3GPP TSG SA WG3 Security — S3#11 **S3-000102**

22-24 February, 2000

Mainz, Germany

TSG-RAN Working Group 2 (Radio layer 2 and Radio layer 3) ***R2-000282***

San Diego, CA, USA, 17 - 21 January 2000

Source: TSG-RAN WG2

To: TSG-SA WG3

Title: LS on an L2&3 based procedure to check whether the UE uses the correct new cipher key during the cipher key change procedure

Contact: Christoph Herrmann

Philips

+49 241 600 3577

herrmann@pfa.research.philips.com

On TSG-RAN-WG2 meeting #9 and #10 a procedure was discussed, that allows for checking – during the cipher key change procedure as described in TS 25.331 – whether the UE will use the correct new cipher key, after the cipher key change procedure, and – in case it is a wrong new cipher key – to switch back to the old cipher configuration. Otherwise the UE may be lost according to the scenario described.

Document TSGR2#10(00)0226 which is attached describes the issue which is being addressed and a proposed solution .

TSG-RAN-WG2 kindly asks TSG-S-WG3 to state their opinion concerning the questions below so that TSG-RAN-WG2 can come to a conclusion on this matter.

- Does the scenario that is described in the attached document exist?
- If the answer is yes, is it addressed by higher layers?
- If the answer is no to the second question, does the proposed solution solve it?

TSG-RAN Working Group 2 (Radio layer 2 and Radio layer 3) ***TSGR2#10(00)0226***

San Diego, California, Jan 17th- 21th 2000

Agenda Item:

Source: Philips

Title: Security mode control procedure for the signalling link allowing to check the new key used by the UE in advance

Document for: Decision

---

1. Introduction

On TSGR2#9, CRs [4][5] (as well as the resulting specs [2][3]) containing specification text for the cipher key change procedure were accepted. [6] contains the description of the cipher key change procedure.

The procedure given there for AM data transfer bases on a *suspend* mechanism that only affects PUs, which are sent for the first time *after* the suspend command was issued. Retransmissions of PUs that were transmitted before the suspend command was launched, are done with the old key. After resumption the new key is used.

Note that there are the following inconsistencies between the CRs [4][5] resp. the specs [2][3] and the description of the procedure in [6], which will be corrected in [7]:

- CR [4] and [2] explicitly state that the DCCH, that carries the signalling link, is *not* suspended. The description in [6], however explains the necessity of the number N in the activiation time VT(S)+N as follows: "Note, RRC should set N to a sufficiently big value for the RRC DCCH using AM in order to make sure that the SECURITY MODE COMMAND message is transferred". This implies that the DCCH carrying the signalling link (since it carries the SECURITY MODE COMMAND message) *is* supended for SN>=VT(S)+N, and N is needed to be able to convey the SECURITY MODE COMMAND message on this DCCH until suspension becomes effective.
  So, if the signalling link is not suspended, there is no need for the parameter N, neither in the uplink nor in the downlink.
- CR [4] and [2] also state that the SECURITY MODE COMPLETE message is ciphered with the NEW key ("The UE shall send a SECURITY MODE COMPLETE message on the uplink DCCH in AM RLC, using any new cipher and/or integrity protection configuration."), while description [6] explicitly states: "UE sends the SECURITY MODE COMPLETE message on the uplink DCCH in AM RLC using confirmation (this message will be transferred using the old ciphering key)."

Though there is no longer a requirement from TSG-SA-WG3 that retransmitted PUs have to be ciphered with the same key as was used when sent for the first time, the adopted solution still fulfils this characteristic.
As a consequence, there is the advantage that the ciphering function in RLC is simplified in that a PU can be ciphered once and for ever with one given cipher key and after this is buffered as long as this PU is expected to be needed for retransmis-

sion. Whenever it has to be retransmitted, it is only read from the buffer and sent, i.e. no deciphering with the old key and then re-ciphering with new key is necessary.

[1] proposed, as a supplement to [4], a number of messages, that would allow to check during the cipher key change procedure, whether the UE uses the *correct* new key, and if this is not the case, to switch back to the old cipher key.

1.1 Why is it desirable to detect that a UE uses a wrong new cipher key, and react to this without tearing down all existing connections ?

