3GPP TSG CN Plenary Meeting #16 5th - 7th June 2002. Marco Island, USA.

| Source: | TSG CN WG 1 |
|---------------|--|
| Title: | CR to R99 (with mirror CRs) on Work Item Security towards 24.008 |
| Agenda item: | 7.2 |
| Document for: | APPROVAL |

Introduction:

This document contains **3** CRs on **R99 including mirror CRs on** Work Item "**Security**", that have been agreed by **TSG CN WG1**, and are forwarded to TSG CN Plenary meeting #16 for approval.

| Spec | CR | Rev | Phase | Subject | Cat | Version | Versio | Meeting- | Doc-2nd- |
|--------|-----|-----|-------|--|-----|---------|--------|-----------|-----------|
| | | | | | | Current | n-New | 2nd-Level | Level |
| 24.008 | 623 | 1 | R99 | Conflicting behaviour when UE receives AUTHENTICATION_REJECT | F | 3.11.0 | 3.12.0 | N1-24 | N1-021370 |
| 24.008 | 624 | 1 | Rel 4 | Conflicting behaviour when UE receives AUTHENTICATION_REJECT | A | 4.6.0 | 4.7.0 | N1-24 | N1-021371 |
| 24.008 | 625 | 1 | Rel 5 | Conflicting behaviour when UE receives AUTHENTICATION_REJECT | A | 5.3.0. | 5.4.0 | N1-24 | N1-021372 |

3GPP TSG-CN1 Meeting #24 Budapest, Hungary, 13. – 17. May 2002

Tdoc N1-021236<u>1370</u>

revision of N1-021236

| CHANGE REQUEST | | | | | | | |
|----------------------------------|---|--|--|---|---|---|--|
| ¥ | <mark>24.008</mark> (| CR 623 | жrev | 1 [#] | Current versi | ^{ion:} 3.11.0 [#] | |
| For <u>HELP</u> on us | ing this form | see bottom of th | s page or | look at th | e pop-up text | over the # symbols. | |
| Proposed change a | ffects: ೫ | (U)SIM ME | E/UE X | Radio Ad | ccess Network | Core Network | |
| Title: ೫ | Conflicting b | <mark>ehaviour when U</mark> | E recieves | S AUTHEI | NTICATION_F | REJECT | |
| Source: ೫ | Ericsson | | | | | | |
| Work item code: % | Security | | | | Date: ೫ | 13 th May 2002 | |
| Category: ⊮ | F Use <u>one</u> of the F (correc A (corres B (additi C (functi D (editor Detailed expla be found in 3G | e following categorie tion) sponds to a correction on of feature), onal modification of ial modification) nations of the above SPP <u>TR 21.900</u> . | es: on in an ear feature) e categories | rlier releas s can | Release: % Use <u>one</u> of t 2 e) R96 R97 R98 R99 REL-4 REL-5 | R99 the following releases: (GSM Phase 2) (Release 1996) (Release 1997) (Release 1998) (Release 1999) (Release 4) (Release 5) | |
| Reason for change: | * # Sec. 4. AUTHE 4.3.2.5 <i>MS has</i> <i>conside</i> This sta and 4.1 | 1.1.2.1 and 4.1.1. ENTICATION_RES it is stated that on a separate ongoing r this separate conr atement in sec. 4. | 2.2. state JECT, the n receipt of <i>RR connection as s</i> 3.2.5. is in | that wher GMM sid of AUTHE ction to a d till being g direct co | the MM side e is also affec NTICATION_I <i>lifferent core ne</i> good [*] . nflict with wha | receives ted. However, in sec. REJECT, then " <i>If the</i> etwork node, it shall at is in sec. 4.1.1.2.1 | |
| Summary of change | e: ೫ Delete | the conflicting sta | tement in | sec. 4.3.2 | 2.5 | | |
| Consequences if not approved: | ۲ It is imp | ossible to impleme | ent conflic | ting requi | rements. | | |
| Clauses affected: | ដ <mark> Sec. 4</mark> . | 3.2.5. | | | | | |
| Other specs affected: | # Othe Test O&N | er core specifications specifications A Specifications | ons ¥ | | | | |
| Other comments: | ж | | | | | | |

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at: <u>http://www.3gpp.org/3G_Specs/CRs.htm</u>. Below is a brief summary:

- 1) Fill out the above form. The symbols above marked **#** contain pop-up help information about the field that they are closest to.
- 2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under <u>ftp://ftp.3gpp.org/specs/</u> For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

4.1.1.2.1 GPRS MS operating in mode A or B in a network that operates in mode I

If the network operates in mode I, GPRS MSs that operate in mode A or B and wish to be or are simultaneously IMSI attached for GPRS and non-GPRS services, shall use the combined GPRS attach and the combined and periodic routing area updating procedures instead of the corresponding MM specific procedures IMSI attach and normal and periodic location area updating.

