3GPP TR 33.859 V11.1.0 (2012-03)

Technical Report

3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Study on the introduction of key hierarchy in Universal Terrestrial Radio Access Network (UTRAN) (Release 11)

Keywords
EUTRAN, UTRAN, security, key management

3GPP

Postal address

3GPP support office address
650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet
http://www.3gpp.org

Contents

Foreword

This Technical Report has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

- x the first digit:
  - 1 presented to TSG for information;
  - 2 presented to TSG for approval;
  - 3 or greater indicates TSG approved document under change control.
- y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the document.

Introduction

Deployments of HSPA UTRAN with part of the RNC functionality, including user plane and signaling protection, moved to HSPA NodeBs present the same threat environment as encountered by E-UTRAN eNBs. To help counter the threats towards the base stations, E UTRAN has introduced a key hierarchy and a key-refresh mechanism, making security breaches of the keys used on the air-interface much less severe. With the current key management in UTRAN it is impossible to achieve the same level of protection as in E-UTRAN.

The introduction of a key hierarchy in UTRAN gives an increased protection level and achieves additional benefits by yielding more secure interworking between UTRAN and E-UTRAN. It also implies a simpler handling in the sense that key management becomes more aligned in the two systems.

1 Scope

The objective of this work item is to study potential solutions for introducing an "E-UTRAN-like" key hierarchy in UTRAN, to improve the security level in UTRAN in the presence of the new deployment scenarios and to ensure that a security breach in UTRAN will not propagate into E-UTRAN. The study covers the technical feasibility and consequences. The impacts of such potential solution on UTRAN of earlier releases are identified. Interworking with earlier releases of UTRAN, GERAN and E-UTRAN is also studied.

The UTRAN key hierarchy is assumed to be built on top of (R99+) UMTS AKA, without requiring any changes to the authentication protocol or USIM. Therefore, it could in principle be used also in GERAN as long as USIMs are used and the SGSN, MSC/VLR, and ME are updated. However, the benefit of introducing the key hierarchy in GPRS is smaller than for the circuit switched part, as the traffic protection already terminates in the core network. Solution details for GERAN are not discussed further.

The study covers both PS and CS part of UTRAN.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] SP-070782, "FS on UTRAN key management enhancements".

[3] 3GPP TS 33.102: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security architecture".

[4] 3GPP TS 33.401: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3GPP System Architecture Evolution (SAE): Security Architecture".

[5] 3GPP TS 24.008: "3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Mobile radio interface Layer 3 specification; Core network protocols; Stage 3".

[6] 3GPP TS 24.301: "3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3".

[7] 3GPP TS 29.060: "3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; General Packet Radio Service (GPRS); GPRS Tunnelling Protocol (GTP) across the Gn and Gp interface".

[8] 3GPP TS 29.274: "3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; 3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunnelling Protocol for Control plane (GTPv2-C); Stage 3".

[9] 3GPP TS 25.413: "3rd Generation Partnership Project; Technical Specification Group Radio Access Network; UTRAN Iu interface Radio Access Network Application Part (RANAP) signalling".

[10] 3GPP TS 25.331: "3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Radio Resource Control (RRC); Protocol Specification".

[11] 3GPP TS 23.060: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; General Packet Radio Service (GPRS); Service description; Stage 2".

[12] 3GPP TS 33.220: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Generic Authentication Architecture (GAA); Generic bootstrapping architecture".

[13] 3GPP TS 25.423: "3rd Generation Partnership Project; Technical Specification Group Radio Access Network; UTRAN Iur interface RNSAP signalling".

[14] 3GPP TS 36.413: "3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access Network (E-UTRAN); S1 Application Protocol (S1AP)".

[15] 3GPP TS 36.331: "3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC); Protocol specification".

[16] 3GPP TS 29.002: "3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Mobile Application Part (MAP) specification".

[17] 3GPP TS 44.018: "3rd Generation Partnership Project; Technical Specification Group GSM/EDGE Radio Access Network; Mobile radio interface layer 3 specification; Radio Resource Control (RRC) protocol".

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in TR 21.905 [1].

UTRAN Key Hierarchy: This refers to the key hierarchy studied in this TR. The root key is KASMEU, see next.

K_{ASMEU}: Root key of the UTRAN key hierarchy. (Relation to KASME is elaborated below)

K_{RNC}: A key kept in an RNC used to derive keying material for use on the Uu reference point.

ME_U: A UMTS terminal not aware of the UTRAN key hierarchy

ME_U+: A UMTS only terminal aware of the UTRAN key hierarchy

SGSN, MSC/VLR, RNC: Legacy nodes, not upgraded to support the UTRAN key hierarchy

SGSN+, MSC/VLR+, RNC+: The corresponding nodes upgraded to support the UTRAN key hierarchy

When it is not important for the discussion whether it is an SGSN or an MSC/VLR, the generic term Core Network Node (CNN) will be used to denote the entity. The term CNN+ is used to denote a Core Network Node that is aware of the UTRAN KH.

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in TR 21.905 [1].

AKA Authentication and Key Agreement
AV Authentication Vector

CK	Ciphering Key
CN	Core Network
CNN	Core Network Node
CS	Circuit Switched
DL	Downlink
EPS	Evolved Packet System
E-UTRAN	Evolved UTRAN
GERAN	GSM/EDGE Radio Access Network
HO	Hand over
HSPA	High Speed Packet Access
HSS	Home Subscriber Server
KDF	Key Derivation Function
IE	Information Element
IK	Integrity Key
IRAT	Inter RAT
KSI	Key Set Identifier
LAU	Location Area Update
LSB	Least Significant Bit
LTE	Long Term Evolution
ME	Mobile Entity
MME	Mobility Management Entity
MSC	Mobile services Switching Centre
NAS	Non Access Stratum
NCC	Next-hop Chaining Counter
NH	Next Hop
NW	Network
PLMN	Public Land Mobile Network
PS	Packet Switched
RAN	Radio Access Network
RANAP	RAN Application Part
RAT	Radio Access Technology
RAU	Routing Area Update
RRC	Radio Resource Control
RNC	Radio Network Controller
RNS	Radio Network Subsystem
SGSN	Serving GPRS Support Node
SMC	Security Mode Command
SRNC	Serving RNC
SRNS	Serving RNS
TAU	Tracking Area Update
UE	User Equipment
UEA	UMTS Encryption Algorithm
UIA	UMTS Integrity Algorithm
UICC	Universal Integrated Circuit Card
UL	Uplink
UMTS	Universal Mobile Telecommunications System
UP	User Plane
URA	UTRAN Registration Area
UTRAN	Universal Terrestrial Radio Access Network
UTRAN KH	UTRAN Key Hierarchy
VLR	Visited Location Registry

4 General

4.1 System overview

4.1.1 Architecture

This clause provides a system overview and a discussion on requirements and basic ideas for technical solutions on how a key hierarchy can be introduced in UTRAN.

