3GPP TSG SA WG3 Security — S3#20 **S3-010556**

16 - 19 October, 2001

Sydney, Australia

Title: **Liaison Statement on HFN Reset and THRESHOLD**

Source: S3

To: RAN2

Cc:

Response to:

Contact Person:

Name: Greg Rose
Tel. Number: +61 2 9817 4188
E-mail Address: ggr@qualcomm.com

Attachments: S3-010474, S3-010476

---

1. Overall Description:

S3 would like to bring attention to two recent changes to RAN2 documents which have had consequences for security and/or documents under the control of S3.

The first of these concerns the RESET procedure, which was changed to allow the HyperFrame Number HFN to be resynchronised. The variable COUNT-C is derived from HFN, and it is a critical assumption for UMTS security that COUNT-C values shall not be repeated during the lifetime of a ciphering or integrity key. Tdoc S3-010476 (attached) examines this problem and some possible solutions. S3 would prefer that the RESET procedure be constrained so that only increasing HFNs could be specified, possibly restricted to be only slightly (1 or 2) larger than the current HFN value.

The second issue concerns a mismatch between the words “reaches” and “is greater than” in relation to START and THRESHOLD. It was S3’s intent that “reaches” means “greater than or equal to”. See Tdoc S3-010474 for a CR to 33.102 which attempted to align the two specifications. This CR was not accepted as the required changes are more far-reaching than was at first realised. A new CR will be produced for the next S3 meeting.

In both of these cases security problems have been introduced without the changes being referred to S3. S3 requests that any changes to text involving security-related parameters, e.g. keys, HFN values, COUNT, START, or THRESHOLD should be referred here, as the security issues might be subtle but quite important.

2. Actions:

To RAN2 group.

ACTION: S3 requests that RAN2 in future refer changes involving security parameters to S3.

3. Date of Next S3 Meetings:

S3 #21	27-30 November, 2001 (Sophia Antipolis, France)
S3 #22	26 February-1 March, 2002 (Bristol, UK)

3GPP TSG-SA WG3 Meeting #20
Sydney, Australia, 16-19 October 2001

Tdoc S3-010474

CR-Form-v4

CHANGE REQUEST

⌘ **33.102** **CR** **zzz** ⌘ ev **-** ⌘ Current version: **3.9.0** ⌘

*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 **X** Radio Access Network **X** Core Network ☐

Title:	⌘	Alignments with 25.331
Source:	⌘	Nokia
Work item code:	⌘	***Date:*** ⌘ 9 Oct 01
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)

Reason for change: ⌘ Inconsistency between 33.102 and 25.331 regarding the lifetime of ciphering and integrity keys. In 33.102 it is specified that when START **reaches** THRESHOLD, ciphering and integrity keys are deleted.
However in 25.331 chapter 8.5.2 it is specified that:

When entering idle mode, the UE shall:

- if the USIM is present:
  - store the current START value for every CN domain in the USIM [50];
  - if the "START" stored in the USIM [50] for a CN domain **is greater than** the value "THRESHOLD" of the variable START_THRESHOLD:
    - delete the ciphering and integrity keys that are stored in the USIM for that CN domain;
    - inform the deletion of these keys to upper layers.

Summary of change: ⌘ 33.102 has been aligned with 25.331:
- "reached" changed to "greater than"
- clarification in START value calculation

Consequences if not approved: ⌘ Inconsistency between specifications.

Clauses affected: ⌘ 6.4.3, 6.4.8, 6.5.4.2, 6.6.4.2

Other specs Affected: ⌘ ☐ Other core specifications ⌘
☐ Test specifications

	☐ 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/3G_Specs/CRs.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.

6.4.3 Cipher key and integrity key lifetime

Authentication and key agreement, which generates cipher/integrity keys, is not mandatory at call set-up, and there is therefore the possibility of unlimited and malicious re-use of compromised keys. A mechanism is needed to ensure that a particular cipher/integrity key set is not used for an unlimited period of time, to avoid attacks using compromised keys. The USIM shall therefore contain a mechanism to limit the amount of data that is protected by an access link key set.

Each time an RRC connection is released the values $START_{CS}$ and $START_{PS}$ of the bearers that were protected in that RRC connection are compared with the maximum value, THRESHOLD. If $START_{CS}$ ~~and~~/or $START_{PS}$ ~~have reached~~is greater than the maximum value (THRESHOLD), the ME ~~marks the START value in the USIM for the corresponding core network domain(s) as invalid by setting the $START_{CS}$ and/or $START_{PS}$ to THRESHOLD,~~ deletes the cipher key and the integrity key for the corresponding core network domain stored on the USIM and sets the KSI to invalid (refer to section 6.4.4). Otherwise, the $START_{CS}$ and $START_{PS}$ are stored in the USIM. The maximum value THRESHOLD is set by the operator and stored in the USIM.

When the next RRC connection is established, START values are read from the USIM. Then, the ME shall trigger the generation of a new access link key set (a cipher key and an integrity key for the corresponding core network domain) if the access link key set has been deleted~~$START_{CS}$ and/or $START_{PS}$ has reached the maximum value, THRESHOLD, for the corresponding core network domain(s)~~.

This mechanism will ensure that a cipher/integrity key set cannot be reused beyond the limit set by the operator.

When the user is attached to a UTRAN, a R99+ ME with a SIM inserted shall use a default value for maximum value of $START_{CS}$ or $START_{PS}$ as described in section 6.8.2.4.

6.4.8 Initialisation of synchronisation for ciphering and integrity protection

The ciphering and integrity protection algorithms are driven by counters (COUNT-C and COUNT-I) that at connection establishment need to be initialised. For that purpose the ME and the USIM have the ability to store a START value. The ME and the USIM store a $START_{CS}$ value for the CS cipher/integrity keys and a $START_{PS}$ value for the PS cipher/integrity keys. The length of START is 20 bits.

The ME only contains (valid) START values when it is powered-on and a USIM is inserted. When the ME is powered-off or the USIM is removed, the ME deletes its START values. After power-on or insertion of a USIM, the USIM sends its START values to the ME, and the ME stores them. During idle mode, the START values in the ME and in the USIM are identical and static.

At radio connection establishment for a particular serving network domain (CS or PS) the ME sends the $START_{CS}$ and the $START_{PS}$ value to the RNC in the *RRC connection setup complete* message. The ME marks the START values in the USIM as invalid by setting $START_{CS}$ and $START_{PS}$ to THRESHOLD.

The ME and the RNC initialise the 20 most significant bits of the RRC HFN (for integrity protection), the RLC HFN (for ciphering) and the MAC-d HFN (for ciphering) to the START value of the corresponding service domain; the remaining bits are initialised to 0. Also the RRC SN (for integrity protection) and the RLC SN (for ciphering) are initialised to 0.

During an ongoing radio connection, the $START_{CS}$ value in the ME and in the SRNC is defined as the 20 most significant bits of the maximum of all current COUNT-C and COUNT-I values for all signalling radio bearers and CS user data radio bearers protected using the most recently configured CK_{CS} and/or $IK_{CS,}$ incremented by 1, i.e.:

$START_{CS}' = MSB_{20}$ (MAX {COUNT-C, COUNT-I | all radio bearers (including signalling) protected with the most recently configured CK_{CS} and IK_{CS}}) + 1.

