3GPP TSG CN Plenary Meeting #15 **NP-020011**
6th – 8th March 2002. Cheju, Korea.

Source: **CN1**

Title: **Reply to Liaison Statement on Configuration of ciphering**

Agenda item: **5.1**

Document for: **INFORMATION**

3GPP TSG-CN1 Meeting #22 ***Tdoc N1-020444***
Sophia Antipolis, France, 28. January - 1. February 2002

To: SA3

Cc: CN, RAN2, T2

Response to: LS (S3-010675 = N1-02005) on Configuration of ciphering from SA3

Contact Person:
Name: Sunil Chotai
Tel. Number: +44 1473 605603
E-mail Address: sunil.chotai@o2.com

Attachments: N1-020005 [Incoming LS S3-010675]

---

1. Overall Description:

CN1 thanks SA3 on their LS on Configuration of ciphering. CN1 would like to indicate that CN1 related specifications will be impacted by the proposed CR to TS 33.102 that requires that the UE to reject CS and PS connections which are not ciphered.

CN1 note that the attached version of the CR was not approved by TSG-SA but forwarded back to SA3. CN1 would be interested in the outcome of any revisions of the requirements.

CN1 believe that RAN2 may also be impacted considering that the ciphering is performed on the individual Radio Bearers (RABs) at different point in time.

Initial analysis of the proposed requirements (TS 33.102) suggest a need to further consider the following aspects:

- What shall be considered as a “unciphered connection”? Should this include Location Update and GPRS attach ?
- What information (protocol cause values) should be sent from the UE to the network when a call is rejected. There may be services in the network which rely on this information and service interactions with existing services need to be considered (call forwarding on Not Reachable etc)
- Should new call attempts allowed from the UE?
- Do the other existing PDP contexts or ongoing CS connections need to be cleared? A UE can change PLMNs with ongoing PDP contexts established in the previous PLMN when the GGSN is located in the home network.
- The need to consider the appropriate possibly new Reject Cause value for failure to deliver Mobile Terminated SMS due to this requirement. The SMS Service Centre may retransmit SMS based of the rejection cause value. Depending on the solution, there may be changes required to the relevant SMS specifications (23.040 24.011, 29.002). Thus the specifications of the TSG T2 would also be impacted.

Additionally CN1 would like to request clarification on the service scenarios behind this feature “Visibility and Configurability”. Understanding clearly the objective and rationale will assist CN1 in responding better to SA3’s requirements.

Considering the timescales for Rel-5 work, CN1 believe that it is unlikely to complete all the necessary work for Rel-5 for these new requirements at this late stage. The next CN1 meeting is in April 2002.

2. Actions:

To SA3 group.

ACTION: CN1 request further clarification on the above issues. CN1 request SA3 to consider if these or revised requirements could be part of a release after Rel-5.

3. Date of Next CN1 Meetings:

CN1_23	8th – 12th April 2002	USA

3GPP TSG-CN1 Meeting #SIPadhoc0201 ***Tdoc N1-020005***
Phoenix, USA, 14. –18. January 2002

Agenda item: 3

3GPP TSG SA WG3 Security — S3#21 **S3-010675**

27-30 November, 2001

Sophia Antipolis, France

From: **SA3**

To: **CN1**

Copy: **T2**

Title: **Configuration of ciphering**

Contact: **Per Christoffersson, Telia**
per.e.christoffersson@telia.se

SA3 has approved the attached Rel-5 CR to TS 33.102 that specifies configuration settings on the UE to allow the user to reject non ciphered connections.

Action to CN1: SA3 requests CN1 to study this CR and notify SA3 if it impacts any CN1 specifications.

Attachment: S3-010679

3GPP TSG SA WG3 Security — S3#20 **S3-010679**

27 - 30 November, 2001, Sophia Antipolis, France

CR-Form-v3

CHANGE REQUEST

⌘ **33.102** **CR** **162** ⌘ rev **-** ⌘ Current version: **4.2.0** ⌘

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

Proposed change affects: ⌘ (U)SIM ☐ ME/UE ☒ Radio Access Network ☐ Core Network ☐

Title:	⌘	Configurability of cipher use
Source:	⌘	Telia
Work item code:	⌘	Security visibility and configurability
Date:	⌘	2001-11-19
Category:	⌘	**C**
Release:	⌘	REL-5

Use one of the following categories:
F *(essential 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)*

Reason for change:	⌘	The visibility and configurability features have never been accurately specified
Summary of change:	⌘	5.5.1 Visibility features are clarified. 5.5.2 Configurability features are clarified and the control functionality specified. 6.4.2 Editorial modification to make it clear that user can control not to accept non-ciphered calls
Consequences if not approved:	⌘	It is not clear how to interprete and implement the features described in 5.5 (requirements, options, examples?) User control mechanism is not specified. Terminal behaviour will be undefined, causing uncertainty for users.

