3GPP TSG CN Plenary Meeting #20 **NP-030267**
4th - 6th June 2003. HÄMEENLINNA, Finland.

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 **4** CRs, **R99 to** Work Item **"Security"**, that have been agreed by **TSG CN WG1**, and are forwarded to TSG CN Plenary meeting #20 for approval.

Spec	CR	Rev	Cat	Phase	Subject	Version-Current	Version-New	Meeting-2nd-Level	Doc-2nd-Level
24.008	773		F	R99	Unciphered transmission of Authentication and Ciphering Failure in A/Gb mode	3.15.0	3.16.0	N1-30	N1-030666
24.008	774		A	Rel-4	Unciphered transmission of Authentication and Ciphering Failure in A/Gb mode	4.10.0	4.11.0	N1-30	N1-030667
24.008	775		A	Rel-5	Unciphered transmission of Authentication and Ciphering Failure in A/Gb mode	5.7.0	5.8.0	N1-30	N1-030668
24.008	776		A	Rel-6	Unciphered transmission of Authentication and Ciphering Failure in A/Gb mode	6.0.0	6.1.0	N1-30	N1-030669

3GPP TSG-CN1 Meeting #30 *Tdoc N1-030666*
San Diego, California, USA, 19 – 23 May 2003

CR-Form-v7

CHANGE REQUEST

⌘ **24.008** **CR** **773** ⌘ **rev** **-** ⌘ Current version: **3.15.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ [ ] ME [X] Radio Access Network [ ] Core Network [X]

Title:	⌘	Unciphered transmission of Authentication and Ciphering Failure in A/Gb mode
Source:	⌘	Siemens AG
Work item code:	⌘	Security
Date:	⌘	09/04/2003
Category:	⌘	**F**
Release:	⌘	R99

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:
2 (GSM Phase 2)
R96 (Release 1996)
R97 (Release 1997)
R98 (Release 1998)
R99 (Release 1999)
Rel-4 (Release 4)
Rel-5 (Release 5)
Rel-6 (Release 6)

Reason for change: ⌘

Since R97, according to subclause 4.7.1.2, the following applies in GSM (or A/Gb mode):
"If ciphering is to be applied on a GMM context, all GMM messages shall be ciphered except the following messages: …"

The list that follows contains
- AUTHENTICATION AND CIPHERING REQUEST,
- AUTHENTICATION AND CIPHERING RESPONSE, and
- AUTHENTICATION AND CIPHERING REJECT,

but not the AUTHENTICATION AND CIPHERING FAILURE message that was added later, in R99, for the UMTS authentication procedure.

However, when the MS sends a ciphered AUTHENTICATION AND CIPHERING FAILURE, as a rule the network will not be able to decipher the message:

- firstly, because in the network, according to subclause 4.7.7.3, the LLC sublayer is notified "if ciphering shall be used or not and if yes which algorithm and GPRS GSM ciphering key that shall be used" only **after** the network has received an AUTHENTICATION AND CIPHERING RESPONSE message.
- secondly, because either the necessary GPRS ciphering key is not available (which was the reason for performing an authentication and key agreement) or because the network got the P-TMSI / IMSI correlation wrong, assumes it is talking to a different subscriber and uses a wrong GPRS ciphering key.

Consequently, the network cannot decide whether the authentication challenge was rejected because of a MAC failure or Synch failure and cannot take the appropriate actions (e.g. perform ID-Request, or get new authentication parameters from the HLR).

Summary of change: ⌘ The AUTHENTICATION AND CIPHERING FAILURE message is added to the

		list of unciphered messages.
Consequences if not approved:	⌘	Inconsistent specification. If an MS implementation sends a ciphered AUTHENTICATION AND CIPHERING FAILURE message (with whatever GPRS ciphering key available), chances are that the network will not be able to decipher the message and that authentication will aborted after four re-transmissions. Depending on the further network reaction, in the worst case the MS will not be able to get PS services.

Clauses affected:	⌘	4.7.1.2			
		Y	**N**		
Other specs affected:	⌘		**X**	Other core specifications	⌘
			X	Test specifications	
			X	O&M Specifications	
Other comments:	⌘				

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm. 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 ftp://ftp.3gpp.org/specs/ 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.