- If current $START_{CS} < START_{CS}'$ then $START_{CS} = START_{CS}'$, otherwise $START_{CS}$ is unchanged.

Likewise, during an ongoing radio connection, the $START_{PS}$ value in the ME and in the SRNC is defined as the 20 most significant bits of the maximum of all current COUNT-C and COUNT-I values for all signalling radio bearers and PS user data radio bearers protected using the most recently configured CK_{PS} and/or IK_{PS}, incremented by 1, i.e.:

$START_{PS}' = MSB_{20}$ (MAX {COUNT-C, COUNT-I | all radio bearers (including signalling) protected with the most recently configured CK_{PS} and IK_{PS}}) + 1.

- If current $START_{PS} < START_{PS}'$ then $START_{PS} = START_{PS}'$, otherwise $START_{PS}$ is unchanged.

If any of the COUNT-C or COUNT-I assigned to the radio bearers of the same CN domain reaches its maximum value, the ME and SRNC shall set START of the corresponding CN domain to its maximum value.

Upon radio connection release and when a set of cipher/integrity keys is no longer used, the ME updates $START_{CS}$ and $START_{PS}$ in the USIM with the current values.

During authentication and key agreement the START value associated with the new key set of the corresponding service domain is set to 0 in the USIM and in the ME.

6.5.4 Input parameters to the integrity algorithm

6.5.4.1 COUNT-I

The integrity sequence number COUNT-I is 32 bits long.

For signalling radio bearers (RB 0-4) there is one COUNT-I value per up-link signalling radio bearer and one COUNT-I value per down-link signalling radio bearer.

COUNT-I is composed of two parts: a "short" sequence number and a "long" sequence number. The "short" sequence number forms the least significant bits of COUNT-I while the "long" sequence number forms the most significant bits of COUNT-I. The "short" sequence number is the 4-bit RRC sequence number (RRC SN) that is available in each RRC PDU. The "long" sequence number is the 28-bit RRC hyper frame number (RRC HFN) which is incremented at each RRC SN cycle.

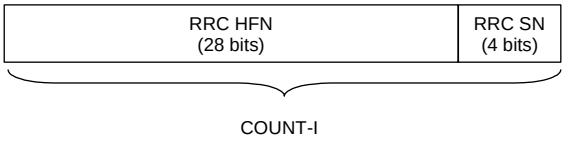


Figure 16a: The structure of COUNT-I

The RRC HFN is initialised by means of the parameter START, which is described in section 6.4.8. The ME and the RNC then initialise the 20 most significant bits of the RRC HFN to START; the remaining bits of the RRC HFN are initialised to 0.

6.5.4.2 IK

The integrity key IK is 128 bits long.

There may be one IK for CS connections (IK_{CS}), established between the CS service domain and the user and one IK for PS connections (IK_{PS}) established between the PS service domain and the user. Which integrity key to use for a particular connection is described in 6.5.5.

For UMTS subscribers IK is established during UMTS AKA as the output of the integrity key derivation function f4, that is available in the USIM and in the HLR/AuC. For GSM subscribers, that access the UTRAN, IK is established following GSM AKA and is derived from the GSM cipher key Kc, as described in 6.8.2.

IK is stored in the USIM and a copy is stored in the ME. IK is sent from the USIM to the ME upon request of the ME. The USIM shall send IK under the condition that a valid IK is available. The ME shall trigger a new authentication procedure if the current value of $START_{CS}$ or $START_{PS}$ in the USIM are not up-to-date or $START_{CS}$ or $START_{PS}$ ~~have reached~~is greater than THRESHOLD. The ME shall delete IK from memory after power-off as well as after removal of the USIM.

IK is sent from the HLR/AuC to the VLR/SGSN and stored in the VLR/SGSNas part of a quintet. It is sent from the VLR/SGSN to the RNC in the (RANAP) *security mode command*.

At handover, the IK is transmitted within the network infrastructure from the old RNC to the new RNC, to enable the communication to proceed, and the synchronisation procedure is resumed. The IK remains unchanged at handover.

6.5.4.3 FRESH

The network-side nonce FRESH is 32 bits long.

There is one FRESH parameter value per user. The input parameter FRESH protects the network against replay of signalling messages by the user. At connection set-up the RNC generates a random value FRESH and sends it to the user in the (RRC) *security mode command*. The value FRESH is subsequently used by both the network and the user throughout the duration of a single connection. This mechanism assures the network that the user is not replaying any old MAC-Is.

At handover with relocation of the S-RNC, the new S-RNC generates its own value for the FRESH parameter and sends it to the ME in the RRC message that indicates a new UTRAN Radio Network Temporary Identity due to a SRNC relocation (see TS 25.331 [17]).

6.5.4.4 DIRECTION

The direction identifier DIRECTION is 1 bit long.

The direction identifier is input to avoid that the integrity algorithm used to compute the message authentication codes would use an identical set of input parameter values for the up-link and for the down-link messages. The value of the DIRECTION is 0 for messages from UE to RNC and 1 for messages from RNC to UE.

6.5.4.5 MESSAGE

The signalling message itself with the radio bearer identity. The latter is appended in front of the message. Note that the radio bearer identity is not transmitted with the message but it is needed to avoid that for different instances of message authentication codes the same set of input parameters is used.

6.6.4 Input parameters to the cipher algorithm

6.6.4.1 COUNT-C

The ciphering sequence number COUNT-C is 32 bits long.

There is one COUNT-C value per up-link radio bearer and one COUNT-C value per down-link radio bearer using RLC AM or RLC UM. For all transparent mode RLC radio bearers of the same CN domain COUNT-C is the same, and COUNT-C is also the same for uplink and downlink.

COUNT-C is composed of two parts: a "short" sequence number and a "long" sequence number. The "short" sequence number forms the least significant bits of COUNT-C while the "long" sequence number forms the most significant bits of COUNT-C. The update of COUNT-C depends on the transmission mode as described below (see figure 16c).

