TSG-RAN meeting #11 RP-010199
Palm Springs, CA, USA, 14-16 March 2001

Agenda Item: **5.2.3**

Source: Nokia

Title: **Checking the integrity of UE security capabilities**

Document for: Decision

---

1 Introduction

UE sends its capability information, including security capability (supported ciphering and integrity algorithms) to UTRAN during the RRC connection setup procedure. This information is sent without any protection (no ciphering nor integrity), since at this phase these functions cannot yet be used.

To ensure that UTRAN has received this information as it was sent by mobile, the "security capability" is returned in SECURITY MODE COMMAND message from UTRAN to UE. This message is integrity protected.

SA WG3 has noticed that there is a need to replay also the GSM Classmark information (CM2 and CM3), since illegal change of this information may cause the connection to be swithed to non-ciphered mode, when UE makes inter-system handover to GSM.

2 Solutions

According to current RRC specification (ver 3.5.0), UE sends GSM CM2 and CM3 (as mandatory infoelements) in the RRC CONNECTION SETUP COMPLETE message. Thus, to replay these to the UE, similar mechanisms as for the UTRAN UE Security Capability can be defined.

Since the length of GSM CM2+CM3 can be max 19 octects (5+14), adding them as such into SECURITY MODE COMMAND message is not the optimal solution.

Three alternative solutions have been identified:

1. Define a new RRC information element, including only the GSM ciphering algorithm capability. This requires 7 bits. This information element is then added to the SECURITY MODE COMMAND message. The drawback of this solution is that to encode this new information element, UTRAN RRC first has to decode the GSM CM2 and CM3 information elements, which encoding/decoding rules are specified in 3GPP TS 24.008.

2. See figure 1. The received GSM CM2+CM3 information (RRC infoelement "Inter-RAT UE radio access capability") is used for calculating MAC-I for the SECURITY MODE COMMAND message, but the actual CM2 + CM3 is not included in the RRC message. Using similar approach, also the size of the existing SECURITY MODE COMMAND can be reduced by 32 bits by taking the IE "Security Capability" out from the message and using it only for calculating the MAC-I. This solution has no drawbacks from security point of view, since the UE does not need to receive the actual "Security Capability" (nor "Inter-RAT UE radio access capability") but only a confirmation that UTRAN has received these infoelements correctly. This 'confirmation' can well be achieved by using the message authentication code (MAC-I) as described in figure 1. From the integrity algorithm viewpoint this solution is OK, since the length of the message used as input to the f9 algorithm does not need to be

the same as the length of the encoded message to be sent over the air. The drawback of this solution is that either these two information elements must be encoded separately by the (PER) encoder or their bit-coding has to be defined explicitely.

3. If the encoding of information elements "Inter-RAT UE radio access capability" and "Security Capability" for the calculation of MAC-I can not easily be defined (alternative 2), the same result is achieved by using the full encoded RRC_CONNECTION_SETUP_COMPLETE message instead of the two information elements only. It is probably quite easy from implementation viewpoint to save a copy of the encoded message before it is sent (UE side) or just after receiving, before passing it to the decoder (UTRAN side). This saved copy would then be used when calculating the MAC-I (UTRAN) and XMAC-I (UE) for the SECURITY_MODE_COMMAND message. Thus, MAC-I for SECURITY_MODE_COMMAND would be calculated by setting the MESSAGE-input parameter for the integrity algorithm as:

   MESSAGE = SECURITY_MODE_COMMAND + RRC_CONNECTION_SETUP_COMPLETE

   Naturally in this case the rules specified in 8.5.10.3 would be only applicable to the SECURITY_MODE_COMMAND part. The drawback (compared to 2) is that this solution requires a bit more memory.

   This solution is illustrated in figure 2.

