3GPP TSG SA WG3 Security — S3#18 **S3-010150**

21 - 24 May, 2001

Phoenix, USA

3GPP TSG GERAN/SA3 joint meeting on 'GERAN security' **TD S3z(01)0065**
Madrid, Spain **Agenda item 6.2**
27 April 2001

3GPP TSG GERAN Adhoc on release 4 and beyond Tdoc GAHW-01 0245
Meeting No. 5
Seattle, WA, US
7-11th May 2001

Source: **TSG-GERAN Adhoc#5**

To: **TSG-SA WG3**

Cc:

Title: **Revised working assumptions made at the joint TSG GERAN / TSG SA WG3**

Contact person: **Jean-Michel Traynard**

jean-michel.traynard@icn.siemens.de

phone: +49 89 722 61048

Date: 14.05.2001
Document for: Information

1 Introduction

GERAN Adhoc#5 has revised the working assumptions made at the joint TSG GERAN / TSG SA WG3 as below and kindly asks TSG SA3 to take the changes into account for the further work.

2 Discussion

2.1 Working assumptions

2.1.1 General

- The stage 2 for GERAN security will be included temporarily in 3GPP TS 43.051 [1] and a reference to 3GPP TS 43.051 will be included in 3GPP TS 33.102 [2]. When the stage 2 becomes stable and the stage 3 changes commence, (at least part of) the stage 2 in 3GPP TS 43.051 [1] will be moved into 3GPP TS 33.102 [2].

2.1.2 RRC

- RRC messages that are integrity protected shall include a MAC-I of 32 bits.
- All RRC messages are integrity protected, with the exception of:
  - RR INITIALISATION REQUEST
  - HANDOVER ACCESS
  - PACKET NOTIFICATION
  - PAGING REQUEST TYPE 1

- PAGING REQUEST TYPE 2
- PAGING REQUEST TYPE 3
- PAGING RESPONSE
- SYSTEM INFORMATION TYPE 1 – 20
- CHANNEL REQUEST
- SYNCHRONIZATION CHANNEL INFORMATION
- RR STATUS
- EXTENDED MEASUREMENT ORDER
- EXTENDED MEASUREMENT REPORT
- MEASURMENT REPORT
- MEASUREMENT INFORMATION
- ENHANCED MEASUREMENT REPORT
- RRC CONNECTION REJECT
- RRC CONNECTION SETUP
- RRC CONNECTION REQUEST
- RRC CONNECTION SETUP COMPLETE

NOTE: Whether the IMMEDIATE ASSIGNMENT/IMMEDIATE ASSIGNMENT EXTENDED/IMMEDIATE ASSIGNMENT REJECT messages are integrity protected is FFS. See section 2.2.

2.1.3 RLC/MAC

- The following RLC/MAC control messages shall be integrity protected:
  - Packet Resource Request
  - Packet Uplink Assignment
  - Packet Downlink Assignment
  - The part of Packet Uplink Ack/Nack allocating radio resources if present
  - The part of (EGPRS) Packet Downlink Ack/Nack describing radio resources request if present
  - Packet Timeslot Reconfigure
  - Packet TBF Release
  - Packet Cell Change Order
  - Additional MS Radio Access Capabilities

- A MAC-I shorter than 32 bits is possible for RLC/MAC control messages that are integrity protected. The following rules shall be obeyed:
  - The minimum MAC-I length is assumed to be of 8 bits.
  - The sending entity shall include as many bits of MAC-I as possible (≥ 8 bits) to fill in possible spare bits of the last RLC/MAC block carrying the message, without causing (additional) segmentation.
  - The length of the MAC-I field needs to be included in the coding
  - The length of the MAC-I shall be ‘bit aligned’ and not necessarily ‘octet aligned’; i.e. any length between 8 and 32 bits shall be possible.
  - TSG SA WG3 shall define how shorter MAC-Is are generated (e.g. truncating to most/least significant bits).
- After contention resolution has been performed then RLC/MAC control messages shall be ciphered and integrity protected provided the MS is under coverage of its Serving BSS.

2.2 Open issues

2.2.1 General

The following questions have been brought up at this meeting, but not answered:

- Shall the IMMEDIATE ASSIGNMENT/IMMEDIATE ASSIGNMENT EXTENDED/IMMEDIATE ASSIGNMENT REJECT messages be integrity protected?
- Can a shorter MAC-I be used for RRC messages?