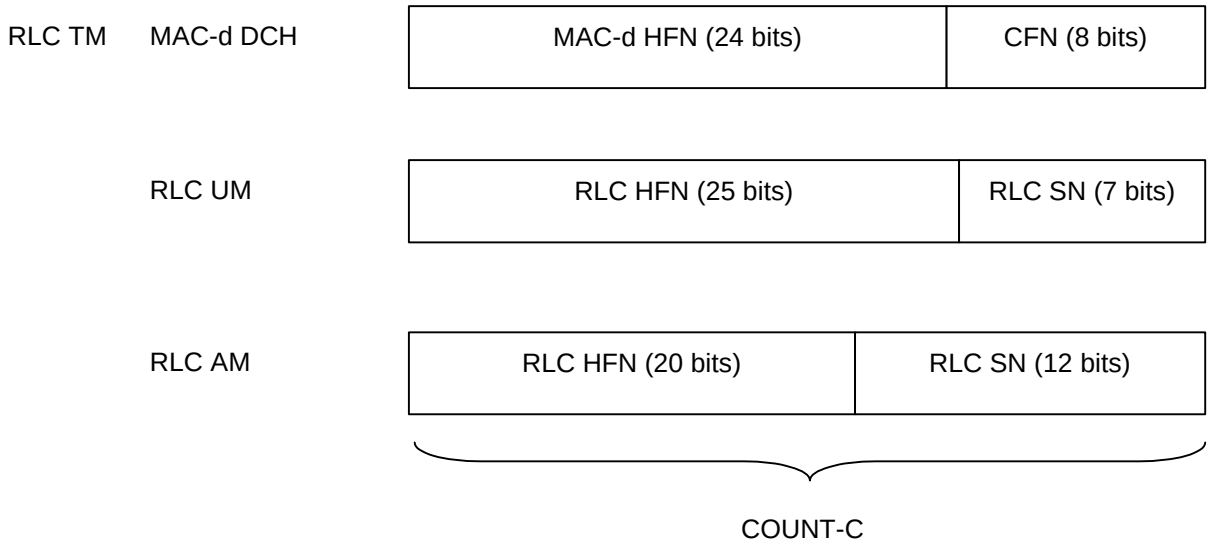


Figure 16c: The structure of COUNT-C for all transmission modes

- For RLC TM on DCH, the "short" sequence number is the 8-bit connection frame number CFN of COUNT-C. It is independently maintained in the ME MAC-d entity and the SRNC MAC-d entity. The "long" sequence number is the 24-bit MAC-d HFN, which is incremented at each CFN cycle.
- For RLC UM mode, the "short" sequence number is the 7-bit RLC sequence number (RLC SN) and this is part of the RLC UM PDU header. The "long" sequence number is the 25-bit RLC UM HFN which is incremented at each RLC SN cycle.
- For RLC AM mode, the "short" sequence number is the 12-bit RLC sequence number (RLC SN) and this is part of the RLC AM PDU header. The "long" sequence number is the 20-bit RLC AM HFN which is incremented at each RLC SN cycle.

The hyperframe number HFN is initialised by means of the parameter START, which is described in section 6.4.8. The ME and the RNC then initialise the 20 most significant bits of the RLC AM HFN, RLC UM HFN and MAC-d HFN to START. The remaining bits of the RLC AM HFN, RLC UM HFN and MAC-d HFN are initialised to zero.

When a new radio bearer is created during a RRC connection in ciphered mode, the HFN is initialised by the current START value (see section 6.4.8).

6.6.4.2 CK

The cipher key CK is 128 bits long.

There may be one CK for CS connections (CK_{CS}), established between the CS service domain and the user and one CK for PS connections (CK_{PS}) established between the PS service domain and the user. The CK to use for a particular radio bearer is described in 6.6.5. For UMTS subscribers, CK is established during UMTS AKA, as the output of the cipher key derivation function f3, available in the USIM and in HLR/AuC. For GSM subscribers that access the UTRAN, CK is established following GSM AKA and is derived from the GSM cipher key Kc, as described in 8.2.

CK is stored in the USIM and a copy is stored in the ME. CK is sent from the USIM to the ME upon request of the ME. The USIM shall send CK under the condition that a valid CK is available. The ME shall trigger a new authentication procedure if the current value of $START_{CS}$ or $START_{PS}$ in the USIM ~~have reached~~is greater than THRESHOLD. The ME shall delete CK from memory after power-off as well as after removal of the USIM.

CK is sent from the HLR/AuC to the VLR/SGSN and stored in the VLR/SGSN as part of the quintet. It is sent from the VLR/SGSN to the RNC in the (RANAP) security mode command.

At handover, the CK is transmitted within the network infrastructure from the old RNC to the new RNC, to enable the communication to proceed. The cipher CK remains unchanged at handover.

6.6.4.3 BEARER

The radio bearer identifier BEARER is 5 bits long.

There is one BEARER parameter per radio bearer associated with the same user and multiplexed on a single 10ms physical layer frame. The radio bearer identifier is input to avoid that for different keystream an identical set of input parameter values is used.

6.6.4.4 DIRECTION

The direction identifier DIRECTION is 1 bit long.

The direction identifier is input to avoid that for the keystreams for the up-link and for the down-link would use the an identical set of input parameter values. The value of the DIRECTION is 0 for messages from UE to RNC and 1 for messages from RNC to UE.

6.6.4.5 LENGTH

The length indicator LENGTH is 16 bits long.

The length indicator determines the length of the required keystream block. LENGTH shall affect only the length of the KEYSTREAM BLOCK, not the actual bits in it.

3GPP TSG SA WG3 Security — S3#20 **S3-010476**

16 - 19 October, 2001

Sydney, Australia

Source: QUALCOMM Europe S.A.R.L.

Title: Security concern with HFN reset procedure

Document for: Discussion and decision

Agenda Item:

Introduction

The RLC Reset procedure, as currently defined in RAN WG2 specifications, could be exploited by malicious attackers. The troublesome behavior was introduced in R99 TS 25.322 with a CR approved at RAN #10 on December 2000 [1]. The changes were introduced to solve an "out of sync" problem discussed on the RAN WG2 e-mail reflector [2]. As a result of the changes the HFNs used in COUNT-C can be re-initialized by UE or RNC by using an RLC Control PDU, which is not ciphered nor authenticated.

Correct use of HFNs is vital to the security of the UMTS system. The ability to reset HFNs was introduced in RAN2 without referring the change to SA3. We have identified some vulnerabilities, but there might be worse ones we have not identified.

Exerpt from TS 25.322 v3.8.0

11.4 RLC reset procedure

11.4.1 General

The RLC reset procedure is used to reset two RLC peer entities, which are operating in acknowledged mode. Figure 11.4 below illustrates the elementary procedure for an RLC reset. During the reset procedure the hyper frame numbers (HFN) in UTRAN and UE are synchronised. Two HFNs used for ciphering needs to be synchronised, DL HFN in downlink and UL HFN in uplink. In the reset procedure, the highest UL HFN and DL HFN used by the RLC entity in the transmitting sides, i.e. the HFNs associated with PDUs of SN=VT(S)-1 if at least one data PDU had been transmitted or of SN=0 if no data PDU had been transmitted, are exchanged between UE and UTRAN.

The RESET PDUs and the RESET ACK PDUs have higher priority than AMD PDUs.

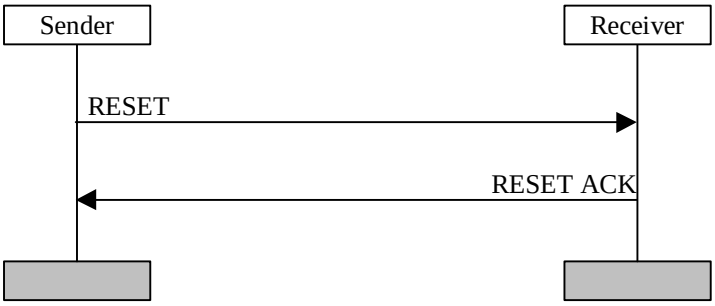


Figure 11.4: RLC reset procedure

[…]

9.2.1.7 RESET, RESET ACK PDU

The RESET PDU (the RESET ACK PDU) have a one-bit sequence number field (RSN) in order to know whether or not it is a retransmission of a previous RESET PDU (of a previous RESET ACK PDU).