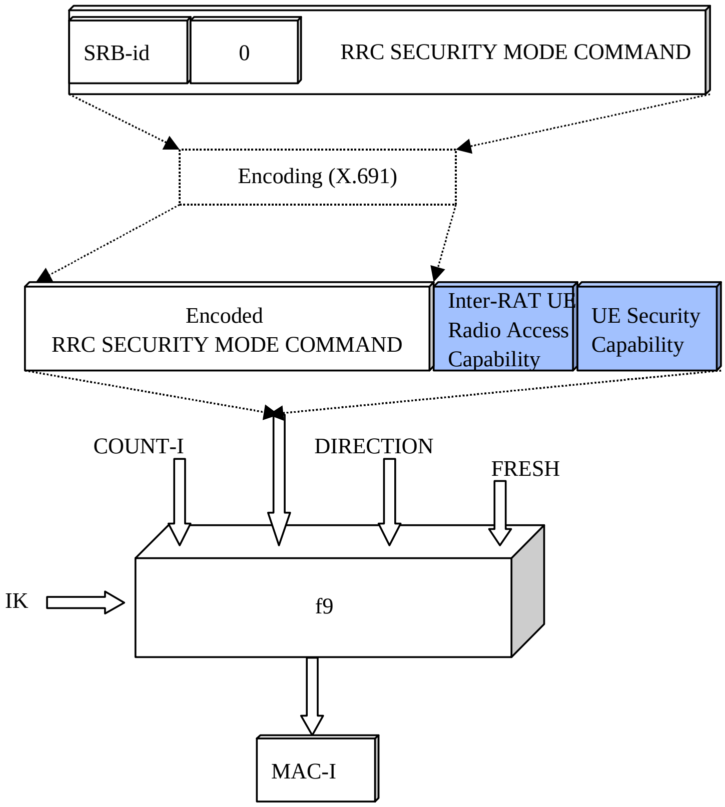
SRB-id
0
RRC SECURITY MODE COMMAND
Encoding (X.691)
Encoded
RRC SECURITY MODE COMMAND
Inter-RAT UE Radio Access Capability
UE Security Capability
COUNT-I
DIRECTION
FRESH
IK
f9
MAC-I

Figure 1: Calculating MAC-I (and XMAC-I) for RRC SECURITY MODE COMMAND message

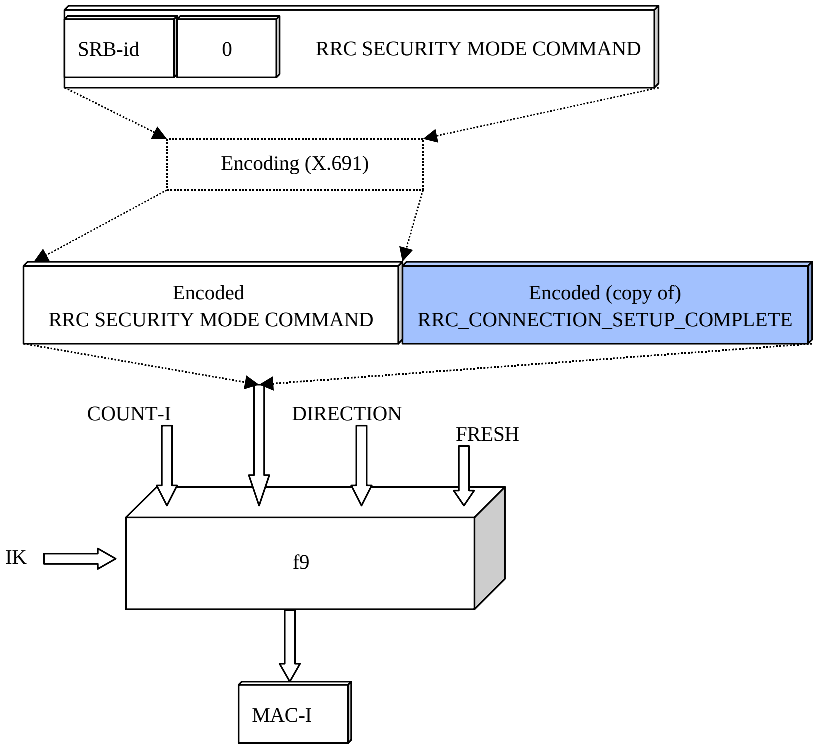
SRB-id
0
RRC SECURITY MODE COMMAND
Encoding (X.691)
Encoded
RRC SECURITY MODE COMMAND
Encoded (copy of)
RRC_CONNECTION_SETUP_COMPLETE
COUNT-I
DIRECTION
FRESH
IK
f9
MAC-I

Figure 2: Calculating MAC-I (and XMAC-I) for RRC SECURITY MODE COMMAND message

3 Proposal

Solution 1 was the preferred solution in RAN WG2 and it is therefore implemented in a proposed CR below.

