

Title: Working assumptions and open issues
Source: Joint TSG GERAN / TSG SA WG 3 meeting
Date: 27th April 2001
Document for: Information

1 Introduction

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
 - MEASUREMENT 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
- Packet Uplink Ack/Nack
- Packet Timeslot Reconfigure
- Packet TBF Release
- Packet Cell Change Order
- 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.

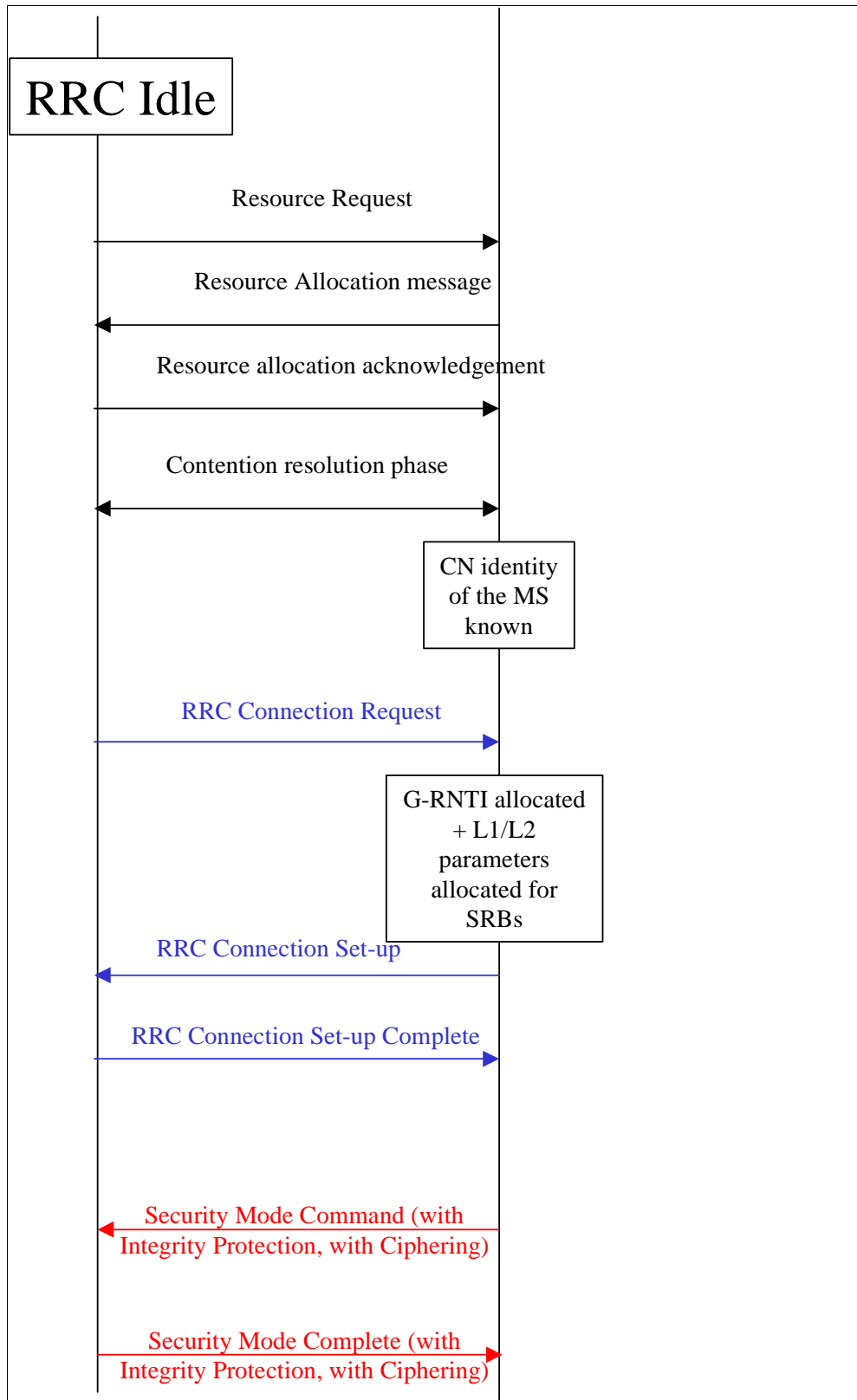


Figure 3 – Start of security procedures after RRC connection set-up

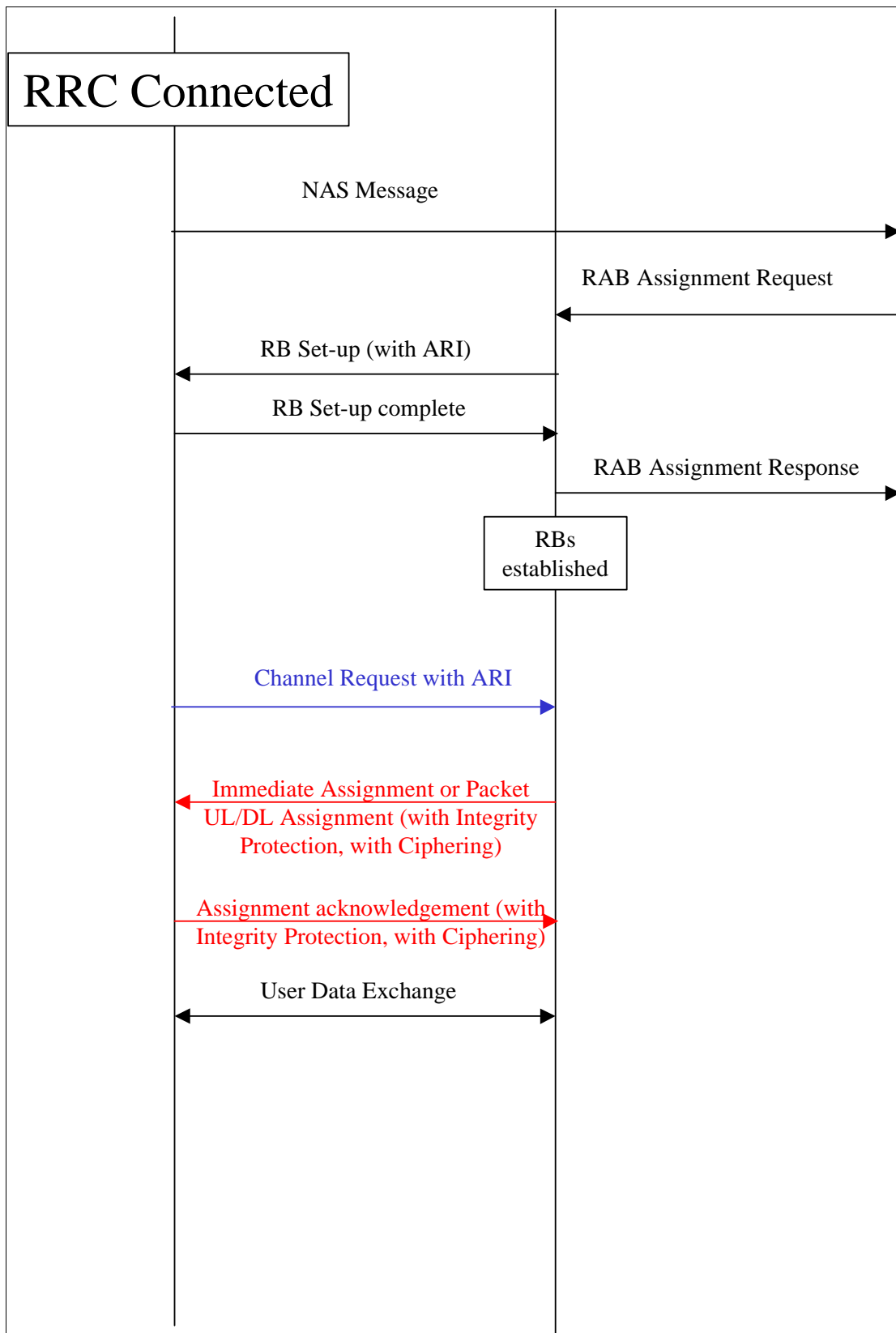


Figure 4 – Start of security procedures when user identity is known

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