4.7.1.2 Ciphering of messages (GSM only)

If ciphering is to be applied on a GMM context, all GMM messages shall be ciphered except the following messages:

-- ATTACH REQUEST;

-- ATTACH REJECT;

-- AUTHENTICATION AND CIPHERING REQUEST;

-- AUTHENTICATION AND CIPHERING RESPONSE;

-- AUTHENTICATION AND CIPHERING FAILURE;

-- AUTHENTICATION AND CIPHERING REJECT;

-- IDENTITY REQUEST;

-- IDENTITY RESPONSE;

-- ROUTING AREA UPDATE REQUEST; and

-- ROUTING AREA UPDATE REJECT.

********** NEXT SECTION INCLUDED FOR INFORMATION *********

4.7.7.3 Authentication and ciphering completion by the network

Upon receipt of the AUTHENTICATION AND CIPHERING RESPONSE message, the network stops the timer T3360 and checks the validity of the response (see 3GPP TS 03.20 [13] and 3GPP TS 33.102). For this, it may use the A&C reference number information element within the AUTHENTICATION AND CIPHERING RESPONSE message to determine whether the response is correlating to the last request that was sent.

In GSM, the GMM layer shall notify the LLC sublayer if ciphering shall be used or not and if yes which algorithm and GPRS GSM ciphering key that shall be used (see 3GPP TS 04.64 [78a]).

Upon receipt of the AUTHENTICATION AND CIPHERING FAILURE message, the network stops the timer T3360. In Synch failure case, the core network may renegotiate with the HLR/AuC and provide the MS with new authentication parameters.

3GPP TSG-CN1 Meeting #30 *Tdoc N1-030667*
San Diego, California, USA, 19 – 23 May 2003

CR-Form-v7

CHANGE REQUEST

⌘ **24.008** **CR** **774** ⌘ **rev** **-** ⌘ Current version: **4.10.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ [ ] ME [X] Radio Access Network [ ] Core Network [X]

Title:	⌘	Unciphered transmission of Authentication and Ciphering Failure in A/Gb mode
Source:	⌘	Siemens AG
Work item code:	⌘	Security
Date:	⌘	09/04/2003
Category:	⌘	**A**
Release:	⌘	Rel-4

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change: ⌘

Since R97, according to subclause 4.7.1.2, the following applies in GSM (or A/Gb mode):
"If ciphering is to be applied on a GMM context, all GMM messages shall be ciphered except the following messages: …"

The list that follows contains
- AUTHENTICATION AND CIPHERING REQUEST,
- AUTHENTICATION AND CIPHERING RESPONSE, and
- AUTHENTICATION AND CIPHERING REJECT,

but not the AUTHENTICATION AND CIPHERING FAILURE message that was added later, in R99, for the UMTS authentication procedure.

However, when the MS sends a ciphered AUTHENTICATION AND CIPHERING FAILURE, as a rule the network will not be able to decipher the message:

- firstly, because in the network, according to subclause 4.7.7.3, the LLC sublayer is notified "if ciphering shall be used or not and if yes which algorithm and GPRS GSM ciphering key that shall be used" only **after** the network has received an AUTHENTICATION AND CIPHERING RESPONSE message.
- secondly, because either the necessary GPRS ciphering key is not available (which was the reason for performing an authentication and key agreement) or because the network got the P-TMSI / IMSI correlation wrong, assumes it is talking to a different subscriber and uses a wrong GPRS ciphering key.

Consequently, the network cannot decide whether the authentication challenge was rejected because of a MAC failure or Synch failure and cannot take the appropriate actions (e.g. perform ID-Request, or get new authentication parameters from the HLR).

Summary of change: ⌘ The AUTHENTICATION AND CIPHERING FAILURE message is added to the

		list of unciphered messages.
Consequences if not approved:	⌘	Inconsistent specification. If an MS implementation sends a ciphered AUTHENTICATION AND CIPHERING FAILURE message (with whatever GPRS ciphering key available), chances are that the network will not be able to decipher the message and that authentication will aborted after four re-transmissions. Depending on the further network reaction, in the worst case the MS will not be able to get PS services.