TSG-RAN meeting #11 RP-010xxx
Palm Springs, CA, USA, 14-16 March 2001

CHANGE REQUEST

⌘ 25.331 CR 676 ⌘ rev R2 ⌘ Current version: 3.5.0 ⌘

*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: ⌘	Checking the integrity of UE security capabilities		
Source: ⌘	Nokia		
Work item code: ⌘		***Date:*** ⌘	21st Feb 2001
Category: ⌘	F	***Release:*** ⌘	R99

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: ⌘ SA WG3 has noticed that there is a need to replay the GSM Security Capability, since illegal change of this information may cause the connection to be swithed to non-ciphered mode, when UE makes inter-system handover to GSM.

Summary of change: ⌘ In revision 1 solution 1 (see above) is implemented: a new RRC information element is defined, including the GSM ciphering algorithm capability. This requires 7 bits. This information element is then added to the SECURITY MODE COMMAND message as an optional IE.

Consequences if not approved: ⌘ A man-in-the middle can force the connection to be switched to non-ciphered mode, when UE makes inter-system handover to GSM.

Clauses affected: ⌘ 8.1.12.3, 8.5.10.2, 10.2.41, 10.2.43, 10.3.8.x(new), 11.2, 11.3, 13.4.28

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://www.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2000-09 contains the specifications resulting from the September 2000 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.

8.1.12 Security mode control

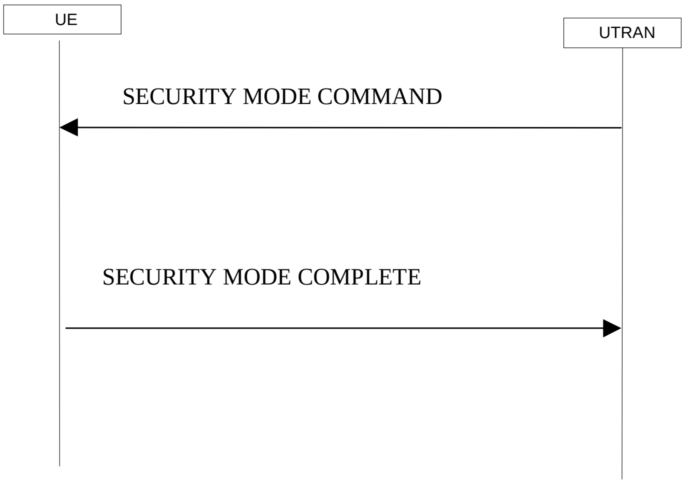

Figure 18: Security mode control procedure

8.1.12.1 General

The purpose of this procedure is to trigger the stop or start of ciphering or to command the restart of the ciphering with a new ciphering configuration, both for the signalling link and for any of the radio bearers.

It is also used to start integrity protection or to modify the integrity protection configuration for uplink and downlink signalling.

8.1.12.2 Initiation

8.1.12.2.1 Ciphering configuration change

To stop or start/restart ciphering, UTRAN sends a SECURITY MODE COMMAND message on the downlink DCCH in AM RLC using the old ciphering configuration. If no old ciphering configuration exists then the SECURITY MODE COMMAND is not ciphered.

