".

3) The ME shall use the URSP rules from USIM instead of any pre-configured USRP rules in ME if service n°132 is "available".

Reference:

- 3GPP TS 31.102 [4], clauses 5.2.34 and 4.4.11.12;

- 3GPP TS 24.526 [50], clause 4.2.2.2 and 5.2;

- 3GPP TS 23.501 [51], clauses 5.15.5.2 and 5.15.5.3,

- 3GPP TS 23.503 [52], clause 6.6.2.

- 3GPP TS 23.003 [14], clause 9A,

#### 16.1.1.3 Test purpose

1) To verify that the ME reads the URSP rules from USIM if service n°132 is "available".

2) To verify that the ME uses the matching URSP rule from USIM to set the PDU session establishment parameters if service n°132 is "available".

#### 16.1.1.4 Method of test

##### 16.1.1.4.1 Initial conditions

The NG-SS parameters of the system simulator are:

- Mobile Country Code (MCC) = 246;

- Mobile Network Code (MNC) = 081;

- Tracking Area Code (TAC) = 000001;

- NG-SS Cell Id = 0001 (36 bits).

The Allowed S-NSSAI list is configured in NG-SS as '01 01 01 01', '01 01 01 02' and '01 01 01 03'.

The ME is pre-configured with the following URSP rules:

USRP rules for one PLMN only

- PLMN: 246 081

Rule Precedence =1

Traffic descriptor:

- DNN=TestGp.rs

Route Selection Descriptor:

- Precedence=1

- Network Slice Selection, S-NSSAI: 01 01 01 02 (ST: MBB, SD: 010102)

- SSC Mode Selection: SSC Mode 1

- Access Type preference: 3GPP access

Rule Precedence = <lowest priority>

Traffic Descriptor: \*

Route Selection Descriptor:

- Precedence = 1

- Network Slice Selection, S-NSSAI: 01 01 01 01 (ST: MBB, SD: 010101)

- SSC Mode Selection: SSC Mode 1

- DNN Selection: internet

The default 5G-NR UICC is used (with the following additions) and the UICC is installed into the ME.

**EFUST (USIM Service Table)**

Logically:

- User controlled PLMN selector available

- Fixed dialling numbers available

- The GSM Access available

- The Group Identifier level 1 and level 2 not available

- Service n 33 (Packed Switched Domain) shall be set to '1'

- Enabled Services Table available

- EPS Mobility Management Information available

- Allowed CSG Lists and corresponding indications available

- 5GS Mobility Management Information available

- 5G Security Parameters available

- Subscription identifier privacy support available

- SUCI calculation by USIM not available

- Support for URSP by USIM

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Byte: | **B1** | **B2** | **B3** | **B4** | **B5** | **B6** | **B7** | **B8** |
| Binary: | xxxx xx1x | xxxx xxxx | xxxx 1x00 | xxxx x1xx | xxxx xx11 | xxxx xxxx | xxxx xxxx | xxxx xxxx |
|  | **B9** | **B10** | **B11** |  | **B16** | **B17** |  |  |
|  | xxxx xxxx | xxxx xxxx | xx11 xxxx | ..... | xxx0 111x | xxxx 1xxx |  |  |

**EFURSP (URSP)**

Logically:

URSP rules for one PLMN only

- PLMN: 246 081

Rule Precedence = 0

Traffic descriptor:

- DNN = TestGp.rs

Route Selection Descriptor:

- Precedence = 0

- Network Slice Selection, S-NSSAI: '01 01 01 03' (ST: MBB, SD: 010103)

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Coding: | 80 | 22 | 42 | 16 | 80 | 1E | 00 | 1C |
|  | 00 | 00 | 0C | 88 | 0A | 06 | 54 | 65 |
| 73 | 74 | 47 | 70 | 02 | 72 | 73 | 00 |
| 0B | 00 | 09 | 00 | 00 | 06 | 02 | 04 |
| 01 | 01 | 01 | 03 |  |  |  |  |

##### 16.1.1.4.2 Procedure

a) The UE is switched on.

b) The UE is successfull authenticated to PLMN 246 081 and the NG-SS indicates Allowed S-NSSAI list as '01 01 01 01', '01 01 01 02' and '01 01 01 03'.

c) No URSP rules are provisioned by the PCF.

d) The UE tries to connect to DNN=TestGp.rs

e) After reception of the PDU SESSION ESTABLISHMENT REQUEST, the NG-SS sends PDU SESSION ESTABLISHMENT ACCEPT message.