The following high level system model is used.

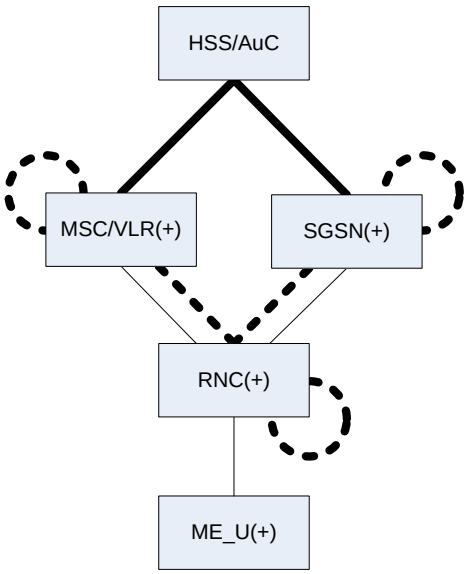

Figure 4.1.1 - System Overview. The figure does not show all possible combinations of involved nodes.

The lines in Figure 4.1.1-1 show the signalling / interworking cases that need to be handled.

Thick solid line: transfer of AVs.

Thin solid line: AKA and security mode command signalling.

Thick dashed line: context transfer and/or transfer of unused AVs.

It should be noted that the present TR assumes transparency with respect to IRAT mobility procedures, i.e. this TR aims to provide a solutions which are fully compatible with already defined IRAT mobility procedures. This does not preclude considering changes to IRAT mobility procedures that are beneficial and cause no issues when inter-working with legacy nodes. The major issue in the design that is foreseen is how to signal between entities that the new key hierarchy can/shall be used in UTRAN. In particular, SRNS relocation should work with the UTRAN key hierarchy. The required signalling along each of the paths of Figure 4.1.1-1 is the main concern of this document.

4.1.2 Node and terminal types

4.1.2.1 Types of MEs

First the different types of terminals that needs to be considered when analyzing the system requirements is identified. The following types of MEs defined by their key handling capabilities have to be considered.

- ME_U: The ME is a UMTS terminal of an earlier release compared to when UTRAN KH is introduced
- ME_U+: The ME is a UMTS terminal aware of the UTRAN key hierarchy.

E-UTRAN only and GERAN only terminals are out of scope, as these devices will never access UTRAN.

An ME that has the capability to handle UTRAN KH is denoted by ME+. An ME that does not have this capability is referred to by the notation ME. If it is irrelevant whether an ME or ME+ is under consideration, ME(*) is used.

4.1.2.2 Types of Core Network Nodes (CNN)

In a way fully analogous to how the different types of MEs are denoted, a SGSN capable of handling the UTRAN key hierarchy will be denoted SGSN+. If it is irrelevant if an SGSN is capable of handling the UTRAN key hierarchy or not, the notation SGSN(*) is used. Similarly, RNC+ is used to denote an RNC that may implement additional functionality to support the UTRAN key hierarchy.

The generic term Core Network Node (CNN) will be used to denote an SGSN or an MSC/VLR, so the term CNN+ is used to denote a Core Network Node that is aware of the UTRAN KH.

4.2 Assumptions and requirements

The study is based on the following assumptions (some of which have already been mentioned).

- R99+ UICC implementing UMTS AKA shall be a sufficient base for the UTRAN key hierarchy.
- CNN+ can distinguish between ME and ME+ at initial attach.
- When serving an ME+, CNN+ can add new IEs to the ME+ signaling.
- New IEs, used by CNN+, will be ignored when received by CNN or an MME (of earlier release than when UTRAN KH is introduced) at handover. This is already fulfilled by the GTP protocol.
- At change of core network anchor node to a CNN(+), the source MME or CNN(+) does not have to be able to distinguish between a target CNN and CNN+.
- The UTRAN key hierarchy shall have no/minimal impact on GERAN and earlier releases of UTRAN.
- CNN and MME of earlier releases shall be able to interoperate with CNN and MME that support UTRAN KH.
- CNN+ could be aware of whether the RNC(+) is capable of the UTRAN key hierarchy.
- It is assumed that strong platform security and backhaul security is provided. An example of platform security requirements are the requirements of clause 5.3 of TS 33.401.
- Whenever this technical report mentions a collapsed RNC/NodeB, it should be understood that this also includes Home NodeBs.

4.3 Desired security properties

The clause considers the security properties that would be desirable to include in an enhancement of UTRAN keying. The final decision on whether to include such properties needs to be taken once the complexity of such solutions are known.

When introducing a key hierarchy in UTRAN, four "levels" of security can be identified that may be worth including;

- Binding the AVs to use in a particular network, i.e., only exposing CK and IK to ME+ and HSS and above
- Separation of CN and RAN keys by "vertical" key derivation. This includes providing fresh keying material to the RAN level at every Idle to Active transition.
- Separation also of RAN keys by "horizontal" key derivation at intra-UTRAN handovers, similar to E-UTRAN eNB handovers. That is, when changing to a new node in charge of UP encryption/decryption, the key(s) are updated.
- The key derivations make the keys depend on the algorithm identifiers.

Note that the terms "vertical key derivation" and "horizontal key derivation" is not the same concept as in TS 33.401, but rather refers to the keys relative positions in the UTRAN key hierarchy.

Regarding the binding of AVs, it appears undesirable that HSS sets the key in the AV to be K_{ASMEU} derived from (CK, IK). First of all, it would require that the HSS is aware of whether the CNN(*) is capable of the UTRAN key hierarchy, since legacy nodes cannot handle a K_{ASMEU}. To avoid this problem, the HSS could include both (CK, IK) and K_{ASMEU}, the latter being ignored by a CNN (which is not updated). However, this would defeat the security benefit of not exposing (CK, IK) outside the HSS Moreover, performing the K_{ASMEU} derivation in the HSS would require that the HSS is made aware of whether the ME(*) is an ME or an ME+. While it would be possible to introduce additional signaling to resolve these issues, the benefits appear somewhat questionable, at least as long legacy CNNs requiring (CK, IK) are still in deployment.