- How is ciphering/integrity protection provided when the controlling RAN node is not the same as the serving RAN node?
- What identity is used to page a MS?

NOTE: it is an SA3's requirement to use the (P)TMSI whenever possible in the paging request and the paging response, instead of the IMSI.

2.2.2 Immediate assignment

The following scenarios have been agreed.

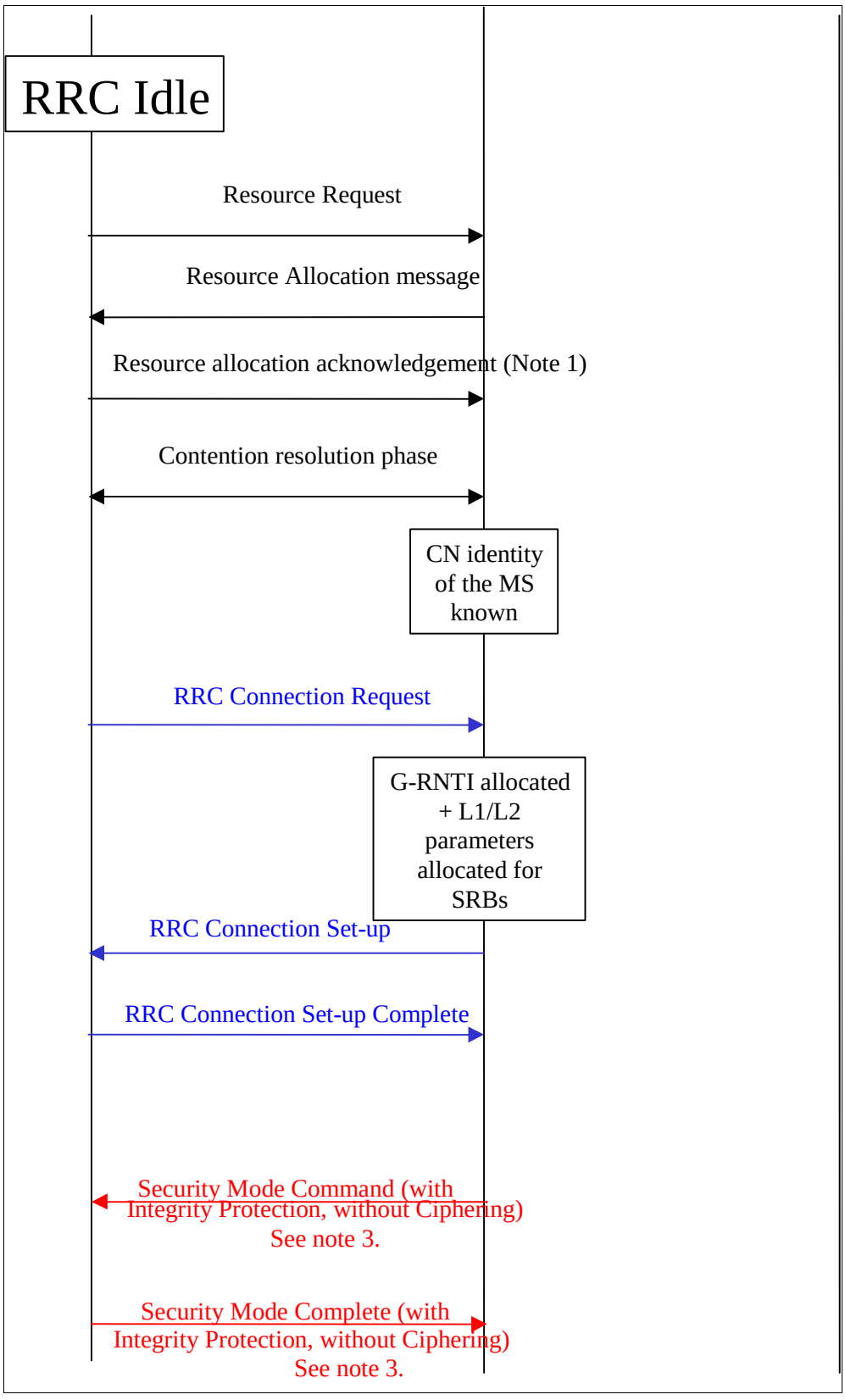
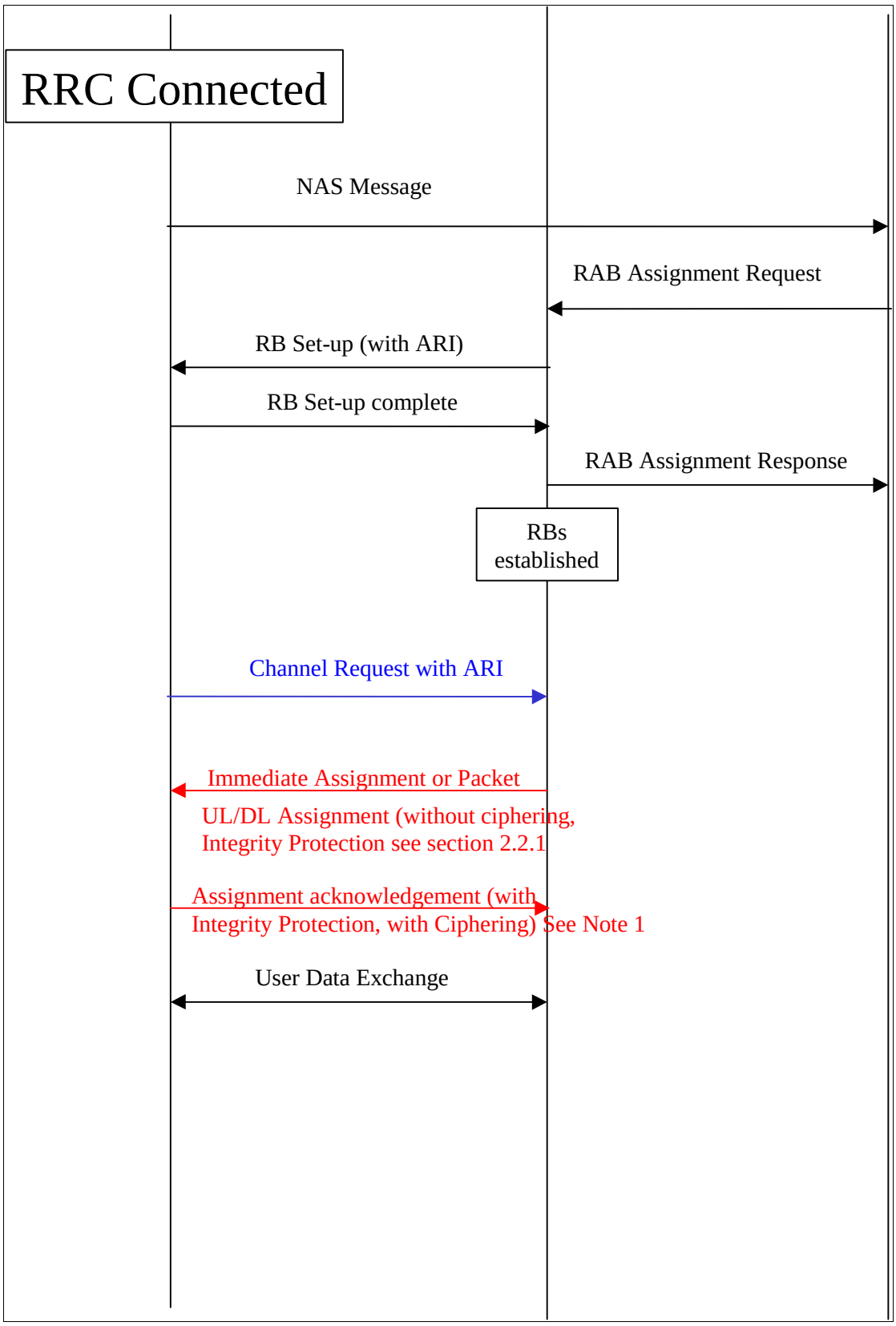