Prior to sending the SECURITY MODE COMMAND, for the CN domain indicated in the IE "CN domain identity" in the SECURITY MODE COMMAND, UTRAN should:

- suspend all radio bearers using RLC-AM and RLC-UM;
- suspend all signalling radio bearers using RLC-AM and RLC-UM, except the signalling radio bearer used to send the SECURITY MODE COMMAND message on the downlink DCCH in RLC-AM;
- set, for the signalling radio bearer used to send the SECURITY MODE COMMAND, the "RLC send sequence number" in IE "Radio bearer downlink ciphering activation time info" in the IE "Ciphering mode info", at which time the new ciphering configuration shall be applied;
- include "Ciphering activation time for DPCH" in IE "Ciphering mode info" when a DPCH exists for radio bearers using transparent mode RLC;
- set, for each suspended radio bearer and signalling radio bearer, the "RLC send sequence number" in IE "Radio bearer downlink ciphering activation time info" in the IE "Ciphering mode info", at which time the new ciphering configuration shall be applied.

While suspended, radio bearers and signalling radio bearers shall not deliver RLC PDUs with sequence number greater than or equal to the number in IE "Radio bearer downlink ciphering activation time info".

When the successful delivery of the SECURITY MODE COMMAND has been confirmed by RLC, UTRAN shall:

- resume all the suspended radio bearers and signalling radio bearers. The old ciphering configuration shall be applied for the transmission of RLC PDUs with RLC sequence number less than the number indicated in the IE

"Radio bearer downlink ciphering activation time info", as sent to the UE. The new ciphering configuration shall be applied for the transmission of RLC PDUs with RLC sequence number greater than or equal to the number indicated in IE "Radio bearer downlink ciphering activation time info", sent to the UE.

8.1.12.2.2 Integrity protection configuration change

To start or modify integrity protection, UTRAN sends a SECURITY MODE COMMAND message on the downlink DCCH in AM RLC using the new integrity protection configuration.

8.1.12.3 Reception of SECURITY MODE COMMAND message by the UE

Upon reception of the SECURITY MODE COMMAND message, the UE shall perform the actions for the received information elements according to 8.6.

If the IE "Security capability" is the same as indicated by variable UE_CAPABILITY_TRANSFERRED, and the IE "GSM security capability" (if included in the SECURITY MODE COMMAND) is the same as indicated by the variable UE_CAPABILITY_TRANSFERRED, the UE shall:

- suspend all radio bearers and signalling radio bearers (except the signalling radio bearer used to receive the SECURITY MODE COMMAND message on the downlink DCCH in RLC-AM) using RLC-AM or RLC-UM that belong to the CN domain indicated in the IE "CN domain identity", with RLC sequence number greater than or equal to the number in IE "Radio bearer downlink ciphering activation time info" in the IE "Ciphering mode info";
- set the IE "RRC transaction identifier" in the SECURITY MODE COMPLETE message to the value of "RRC transaction identifier" in the entry for the SECURITY MODE CONTROL message in the table "Accepted transactions" in the variable TRANSACTIONS; and
- clear that entry;
- if the variable RB_UPLINK_CIPHERING_ACTIVATION_TIME_INFO is set:
    - include and set the IE "Radio bearer uplink ciphering activation time info" to the value of that variable, for the respective radio bearer and signalling radio bearer;
- when the radio bearers and signalling radio bearers have been suspended:
    - send a SECURITY MODE COMPLETE message on the uplink DCCH in AM RLC, using the old ciphering and the new integrity protection configurations;
- when the successful delivery of the SECURITY MODE COMPLETE message has been confirmed by RLC:
    - resume data transmission on any suspended radio bearer and signalling radio bearer mapped on RLC-AM or RLC-UM;
    - clear the variable RB_UPLINK_CIPHERING_ACTIVATION_TIME_INFO and the procedure ends. If a RLC reset or re-establishment occurs after the SECURITY MODE COMPLETE message has been confirmed by RLC, but before the activation time for the new ciphering configuration has been reached, then the activation time shall be ignored and the new ciphering configuration shall be applied immediately after the RLC reset or RLC re-establishment.