Regarding the 2nd bullet above it is clearly beneficial to separate the CN and RAN keys and in particular if fresh RAN keys can be provided from Idle to Active transition. Hence the following property should be included in this study

Property 1: It shall be possible to separate the CN and RAN level key and in particular it should be possible to provide fresh RAN keys at every Idle to Active transition.

Due to the architectural differences between UTRAN and E-UTRAN (the former having an anchor in the Serving RNC) it appears that the horizontal key derivation would be more difficult to handle in UTRAN and provides less benefit than in E-UTRAN, since Serving RNC relocation is far less frequent than eNB handovers. However, with collapsed RNC/NodeB deployments (e.g., HSPA), SRNC relocation may be of higher interest to protect by means of key derivation.

Property 2: It shall be possible to update keys at intra-UTRAN handovers (e.g. SRNC mobility).

Rationale: Improved "backward" security in UTRAN.

The 4th bullet covers good cryptographic practice and hence is worth including in this study to provide separation between algorithms.

Property 3: It shall be possible to make the key derivations depend on the algorithm identifiers

The current specifications of UTRAN imply that the context handed over from UTRAN to E-UTRAN must depend on CK, IK (which have been used on the air interface). Even if the scope of this study was extended to cover enhancements for IRAT handovers, compatibility with existing specifications imply that a security breach in UTRAN (break of algorithm or compromise of a collapsed HSPA NodeB) may propagate into E-UTRAN, no matter how strong key conversion functions are used to derive the E-UTRAN keys. A UTRAN key hierarchy can thus not completely remove these issues but if the UTRAN key hierarchy separates CN keys from RAN keys, a handover based on UTRAN CN keys will indeed be made more secure even in the presence of security breaches in UTRAN. This is in line with what is specified as a requirement in TS 22.258, namely:

Property 4: "Any possible lapse in security in one access technology shall not compromise security of other accesses."

4.4 The UTRAN Key Hierarchy

4.4.1 Proposed solution 1

The already defined E-UTRAN key hierarchy is, as noted, required to be unchanged (using UMTS AKA and producing K_{ASME} from CK, IK and further deriving K_{eNB} and NAS keys). Notice that E-UTRAN uses many more keys than UTRAN does so that the hierarchies will not be identical. The UTRAN key hierarchy is assumed to be based on a key K_{RNC}, derived from USIM provided (CK, IK) by CNN+ and ME+ respectively. And another two new keys are defined: CK_U and IK_U, which are derived from K_{RNC}. CK_U is the ciphering key and IK_U is the integrity key. In order to avoid CK/IK exposure of RAN and air interface during SGSN relocation, one new pair of keys (CK_L, IK_L) which are derived by CNN+ and ME+ respectively are also defined. The UTRAN Key Hierarchy is shown in the figure 4.4.1-1 below:

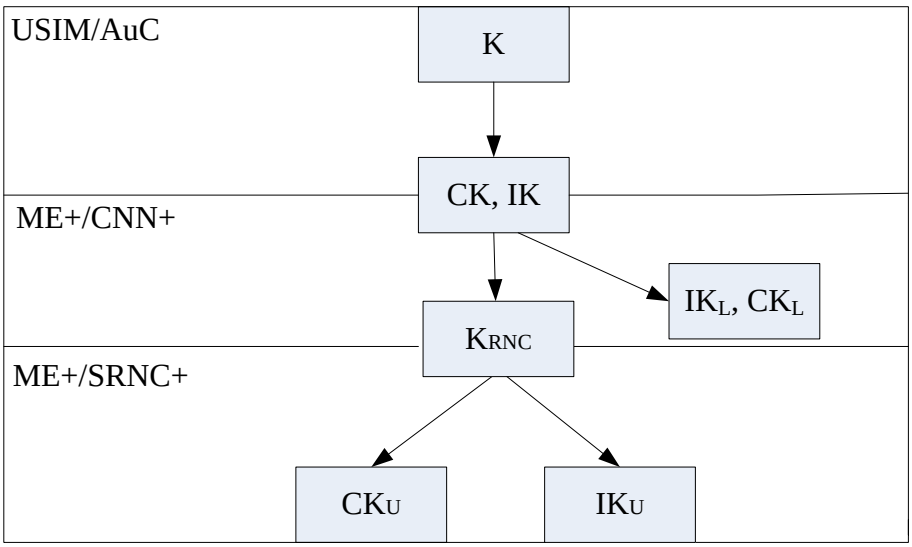

Figure 4.4.1-1: UTRAN Key hierarchy

Figure 4.4.1-2 shows the dependencies between the keys at initial setup (i.e., when the UE goes to Active mode), and at combined hard handover and SRNS relocation as well as combined cell/URA updated and SRNS relocation. At the initial connection setup, three sets of keys are derived by CNN+:

- K_{RNC}= KDF(IK||CK, COUNT), which will be used to derive IK_U/CK_U by SRNC+ and ME+ respectively.
- K_{RNC}*=KDF(IK||CK, K_{RNC}), which will be used to derive IK_U/CK_U during SRNS relocation.
- (IK_L, CK_L)=KDF(IK||CK), which will be used as mapping legacy IK/CK when target CNN is a legacy one.

Where COUNT is a counter value maintained by CNN+. When a new AV is used, the COUNT is initialized to 0.

K_{RNC}, K_{RNC}* and corresponding NCC (which is used to synchronize key derivation between network and UE) shall be transmitted to SRNC+ at the intial connetion setup. SRNC+ shall derive IK_U/CK_U based on the received K_{RNC} and other parameters.When SRNC relocation is performed, another pair of mapping keys CK'/IK' are derived and transmitted to the target RNC together with the {K_{RNC}*, NCC}. If target RNC is not updated, it will regard IK'/CK' as legacy IK/CK. And if target RNC is updated, it will regard K_{RNC}* as K_{RNC} to derive CK_U/IK_U.