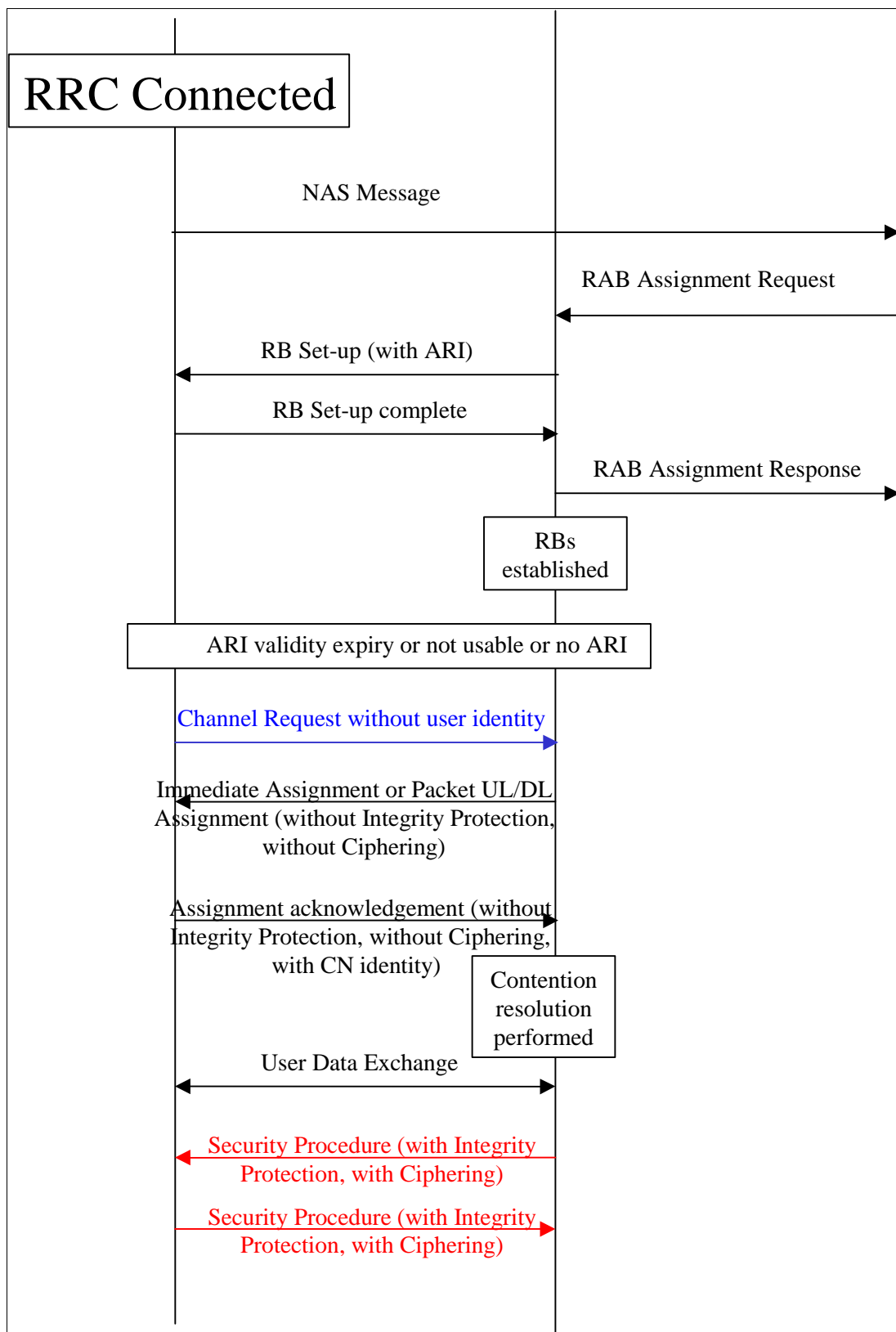


Figure 5 – Start of security procedures when user identity is no longer known to the GERAN

NOTE: The security procedure term does not constrain which actual RRC messages will be used in GERAN to achieve such functionality.

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"