#### 16.1.1.5 Acceptance criteria

1) After step a) the UE shall read EFUST and EFURSP.

2) After step d) the UE sends PDU SESSION ESTABLISHMENT REQUEST to the network via UL NAS TRANSPORT with:

DNN: TestGp.rs

S-NSSAI: '01 01 01 03'

### 16.1.2 Support for URSP by ME

#### 16.1.2.1 Definition and applicability

If the UE has no signalled URSP and the UE has only pre-configured URSPs configured in the ME, then the UE shall use the pre-configured URSP in the ME.

The pre-configured URSP can only be used if the SUPI from the USIM matches the SUPI stored in the non-volatile memory of the ME.

#### 16.1.2.2 Conformance requirement

1) The UE shall support the URSP procedure.

2) The ME shall use the pre-configured URSP rules in the ME if there is no signalled URSP and UE has only pre-configured URSP in the ME.

3) The URSP can only be used if the SUPI from the USIM matches the SUPI stored in the non-volatile memory of the ME.

Reference:

- 3GPP TS 24.526 [50], clause 4.2.2.2 and 5.2;

- 3GPP TS 23.503 [52], clause 6.6.2.

#### 16.1.2.3 Test purpose

1) To verify that the ME uses the matching URSP rule from ME to set the PDU session establishment parameters if there is no signalled URSP and there is no pre-configured URSP in the USIM.

#### 16.1.2.4 Method of test

##### 16.1.2.4.1 Initial conditions

The NG-SS parameters of the system simulator are:

- Mobile Country Code (MCC) = 244;

- Mobile Network Code (MNC) = 083;

- Tracking Area Code (TAC) = 000001;

- NG-SS Cell Id = 0001 (36 bits).

The Allowed S-NSSAI list is configured in NG-SS to include S-NSSAIs ('01 01 01 01’, '01 01 01 01’), and ('01 01 01 02’, '01 01 01 02’).

The ME is pre-configured with the following URSP rules:

USRP rules for one PLMN only

- PLMN: 244 083

Rule Precedence = 1

Traffic descriptor:

- DNN = TestGp.rs

Route Selection Descriptor:

- Precedence = 1

- Network Slice Selection, S-NSSAI: 01 01 01 02 (ST: MBB, SD: 010102)

- SSC Mode Selection: SSC Mode 1

- Access Type preference: 3GPP access

Rule Precedence = <lowest priority>

Traffic Descriptor: \*

Route Selection Descriptor:

- Precedence =1

- Network Slice Selection, S-NSSAI: 01 01 01 01 (ST: MBB, SD: 010101)

- SSC Mode Selection: SSC Mode 1

- DNN Selection: internet

The default 5G-NR UICC is used and the UICC is installed into the ME.

##### 16.1.2.4.2 Procedure

a) The UE is switched on.

b) The UE successfully registers to PLMN 244 083 and the NG-SS indicates Allowed S-NSSAI list as '01 01 01 01' and '01 01 01 02'.

c) No URSP rules are provisioned by the PCF.

d) The UE tries to connect to DNN: TestGp.rs.

e) After reception of the PDU SESSION ESTABLISHMENT REQUEST, the NG-SS sends PDU SESSION ESTABLISHMENT ACCEPT.

#### 16.1.2.5 Acceptance criteria

1) After step a) the UE shall read EFUST.

2) After step d) the UE sends PDU SESSION ESTABLISHMENT REQUEST to the network via UL NAS TRANSPORT with

DNN: TestGp.rs

S-NSSAI: '01 01 01 02'

### 16.1.3 Support of Signalled URSP

#### 16.1.3.1 Definition and applicability

The HPLMN pre-configured URSP in the ME and the HPLMN signalled URSP shall be stored in a non-volatile memory in the ME together with the SUPI from the USIM.

If the UE has both pre-configured URSP(s) and signalled URSP, the UE shall only use the signalled URSP. For a UE not operating in SNPN access mode, if the UE has no signalled URSP, and the UE has pre-configured URSPs configured in both the USIM and the ME, then the UE shall use the pre-configured URSP in the USIM. The HPLMN pre-configured URSP in the ME shall be stored until a new URSP is configured by HPLMN or the USIM is removed.

#### 16.1.3.2 Conformance requirement

1) The UE shall support the URSP procedure.