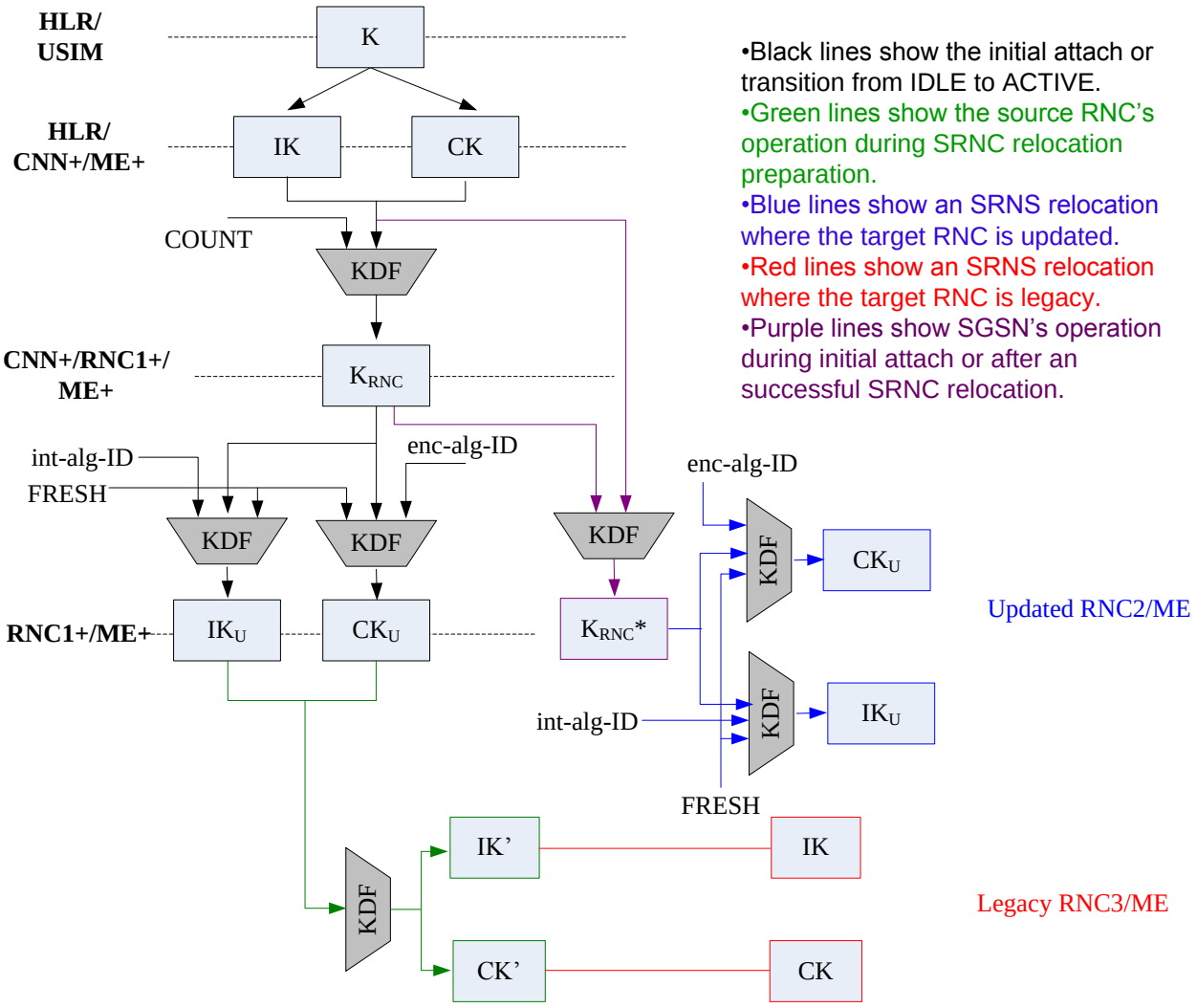

Figure 4.4.1-2: Key distribution and key derivation scheme for UTRAN Key hierarchy

The KDF is assumed to be the one from TS 33.220 [12] taking a 256-bit input key and generates a 256-bit output key. When two 128-bit output keys (IK_U/CK_U and IK'/CK') are needed, truncate the 256-bit key to 128-bit for IK_U/CK_U, and take 128 MSBs of the output as the IK' and the 128 LSBs as the CK'.

4.4.2 Proposed solution 2

The UTRAN Key Hierarchy is shown in the figure 4.4.2-1 below.

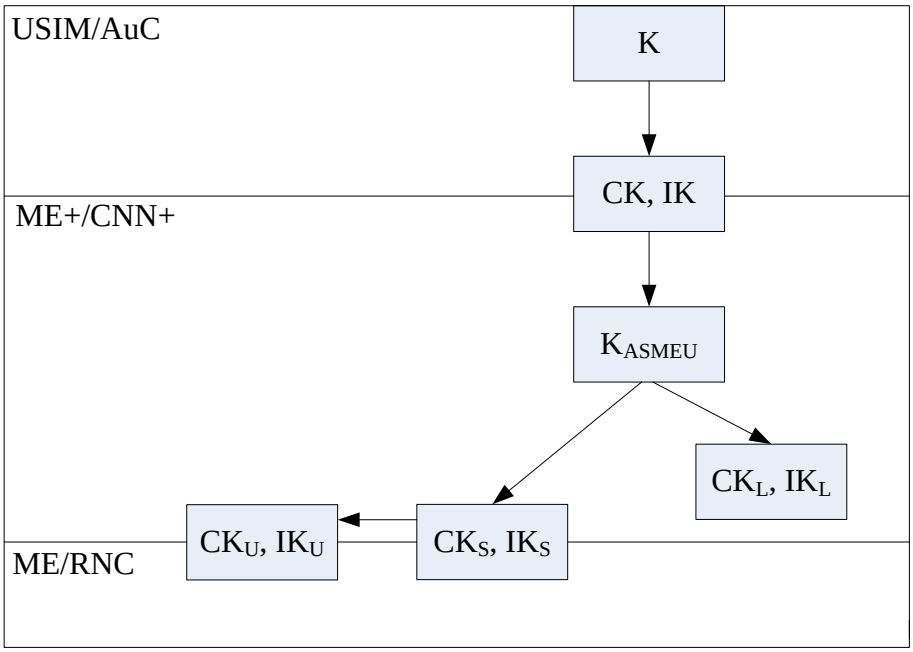

Figure 4.4.2-1: UTRAN Key hierarchy

The key hierarchy in solution 2 adds two layers of keys between the CK and IK that result from an AKA run and the keys (either CK_S and IK_S or at fallback a legacy context when connecting to a legacy CN node CK_L and IK_L) that are passed to the RNC.