If there is no mechanism available to recover from the situation, that the UE uses a wrong new cipher key, this is only visible on application level, and the user (or perhaps also UTRAN via its signalling link) will just recognise that all his connections no longer work properly. Whether this is because of fading conditions on the radio channel or for other reasons, cannot be detected. As a consequence,

- the user will tear down all connections between this UE and UTRAN (possibly by switching off the UE),
- the UE has again to authenticate and register with the network, and
- the user will have to set up all connections again.

For a simple speech phone, this might not be the biggest issue, especially since phone calls usually do not take as long as the period within which a cipher key change would become necessary for security reasons.
However, for a UE that supports internet access with a number of connections to the internet, a user will very much dislike *any* service interruption for whichever reason. If the number of possible reasons for service interruptions can be reduced, this should be done.

It is probably for the above mentioned reasons, that in the discussions on the topic of the cipher key change procedure in previous meetings, it had been stated several times that it would be desirable, to have a simple solution, that could avoid, that all connections between UE and UTRAN had to be closed in case the UE used the wrong new cipher key, and that the UE has to register again with the network.

1.2 Is there really a need for a mechanism to react to a UE using a wrong new cipher key?

Whether such a mechanism, that avoids breaking down of all connections between UE and UTRAN just because the UE uses the wrong cipher key, is really necessary, strongly depends on *how often* the cipher key is changed, and how often it has to be expected that the UE uses the wrong new cipher key.

It should be kept in mind that

- the frequency of a cipher key change will increase in the future with increasing processing power available to an eavesdropper.
- for a debugging of SW errors in a UE or a base station, it is of importance to know the reason, why connections are torn down. If the UE uses the wrong cipher key, this will not be visible to the network. If connections have to be torn down due to the usage of a wrong new cipher key, this should be visible.
- a check, whether the UE uses the correct new key, in one of the higher layers (e.g. MM) is, of course, possible, but will confuse the layering, since it requires in UTRAN *on a layer above RLC or MAC* deciphering of some test message, that was ciphered with the new key *on a layer above RLC or MAC* and sent by the UE. Exchange of the number RAND, which is used to compute the cipher key in the UE will not suffice for a complete error check.

Therefore, Philips believes that a solution to this problem on L2 level should be contained (at least as an option) in the specification for 3G mobile networks.

2. Recap on the current cipher change procedure as described in [2][3]

The same procedure is applied for both AM and UM radio bearers (see Figure 1, which already indicates where additional messages for the cipher key check would simply be added). The RLC entity of the signalling link is *not* suspended, as explicitly stated in [2]. This is only a minor issue, since RRC is completely in control of the signalling link: I.e. the suspension

need not be done on RLC level, but can also be done on RRC level. However, [7] is going to change this in order to get a more unified picture.

UTRAN-RRC retrieves, for any AM bearer (except for the signalling link), from UTRAN-RLC the sequence number $VT_{DL}(S)$ of the next new PU to be sent by UTRAN-RLC on the DTCH considered. UTRAN-RRC tells UTRAN-RLC the number N_{DL}, which according to [6] is chosen so big that it is ensured that the SECURITY MODE COMMAND message (ciphered with the OLD key), which is sent next by UTRAN-RRC, can be conveyed [1]. Both is done by exchanging the CRLC-SUSPEND-req and CRLC-SUSPEND-confirm primitives (see mark 1 in Figure 1). UTRAN-RLC is furthermore instructed by this primitive exchange to suspend transmission of all PUs with SN>= $VT_{DL}(S) + N_{DL}$. With the exchange of the CRLC-CONFIG primitives (mark 2 in Figure 1), UTRAN-RLC is informed about the new cipher configuration to be used from the activation time onwards.
Then UTRAN-RRC sends the SECURITY MODE COMMAND (ciphered with the OLD key) containing $VT_{DL}(S)$ and N_{DL} to UE-RRC (see mark 3 in Figure 1).

On receiving the SECURITY MODE COMMAND (see mark 4 in Figure 1), UE-RRC instructs UE-RLC for any AM bearer (except for the signalling link) to suspend transmission of further PUs and also instructs UE-RLC to use SN = $VT_{DL}(S) + N_{DL}$ as activation time for the new cipher key, i.e. UE-RLC will decipher any PU with SN >= $VT_{DL}(S) + N_{DL}$ with the new key (see mark 5 in Figure 1). Furthermore, UE-RRC retrieves the sequence number $VT_{UL}(S)$ of the next new PU to be sent by UE-RLC, and tells UTRAN-RLC the number N_{UL} , which according to [6] is chosen so big that the conveyance of the SECURITY MODE COMPLETE message, which is sent next by UE-RRC, is guaranteed[2]. All three instructions are done by exchanging the CRLC-SUSPEND-req and CRLC-SUSPEND-confirm primitives (mark 5 in Figure 1). UE-RLC is furthermore instructed by this primitive exchange to suspend transmission of all PUs with with SN>= $VT_{UL}(S) + N_{UL}$. Then UE-RRC sends the SECURITY MODE COMPLETE (ciphered with the OLD key) message containing $VT_{UL}(S)$ and N_{UL} to UTRAN-RRC (mark 8 in Figure 1).