Figure 3 – Start of security procedures after RRC connection set-up


RRC Connected
NAS Message
RAB Assignment Request
RB Set-up (with ARI)
RB Set-up complete
RAB Assignment Response
RBs established
Channel Request with ARI
Immediate Assignment or Packet
UL/DL Assignment (without ciphering, Integrity Protection see section 2.2.1
Assignment acknowledgement (with Integrity Protection, with Ciphering) See Note 1
User Data Exchange

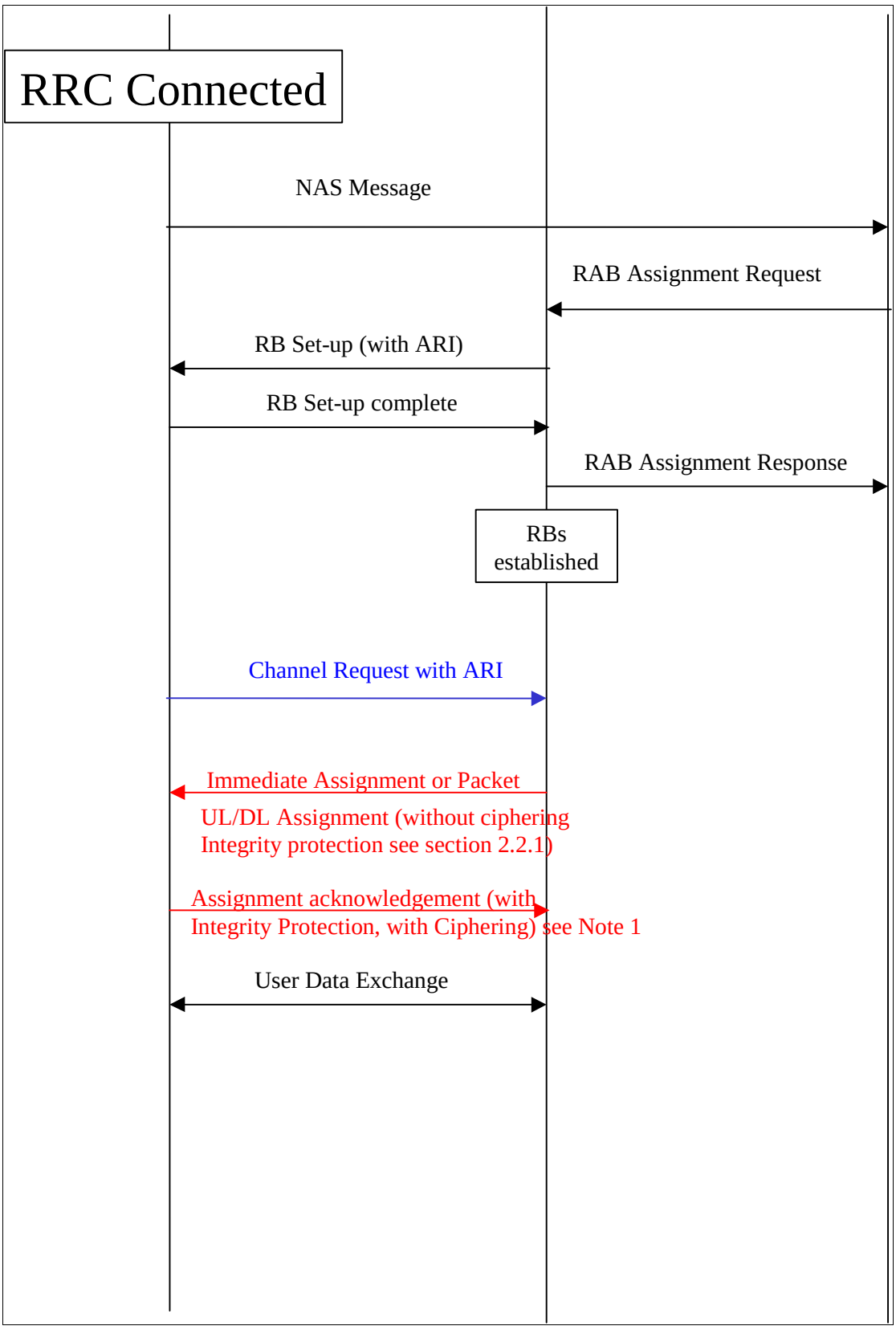


Figure 4 – Start of security procedures when user identity is known

NOTE: The assignment acknowledgement term does not constrain which actual RRC message will be used in GERAN to achieve this function.