NOTE 1: A GPRS MS operating in mode A or B in a network that operates in mode I, shall perform the combined GPRS attach or routing area update procedure regardless the value of the ATT flag.

If a GPRS MS is operating in mode A or B in a network that operates in mode I the IMSI detach shall be performed by the GMM using the combined GPRS detach procedure

NOTE 2: A GPRS MS operating in mode A or B in a network that operates in mode I, shall perform the combined GPRS detach procedure regardless the value of the ATT flag.

A GPRS MS operating in mode A or B in network that operates in mode I, uses the combined GMM specific procedures in place of the MM specific procedures, so all conditions describing when to trigger a MM specific procedure listed in clauses 4.3 and 4.4 shall not apply.

A GPRS MS operating in mode A or B in a network that operates in mode I should not use any MM timers relating to MM specific procedures, (e.g T3210, T3211, T3212, T3213) except in some error and abnormal cases. If the MM timers are already running, the MS should not react on the expiration of the timers.

NOTE 3: Whenever GMM performs a combined GMM procedure, a GPRS MS enters the MM state MM LOCATION UPDATING PENDING in order to prevent the MM to perform a location update procedure.

If the authentication procedure is performed by MM and the authentication is rejected by the network (i.e upon receive of AUTHENTICATION REJECT), the MS shall in addition set the GPRS update status to GU3 ROAMING NOT ALLOWED and shall, if available, delete the P-TMSI, P-TMSI signature, RAI and GPRS ciphering key sequence number stored. The SIM shall be considered as invalid for GPRS and non-GPRS services until switching off or the SIM is removed. The MS shall abort any GMM procedure and shall enter state GMM-DEREGISTERED.

4.1.1.2.2 GPRS MS operating in mode A or B in a network that operates in mode II or III

If the network operates in mode II or III, a GPRS MSs that operate in mode A or B and wish to be or are simultaneously IMSI attached for GPRS and non-GPRS services, shall use the MM specific procedures listed in clauses 4.3 and 4.4 and the GMM specific procedures listed in clauses 4.7.3, 4.7.4 and 4.7.5. The applicability of periodic location updating is further specified in clause 4.4.2 and the periodic routing area updating is specified in clause 4.7.2.2.

If the authentication procedure is performed by MM and the authentication is rejected by the network (i.e upon receive of AUTHENTICATION REJECT), the MS shall in addition set the GPRS update status to GU3 ROAMING NOT ALLOWED and shall, if available, delete the P-TMSI, P-TMSI signature, RAI and GPRS ciphering key sequence number stored. The SIM shall be considered as invalid for GPRS and non-GPRS services until switching off or the SIM is removed. The MS shall abort any GMM procedure and shall enter state GMM-DEREGISTERED.

4.3.2.5 Authentication not accepted by the network

If authentication fails, i.e. if the response is not valid, the network may distinguish between the two different ways of identification used by the mobile station:

- the TMSI was used;
- the IMSI was used.

If the TMSI has been used, the network may decide to initiate the identification procedure. If the IMSI given by the mobile station then differs from the one the network had associated with the TMSI, the authentication should be restarted with the correct parameters. If the IMSI provided by the MS is the expected one (i.e. authentication has really failed), the network should proceed as described below.

If the IMSI has been used, or the network decides not to try the identification procedure, an AUTHENTICATION REJECT message should be transferred to the mobile station.

After having sent this message, all MM connections in progress (if any) are released and the network should initiate the RR connection release procedure described in clause 3.5.of 04.18 (GSM) or in 3GPP TS 25.331 (UMTS).

Upon receipt of an AUTHENTICATION REJECT message, the mobile station shall set the update status in the SIM to U3 ROAMING NOT ALLOWED, delete from the SIM the stored TMSI, LAI and ciphering key sequence number. The SIM shall be considered as invalid until switching off or the SIM is removed.