On receiving the SECURITY MODE COMPLETE message (mark 9 in Figure 1), UTRAN-RRC instructs UTRAN-RLC to use SN = $VT_{UL}(S) + N_{UL}$ as activation time for the new cipher key, i.e. UTRAN-RLC will decipher any PU with SN >= $VT_{UL}(S) + N_{UL}$ with the new key (mark 10 in Figure 1).

After UTRAN-RRC receives the RLC-AM-DATA-Confirm primitive, that acknowledges the correct reception of the SECURITY MODE COMMAND by the UE (mark 3b in Figure 1), UTRAN-RRC knows that the UE *knows* the DL activation time for the new cipher key, i.e. from which SN on it has to decipher a received DL messages with the new key. Therefore, UTRAN-RRC can tell UTRAN-RLC to undo the suspension of data transmission for all SNs with SN>= $VT_{DL}(S) + N_{DL}$, after the above mentioned RLC-AM-DATA-confirm primitive is received (mark 6 in Figure 1).
Likewise, it is after the reception of the RLC-AM-DATA-Confirm primitive, which acknowledges the correct reception of the SECURITY MODE COMPLETE (mark 10b in Figure 1), that UE-RRC knows that UTRAN *knows* the UL activation time for the new cipher key, i.e. from which SN on it has to decipher a received UL message with the new key.[3] Therefore, UE-RRC can make UE-RLC undo the suspension (mark 11 in Figure 1) of data transmission for all SNs with SN >= $VT_{UL}(S) + N_{UL}$.

---

[1] Since the signalling link is not suspended according to [2], N_{DL} is not necessarily needed: With N_{DL} =0, the DTCH on the downlink is suspended for SN>=$VT_{DL}(S)$, and the UE will not receive any PUs on this DTCH with SN>= $VT_{DL}(S)$, whether the SECURITY MODE COMMAND message is transmitted or not.

[2] Again, since the signalling link is not suspended according to [2], N_{UL} is not necessarily needed: With N_{UL} =0, the DTCH on the uplink is suspended for SN>=$VT_{UL}(S)$, and the UTRAN will not receive any PUs on this DTCH with SN>= $VT_{UL}(S)$, whether the SECURITY MODE COMPLETEmessage is transmitted or not.

[3] Note that UE-RRC only knows that *UTRAN* knows the activation time …, and not that UTRAN-RLC knows the activation time. If UTRAN-RLC received a message *M* ciphered with the new key (which was sent after the UE resumed transmission on the DTCHs (mark 11 in Figure 1) , before UTRAN-RLC received the CRLC-CONFIG-Req($VT_{UL}(S)+N_{UL}$)- primitive (mark 10 in Figure 1), which contains the activation time, *M* would be deciphered with the wrong key. This problem could be alleviated, if N_{UL} were chosen considerably bigger than needed to only convey the SECURITY MODE COMPLETE message. The same is true for N_{DL} .Therefore, the only advantage of having N_{UL} >0 and N_{DL} > 0 would be that this implements some timer functionality to avoid that the messages are sent with the new cipher key and the configuration on the receiving side has not yet happened.

3. Supplements to incorporate an implicit check whether the UE uses the correct new cipher key including counter-measures to avoid a loss of the connection to the UE

The following procedure already takes into consideration the corrections to 25.331 as contained in [7], i.e. the RLC entity of the signalling link is suspended, and the SECURITY MODE COMPLETE message is ciphered with the OLD key.

Figure 2 and Figure 3 display, which supplements are needed to let UTRAN recognise if the UE uses a wrong cipher key, and how to deal with the cases that the UE uses the correct or a wrong new cipher key.