For radio bearers and signalling radio bearers used by the CN indicated in the IE "CN domain identity", the UE shall:

- if a new integrity protection key has been received:
    - in the downlink:
        - use the new key;
        - set the HFN component of the downlink COUNT-I to zero at the RRC sequence number indicated in IE "Downlink integrity protection activation info" included in the IE "Integrity protection mode info";

in the uplink:

use the new key;

    - set the HFN component of the uplink COUNT-I to zero at the RRC sequence number indicated in IE "Uplink integrity protection activation info" included in the IE "Integrity protection mode info";

- if a new ciphering key is available:
  - in the downlink:
    - use the new key;
    - set the HFN component of the downlink COUNT-C to zero at the RLC sequence number indicated in IE "Radio bearer downlink ciphering activation time info" in the IE "Ciphering mode info";
  - in the uplink:
    - use the new key;
    - set the HFN component of the uplink COUNT-C to zero at the RLC sequence number indicated in IE "Radio bearer uplink ciphering activation time info".

If the IE "Security capability" is not the same as indicated by the variable UE_CAPABILITY_TRANSFERRED, or the IE "GSM security capability" (if included in the SECURITY MODE COMMAND) is not the same as indicated by the variable UE_CAPABILITY_TRANSFERRED, the UE shall release all its radio resources, enter idle mode and the procedure ends on the UE side. Actions the UE shall perform when entering idle mode are given in subclause 8.5.2.

8.1.12.4 Cipher activation time too short

If the time specified by the IE "Ciphering activation time for DPCH" or the IE "Radio bearer downlink ciphering activation time info" contained in the IE "Ciphering mode info" has elapsed, the UE shall switch immediately to the new ciphering configuration.

8.1.12.5 Reception of SECURITY MODE COMPLETE message by the UTRAN

UTRAN should apply integrity protection on the received SECURITY MODE COMPLETE message and all subsequent messages with the new integrity protection configuration, if changed. When UTRAN has received a SECURITY MODE COMPLETE message and the integrity protection has successfully been applied, UTRAN shall:

- for radio bearers using RLC-AM or RLC-UM:
  - use the old ciphering configuration for received RLC PDUs with RLC sequence number less than the RLC sequence number indicated in the IE "Radio bearer uplink ciphering activation time info" sent by the UE;
  - use the new ciphering configuration for received RLC PDUs with RLC sequence number greater than or equal to the RLC sequence number indicated in the IE "Radio bearer uplink ciphering activation time info" sent by the UE;
  - if an RLC reset or re-establishment occurs after the SECURITY MODE COMPLETE message has been received by UTRAN before the activation time for the new ciphering configuration has been reached, ignore the activation time and apply the new ciphering configuration immediately after the RLC reset or RLC re-establishment;
- for radio bearers using RLC-TM:
  - use the new ciphering configuration for the received RLC PDUs at the CFN as indicated in the IE "Ciphering activation time for DPCH" in the IE "Ciphering mode info";
- and the procedure ends.

8.1.12.6 Invalid SECURITY MODE COMMAND message

If the SECURITY MODE COMMAND message contains a protocol error causing the variable PROTOCOL_ERROR_REJECT to be set to TRUE according to clause 9, the UE shall perform procedure specific error handling as follows:

- transmit a SECURITY MODE FAILURE message on the uplink DCCH using AM RLC;

- set the IE "RRC transaction identifier" in the SECURITY MODE FAILURE message to the value of "RRC transaction identifier" in the entry for the SECURITY MODE CONTROL message in the table "Rejected transactions" in the variable TRANSACTIONS; and
- clear that entry;
- set the IE "failure cause" to the cause value "protocol error";
- include the IE "Protocol error information" with contents set to the value of the variable PROTOCOL_ERROR_INFORMATION.
- when the successful delivery of the SECURITY MODE FAILURE message has been confirmed by RLC:
    - resume normal operation as if the invalid SECURITY MODE COMMAND message has not been received and the procedure ends.