If the AUTHENTICATION REJECT message is received in the state IMSI DETACH INITIATED the mobile station shall follow clause 4.3.4.3.

If the AUTHENTICATION REJECT message is received in any other state the mobile station shall abort any MM specific, MM connection establishment or call re-establishment procedure, stop any of the timers T3210 or T3230 (if running), release all MM connections (if any), start timer T3240 and enter the state WAIT FOR NETWORK COMMAND, expecting the release of the RR connection. If the RR connection is not released within a given time controlled by the timer T3240, the mobile station shall abort the RR connection. In both cases, either after a RR connection release triggered from the network side or after a RR connection abort requested by the MS-side, the MS enters state MM IDLE, substate NO IMSI. If the MS has a separate ongoing RR connection to a different core network node, it shall consider this separate connection as still being good.

3GPP TSG-CN1 Meeting #24 Budapest, Hungary, 13. – 17. May 2002

Tdoc N1-021237<u>1371</u>

revision of N1-021237

| ¥ | <mark>24.008</mark> | CR 624 | жrev | 1 [#] | Current versio | ^{on:} 4.6.0 | ж | |
|----------------------------------|---|--|--|---|--|--|--|--|
| For <u>HELP</u> on us | ing this forn | n, see bottom of t | this page or | look at th | ne pop-up text o | ver the # syn | nbols. | |
| Proposed change at | ffects: ೫ | (U)SIM | ME/UE X | Radio A | ccess Network | Core Ne | twork | |
| Title: ೫ | Conflicting | behaviour when | UE recieves | S AUTHE | NTICATION_RE | EJECT | | |
| Source: ೫ | Ericsson | | | | | | | |
| Work item code: ೫ | Security | | | | Date: ೫ | 13 th May 200 | 2 | |
| Category: # | A Use <u>one</u> of th F (corre A (corre B (addit C (funct D (edito Detailed expl be found in 3 | ne following catego ection) esponds to a correction of feature), tional modification of orial modification) anations of the abo GPP <u>TR 21.900</u> . | ries: ction in an ea of feature) ove categorie | rlier releas s can | Release: # Use <u>one</u> of th 2 (C se) R96 (F R97 (F R98 (F R99 (F REL-4 (F REL-5 (F | Rel 4 De following rele GSM Phase 2) Release 1996) Release 1997) Release 1998) Release 1999) Release 4) Release 5) | ases: | |
| Reason for change: | Sec. 4 AUTH 4.3.2. <i>MS hat</i> <i>consid</i> This s and 4. | 1.1.1.2.1 and 4.1. ENTICATION_R 5. it is stated that s a separate ongoin for this separate co tatement in sec. 1.1.2.2. | 1.2.2. state EJECT, the on receipt on <i>RR connection as s</i> 4.3.2.5. is in | that when GMM sid of AUTHE <i>ction to a c</i> <i>till being</i> o direct cc | n the MM side re de is also affecte ENTICATION_R <i>different core network</i> good". | eceives ed. However, EJECT, then <i>work node, it sl</i> is in sec. 4.1. | in sec. <i>"If the</i> hall 1.2.1 | |
| Summary of change | e: # Delete | e the conflicting s | tatement in | sec. 4.3.2 | 2.5 | | | |
| Consequences if not approved: | ж <mark>It is imp</mark> | possible to impler | ment conflic | ting requi | rements. | | | |
| Clauses affected: | 쁐 <mark>Sec. 4</mark> | 1.3.2.5. | | | | | | |
| Other specs affected: | X Oth Tes O& | ner core specifica st specifications M Specifications | itions # | | | | | |
| Other comments: | ж | | | | | | | |

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at: <u>http://www.3gpp.org/3G_Specs/CRs.htm</u>. Below is a brief summary:

- 1) Fill out the above form. The symbols above marked **#** contain pop-up help information about the field that they are closest to.
- 2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under <u>ftp://ftp.3gpp.org/specs/</u> For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

4.1.1.2.1 GPRS MS operating in mode A or B in a network that operates in mode I

If the network operates in mode I, GPRS MSs that operate in mode A or B and wish to be or are simultaneously IMSI attached for GPRS and non-GPRS services, shall use the combined GPRS attach and the combined and periodic routing area updating procedures instead of the corresponding MM specific procedures IMSI attach and normal and periodic location area updating.