The basic idea of incorporating an implicit check whether the UE uses the correct new cipher key or not, is the introduction of a SECURITY MODE KEY CHECK message (sent by UE-RRC) and a SECURITY MODE KEY CHECK STATUS message (sent by UTRAN-RRC) between the SECURITY MODE COMMAND and COMPLETE messages.

This SECURITY MODE KEY CHECK message

- *per definition* is ciphered with the NEW key. To tell UE-RLC that the SECURITY MODE KEY CHECK message has to be ciphered with the NEW key, UE-RRC gives an indication, that the new cipher key should be used for the SECURITY MODE KEY CHECK message in the RLC-AM-DATA-Req- primitive. This indication can easily be done by means of an additional parameter CT (Cipher Type) in the RLC-AM-DATA-Req-primitive. CT is set to "1", if the new cipher key shall be used, and to "0" otherwise.
- is *per definition* the very message that UE-RRC sends as the next message after receiving the SECURITY MODE COMMAND message. As a consequence, the first PU containing the SECURITY MODE KEY CHECK message has, as SN from the point-of-view of UTRAN-RLC, the value VR(R) of the next new (i.e. sent for the first time) PU expected after the transmission of the SECURITY MODE COMMAND message.
  Therefore, after UTRAN-RRC receives the RLC-AM-DATA-Confirm for the SECURITY MODE COMMAND, UTRAN-RRC instructs via the following CRLC-CONFIG-Req primitive UTRAN-RLC to decipher *all* PUs of the *next* SDU (which is the SECURITY MODE KEY CHECK message) with the new cipher key. For these PUs the SN fulfills the condition SN >= VR(R).

  Since the PUs of the received SECURITY MODE KEY CHECK message are ciphered with the new key, UTRAN-RLC uses the RLC-AM-DATA-Ind primitive with the IE Cipher Type (CT=New Cipher) for conveying the reassembled SDU to UTRAN-RRC, thus indicating to UTRAN-RRC that the contained SDU was deciphered with the new key.

  The indication of whether the new or the old cipher key was used for deciphering is necessary for the following reason: If the UE uses a wrong new cipher key, UTRAN-RRC will receive no meaningful information or perhaps an unknown message type, which would have to be discarded according to TS 25.921.
  Consequently, the rule for UTRAN-RRC is: If UTRAN-RRC gets an SDU from UTRAN-RLC containing no meaningful contents, and CT parameter indicates that the new cipher key was used for deciphering, UTRAN-RRC concludes that this SDU is the SECURITY MODE KEY CHECK message, and that the UE used a wrong cipher key to cipher this message.

In sending the SECURITY MODE KEY CHECK STATUS message (ciphered with the OLD key) UTRAN-RRC indicates (via an IE) to the UE whether it used the correct or a wrong new cipher key.
On reception of the SECURITY MODE KEY CHECK STATUS message indicating that the new cipher key is wrong, the UE shall switch back to the old cipher configuration, and then resumes the suspended DCCHs and DTCHs. If the SECURITY MODE KEY CHECK STATUS message indicates that the correct new cipher key was used, the UE resumes the suspended DCCHs and DTCHs with the new cipher configuration.

3.1 Procedure complexity

Note that the implementation of the proposed procedure only needs the 2 additional messages , which are inserted between the SECURITY MODE COMMAND and the SECURITY MODE COMPLETE messages, as well as the additional parameter CT (Cipher Type (type BOOLEAN)) as part of the RLC-AM-DATA-Req and RLC-AM-DATA-Req primitives.

These primitives are not sent via the air interface, so that it should not be an issue to add it. There is no need for an application specific CRC to be added to SDUs.

4. Proposal

It is proposed to accept the procedure as a part of the security mode procedure. Corresponding CRs to 25.331 (procedure description and additional IEs) and 25.322 (the CT parameter of the local RLC-AM-DATA-Req/Ind parameters) are available in [8][9].

5. References

[1] TSGR2#9(99)k67, Cipher key change procedure for the Signalling Link, Source: Philips.

[2] TSGR2#10(00)000013, TS 25.331v310.

[3] TSGR2#10(00)000010, TS 25.322v311.

[4] TSGR2#9(99)J70, Proposed update on CR 010 on the security mode control procedure, Source: Ericsson.

[5] TSGR2#9(99)K57, Proposed CR to 25.322 on introduction of RLC suspend state, Source: Ericsson

[6] TSGR2#9(99)K58, Clarification of the security mode control procedure, Source: Ericsson.