The first layer derivation from CK and IK to K_{ASMEU} is to enable the creation of a root key for the enhanced security context and is included to simplify the description of the procedures, i..e. it is simpler to say that the K_{ASMEU} is passed between enhanced nodes in a new IE rather than CK and IK are passed which happens in the legacy case. The proposed derivation of K_{ASMEU} is just a concatenation of CK and IK.

The derivation from K_{ASMEU} of the other keys enables fresh keys to be passed to the RNC at each Idle to Active transition, i.e. CK_S and IK_S with COUNT used to provide freshness (see subclause 5.2.2), or fresh keys when a fallback to a legacy security context at Idle mobility is required, i.e. CK_L and IK_L (see subclause 5.2.2).

In addition to these key derivations, the following cases also require fresh key(s) to be derived

- PS Handover from E-UTRAN/UTRAN to GERAN: A fresh pair of CK_S and IK_S are derived in GERAN SGSN+ and ME+ from K_{ASMEU} and the CK_S and IK_S passed to the GERAN SGSN (see subclause 5.2.3.2.4.2)
- Handover from E-UTRAN to UTRAN/GERAN: K_{ASMEU} is calculated from K_{ASME} (see subclause 5.2.3.3.4.2)
- Idle mobility from E-UTRAN to UTRAN/GERAN: K_{ASMEU} is calculated from K_{ASME} (see subclause 5.2.3.3.3.2)
- Handover from UTRAN/GERAN to E-UTRAN: K_{ASME} is derived in the MME+ and ME+ from the K_{ASMEU} and CK_S and IK_S that are passed to the MME+ (see subclasue 5.2.3.3.4.3)

Idle mobility from UTRAN/GERAN to E-UTRAN: K_{ASME} is derived in the MME+ and ME+ from the K_{ASMEU} and that is passed to the MME+ and the exchanged nonces (see subclause 5.2.3.3.3.1)

The KDF is assumed to be the one from TS 33.220 [12] taking a 256-bit input key and generates a 256-bit output key. When two 128-bit output keys (CK/IK) are needed, take 128 MSBs of the output as the CK and the 128 LSBs as the IK. When two 128-bit keys are used as input, take their concatenation as the 256-bit input key.

4.4.3 Proposed solution 3

Solution 2 proposes a mechanism for improved key handling for all situations except SRNS relocation. Solution 3 proposes a compatible improved key handling for SRNS relocation. In Solution 2, the source RNC(+) pass the currently used CK/IK to the target RNC. In Solution 3, this is modified so that an updated source RNC first applies a KDF to the current CK_U/IK_U to ensure that the target RNC does not get access to the keys used in the source RNC. Solution 3 hence adds the possibility to derive a new pair CK_U/IK_U from an existing one as shown in Figure 4.4.3-1.

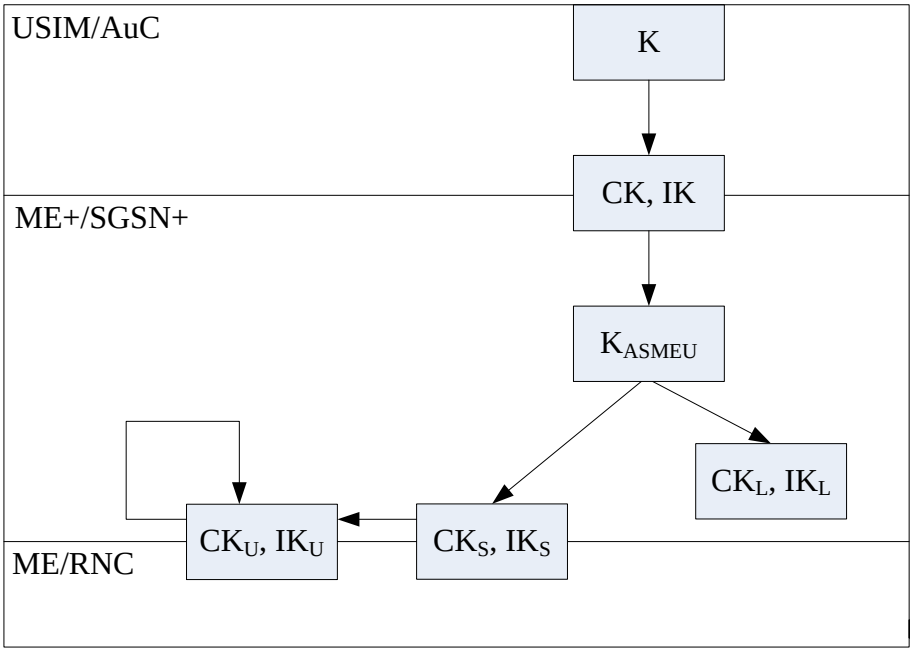

Figure 4.4.3-1: UTRAN Key hierarchy

4.4.4 Freshness options for vertical key derivations

4.4.4.1 Timestamp

Using timestamps as input to key establishment protocols works well in settings where the peers can be assumed to have relatively synchronized clocks and where the key establishments are not more frequent that the expected deviation of the clock sync. In the case of Idle to Active transitions in UTRAN, it seems unlikely that the UE and the NW will have clocks so well synchronized that it can cater for the frequency of required key establishments. Therefore timestamps are not suitable as freshness input in this study.

4.4.4.2 Counters

Uplink counter

Solution 2 proposes that the ME_U+ includes a COUNT value in initial layer 3 message to the core network. This COUNT value is increased in the ME after it has been sent in the initial layer 3 messages to the SGSN.

When ME_U+ moves during Idle mode and enters a new cell, then the ME_U+ is not aware of whether this cell belongs to a new SGSN or not. The ME_U+ neither knows whether it is a SGSN+ or a legacy SGSN when it sends the initial layer 3 message. The ME_U+ therefore needs to always provide a new COUNT value in the initial layer 3 NAS signaling message to the SGSN.

If ME_U+ connects to a SGSN+ after being connected to a legacy SGSN, then the SGSN+ does not have any stored COUNT value and can therefore not check the received COUNT value from the ME_U+ (i.e. whether its greater than or equal to the stored COUNT). This could imply that ME_U+ or an attacker may replay the same COUNT values in the new SGSN+. But if the old SGSN was a legacy SGSN, then it ether was using a CK_l/IK_l key set received from an updated SGSN+ or it uses a normal, legacy CK/IK. In both cases it is guaranteed that the CK_s/IK_s the new SGSN+ is using have never been derived using any COUNT before. Therefore no replay attack which results in the same CK_s/IK_s being derived in the SGSN+ and ME_U+ is possible, even if an attacker replays the COUNT.