Clauses affected:	⌘	4.7.1.2			
		Y	**N**		
Other specs affected:	⌘		**X**	Other core specifications	⌘
			X	Test specifications	
			X	O&M Specifications	
Other comments:	⌘				

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm. 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 ftp://ftp.3gpp.org/specs/ 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.

4.7.1.2 Ciphering of messages (GSM only)

If ciphering is to be applied on a GMM context, all GMM messages shall be ciphered except the following messages:

-- ATTACH REQUEST;

-- ATTACH REJECT;

-- AUTHENTICATION AND CIPHERING REQUEST;

-- AUTHENTICATION AND CIPHERING RESPONSE;

-- AUTHENTICATION AND CIPHERING FAILURE;

-- AUTHENTICATION AND CIPHERING REJECT;

-- IDENTITY REQUEST;

-- IDENTITY RESPONSE;

-- ROUTING AREA UPDATE REQUEST; and

-- ROUTING AREA UPDATE REJECT.

3GPP TSG-CN1 Meeting #30 *Tdoc N1-030668*
San Diego, California, USA, 19 – 23 May 2003

CR-Form-v7

CHANGE REQUEST

⌘ **24.008** **CR** **775** ⌘ **rev** **-** ⌘ Current version: **5.7.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ ☐ ME ☒ Radio Access Network ☐ Core Network ☒

Title:	⌘	Unciphered transmission of Authentication and Ciphering Failure in A/Gb mode
Source:	⌘	Siemens AG
Work item code:	⌘	Security
Date:	⌘	09/04/2003
Category:	⌘	**A**
Release:	⌘	Rel-5

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change: ⌘

Since R97, according to subclause 4.7.1.2, the following applies in GSM (or A/Gb mode):
"If ciphering is to be applied on a GMM context, all GMM messages shall be ciphered except the following messages: …"

The list that follows contains
- AUTHENTICATION AND CIPHERING REQUEST,
- AUTHENTICATION AND CIPHERING RESPONSE, and
- AUTHENTICATION AND CIPHERING REJECT,

but not the AUTHENTICATION AND CIPHERING FAILURE message that was added later, in R99, for the UMTS authentication procedure.

However, when the MS sends a ciphered AUTHENTICATION AND CIPHERING FAILURE, as a rule the network will not be able to decipher the message:

- firstly, because in the network, according to subclause 4.7.7.3, the LLC sublayer is notified "if ciphering shall be used or not and if yes which algorithm and GPRS GSM ciphering key that shall be used" only **after** the network has received an AUTHENTICATION AND CIPHERING RESPONSE message.
- secondly, because either the necessary GPRS ciphering key is not available (which was the reason for performing an authentication and key agreement) or because the network got the P-TMSI / IMSI correlation wrong, assumes it is talking to a different subscriber and uses a wrong GPRS ciphering key.

Consequently, the network cannot decide whether the authentication challenge was rejected because of a MAC failure or Synch failure and cannot take the appropriate actions (e.g. perform ID-Request, or get new authentication parameters from the HLR).

Summary of change: ⌘ The AUTHENTICATION AND CIPHERING FAILURE message is added to the

		list of unciphered messages.
Consequences if not approved:	⌘	Inconsistent specification. If an MS implementation sends a ciphered AUTHENTICATION AND CIPHERING FAILURE message (with whatever GPRS ciphering key available), chances are that the network will not be able to decipher the message and that authentication will aborted after four re-transmissions. Depending on the further network reaction, in the worst case the MS will not be able to get PS services.

Clauses affected:	⌘	4.7.1.2			
		Y	**N**		
Other specs affected:	⌘		**X**	Other core specifications	⌘
			X	Test specifications	
			X	O&M Specifications	
Other comments:	⌘				

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm. 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 ftp://ftp.3gpp.org/specs/ 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.