[7] TSGR2#10(00)206, Proposed CR to 25.331 on correction of the security mode control procedure, Source Ericsson and Philips.

[8] TSGR2#10(00)225, CR 101 to 25.331 to include a cipher key check for the signalling link during the cipher key change procedure, Source: Philips.

[9] TSGR2#10(00)226, CR 022 to 25.322 to support the cipher key check for the signalling link during the cipher key change procedure, Source: Philips.

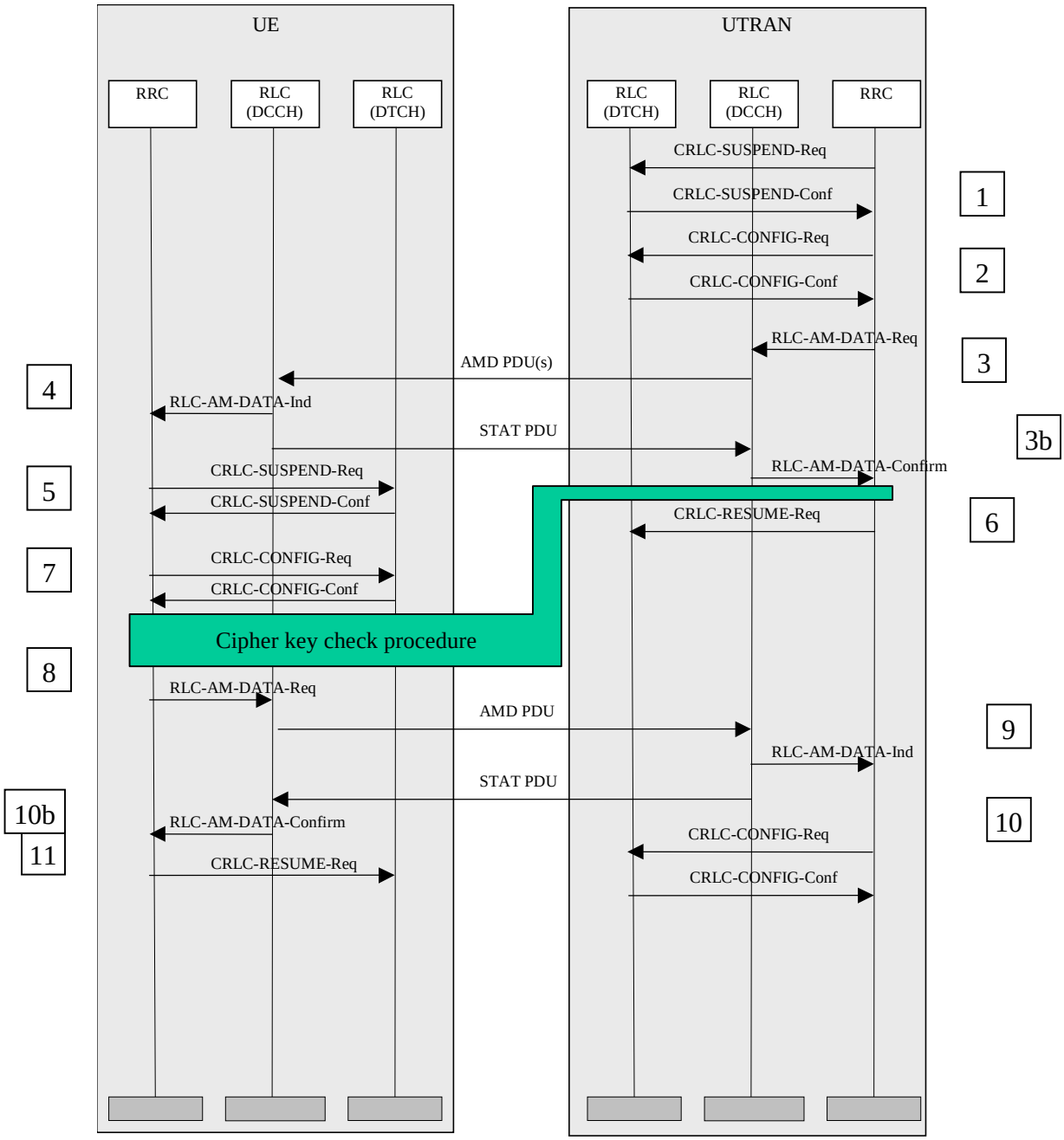


Figure 1: Current cipher key change procedure according to [4] with an indication on where the cipher key check messages would have to be inserted.