NOTE 1: A GPRS MS operating in mode A or B in a network that operates in mode I, shall perform the combined GPRS attach or routing area update procedure regardless the value of the ATT flag.

If a GPRS MS is operating in mode A or B in a network that operates in mode I the IMSI detach shall be performed by the GMM using the combined GPRS detach procedure

NOTE 2: A GPRS MS operating in mode A or B in a network that operates in mode I, shall perform the combined GPRS detach procedure regardless the value of the ATT flag.

A GPRS MS operating in mode A or B in network that operates in mode I, uses the combined GMM specific procedures in place of the MM specific procedures, so all conditions describing when to trigger a MM specific procedure listed in clauses 4.3 and 4.4 shall not apply.

A GPRS MS operating in mode A or B in a network that operates in mode I should not use any MM timers relating to MM specific procedures, (e.g T3210, T3211, T3212, T3213) except in some error and abnormal cases. If the MM timers are already running, the MS should not react on the expiration of the timers.

NOTE 3: Whenever GMM performs a combined GMM procedure, a GPRS MS enters the MM state MM LOCATION UPDATING PENDING in order to prevent the MM to perform a location update procedure.

If the authentication procedure is performed by MM and the authentication is rejected by the network (i.e upon receive of AUTHENTICATION REJECT), the MS shall in addition set the GPRS update status to GU3 ROAMING NOT ALLOWED and shall, if available, delete the P-TMSI, P-TMSI signature, RAI and GPRS ciphering key sequence number stored. The SIM shall be considered as invalid for GPRS and non-GPRS services until switching off or the SIM is removed. The MS shall abort any GMM procedure and shall enter state GMM-DEREGISTERED.

4.1.1.2.2 GPRS MS operating in mode A or B in a network that operates in mode II or III

If the network operates in mode II or III, a GPRS MSs that operate in mode A or B and wish to be or are simultaneously IMSI attached for GPRS and non-GPRS services, shall use the MM specific procedures listed in clauses 4.3 and 4.4 and the GMM specific procedures listed in clauses 4.7.3, 4.7.4 and 4.7.5. The applicability of periodic location updating is further specified in clause 4.4.2 and the periodic routing area updating is specified in clause 4.7.2.2.

If the authentication procedure is performed by MM and the authentication is rejected by the network (i.e upon receive of AUTHENTICATION REJECT), the MS shall in addition set the GPRS update status to GU3 ROAMING NOT ALLOWED and shall, if available, delete the P-TMSI, P-TMSI signature, RAI and GPRS ciphering key sequence number stored. The SIM shall be considered as invalid for GPRS and non-GPRS services until switching off or the SIM is removed. The MS shall abort any GMM procedure and shall enter state GMM-DEREGISTERED.

4.3.2.5 Authentication not accepted by the network

If authentication fails, i.e. if the response is not valid, the network may distinguish between the two different ways of identification used by the mobile station:

- the TMSI was used;
- the IMSI was used.

If the TMSI has been used, the network may decide to initiate the identification procedure. If the IMSI given by the mobile station then differs from the one the network had associated with the TMSI, the authentication should be restarted with the correct parameters. If the IMSI provided by the MS is the expected one (i.e. authentication has really failed), the network should proceed as described below.

If the IMSI has been used, or the network decides not to try the identification procedure, an AUTHENTICATION REJECT message should be transferred to the mobile station.

After having sent this message, all MM connections in progress (if any) are released and the network should initiate the RR connection release procedure described in clause 3.5.of 04.18 (GSM) or in 3GPP TS 25.331 (UMTS).

Upon receipt of an AUTHENTICATION REJECT message, the mobile station shall set the update status in the SIM to U3 ROAMING NOT ALLOWED, delete from the SIM the stored TMSI, LAI and ciphering key sequence number. The SIM shall be considered as invalid until switching off or the SIM is removed.

If the AUTHENTICATION REJECT message is received in the state IMSI DETACH INITIATED the mobile station shall follow clause 4.3.4.3.