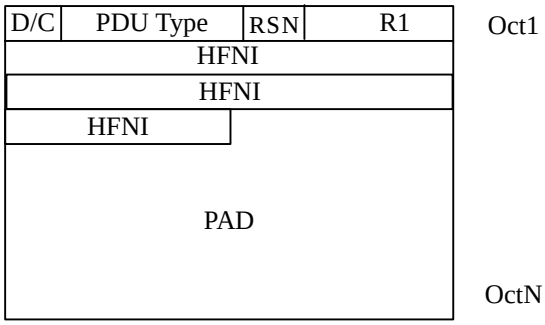


Figure 9.6: RESET, RESET ACK PDU

The size of a RESET or RESET ACK PDU is variable and upper bounded by the maximum RLC PDU size used by the logical channel on which the control PDUs are sent. Padding shall be included to exactly fit one of the PDU sizes used by the logical channel on which the control PDUs are sent. The length of the RESET or RESET ACK PDU shall be a multiple of 8 bits.

[…]

9.2.2.14 Hyper Frame Number Indicator (HFNI)

Length: 20 bit

This field is used to indicate the hyper frame number (HFN) to the peer entity. With the aid of this field the HFN in UE and UTRAN can be synchronised.

[…]

[…From TS 33.102v3.9.0…]

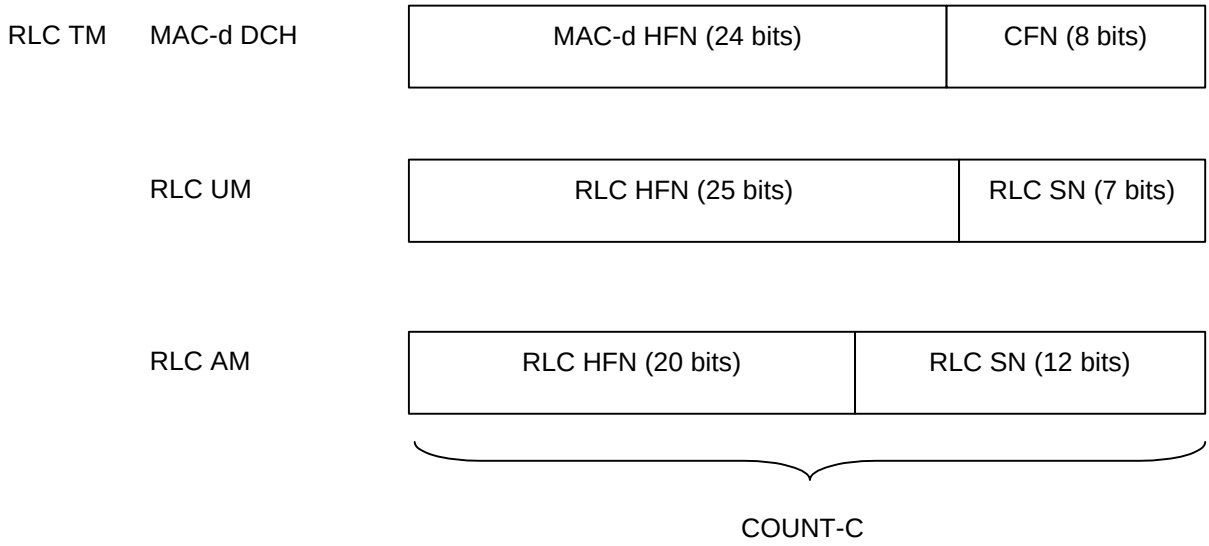


Figure 16c: The structure of COUNT-C for all transmission modes

[…]

Note that RLC Sequence Numbers (SN) are always sent in clear over the air (Uu interface) both in Uplink and in Downlink.

Discussion

All RLC Control PDUs, including RESET/RESET ACK, are not ciphered and are not integrity protected. The RESET and RESET ACK are always associated to an AM RLC entity and they carry the HFN value to be used in the UL COUNT-C. Both UE and UTRAN can initiate a RESET procedure by sending the RESET PDU. The receiving entity will then send a RESET ACK PDU. We can envisage a multiplicity of security threats that could take advantage of this procedure:

- *Denial of service attack*. A third party can transmit a RESET PDU with an incorrect HFN. The RESET ACK PDU response will be ignored by the supposed sender. From then on, decryption of the packets will result in incorrect and unintelligible data being received, but since there is no integrity check, the lower layers cannot detect or recover from the situation. Furthermore, by setting a large HFN, past the threshold, a new AKA might be triggered, resulting in exhaustion of Authentication Vectors, delays and excessive network traffic.

- *Exposure of HFNs*. If an eavesdropper is recording the call from its beginning he will be able to deduce the HFN values used in COUNT-C. But if he starts recording it while in progress, or if he loses part of it due to bad radio conditions (quite a likely scenario), he may lose track of the current value of the HFN and therefore he will not be able to reconstruct COUNT-C. However, he could take advantage of the RESET procedure to read the correct HFN values being sent in the RESET/RESET ACK PDUs. By the way, to cause a RESET for a "man in the middle" is very simple. He only has to change the sequence number (always in clear) to a value that is outside of the "expected" window of sequence numbers.

- *Rogue equipment can avoid re-authentication*. The COUNT-C value triggers re-authentication when it exceeds the threshold value. But non-conforming equipment can reset the HFN “backwards” so that its COUNT-C never reaches THRESH. This partly avoids re-authentication (it might be triggered by the HFN in the other direction) and at the same time compromises privacy by reuse of COUNT-C values.

The initiator of a RESET procedure seems to be in control of its corresponding HFN (uplink or downlink). We are unaware of a mechanism whereby a third party can compromise privacy or negotiate specific HFNs, but we are not convinced that such a mechanism does not exist.

In general the use of messages that are not ciphered nor authenticated to modify the values of COUNT-C is not a good idea. We understand that RAN WG2 had good reasons [2] to approve these changes, but unfortunately did not involve SA WG3 in the discussion.

Conclusion

We propose that RAN WG2 should take a second look at the problem discussed in [2] and solve it differently, by using methods that do not compromise security. In particular, the use of the RESET/RESET ACK PDUs, which currently include HFN values, should be modified. In order to not modify the PDU format, the transmitter could include dummy HFN values in the RESET/RESET ACK PDUs that the receiver would ignore. These corrections should be included in all affected releases of TS 25.322, starting from R99.

SA WG3 cannot provide further guidance for the resolution of the specific problem raised in [2], but it can recommend the following:

1. The HFN values should not be sent in clear and without integrity protection.
2. If HFN have to be re-synchronized, the new values should grow monotonically; while this is specified behaviour for a conforming transmitter, no provision is made for it to be checked in the receiver. Provision should be incorporated for the re-syncronization procedure to fail or be refused.

With monotonically increasing HFN values to ensure freshness and defeat replay, it would be possible (and it would be recommened) to apply message integrity to the re-syncronization messages using IK.The presence of SA WG3 experts at next RAN WG2 meeting, to be held in New York City next week, would be extremely valuable.

References

The following references are enclosed in the soft copy. Note that the current text of 25.322 has been further updated after the CR mentioned.

[1] 25322CR088R1 in RP-000568, Agreed CRs to TS 25.322, TSG-RAN Meeting #10, Bangkok, Thailand, 6 - 8 December 2000

[2] E-mail exchange: “Re: RLC RESET Procedure: Email discussion kick-off (fwd)”, 3GPP_TSG_RAN_WG2 reflector, 5 Oct 2000.