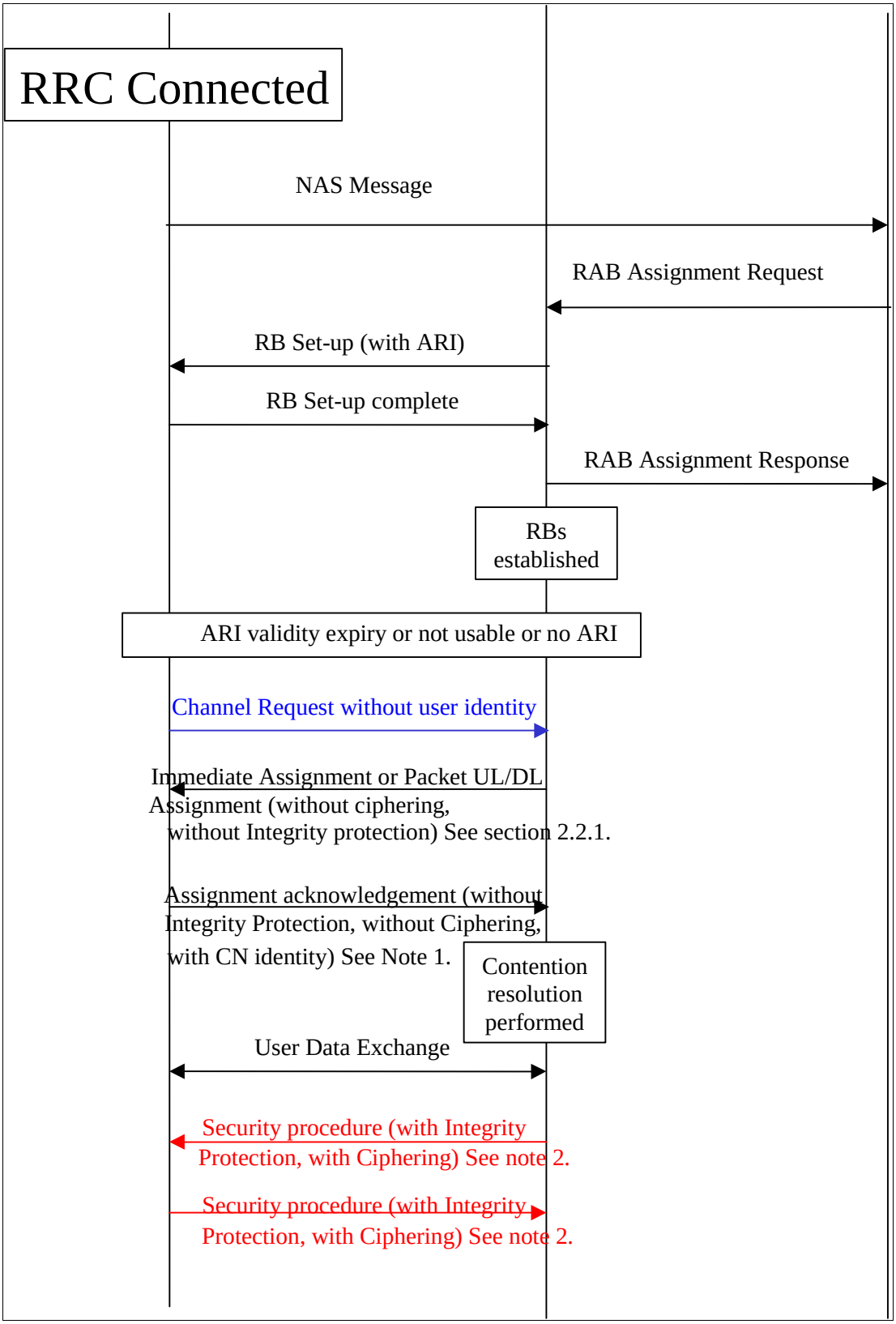


Figure 5 – Start of security procedures when user identity is no longer known to the GERAN

Note 1: The use/existence of the (Packet) Resource allocation Acknowledgement is FFS.

Note 2: This security procedure allows the receiving end to verify unambiguously the integrity of the sending end. It is an open issue whether this procedure will be realised with special messages or with any RRC message using a full sized MAC-I.

Note 3: Ciphering of Security mode Command and Security Mode Complete is conditioned by the availability of an agreed ciphering key in both network and MS. Integrity Protection of Security mode Command and Security Mode Complete is mandatory with a full sized MAC-I.

.

References

[1] 3GPP TS 43.051, “3rd Generation Partnership Project; Technical Specification Group GERAN; GSM/EDGE Radio Access Network (GERAN); Overall Description – Stage 2”

[2] 3GPP TS 33.102; “3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security Architecture”

Note

The following companies were represented at the GERAN Adhoc#5 held in Seattle:

Alcatel, AT&T Wireless, Cingular, Comsys, Ericsson, IDC, Lucent Technologies, Mannesmann, Motorola, Nokia, Nortel Networks, Qualcomm, Siemens.