2) If the UE has both pre-configured URSP(s) and signalled URSP, the UE shall only use the signalled URSP.

Reference:

- 3GPP TS 24.526 [50], clause 4.2.2.2 and 5.2;

- 3GPP TS 23.503 [52], clause 6.6.2.

#### 16.1.3.3 Test purpose

1) To verify that the ME uses signalled URSP when provided rather than pre-configured URSP in the USIM or the ME.

#### 16.1.3.4 Method of test

##### 16.1.3.4.1 Initial conditions

The NG-SS is configured with the following parameters:

- Mobile Country Code (MCC) = 246;

- Mobile Network Code (MNC) = 081;

- Tracking Area Code (TAC) = 000001;

- NG-SS Cell Id = 0001 (36 bits).

The Allowed S-NSSAI list is configured in NG-SS as '01 01 01 01', '01 01 01 02' and '01 01 01 03'.

The ME is pre-configured with the following URSP rules:

USRP rules for one PLMN only

- PLMN: 246 081

Rule Precedence =1

Traffic descriptor:

- DNN=TestGp.rs

Route Selection Descriptor:

- Precedence=1

- Network Slice Selection, S-NSSAI: 01 01 01 01 (ST:MBB, SD: 010101)

- SSC Mode Selection: SSC Mode 1

- Access Type preference: 3GPP access

The default 5G-NR UICC is used with the following exceptions:

**EFUST (USIM Service Table)**

Logically:

- User controlled PLMN selector available

- Fixed dialling numbers available

- The GSM Access available

- The Group Identifier level 1 and level 2 not available

- Service n 33 (Packed Switched Domain) shall be set to '1'

- Enabled Services Table available

- EPS Mobility Management Information available

- Allowed CSG Lists and corresponding indications available

- 5GS Mobility Management Information available

- 5G Security Parameters available

- Subscription identifier privacy support available

- SUCI calculation by USIM not available

- Support for URSP by USIM available

Coding:

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Byte:** | **B1** | **B2** | **B3** | **B4** | **B5** | **B6** | **B7** | **B8** |
| Binary: | xxxx xx1x | xxxx xxxx | xxxx 1x00 | xxxx x1xx | xxxx xx11 | xxxx xxxx | xxxx xxxx | xxxx xxxx |
|  | **B9** | **B10** | **B11** |  | **B16** | **B17** |
|  | xxxx xxxx | xxxx xxxx | xx11 xxxx | ..... | xxx0 111x | xxxx 1xxx |

**EFURSP (URSP)**

Logically:

URSP rules for one PLMN only

- PLMN: 246 081

Rule Precedence = 0

Traffic descriptor:

- DNN=TestGp.rs

Route Selection Descriptor:

- Precedence=0

- Network Slice Selection, S-NSSAI: '01 01 01 02' (ST: MBB, SD: 010102)

Coding:

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Byte:** | **B1** | **B2** | **B3** | **B4** | **B5** | **B6** | **B7** | **B8** | **B9** | **B10** | **B11** | **B12** |
| Hex: | 80 | 22 | 42 | 16 | 80 | 1E | 00 | 1C | 00 | 00 | 0C | 88 |
|  | **B13** | **B14** | **B15** | **B16** | **B17** | **B18** | **B19** | **B20** | **B21** | **B22** | **B23** | **B24** |
|  | 0A | 06 | 54 | 65 | 73 | 74 | 47 | 70 | 02 | 72 | 73 | 00 |
|  | **B25** | **B26** | **B27** | **B28** | **B29** | **B30** | **B31** | **B32** | **B33** | **B34** | **B35** | **B36** |
|  | 0B | 00 | 09 | 00 | 00 | 06 | 02 | 04 | 01 | 01 | 01 | 02 |

##### 16.1.3.4.2 Procedure

a) The UE is switched on;

b) The UE successfully registers to PLMN 246 081 and the NG-SS indicates Allowed S-NSSAI list as '01 01 01 01', '01 01 01 02' and '01 01 01 03';

c) No URSP rules are provisioned by the PCF;

d) The UE tries to connect to DNN=TestGp.rs:

e) After reception of the PDU SESSION ESTABLISHMENT REQUEST, the NG-SS sends PDU SESSION ESTABLISHMENT ACCEPT.

f) The NG-SS releases the PDU Session;

g) The NG-SS sends MANAGE UE POLICY COMMAND to the UE to update the URSP rule for DNN: "TestGp.rs"

Traffic Descriptor: DNN: 'TestGp.rs'

Route Selection Descriptor: S-NSSAI: '01 01 01 03'

h) The UE tries to connect to DNN: TestGp.rs

i) After reception of the PDU SESSION ESTABLISHMENT REQUEST, the NG-SS sends PDU SESSION ESTABLISHMENT ACCEPT.