8.5.10.1 Integrity protection in downlink

If the UE receives an RRC message on signalling radio bearer with RB identity n, the "Status" in the variable INTEGRITY_ PROTECTION_INFO has the value "Started" and the IE 'Integrity check info' is present the UE shall:

- check the value of the IE "RRC message sequence number" included in the IE "Integrity check info". If the RRC message sequence number is lower than the "Downlink RRC Message sequence number" for RB#n in the variable INTEGRITY_PROTECTION_INFO, the UE shall increment "Downlink RRC HFN" for RB#n in the variable INTEGRITY_PROTECTION_INFO with one. If the RRC message sequence number is equal to the "Downlink RRC Message sequence number" for RB#n in the variable INTEGRITY_PROTECTION_INFO, the message shall be discarded.
- calculate an expected message authentication code in accordance with subclause 8.5.10.3.
- compare the expected message authentication code with the value of the received IE "message authentication code" contained in the IE 'Integrity check info'.
    - If the expected message authentication code and the received message authentication code are the same, the integrity check is successful.
    - If the calculated expected message authentication code and the received message authentication code differ:
        - if the IE "RRC message sequence number" included in the IE "Integrity check info" is lower than the "Downlink RRC Message sequence number" for RB#n in the variable INTEGRITY_PROTECTION_INFO (in this case the "Downlink RRC HFN" for RB#n in the variable INTEGRITY_PROTECTION_INFO was incremented by one, as stated above):
            - decrement "Downlink RRC HFN" for RB#n in the variable INTEGRITY_PROTECTION_INFO by one.
            - discard the message.

If the UE receives an RRC message on signalling radio bearer with identity n, the "Status" in the variable INTEGRITY_ PROTECTION_INFO has the value "Started" and the IE 'Integrity check info' is not present the UE shall discard the message.

8.5.10.2 Integrity protection in uplink

Upon transmitting an RRC message using the signalling radio bearer with radio bearer identity n, and the "Status" in the variable INTEGRITY_ PROTECTION_INFO has the value "Started" the UE shall:

- increment "Uplink RRC Message sequence number" for RB#n in the variable INTEGRITY_PROTECTION_INFO with 1. When "Uplink RRC Message sequence number" for RB#n in the variable INTEGRITY_PROTECTION_INFO becomes 0, the UE shall increment "Uplink RRC HFN" for RB#n in the variable INTEGRITY_PROTECTION_INFO with 1
- calculate the message authentication code in accordance with subclause 8.5.10~~11~~.3
- replace the "Message authentication code" in the IE "Integrity check info" in the message with the calculated message authentication code.
- replace the "RRC Message sequence number" in the IE "Integrity check info" in the message with contents set to the new value of the "Uplink RRC Message sequence number" for RB#n in the variable INTEGRITY_PROTECTION_INFO

8.5.10.3 Calculation of message authentication code

The UE shall calculate the message authentication code in accordance with 3GPP TS 33.102. The input parameter MESSAGE (3GPP TS 33.102) for the integrity algorithm shall be constructed by:

- setting the "Message authentication code" in the IE "Integrity check info" in the message to the signalling radio bearer identity

- setting the "RRC Message sequence number" in the IE "Integrity check info" in the message to zero
- encoding the message
- appending RRC padding (if any) as a bitstring to the encoded bitstring as the least significant bits

10.2.43 SECURITY MODE COMMAND

This message is sent by UTRAN to start or reconfigure ciphering and/or integrity protection parameters.

RLC-SAP: AM

Logical channel: DCCH

Direction: UTRAN to UE

Information Element/Group name	Need	Multi	Type and reference	Semantics description
Message Type	MP		Message Type	
UE information elements				
RRC transaction identifier	MP		RRC transaction identifier 10.3.3.36	
Integrity check info	MP		Integrity check info 10.3.3.16	
Security capability	MP		Security capability 10.3.3.37	
Ciphering mode info	OP		Ciphering mode info 10.3.3.5	Only present if ciphering shall be controlled
Integrity protection mode info	OP		Integrity protection mode info 10.3.3.19	Only present if integrity protection shall be controlled
CN Information elements				
CN domain identity	MP		CN domain identity 10.3.1.1	Indicates which cipher and integrity protection keys are applicable
Other information elements				
UE system specific security capability	CH	1 to <maxSystemCapability>		This IE is included if the IE "Inter-RAT UE radio access capability" was included in RRC CONNECTION SETUP COMPLETE message
Inter-RAT UE security capability	MP		Inter-RAT UE security capability 10.3.8.x	