4.7.1.2 Ciphering of messages (GSM only)

If ciphering is to be applied on a GMM context, all GMM messages shall be ciphered except the following messages:

-- ATTACH REQUEST;

-- ATTACH REJECT;

-- AUTHENTICATION AND CIPHERING REQUEST;

-- AUTHENTICATION AND CIPHERING RESPONSE;

-- AUTHENTICATION AND CIPHERING FAILURE;

-- AUTHENTICATION AND CIPHERING REJECT;

-- IDENTITY REQUEST;

-- IDENTITY RESPONSE;

-- ROUTING AREA UPDATE REQUEST; and

-- ROUTING AREA UPDATE REJECT.

3GPP TSG-CN1 Meeting #30 *Tdoc N1-030669*
San Diego, California, USA, 19 – 23 May 2003

CR-Form-v7

CHANGE REQUEST

⌘ **24.008** **CR** **776** ⌘ **rev** **-** ⌘ Current version: **6.0.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ ☐ ME ☒ Radio Access Network ☐ Core Network ☒

Title:	⌘	Unciphered transmission of Authentication and Ciphering Failure in A/Gb mode
Source:	⌘	Siemens AG
Work item code:	⌘	Security
Date:	⌘	09/04/2003
Category:	⌘	**A**
Release:	⌘	Rel-6

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change: ⌘

Since R97, according to subclause 4.7.1.2, the following applies in GSM (or A/Gb mode):
"If ciphering is to be applied on a GMM context, all GMM messages shall be ciphered except the following messages: …"

The list that follows contains
- AUTHENTICATION AND CIPHERING REQUEST,
- AUTHENTICATION AND CIPHERING RESPONSE, and
- AUTHENTICATION AND CIPHERING REJECT,

but not the AUTHENTICATION AND CIPHERING FAILURE message that was added later, in R99, for the UMTS authentication procedure.

However, when the MS sends a ciphered AUTHENTICATION AND CIPHERING FAILURE, as a rule the network will not be able to decipher the message:

- firstly, because in the network, according to subclause 4.7.7.3, the LLC sublayer is notified "if ciphering shall be used or not and if yes which algorithm and GPRS GSM ciphering key that shall be used" only **after** the network has received an AUTHENTICATION AND CIPHERING RESPONSE message.
- secondly, because either the necessary GPRS ciphering key is not available (which was the reason for performing an authentication and key agreement) or because the network got the P-TMSI / IMSI correlation wrong, assumes it is talking to a different subscriber and uses a wrong GPRS ciphering key.

Consequently, the network cannot decide whether the authentication challenge was rejected because of a MAC failure or Synch failure and cannot take the appropriate actions (e.g. perform ID-Request, or get new authentication parameters from the HLR).

Summary of change: ⌘ The AUTHENTICATION AND CIPHERING FAILURE message is added to the

		list of unciphered messages.
Consequences if not approved:	⌘	Inconsistent specification. If an MS implementation sends a ciphered AUTHENTICATION AND CIPHERING FAILURE message (with whatever GPRS ciphering key available), chances are that the network will not be able to decipher the message and that authentication will aborted after four re-transmissions. Depending on the further network reaction, in the worst case the MS will not be able to get PS services.

Clauses affected:	⌘	4.7.1.2			
		Y	**N**		
Other specs affected:	⌘		**X**	Other core specifications	⌘
			X	Test specifications	
			X	O&M Specifications	
Other comments:	⌘				

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm. 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 ftp://ftp.3gpp.org/specs/ 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.

4.7.1.2 Ciphering of messages (GSM only)

If ciphering is to be applied on a GMM context, all GMM messages shall be ciphered except the following messages:

-- ATTACH REQUEST;

-- ATTACH REJECT;

-- AUTHENTICATION AND CIPHERING REQUEST;

-- AUTHENTICATION AND CIPHERING RESPONSE;

-- AUTHENTICATION AND CIPHERING FAILURE;

-- AUTHENTICATION AND CIPHERING REJECT;

-- IDENTITY REQUEST;

-- IDENTITY RESPONSE;

-- ROUTING AREA UPDATE REQUEST; and

-- ROUTING AREA UPDATE REJECT.