Clauses affected:	⌘	5.5 and 6.4
Other specs affected:	⌘	☐ Other core specifications ⌘ ☐ Test specifications ☐ O&M Specifications
Other comments:	⌘	UEA0 capability bit shall be user changeable and set to 0 as default

5.5 Security visibility and configurability

5.5.1 Visibility

Although in general the security features should be transparent to the user, for certain events and according to the user's concern, ~~greater~~ some user visibility of the operation of security features shall ~~should~~ be provided. This yields to a number of features that inform the user of security-related events,~~ such as~~:

- mandatory indication of access network encryption: the property that the user is informed whether the confidentiality of user data is protected on the radio access link, in particular when non-ciphered calls are set-up;

- indication of the level of security: the property that the user is informed on the level of security that is provided by the visited network, in particular when a user is handed over or roams into a network with lower security level (3G → 2G) This indication is optional from manufacturer.

5.5.2 Configurability

Configurability is the property that ~~that~~ the user can configure ~~whether~~ the use or the provision of ~~a service should depend on whether a~~ a certain security feature ~~is in operation. A service can only be used if all security features, which are relevant to that service and which are required by the configurations of the user, are in operation.~~ The following configurability features ~~are suggested~~shall be provided:

- Enabling/disabling user-USIM authentication: the user should be able to control the operation of user-USIM authentication;~~, e.g., for some events, services or use.~~

- Accepting/rejecting ~~incoming~~ non-ciphered ~~calls~~connections: the user should be able to control via the MS user interface whether the user accepts or rejects ~~incoming~~ non-ciphered connections~~calls~~ with the following provisions~~;~~:

  - the user control for accepting/rejecting non-ciphered connections shall be pre-set to 'reject' in ME from manufacturer and shall return automatically to 'reject' position after a ciphered connection has been set up

  - if the terminal is in 'reject' position, and a ciphered connection can not be provided the connection attempt is rejected and the user should be informed of this and prompted if she wants to allow non-ciphered connections until ciphering is available

  - emergency calls shall override the reject of non-ciphered connections feature

~~- Setting up or not setting up non-ciphered calls: the user should be able to control whether the user sets up connections when ciphering is not enabled by the network;~~

- the user shall be able to disable the reject of non-ciphered connections feature so that non-ciphered connections will always be accepted (until further notice)

~~- Accepting/rejecting the use of certain ciphering algorithms: the user should be able to control which ciphering algorithms are acceptable for use.~~

6.4.2 Ciphering and integrity mode negotiation

When an MS wishes to establish a connection with the network, the MS shall indicate to the network in the MS/USIM Classmark which cipher and integrity algorithms the MS supports. This information itself must be integrity protected. As it is the case that the RNC does not have the integrity key IK when receiving the MS/USIM Classmark this information must be stored in the RNC. The data integrity of the classmark is performed, during the security mode set-up procedure by use of the most recently generated IK (see section 6.4.5).

The network shall compare its integrity protection capabilities and preferences, and any special requirements of the subscription of the MS, with those indicated by the MS and act according to the following rules:

1) If the MS and the network have no versions of the UIA algorithm in common, then the connection shall be released.

2) If the MS and the network have at least one version of the UIA algorithm in common, then the network shall select one of the mutually acceptable versions of the UIA algorithm for use on that connection.

The network shall compare its ciphering capabilities and preferences, ~~and any special requirements of the subscription of the MS,~~ with those indicated by the MS and act according to the following rules:

1) If the MS and the network have no versions of the UEA algorithm in common and the network or the MS is not prepared to use an unciphered connection, then the connection shall be released.

2) If the MS and the network have no versions of the UEA algorithm in common and both the ~~user~~ MS ~~(respectively the user's HE)~~ and the network are willing to use an unciphered connection, then an unciphered connection shall be used.

3) If the MS and the network have at least one version of the UEA algorithm in common, then the network shall select one of the mutually acceptable versions of the UEA algorithm for use on that connection.

Because of the separate mobility management for CS and PS services, one CN domain may, independent of the other CN, establish a connection to one and the same MS. Change of ciphering and integrity mode (algorithms) at establishment of a second MS to CN connection shall not be permitted. The preferences and special requirements for the ciphering and integrity mode setting shall be common for both domains. (e.g. the order of preference of the algorithms).