10.3.8.x Inter-RAT UE security capability

Information Element/Group name	Need	Multi	Type and reference	Semantics description
CHOICE *system*	MP			
>GSM				
>>GSM security capability	MP		Bit string(7)	"0000001_2": A5/1 supported, "0000010_2": A5/2 supported, "0000100_2": A5/3 supported, "0001000_2": A5/4 supported, "0010000_2": A5/5 supported, "0100000_2": A5/6 supported, "1000000_2": A5/7 supported

11.2 PDU definitions

```
--**************************************************************
--
-- TABULAR: The message type and integrity check info are not
-- visible in this module as they are defined in the class module.
-- Also, all FDD/TDD specific choices have the FDD option first
-- and TDD second, just for consistency.
--
--**************************************************************

PDU-definitions DEFINITIONS AUTOMATIC TAGS ::=

BEGIN

--**************************************************************
--
-- IE parameter types from other modules
--
--**************************************************************

IMPORTS

-- Core Network IEs :
    CN-DomainIdentity,
    CN-InformationInfo,
    NAS-Message,
    PagingRecordTypeID,
-- UTRAN Mobility IEs :
    URA-Identity,
-- User Equipment IEs :
    ActivationTime,
    C-RNTI,
    CapabilityUpdateRequirement,
    CellUpdateCause,
    CipheringAlgorithm,
    CipheringModeInfo,
    EstablishmentCause,
    FailureCauseWithProtErr,
    FailureCauseWithProtErrTrId,
    InitialUE-Identity,
    IntegrityProtActivationInfo,
    IntegrityProtectionModeInfo,
    N-308,
    PagingCause,
    PagingRecordList,
    ProtocolErrorIndicator,
    ProtocolErrorIndicatorWithMoreInfo,
    Rb-timer-indicator,
    Re-EstablishmentTimer,
    RedirectionInfo,
    RejectionCause,
    ReleaseCause,
    RRC-StateIndicator,
    RRC-TransactionIdentifier,
    SecurityCapability,
    START-Value,
    STARTList,
    U-RNTI,
    U-RNTI-Short,
    UE-RadioAccessCapability,
    UE-ConnTimersAndConstants,
    URA-UpdateCause,
    UTRAN-DRX-CycleLengthCoefficient,
    WaitTime,
-- Radio Bearer IEs :
    PredefinedConfigIdentity,
    RAB-Info,
    RAB-Info-Post,
    RAB-InformationList,
    RAB-InformationReconfigList,
    RAB-InformationSetupList,
    RB-ActivationTimeInfo,
    RB-ActivationTimeInfoList,
    RB-COUNT-C-InformationList,
    RB-COUNT-C-MSB-InformationList,
    RB-IdentityList,
    RB-InformationAffectedList,
    RB-InformationReconfigList,
    RB-InformationReleaseList,
    RB-InformationSetupList,
    RB-WithPDCP-InfoList,
    SRB-InformationSetupList,
    SRB-InformationSetupList2,
-- Transport Channel IEs:
    CPCH-SetID,
    DL-AddReconfTransChInfo2List,
    DL-AddReconfTransChInfoList,
    DL-CommonTransChInfo,
    DL-DeletedTransChInfoList,
    DRAC-StaticInformationList,
    TFC-Subset,
    TFCS-Identity,
    UL-AddReconfTransChInfoList,
    UL-CommonTransChInfo,
    UL-DeletedTransChInfoList,
-- Physical Channel IEs :
    AllocationPeriodInfo,
    Alpha,
    CCTrCH-PowerControlInfo,
    ConstantValue,
    CPCH-SetInfo,
    DL-CommonInformation,
    DL-CommonInformationPost,
    DL-InformationPerRL,
    DL-InformationPerRL-List,
    DL-InformationPerRL-ListPostFDD,
    DL-InformationPerRL-PostTDD,
    DL-DPCH-PowerControlInfo,
    DL-PDSCH-Information,
    DPCH-CompressedModeStatusInfo,
    FrequencyInfo,
    FrequencyInfoFDD,
    FrequencyInfoTDD,