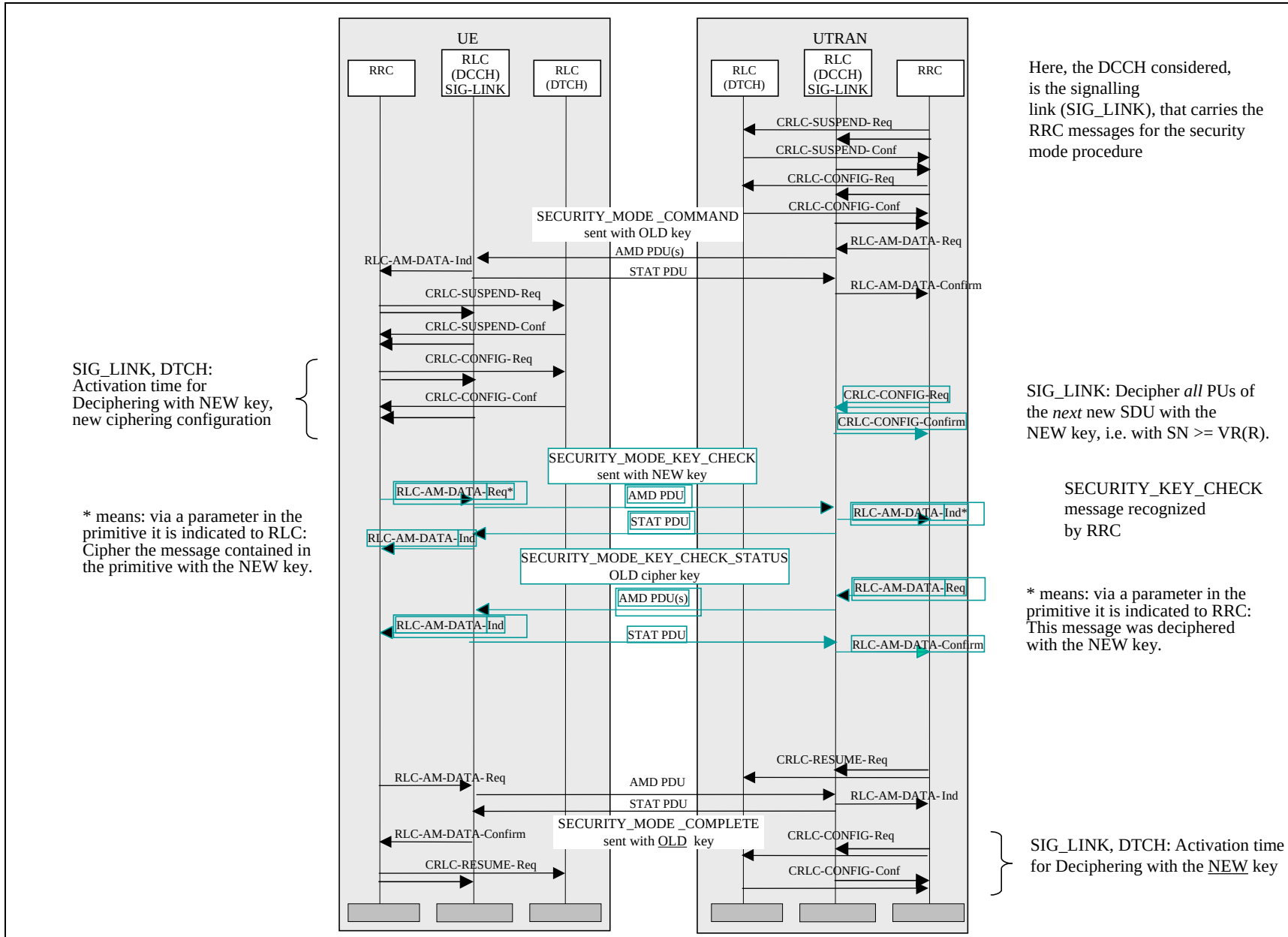
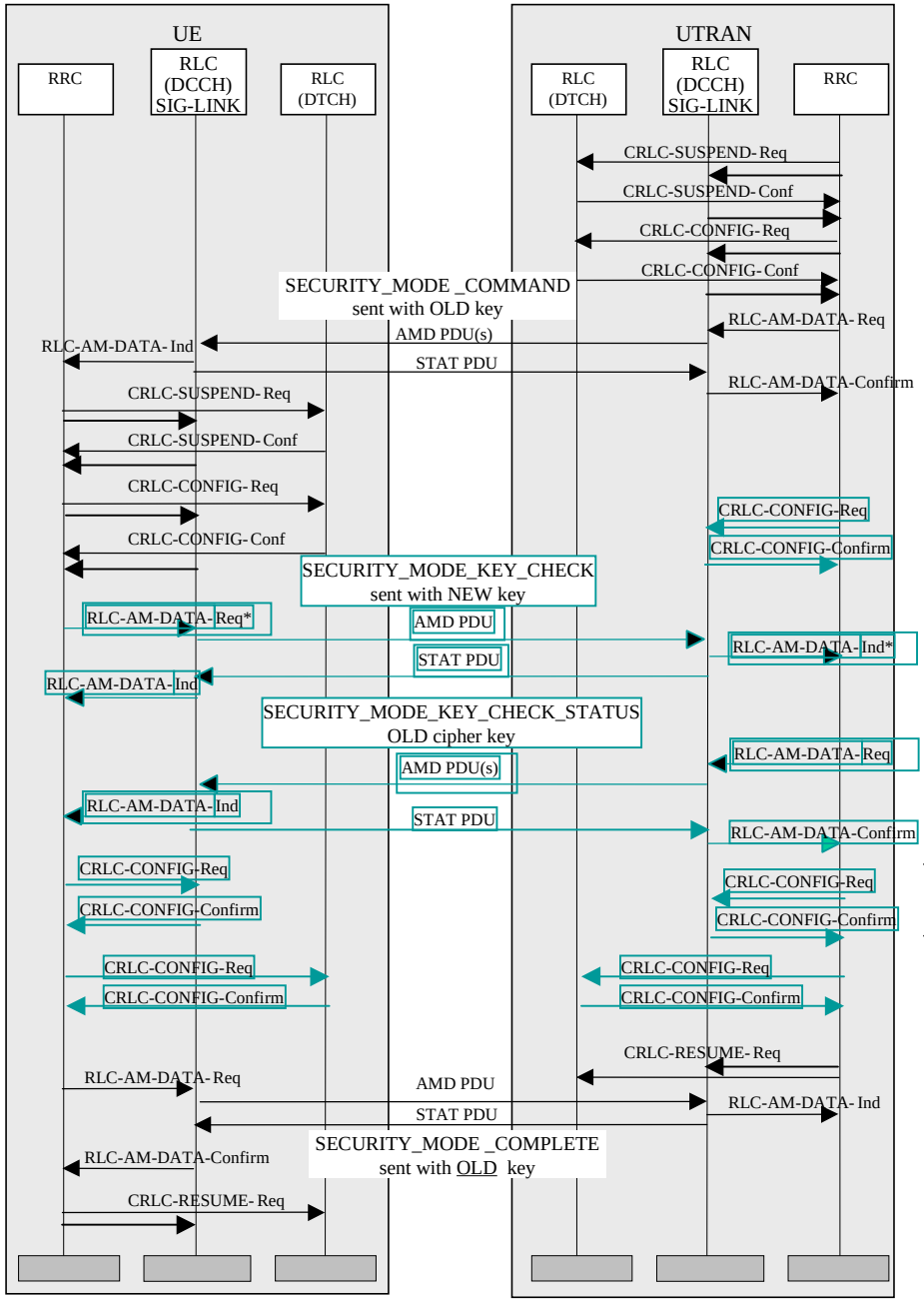


Figure 2 Signalling Link: Cipher key change procedure with cipher key check, UE uses the correct new cipher key.



Here, the DCCH considered, is the signalling link (SIG_LINK), that carries the RRC messages for the security mode procedure

SIG_LINK, DTCH: Activation time for Deciphering with NEW key, new ciphering configuration

SIG_LINK: Decipher *all* PUs of the *next* new SDU with the NEW key, i.e. with SN >= VR(R).

SECURITY_KEY_CHECK message *NOT* recognized by RRC

* means: via a parameter in the primitive it is indicated to RLC: Cipher the message contained in the primitive with the NEW key.

* means: via a parameter in the primitive it is indicated to RRC: This message was deciphered with the NEW key.

SIG_LINK: Cipher and Decipher with the OLD key

SIG_LINK: Cipher with the OLD key

DTCH: Cipher and Decipher with the OLD key

DTCH: Ciphering with the OLD key