Date: Thu, 5 Oct 2000 17:30:43 +0530
Reply-To: Atul Suresh Joshi <atul@sasi.com>
Sender: "3GPP_TSG_RAN_WG2: TSG RAN Working Group 2"
<3GPP_TSG_RAN_WG2@list.etsi.fr>
From: Atul Suresh Joshi <atul@sasi.com>
Subject: Re: RLC RESET Procedure: Email discussion kick-off (fwd)
Comments: cc: Sujatha <sujatha@sasi.com>
To: 3GPP_TSG_RAN_WG2@list.etsi.fr
Content-Type: TEXT/PLAIN; charset=US-ASCII
X-UIDL: pAG"!n(<!!6@'!!@4l"!

Hi all,
Further to the problems stated in the Email discussion on problems with RESET procedure, in this mail we state another problem and probable solutions to the stated problems.

Problem 1. CRLC_SUSPEND_Req in RLC RPS state

Stated below.
Solution: Reset the state variables while entering the RPS state.

Problem 2. Out of Sync HFN
---
stated below.
Solution : Change in RESET PDU format. (detailed solution is given below.)

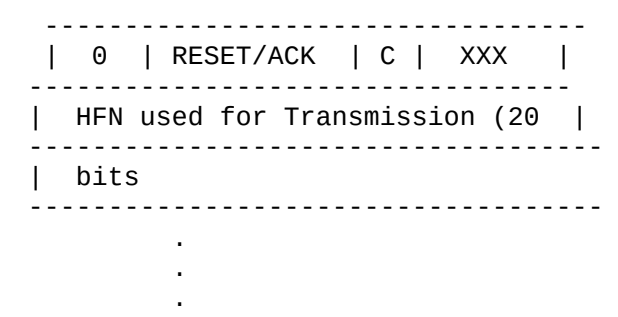
Problem3 . Problem with Ciphering Configuration

RLC can get RESET in either LS or DTR state. If it gets RESET in LS then after coming out of RESET it will be in LS only and use old configuration. The problem would arise if it gets RESET in DTR . In DTR an RLC entity may have two configurations old and new. (This would be the case when the state transitions are LS->DTR->RESET and there are some PUs with sequence number < activation time which are not confirmed). Which configuration should be used in such a case needs to be specified in the standards and RESET PDU format needs to altered accordingly becuase the receiver of RESET PDU is not aware of the state transitions in the peer.
An example is given below.
Consider RLC(1) and RLC(2) entities.
RLC(1) has done state transitions DTR->LS->DTR and has
VT(A)(1) = 20, VT(S)(1) = 40, Activation time = 30.
So it uses old configuration for PUs[20-29] while it uses new configuration[30-...]
If RLC(1) is reset, after coming out of RESET which configuration should be used?
note that it is not always possible to use old configuration after coing out of RESET.
This is because, if at RLC(2) VR(R) = 32 VR(H) = 35, RLC(2) might have deleted old configuration because it has crossed 30 (the activation time). In such a case
RLC should use new configuration and the activation time should be discarded.
In case where, VT(S)(1) is less than activation time and RLC is in DTR then RLC can use
old or new configuration,but it is always better to new configuration.
In case there was no valid activation time (activation time elapsed so that VT(S)>=VT(A) >=Activation time) the current configuration should be used but as mentioned earlier RLC is not aware of peer RLC state transitions.(RLC doesn't know whether the peer RLC has gone LS->RESET or DTR->RESET and it can have old and
new configurations)
Thus an indication is needed in the RESET PDU to indicate which configuration to be used after resetting the variables.

Thus we think that RESET PDU should indicate
1. Configuration to be used (old/new)
2. HFN to be used

We propose following RESET PDU format and theRESET procedure

Format



Note that HFN used for reception can be different from HFN used for transmission.(RESET and RESET ACK PDU format is exactly same except for PDU type field.)
After Receiving RESET/RESET ACK PDU HFN used for reception is updated to the HFN indicated in the PDU.
Tx-HFN : HFN used by an RLC entity for ciphering
Rx-HFN : HFN used by an RLC entity for deciphering

Modified RESET procedure is described below.
1. When RLC enters in RPS , it flushes off buffers , resets state variables and Tx-HFN is incremented by one and sends a RESET PDU with(updated) Tx-HFN and C is set according to following rules:
   C : 0 if RPS is enterd from LS or if DTR->RPS has taken place and activation time has elapsed
   C : 1 if DTR->RPS has taken place with valid Activation time.
2. Upon reception of RESET PDU
   a) RLC updates Rx-HFN to HFN value indicated in the RESET PDU increments its Tx-HFN, flushes off buffers , resets state variables
   b) RESET ACKPDU is transmitted and RLC comes out of RPS to enter into either LS or DTR state.
   c) In RESET ACK PDU C is set as given below

   C : 0 if it is in LS or it is in DTR and activation time has elapsed
   C : 1 if activation time is still valid and RLC is in DTR in RESET PDU and HFN equal its (updated) Tx-HFN .
   RLC then starts using the configuration for RX as indicated by C bit in the received PDU.

3. Upon reception of RESET ACK PDU
   1.if RLC is in RPS , Rx HFN is updated accordingly and RLC comes out of RPS
   2. RESET ACK PDU is ignored in LS/DTR state.

   3.Once RLC entity comes out of RPS, it uses ciphering configuration indicated by C bit in the received PDU.

This procedure would solve the problems mentioned above though this procedure should be studied more throughly.

thanks
atul,sujatha

Atul Suresh Joshi wrote:

> Hi all,
>
> It was decided in the WG2#15 meeting in Sophia Antipolis that, the problems
> regarding the RESET procedure should be discussed on mailing list.
> With this mail we intend to start an email discussion on the issue.
> Johan Torsner from Ericsson will be the repaurter for this email
> discussion.
>
> Problem 1. CRLC_SUSPEND_Req in RLC RPS state
> ---
> As per the current specifications state variablesare reset whenever
> RLC comes out of RPS. Which means that value of VT(S) is is preserved
> during RPS. In RPS if RLC receives an CRLC_SUSPEND_Req , RLC reports
> back VT(S) in CRLC_Confirm. What should be the value of VT(S)
> which needs to be reported in this case ? old VT(S) or 0?
> Because RLC is not going to send anything between VT(A) to VT(S)+number
> of segmented PDUs as the buffers are anyway going to be flushed out.
> In such a case VT(S) should be reported as 0 rather than old VT(S).
> other wise RLC will be using old ciphering config for more time.
> e.g. if VT(S) = 1000 and N = 100 => activation time will be 1100
> whereas it should have been 100 only.
>
> Another more serious problem is stated below.
> Suppose RRC suspends DCCH on which security mode command is to be transmitted.
> Which is in RESET state with N "sufficiently large", so the activation time
> is (VT(S)+N)Mod 4096. But by the time Security mode command is transmitted
> RLC is in DTR state,Activation time might be too short and
> security mode command may not be completely transmitted.
> e.g.
> DCCH RLC in RPS VT(S) = 4040. RRC suspends RLC with N = 100
> where as security mode command requires 50 RLC PDUs .
> RLC reports back VT(S) = 4060. So the activation time is 44.
> Now RLC returns to LS and VT(S) = 0. RLC in this case is allowed to
> transmit PDUs up to 44 only whereas security mode command spans upto 50.
> Thus RLC gets stuck up.
>
> Reporting of VT(S) = 0 can be done in one of the following ways.
> 1. Explicit mention in RLC specs that if CRLC_SUSPEND_Req is received in RPS
>   RLC reports 0 in CRLC_CONFIRM
> 2. RESET all the state variables to their intial vales while entering into
>   RPS.
>
> Problem 2. Out of Sync HFN
> ---
> HFNs in RLC AM are incremented by one when corresponding state variables
> wrap around. e.g. For Tx HFN is incremented when VT(S) or VT(A) reaches 0.
> and for RX HFN is incremented when VR(R) or VR(H) reaches 0.
> Note that Tx HFN in RLC entity and corresponding RX HFN on peer RLC entity
> are incremented at different times. This can lead to a problem if
> RESET occrs inbetween.
> e.g.
> Tx HFN = 100 VT(S) = 4095   Rx HFN = 100 VR(H) = 4090
> In the next TTI
> TX HFN = 101 VT(S) = 0   RX HFN = 100 VR(H) = 4090.
>
> and a RESET occurs.