    IndividualTS-InterferenceList,
    MaxAllowedUL-TX-Power,
    PDSCH-CapacityAllocationInfo,
    PDSCH-Identity,
    PDSCH-Info,
    PRACH-RACH-Info,
    PrimaryCCPCH-TX-Power,
    PUSCH-CapacityAllocationInfo,
    PUSCH-Identity,
    RL-AdditionInformationList,
    RL-RemovalInformationList,
    SSDT-Information,
    TFC-ControlDuration,
    TimeslotList,
    TX-DiversityMode,
    UL-ChannelRequirement,
    UL-ChannelRequirementWithCPCH-SetID,
    UL-DPCH-Info,
    UL-DPCH-InfoPostFDD,
    UL-DPCH-InfoPostTDD,
    UL-TimingAdvance,
    UL-TimingAdvanceControl,
-- Measurement IEs :
    AdditionalMeasurementID-List,
    EventResults,
    InterRAT-TargetCellDescription,
    MeasuredResults,
    MeasuredResultsList,
    MeasuredResultsOnRACH,
    MeasurementCommand,
    MeasurementIdentity,
    MeasurementReportingMode,
    PrimaryCCPCH-RSCP,
    TimeslotListWithISCP,
    TrafficVolumeMeasuredResultsList,
    UP-GPS-AssistanceData,
    UP-OTDOA-AssistanceData,
-- Other IEs :
    BCCH-ModificationInfo,
    CDMA2000-MessageList,
    GSM-MessageList,
    InterRAT-ChangeFailureCause,
    InterRAT-HO-Failure,
    InterRAT-UE-RadioAccessCapabilityList,
    InterRAT-UE-SecurityCapList,
    InterRATMessage,
    IntraDomainNasNodeSelector,
    ProtocolErrorInformation,
    ProtocolErrorMoreInformation,
    Rplmn-Information,
    SegCount,
    SegmentIndex,
    SFN-Prime,
    SIB-Data-fixed,
    SIB-Data-variable,
    SIB-Type
FROM InformationElements
```

```
    maxSIBperMsg,
    maxSystemCapability
FROM Constant-definitions;



-- ***************************************************
--
-- SECURITY MODE COMMAND
--
-- ***************************************************

SecurityModeCommand-r3-IEs ::= SEQUENCE {
-- TABULAR: Integrity protection shall always be performed on this message.
    -- User equipment IEs
        rrc-TransactionIdentifier       RRC-TransactionIdentifier,
        securityCapability              SecurityCapability,
        cipheringModeInfo               CipheringModeInfo                   OPTIONAL,
        integrityProtectionModeInfo     IntegrityProtectionModeInfo         OPTIONAL,
    -- Core network IEs
        cn-DomainIdentity               CN-DomainIdentity,
    --  Other IEs
        ue-SystemSpecificSecurityCap    InterRAT-UE-SecurityCapList         OPTIONAL

}
```

11.3 Information element definitions

```
-- ***************************************************
--
--     OTHER INFORMATION ELEMENTS (10.3.8)
--
-- ***************************************************

GsmSecurityCapability ::=           BIT STRING (SIZE (7))

InterRAT-UE-SecurityCapability ::= CHOICE {
    gsm                                 SEQUENCE {
        gsmSecurityCapability           GsmSecurityCapability
    }
}

InterRAT-UE-SecurityCapList ::=     SEQUENCE (SIZE(1..maxInterSysMessages)) OF
                                        InterRAT-UE-SecurityCapability
```

13.4.28 UE_CAPABILITY_TRANSFERRED

This variable stores information about which UE capabilities that have been transferred to UTRAN.

Information Element/Group name	Need	Multi	Type and reference	Semantics description
UE radio access capability	OP		UE radio access capability 10.3.3.42	
UE system specific capability	OP		~~Inter-RAT message 10.3.8.8~~Inter-RAT UE radio access capability 10.3.8.7	Includes inter-RAT classmark