Also if the COUNT was altered in between the ME_U+ sent it and when the SGSN+ receives it (this would not be detected by the SGSN+ at the point of receiving the initial NAS message as it is not integrity protected), the ME_U+ and SGSN+ would derive different keys. The RRC SMC would hence fail integrity protection verification in the ME_U+. It does not seem possible to do a replay attack that fools both ME_U+ and the network into using an old key. It would not be known to the ME_U+ or the network why the RRC SMC procedure failed though, only that it failed.

It would be possible to record an initial NAS message from a ME_U+ and then replay it to a different SGSN+). The UL COUNT value would then be re-used, but this attack would however be stopped by the fact that the keys (CK_s/IK_s) would be different in the new SGSN+ so the integrity protection of the RRC SMC would fail verification in the ME_U+.

As the counter is kept in each SGSN+, this implies that both the SGSN+ and the ME_U+ can be assured about the freshness of the key regardless of the subsequent signaling as long as the ME_U+ stays with the same SGSN+. There is no need to transfer the counter between different SGSN+s when there is a change of SGSN+: replay of a message to a new SGSN is taken care of by using different keys in the target SGSN+ and by the fact that the UE will reject the subsequent RRC SMC.

Downlink counter

Using a downlink counter from the network to the ME_U+ has much in common with using an uplink counter. However, in this case it is the ME that does not get any freshness guarantee until the RRC SMC complete message is rejected by the network (due to key mismatch as a result of a replay attack). The counter could be included in the security mode control procedure.

Use of a downlink counter implies that the enhanced SGSN/MSC will not insert the counter value in a downlink message to a ME if the RNC is not an enhanced RNC. If an uplink counter is used, the ME_U+ always has to include the counter, since it does not know whether the network supports UTRAN key management enhancements or not.

4.4.4.3 NONCE

4.4.4.3.1 One sided NONCE

Nonce allocated by ME_U+

The ME_U+ could use a 32 bit value, allocated randomly, called $NONCE_{UE}$.

As a new NONCE value is allocated in ME_U+ in each Attach Request, Service Request and Routing Area Update Request message, the ME_U+ is ensured that at a change of SGSN the NONCE value included to the SGSN+ is unique. This NONCE could be used as input to derive the keys CK_S and IK_S as described in the proposal 2, replacing the COUNT parameter:

CK_S and IK_S can then be calculated as follows $CK_S \,||\, IK_S = KDF(K_{ASMEU}, NONCE_{UE})$

The SGSN+ does however not get any freshness guarantee for the keys with this approach. The result of this is that (unless the SGSN+/SMC+ stores all NONCEs which is infeasible), it is possible for an attacker to replay the same initial layer 3 message to the SGSN+ and even to a different SGSN. In case the message is replayed to an SGSN, the result is that the SGSN+ will derive the same CK_s/IK_s and will use them for downlink traffic. The result is a two time pad. However, if integrity protection is enabled by the network, the first downlink message will be an RRC security mode command. The ME_U+ is supposed to reply with an RRC security mode complete message (which shall be integrity protected). This implies that since the attacker is assumed not to have access to the CK_s/IK_s he cannot integrity protected the message and the network will not allow the attacker access.

No serious attacks have been identified if a nonce is used instead of a counter in this case. However, a one sided nonce approach is not inherently immune to replay attacks. It relies on subsequent signalling to provide the protection. This complicates the analysis. If this approach is still taken, solid reasoning must be supplied for all possible cases of signalling that follows to ensure that no replay attack is possible.

Nonce allocated by the network

For the same reasons given for the approach where the ME_U+ allocates the nonce, it is not immediate that the use of a single nonce is secure and if this approach is taken, complete and solid reasoning needs to be supplied for all possible cases of signalling following the initial layer 3 message.

Use of a downlink nonce implies that the enhanced SGSN/MSC will not insert the nonce value in a downlink message to a ME if the RNC is not an enhanced RNC. If an uplink nonce is used, the ME_U+ always has to include the nonce, since it does not know whether the network supports UTRAN key management enhancements or not.

If an attacker breaks in to an RNC and gets hold of a downlink nonce and receives the CK_U/IK_U from the core network, the attacker can re-play this nonce and the use the CK_U/IK_U with that UE multiple times.

4.4.4.3.2 NONCE values allocated in both ME_U+ and SGSN+

The ME_U+ and SGSN+ could use a 32 bit value, allocated randomly respectively, named $NONCE_{UE}$ and $NONCE_{CN}$.

As a new $NONCE_{UE}$ value is allocated in ME_U+ in each Attach Request, Service Request and Routing Area Update Request message to the SGSN+, the ME_U+ is ensured that at a change of SGSN the $NONCE_{UE}$ value included to the SGSN+ is unique and differently from previously $NONCE_{UE}$ value in previous SGSN+:s. This $NONCE_{UE}$ could be used as input to derive the keys CK_S and IK_S as described in the proposal 2, replacing the COUNT parameter (see further below). In addition, the SGSN+ also allocates a new NONCE value (i.e. $NONCE_{CN}$) at Idle to Active mode transition, to achieve freshness on both sides, and this $NONCE_{CN}$ is used as input as well to derive the keys CK_S and IK_S as described in the proposal 2:

CK_S and IK_S which are calculated as follows $CK_S \parallel IK_S = KDF(K_{ASMEU}, NONCE_{UE,} NONCE_{CN})$

The SGSN+ would with this approach ensure that even if the $NONCE_{UE}$ is replayed from an attacker, the SGSN+ would still get a guarantee of freshness because of $NONCE_{CN}$ when deriving $CK_S \parallel IK_S$.

Since both sides (ME_U+ and SGSN+) are assured of the freshness of their own inputs this approach ensures both sides that the keys are fresh. Due to that this approach gives such guarantees, there is no reliance on subsequent signalling to provide the guarantee. Even so, if an attacker modifies one of the nonces, it is still necessary to rely on subsequent signalling to enable security.

4.4.5 Handling of START/COUNT-C/COUNT-I

When enhanced UTRAN KH is supported, two methods to handle START value and COUNT-I/COUNT-C should be considered :

Method one :

ME and RNC+ will handle START value and COUNT-I/COUNT-C according to current 3GPP specifications, e.g., TS 33.102, TS 25.331, etc.