> RESET/RESET_ACK PDUs are exchanged which are not ciphered and RLC entities
> get back to DTR state. with
>
> TX HFN = 102 VT(S) = 0   and RX HFN = 101 VR(H) = 0.
>
> Thus there is a mismatch. Also as it is not specified in specifications
> as to when one shall increment HFN (either with VT(S) or with VT(A))
> this issue will depend on the window size. As SDU discard functionality
> can not be enabled if windowsize > 2047 , RESET will occur more often
> and this problem would be prominent.
> A solution may be transfer information about HFN in RESET and RESET_ACK
> PDU.
> If this occurs one of the following things will take place.
> 1. LI check doesnt match for any PDU and all the PDUs are discarded.
>   in such a case there is information transfer but unncessary
>   wastage of bw and power.
> 2. If LI check doesnt match for any PDU and SDU discard functionality is
>   not enabled RLC would go back and forth in DTR and RPS states
>   without transmitting information as described in 1.
> 3. If LI check fails to detect errors(this is not very improbable
>   as the LI check is not sufficient if # of LIs is 1 and PU size
>   is big), RLC would pass incorrect data to upper layer.
>
> Thus we think RPS procedure should be corrected and made fool proof
> We would like to know views of RLC experts on the problems
> and suggested solutions.
>
> thanks
> atul
> **
> Atul Suresh Joshi
> Silicon Automation Systems (India) Ltd.
> phone res: +91-080-5483310
>   office: +91-080-5281461 extn:4241
> e-mail: atul@sasi.com
> **
> Status: RO
> X-Status:
> X-Keywords:
> X-UID: 11

3GPP TSG RAN WG2 meeting #16
Beijing, China, 09-13 October 2000

***Document* R2-002076**
e.g. for 3GPP use the format TP-99xxx
or for SMG, use the format P-99-xxx

CHANGE REQUEST

Please see embedded help file at the bottom of this page for instructions on how to fill in this form correctly.

25.322	CR	088r1	Current Version:	3.4.0

GSM (AA.BB) or 3G (AA.BBB) specification number ↑ *↑ CR number as allocated by MCC support team*

For submission to:	TSG-RAN #10	for approval	X	strategic		(for SMG Use only)
list expected approval meeting # here ↑		for information		non-strategic		

Form: CR cover sheet, version 2 for 3GPP and SMG *The latest version of this form is available from: ftp://ftp.3gpp.org/Information/CR-Form-v2.doc*

Proposed change affects: *(at least one should be marked with an X)*	(U)SIM		ME	X	UTRAN / Radio	X	Core Network	

Source:	TSG-RAN WG2	**Date:**	2000-09-21

Subject: Reset procedure

Work item:

Category: *(only one category shall be marked with an X)*

F	Correction	X	**Release:**	Phase 2	
A	Corresponds to a correction in an earlier release			Release 96	
B	Addition of feature			Release 97	
C	Functional modification of feature			Release 98	
D	Editorial modification			Release 99	X
				Release 00	

Reason for change:

1. The current RLC reset procedure can lead to unsynchronised hyper frame number (HFN) values between UE and UTRAN, which will lead to ciphering failure as discussed on the email reflector. To correct this mechanism, HFN values are indicated in the RESET PDU and RESET ACK PDU. With this correction, RLC can maintain synchronisation of HFN values during reset.

2. Minor editorial updates after RLC-adhoc has been made in 11.4.1.

Clauses affected: 9.2.1.7, 9.2.2.X (new), 9.3.3.2, 9.3.3.3, 11.4.1, 11.4.2.1, 11.4.3, 11.4.3.1, 11.4.4, 11.4.5.3

Other specs affected:

Other 3G core specifications		→ List of CRs:
Other GSM core specifications		→ List of CRs:
MS test specifications		→ List of CRs:
BSS test specifications		→ List of CRs:
O&M specifications		→ List of CRs:

Other comments:

help.doc

<--------- double-click here for help and instructions on how to create a CR.

9.2.1.7 RESET, RESET ACK PDU

The RESET PDU and RESET ACK PDU has a one-bit sequence number field (RSN). With the aid of this field the Receiver can define whether the received RESET PDU is transmitted by the Sender for the first time or whether it is a retransmission of a previous RESET PDU..

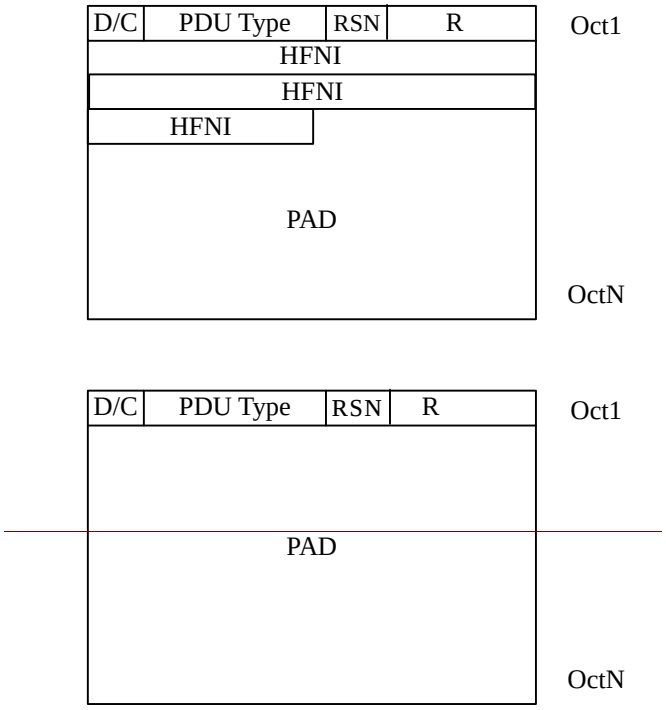


Figure 9.6: RESET, RESET ACK PDU

9.2.2.13 Reset Sequence Number (RSN)

Length: 1 bit

This field is used to indicate the sequence number of the transmitted RESET PDU. If this RESET PDU is a retransmission of the original RESET PDU then the retransmitted RESET PDU would have the same sequence number value as the original RESET PDU. Otherwise it will have the next reset sequence number. The initial value of this field is zero. The value of this field shall be reinitialized when the RLC is re-established. It shall not be reinitialized when the RLC is reset.