#### 16.1.3.5 Acceptance criteria

1) After step a) the UE shall read EFUST and EFURSP.

2) After step d) the UE sends PDU SESSION ESTABLISHMENT REQUEST to the network via UL NAS TRANSPORT with

DNN: TestGp.rs

S-NSSAI: '01 01 01 02'

3) After step g) the UE sends MANAGE UE POLICY COMPLETE to the NG-SS

4) After step h) the UE sends PDU SESSION ESTABLISHMENT REQUEST to the network via UL NAS TRANSPORT with

DNN: TestGp.rs

S-NSSAI: '01 01 01 03'

# 17 CAG list handling

## 17.1 CAG list handling for 5G

### 17.1.1 Automatic CAG selection with preconfigured CAG list on USIM

#### 17.1.1.1 Definition and applicability

If MS supports CAG and is pre-configured with a non-empty "CAG information list" stored in the USIM, the MS in automatic PLMN selection mode shall consider a PLMN indicated by an NG-RAN cell only if

1. the cell is a CAG cell and broadcasts a CAG-ID for the PLMN such that there exists an entry with the PLMN ID of the PLMN in the "CAG information list" and the CAG-ID is included in the "Allowed CAG list" of the entry; or
2. the cell is not a CAG cell and:
   1. there is no entry with the PLMN ID of the PLMN in the "CAG information list"; or
   2. there exists an entry with the PLMN ID of the PLMN in the "CAG information list" but the "indication that the MS is only allowed to access 5GS via CAG cells" is not included in the entry.

#### 17.1.1.2 Conformance requirement

1) If service n°137 is "available" in EFUST and preconfigured "CAG information list" is available on USIM, then an ME that supports CAG shall read EFCAG and consider the PLMN indicated by the NG-RAN to perform automatic PLMN selection procedure.

2) If the available CAG cell broadcasts a CAG-ID for the PLMN such that there exists an entry with the PLMN ID of the PLMN in the "CAG information list" and the CAG-ID is included in the "Allowed CAG list" of the entry, then UE shall select the CAG cell.

Reference:

- TS 31.102 [4], clauses 4.4.11.14.

- TS 23.122 [31], clauses 3.8, 4.4.3.1.1

- TS 24.501 [42], clauses 9.11.3.18A

#### 17.1.1.3 Test purpose

To verify that ME only selects the CAG cell if the PLMN ID and CAG ID of the cell is found in the EFCAG (Pre-configured CAG information list) available on USIM.

#### 17.1.1.4 Method of tests

##### 17.1.1.4.1 Initial conditions

The NG-SS is configured with the following network parameters, and both cells are switched off:

CAG Cell A

- TAI (MCC/MNC/TAC): 244/083/000001.

- cag-Identity: 00 00 00 02

CAG Cell B

- TAI (MCC/MNC/TAC): 244/083/000002.

- cag-Identity: 00 00 00 09

The default CAG 5G-NR UICC is used and the UICC is installed into the Terminal.

##### 17.1.1.4.2 Procedure

a) Bring up CAG Cell B, and the UE is switched on.

b) After 5 mins, bring up CAG Cell A and power down Cell B.

c) The UE sends REGISTRATION REQUEST to the available CAG Cell A, indicates the registration type IE as "initial registration".

d) The NG-SS sends REGISTRATION ACCEPT with a 5G-GUTI.

e) The UE sends REGISTRATION COMPLETE to NG-SS.

f) UE is switched off, and then Cell A is powered down.

g) CAG Cell B is powered up again with SIB1 modified to indicate new cag-identity 00 00 00 07.

h) The UE is now switched on.

i) The UE sends REGISTRATION REQUEST to CAG Cell B, indicates the registration type IE as "initial registration".

j) UE is switched off, and then NG-SS is powered down.

##### 17.1.1.4.3 Acceptance criteria

1) After step a) ME shall not attempt registration to CAG Cell B.

2) At step c) ME shall send REGISTRATION REQUEST to CAG Cell A.

3) After step i) ME shall send REGISTRATION REQUEST to CAG Cell B.