Method two :

In this method, the handling of START value and COUNT-I/COUNT-C will be different with current 3GPP specifications when the target RNC use the different keys with the source RNC after SRNS Relocation, that is, the keys which used by the target RNC are the derived keys. In this case, since the derived keys are different, the START value and value of COUNT-I/COUNT-C can be set to zero by ME+ and target RNC+. This reduces the number of AKA runs and extends the life cycle of CK/IK.

Except the above case, ME and RNC+ also handle START value and COUNT-I/COUNT-C according to current 3GPP specifications.

For method two, the life cycle of the CK/IK can be extend and the number of running AKA also can be reduced.

However, setting START/COUNT-C/COUNT-I to zero in case of SRNC relocation with key change may introduce undesired implications. The feasibility of method two should be studied further considering the complexity of START mechanism. But it is not considered in this TR.

NOTE: It is not decided which method will be used since it is not possible to investigate all implications of changing the COUNT-I/COUNT-C/START handling in UTRAN in timeframe of this TR. The decision is left to future possible Work Item work.

5 Analysis and design

Editor's Note: It is ffs whether and how SRVCC impacts solutions 1, 2, 3, and 4.

5.1 Proposed solution 1

5.1.1 General

MMEs and legacy SGSNs must be expected to operate according to currently specified procedures/working assumptions. New processing and signaling can thus only be introduced in the HSS, SGSN+, MSC/VLR+ and ME+.

The following clauses give an outline of the signaling principles. Details and deeper rationale/analysis is elaborated in subsequent clauses.

5.1.2 Key handling capability negotiation

5.1.2.1 General

An important aspect is to ensure that network and ME can interoperate and are aware of whether to use the UTRAN KH or not. This in turn implies that it is necessary to signal UTRAN KH capabilities between the UE and network and between nodes in the network.

5.1.2.2 UTRAN KH negotiation in the attach procedure

A ME+ needs to operate differently depending on if it connects towards a SGSN or to a SGSN+, an MSC/VLR or a MSC/VLR+ and conversely, a SGSN+ and MSC/VLR+ needs to behave differently depending on ME/ME+ capabilities. We have two cases:

- ME+ connects to a SGSN+ or MSC/VLR+: both shall use the UTRAN key hierarchy.
- All other combinations involving legacy ME and/or SGSN or legacy MSC/VLR: standard CK/IK derivations must be used.

This means that a ME+ has to be able to signal its key handling capabilities (UTRAN key hierarchy) to the SGSN+ or MSC/VLR+. But it is also necessary that the ME+ will know if it connects to a SGSN or a SGSN+ (or MSC/VLR or MSC/VLR+ in the CS case) and if it should perform UTRAN key hierarchy derivations or if standard UMTS key management should be performed.

Here it is noted that SGSN+ or MSC/VLR+, for a ME+, can add a specific information element (IE) to the SECURITY MODE COMMAND or that a new type of SECURITY MODE COMMAND is introduced that tells the ME+ to apply the UTRAN key hierarchy.

It is natural to incorporate the UTRAN KH negotiation into the normal attach procedure. The negotiation is essentially the same as the algorithm negotiation procedure, except that different IEs carry the capability information from the UE to the SGSN(*) or MSC/VLR(*) and echoing back the capability information from the SGSN+ or MSC/VLR+ to the UE and the activation of the UTRAN KH by the SGSN+ or MSC/VLR+.

5.1.2.3 Capability indication at intra-UTRAN mobility

At Idle mode mobility, ME+ can signal its UTRAN KH capability indication to the CNN(*) in RAU/LAU request messages. And CNN+ can indicate its UTRAN KH capability to the ME+ in RAU/LAU Accept messages.

During the SMC procedure, if needed, the CNN(*) can indicate their UTRAN KH capability to the ME+, just the same as in the initial attach procedure.

At SRNS relocation, the source RNC+ should send UE UTRAN KH capability to the target RNC(*) in **source RNC to target RNC transparent container IE**. However, the current specs do not seem to guarantee that a legacy source RNC includes an IE that it doesn't understand to the target RNC(*). In this case ME+ should signal its UTRAN KH capability to the target RNC(*) in the first UL message (i.e., **UTRAN Mobility Information Confirm/Physical Channel Reconfiguration Complete/Cell Update Confirm/URA Update Confirm**) to the target one. While the target RNC+ can indicate its UTRAN KH capability to ME+ in the first DL message (i.e., **Physical Channel Reconfiguration/UTRAN Mobility Information**) to the ME+.

At SGSN relocation, the source CNN+ should send UE UTRAN KH capability to the target CNN(*).

5.1.2.4 Capability indication at IRAT mobility

When an inter-RAT handover from UTRAN to E-UTRAN occurs, existing SGSN-MME signalling is used and the ME(*) will know that EPS supports the use of the EPS key hierarchy. However, at E-UTRAN to UTRAN handover, some problems could occur.

The MME performs a regular context transfer to the SGSN(*) as specified for the release the MME implements. There should be no requirement for the MME to know whether the target is an SGSN or an SGSN+. This means that the ME(*) will always be sure of which "root" key that is transferred, regardless of whether the target is SGSN or SGSN+, namely CK' and IK' as derived from the K_{ASME} used in E-UTRAN. A target SGSN(*) would interpret the given CK' and IK' as a (CK, IK) pair.

At handover, an ME+ will not, from current signalling, know if it is handed over to an SGSN+ which is capable of applying the UTRAN key hierarchy or to an SGSN which is not. This is however not necessary as the CK and IK used are derived in the same manner in both cases.

The same principle would apply at GERAN-to-UTRAN handover for an ME that has an established UMTS security context.

UTRAN to GERAN handovers are not affected.

5.1.3 Signalling procedures

5.1.3.1 Attach

1. An ME+ performing attach, signals its key handling capabilities for UTRAN to the SGSN(*) or the MSC/VLR+ in the Attach Request. (The capabilities should be signaled in such a way that a SGSN+ or MSC/VLR+ will understand the key handling requirements but a legacy SGSN would ignore the capability signaling.)

NOTE: This type of capability signaling is already specified for Rel-8.