9.2.2.14~~X~~ Hyper Frame Number Indicator (HFNI)

Length: 20 bit

This field is used to indicate the hyper frame number (HFN) to the peer entity. With the aid of this field the HFN in UE and UTRAN can be synchronised.

9.3.3 State model for acknowledged mode entities

Figure 9.18 illustrates the state model for the acknowledged mode RLC entity (both transmitting and receiving). An acknowledged mode entity can be in one of following states.

9.3.3.1 Null State

In the null state the RLC entity does not exist and therefore it is not possible to transfer any data through it.

Upon reception of an CRLC-CONFIG-Req from higher layer the RLC entity is created and acknowledged data transfer ready state is entered.

9.3.3.2 Acknowledged Data Transfer Ready State

In the acknowledged data transfer ready state, acknowledged mode data can be exchanged between the entities. Upon reception of a CRLC-CONFIG-Req from higher layer the RLC entity is terminated and the null state is entered.

Upon errors in the protocol, the RLC entity sends a RESET PDU to its peer and enters the reset pending state.

Upon reception of a RESET PDU, the RLC entity resets the protocol (resets the state variables in 9.4 to their initial value and resets configurable parameters to their configured value, ~~increments the hyper frame number if the RSN field indicates that the RESET PDU is not a retransmitted RESET PDU~~ sets the hyper frame number HFN (DL HFN when the RESET is received in UE or UL HFN when the RESET is received in UTRAN) equal to the HFNI field in the RESET PDU~~)~~ and responds to the peer entity with a RESET ACK PDU.

Upon reception of a RESET ACK PDU, the RLC takes no action.

9.3.3.3 *Reset* Pending State

In the reset pending state the entity waits for a response from its peer entity and no data can be exchanged between the entities. Upon reception of CRLC-CONFIG-Req from higher layer the RLC entity is terminated and the null state is entered.

Upon reception of a RESET ACK PDU with the same RSN value as in the corresponding RESET PDU, the RLC entity resets the protocol (resets the state variables in 9.4 to their initial value, resets configurable parameters to their configured value, ~~-~~ sets the hyper frame number HFN (DL HFN when the RESET ACK is received in UE or UL HFN when the RESET ACK is received in UTRAN) equal to the HFNI field in the RESET ACK ~~increments the hyper frame number~~) and one of the following state transitions take place.

The RLC entity enters the acknowledged data transfer ready state if Reset Pending State was entered from Acknowledged Data Transfer Ready State or if Reset Pending State was entered from Local Suspend State and a CRLC-RESUME–Req was received in Reset Pending State.

The RLC entity enters into Local Suspend State if Reset Pending State was entered from Local Suspend State or if Reset Pending State was entered from Acknowledged Data Transfer Ready State and a CRLC-SUSPEND-Req was received in Reset Pending State.

Upon reception of a RESET ACK PDU with a different RSN value as in the corresponding RESET PDU the RESET ACK PDU is discarded.~~-~~

Upon reception of a RESET PDU, the RLC entity resets the protocol (resets the state variables in 9.4 to their initial value, resets configurable parameters to their configured value, sets the hyper frame number HFN (DL HFN when the RESET is received in UE or UL HFN when the RESET is received in UTRAN) equal to the HFNI field in the RESET PDU~~increments the hyper frame number if the RSN field indicates that the RESET PDU is not a retransmitted RESET PDU~~), sends a RESET ACK PDU and stays in the reset pending state.

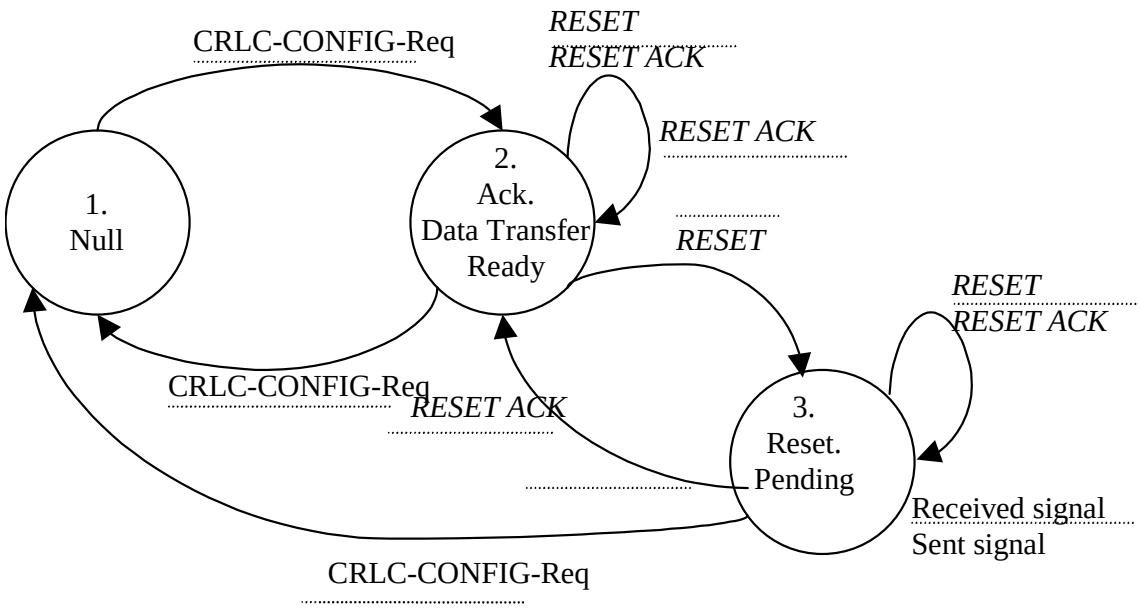


Figure 9.18: The state model for the acknowledged mode entities when reset is performed

9.3.3.4 Local Suspend State

Upon reception of CRLC-SUSPEND-Req from higher layer (RRC) in Acknowledge Data Transfer Ready State the RLC entity is suspended and the Local Suspend state is entered. In the Local Suspend state RLC shall not send a RLC-PDUs with a SN>=VT(S)+N. Upon reception of CRLC-RESUME-Req from higher layer (RRC) in this state, the RLC entity is resumed and the Data Transfer Ready state is entered.