If the AUTHENTICATION REJECT message is received in any other state the mobile station shall abort any MM specific, MM connection establishment or call re-establishment procedure, stop any of the timers T3210 or T3230 (if running), release all MM connections (if any), start timer T3240 and enter the state WAIT FOR NETWORK COMMAND, expecting the release of the RR connection. If the RR connection is not released within a given time controlled by the timer T3240, the mobile station shall abort the RR connection. In both cases, either after a RR connection release triggered from the network side or after a RR connection abort requested by the MS-side, the MS enters state MM IDLE, substate NO IMSI. If the MS has a separate ongoing RR connection to a different core network node, it shall consider this separate connection as still being good.

3GPP TSG-CN1 Meeting #24 Budapest, Hungary, 13. – 17. May 2002

Tdoc N1-021238<u>1372</u>

revision of N1-021238

| CHANGE REQUEST | | | | | | | | | CR-Form-v5 | |
|--|---|--|--|---|---------------------|-------|---|---|---|--------|
| ¥ | 24.008 | CR | 625 | жrev | <u>1</u> | ж | Current vers | ion: | 5.3.0 | ж |
| For <u>HELP</u> on us | ing this for | m, see bo | ttom of th | is page or | look a | t the | e pop-up text | over t | he | nbols. |
| Proposed change a | ffects: ೫ | (U)SIM | I MI | E/UE X | Radio | o Ac | cess Network | < 📃 | Core Ne | twork |
| Title: ೫ | Conflicting | g behavio | ur when U | E recieve | s AUTI | HEN | ITICATION_F | REJEC | CT | |
| Source: ೫ | Ericsson | | | | | | | | | |
| Work item code: ℜ | Security | | | | | | Date: ೫ | 13 th | May 200 | 2 |
| Category: # | A Use <u>one</u> of a F (corr A (corr B (ada C (fund D (edia Detailed exp be found in a second | the followin rection) responds to lition of fea ctional modif olanations of 3GPP <u>TR 2</u> | ng categorie ture), dification of ication) of the above 21.900. | es: on in an ea feature) e categorie | rlier rele s can | ease | Release: # Use <u>one</u> of 2 e) R96 R97 R98 R99 REL-4 REL-5 | Rel the foll (GSM (Relea (Relea (Relea (Relea (Relea | 5 lowing rele Phase 2) ase 1996) ase 1997) ase 1998) ase 1999) ase 4) ase 5) /es | pases: |
| AUTHENTICATION_REJECT, the GMM side is also affected. However, 4.3.2.5. it is stated that on receipt of AUTHENTICATION_REJECT, then MS has a separate ongoing RR connection to a different core network node, it is consider this separate connection as still being good". This statement in sec. 4.3.2.5. is in direct conflict with what is in sec. 4.1 and 4.1.1.2.2. | | | | | | | lowever, CT, then <i>node, it s</i> sec. 4.1. | in sec. <i>"If the</i> hall 1.2.1 | | |
| Summary of change | e: ೫ Delet | te the con | flicting sta | tement in | sec. 4 | .3.2 | .5 | | | |
| Consequences if not approved: | ж <mark>It is in</mark> | possible | to implem | ent conflic | ting re | quir | ements. | | | |
| Clauses affected: | ж <mark>Sec.</mark> | 4.3.2.5. | | | | | | | | |
| Other specs affected: | ж Ot Te Ot | her core s est specific &M Specif | specificatio cations fications | ons ¥ | | | | | | |
| Other comments: | ж | | | | | | | | | |

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at: <u>http://www.3gpp.org/3G_Specs/CRs.htm</u>. Below is a brief summary:

- 1) Fill out the above form. The symbols above marked **#** contain pop-up help information about the field that they are closest to.
- 2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under <u>ftp://ftp.3gpp.org/specs/</u> For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

4.1.1.2.1 GPRS MS operating in mode A or B in a network that operates in mode I

If the network operates in mode I, GPRS MSs that operate in mode A or B and wish to be or are simultaneously IMSI attached for GPRS and non-GPRS services, shall use the combined GPRS attach and the combined and periodic routing area updating procedures instead of the corresponding MM specific procedures IMSI attach and normal and periodic location area updating.

NOTE 1: A GPRS MS operating in mode A or B in a network that operates in mode I, shall perform the combined GPRS attach or routing area update procedure regardless the value of the ATT flag.

If a GPRS MS is operating in mode A or B in a network that operates in mode I the IMSI detach shall be performed by the GMM using the combined GPRS detach procedure

NOTE 2: A GPRS MS operating in mode A or B in a network that operates in mode I, shall perform the combined GPRS detach procedure regardless the value of the ATT flag.