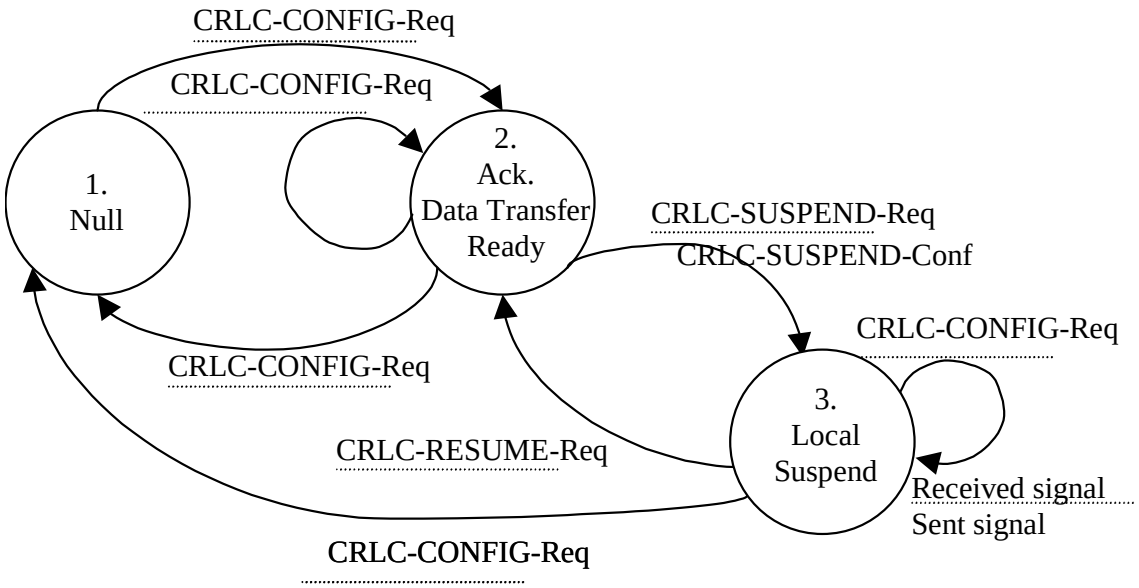


Figure 9.19: The state model for the acknowledged mode entities when local suspend is performed

11.4 RLC reset procedure

11.4.1 Purpose

The RLC reset procedure is used to reset two RLC peer entities, which are operating in acknowledged mode. Figure 11.4 below illustrates the elementary procedure for a RLC reset. The sender can be either the UE or the network and the receiver is either the network or the UE. During the reset procedure the hyper frame numbers (HFN) in UTRAN and UE are synchronised. Two HFNs used for ciphering needs to be synchronised, DL HFN in downlink and UL HFN in uplink. In the reset procedure, the highest~~currently used~~ UL HFN and DL HFN used by the RLC entity are exchanged between UE and UTRAN. After the reset procedure is terminated, the UL HFN and DL HFN shall be increased with one in both UE and UTRAN, and the updated HFN values shall be used after the reset procedure.

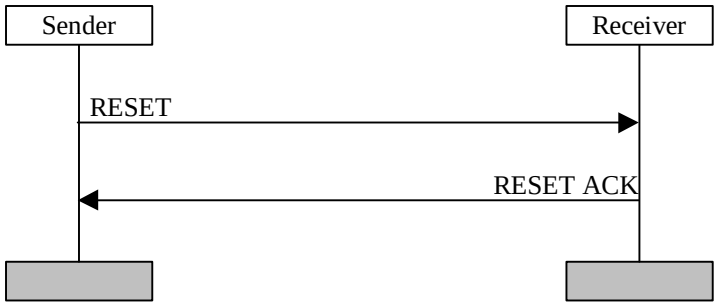


Figure 11.4: RLC reset procedure

11.4.2 Initiation

The procedure shall be initiated when a protocol error occurs.

The sender sends the RESET PDU when it is in data transfer ready state and enters reset pending state. The sender shall start the timer Timer_RST and increase VT(RST) with 1. The RESET PDU shall be transmitted on the DCCH logical channel if the sender is located in the control plane and on the DTCH if it is located in the user plane.

The RESET PDU has higher priority than data PDUs.

When a reset procedure has been initiated it can only be ended upon reception of a RESET ACK PDU with the same RSN value as in the corresponding RESET PDU, i.e., a reset procedure is not interrupted by the reception of a RESET PDU from the peer entity.

11.4.2.1 RESET PDU contents to set

The size of the RESET PDU shall be equal to one of the allowed PDU sizes. The hyper frame number indicator field (HFNI) shall be set equal to the currently used HFN (DL HFN when the RESET is sent by UTRAN or UL HFN when the RESET is sent by the UE). The RSN field shall indicate the sequence number of the RESET PDU. This sequence number is incremented every time a new RESET PDU is transmitted, but not when a RESET PDU is retransmitted.

11.4.3 Reception of the RESET PDU by the receiver

Upon reception of a RESET PDU the receiver shall respond with a RESET ACK PDU. The receiver resets the state variables in 9.4 to their initial value and resets configurable parameters to their configured value.

~~In the received RESET PDU the Receiver shall check the value of RSN (Reset Sequence Number) field. If the value of the RSN field is different from the RSN value in the previously received RESET PDU the~~ When a RESET PDU is received, the r~~R~~eceiver shall ~~increase the value of the~~set the HFN (DL HFN when the RESET is received in UE or UL HFN when the RESET is received in UTRAN) equal to the HFNI field in the received RESET PDU.~~by one.~~

~~If the value of the RSN is equal to the RSN value in the previously received RESET PDU, (i.e. the RESET PDU is a retransmitted RESET PDU) the value of the HFN shall not be increased and only a RESET ACK PDU shall be sent to the peer RLC entity.~~

The RESET ACK PDU shall be transmitted on the DCCH logical channel if the sender is located in the control plane and on the DTCH if it is located in the user plane.

The RESET ACK PDU has higher priority than data PDUs.

11.4.3.1 RESET ACK PDU contents to set

The size of the RESET ACK PDU shall be equal to one of the allowed PDU sizes. The RSN field shall always be set to the same value as in the corresponding RESET PDU. ~~.~~The hyper frame number indicator field (HFNI) shall be set equal to the currently used HFN (DL HFN when the RESET ACK is sent by UTRAN or UL HFN when the RESET ACK is sent by the UE).

11.4.4 Reception of the RESET ACK PDU by the sender

When the sender is in reset pending state and receives a RESET ACK PDU with the same RSN value as in the corresponding RESET PDU the Timer_RST shall be stopped and the value of the HFN (DL HFN when the RESET ACK is received in UE or UL HFN when the RESET ACK is received in UTRAN) shall be ~~increased by one~~set equal to the HFNI field in the received RESET ACK PDU. The sender resets the state variables in 9.4 to their initial value and resets configurable parameters to their configured value. The sender shall enter data transfer ready state.

Upon reception of a RESET ACK PDU with a different RSN value as in the corresponding RESET PDU the RESET ACK PDU is discarded.

Upon reception of a RESET ACK PDU in data transfer ready state the RESET ACK PDU is discarded.

11.4.5 Abnormal cases

11.4.5.1 Timer_RST timeout

Upon expiry of Timer_RST the sender shall retransmit the RESET PDU and increase VT(RST) with 1. In the retransmitted RESET PDU the value of the RSN field shall not be incremented.

11.4.5.2 VT(RST) ≥ MaxRST

If VT(RST) becomes larger or equal to MaxRST the RRC layer shall be informed.

11.4.5.3 Reception of the RESET PDU by the sender

Upon reception of a RESET PDU in reset pending state the sender shall respond with a RESET ACK PDU. The sender resets the state variables in 9.4 to their initial value, resets configurable parameters to their configured value. However, VT(RST) and Timer_RST are not reset. The hyper frame number, HFN (DL HFN when the RESET is received in UE or UL HFN when the RESET is received in UTRAN) is set equal to the HFNI field in the received RESET PDU~~incremented if the RSN field indicates that the RESET PDU is not a retransmitted RESET PDU~~. The sender shall stay in the reset pending state. The sender shall enter data transfer ready state only upon reception of a RESET ACK PDU with the same RSN value as in the corresponding RESET PDU.