A GPRS MS operating in mode A or B in network that operates in mode I, uses the combined GMM specific procedures in place of the MM specific procedures, so all conditions describing when to trigger a MM specific procedure listed in clauses 4.3 and 4.4 shall not apply.

A GPRS MS operating in mode A or B in a network that operates in mode I should not use any MM timers relating to MM specific procedures, (e.g T3210, T3211, T3212, T3213) except in some error and abnormal cases. If the MM timers are already running, the MS should not react on the expiration of the timers.

NOTE 3: Whenever GMM performs a combined GMM procedure, a GPRS MS enters the MM state MM LOCATION UPDATING PENDING in order to prevent the MM to perform a location update procedure.

If the authentication procedure is performed by MM and the authentication is rejected by the network (i.e upon receive of AUTHENTICATION REJECT), the MS shall in addition set the GPRS update status to GU3 ROAMING NOT ALLOWED and shall, if available, delete the P-TMSI, P-TMSI signature, RAI and GPRS ciphering key sequence number stored. The SIM shall be considered as invalid for GPRS and non-GPRS services until switching off or the SIM is removed. The MS shall abort any GMM procedure and shall enter state GMM-DEREGISTERED.

4.1.1.2.2 GPRS MS operating in mode A or B in a network that operates in mode II or III

If the network operates in mode II or III, a GPRS MSs that operate in mode A or B and wish to be or are simultaneously IMSI attached for GPRS and non-GPRS services, shall use the MM specific procedures listed in clauses 4.3 and 4.4 and the GMM specific procedures listed in clauses 4.7.3, 4.7.4 and 4.7.5. The applicability of periodic location updating is further specified in clause 4.4.2 and the periodic routing area updating is specified in clause 4.7.2.2.

If the authentication procedure is performed by MM and the authentication is rejected by the network (i.e upon receive of AUTHENTICATION REJECT), the MS shall in addition set the GPRS update status to GU3 ROAMING NOT ALLOWED and shall, if available, delete the P-TMSI, P-TMSI signature, RAI and GPRS ciphering key sequence number stored. The SIM shall be considered as invalid for GPRS and non-GPRS services until switching off or the SIM is removed. The MS shall abort any GMM procedure and shall enter state GMM-DEREGISTERED.

4.3.2.5 Authentication not accepted by the network

If authentication fails, i.e. if the response is not valid, the network may distinguish between the two different ways of identification used by the mobile station:

- the TMSI was used;
- the IMSI was used.

If the TMSI has been used, the network may decide to initiate the identification procedure. If the IMSI given by the mobile station then differs from the one the network had associated with the TMSI, the authentication should be restarted with the correct parameters. If the IMSI provided by the MS is the expected one (i.e. authentication has really failed), the network should proceed as described below.

If the IMSI has been used, or the network decides not to try the identification procedure, an AUTHENTICATION REJECT message should be transferred to the mobile station.

After having sent this message, all MM connections in progress (if any) are released and the network should initiate the RR connection release procedure described in clause 3.5.of 04.18 (GSM) or in 3GPP TS 25.331 (UMTS).

Upon receipt of an AUTHENTICATION REJECT message, the mobile station shall set the update status in the SIM to U3 ROAMING NOT ALLOWED, delete from the SIM the stored TMSI, LAI and ciphering key sequence number. The SIM shall be considered as invalid until switching off or the SIM is removed.

If the AUTHENTICATION REJECT message is received in the state IMSI DETACH INITIATED the mobile station shall follow clause 4.3.4.3.

If the AUTHENTICATION REJECT message is received in any other state the mobile station shall abort any MM specific, MM connection establishment or call re-establishment procedure, stop any of the timers T3210 or T3230 (if running), release all MM connections (if any), start timer T3240 and enter the state WAIT FOR NETWORK COMMAND, expecting the release of the RR connection. If the RR connection is not released within a given time controlled by the timer T3240, the mobile station shall abort the RR connection. In both cases, either after a RR connection release triggered from the network side or after a RR connection abort requested by the MS-side, the MS enters state MM IDLE, substate NO IMSI. If the MS has a separate ongoing RR connection to a different core network node, it shall consider this separate connection as still being good.