2. The SGSN(*) or MSC/VLR+ requests an AV from the HSS.
3. The HSS returns the AV.
4. The SGSN+ or MSC/VLR+ sends the RAND and the AUTN to the ME+.
5. The SGSN+ or MSC/VLR+ shall increase the COUNT by one, and derives K_{RNC} based on CK/IK and the COUNT.
6. The SGSN+ or MSC/VLR+ determines which UIAs and UEAs that are allowed to be used in order of preference.
7. The SGSN+ or MSC/VLR+ issues the SECURITY MODE COMMAND. This message contains an ordered list of allowed UIAs in order of preference, the COUNT, UE UTRAN KH capability, and the derived K_{RNC}. If ciphering shall be started, it contains the ordered list of allowed UEAs in order of preference. It also indicates, for a ME+, that the UTRAN key hierarchy handling is applicable.
8. The SRNC+ decides which algorithms to use by selecting the highest preference algorithm from the list of allowed algorithms that matches any of the algorithms supported by the ME+ and generates a random value FRESH.
9. The SRNC+ derives IK_U and CK_U (if applicable) based on K_{RNC} and initiates the downlink integrity protection.
10. The SRNC+ generates the RRC message Security mode command. The message includes the ME security capability, UE UTRAN KH capability, the UIA, the COUNT and FRESH to be used and if ciphering shall be started also the UEA to be used, the CN type indicator information. Additional information (start of ciphering) may also be included. Before sending this message to the ME+, the SRNC+ generates the MAC-I (Message Authentication Code for Integrity) and attaches this information to the message.
11. When the ME+ receives the COUNT from network, it shall check the COUNT received with the one it maintains in order to avoid replay attack.

If the received COUNT is larger than the stored one, the ME+ sets the stored COUNT equal to the received COUNT, and derives K_{RNC} based on IK/CK and the COUNT, and then derives IK_U and CK_U (if applicable) based on KRNC. Otherwise, ME+ regards this message as an invalid one.

12. At reception of the Security mode command message, the ME+ controls that the "UE security capability"and "UE UTRAN KH capability" received is equal to the ones sent in the initial message. The ME+ verifies the integrity of the message by comparing the received MAC-I with the generated XMAC-I.

13. If all controls are successful, the ME+ compiles the RRC message Security mode complete and generates the MAC-I for this message. If any control is not successful, the procedure ends in the ME+.

14. At reception of the response message, the SRNC+ computes the XMAC-I on the message. The SRNC+ verifies the data integrity of the message by comparing the received MAC-I with the generated XMAC-I.

15. The transfer of the RANAP message Security Mode Complete response, including the selected algorithms, from SRNC+ to the SGSN+ or MSC/VLR+ ends the procedure.

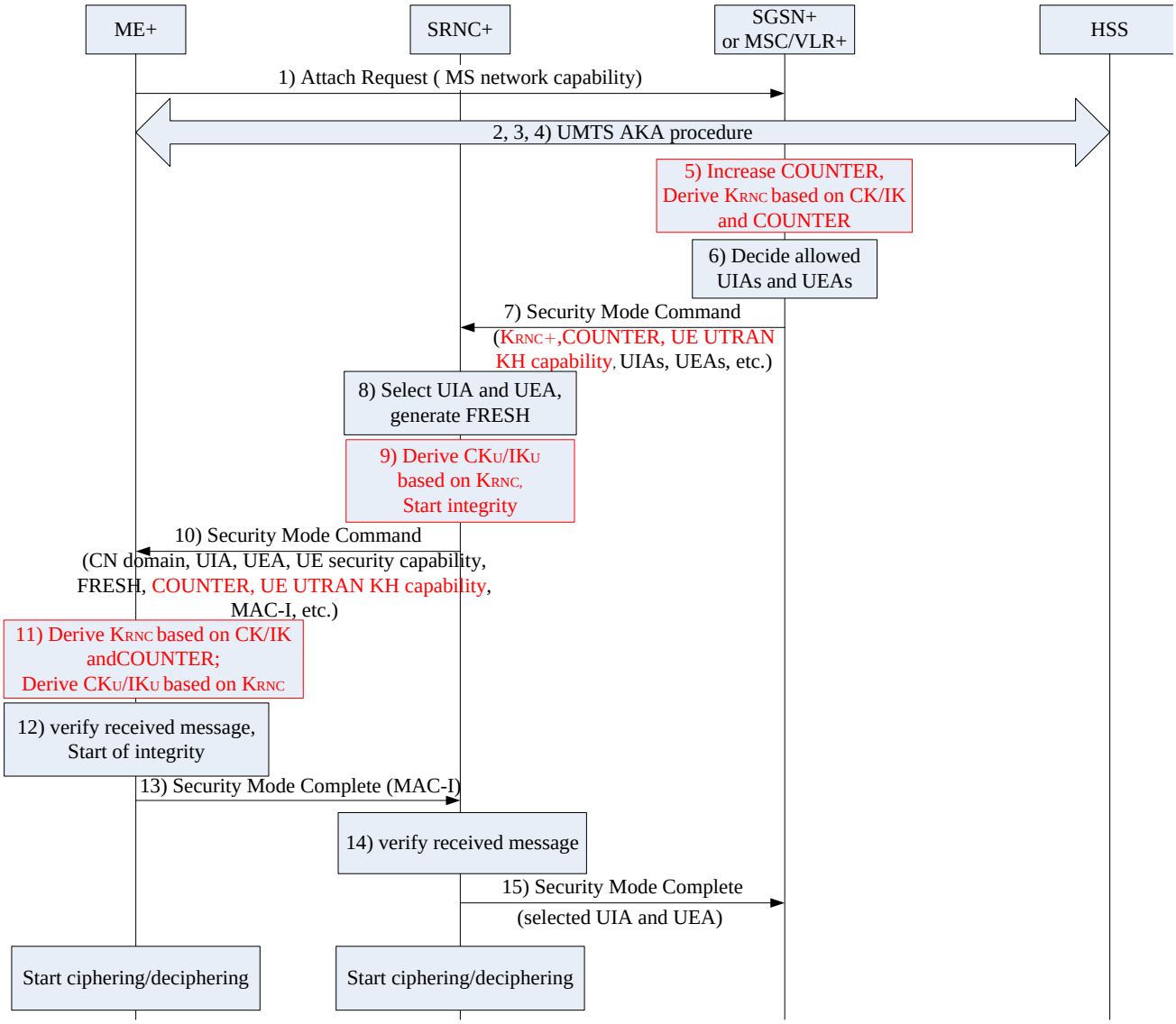

Figure 5.1.3.1-1: Security mode set-up in attachment procedure

The HSS shall for these reasons always transfer standard UMTS AVs and that all the additional key derivations are performed in the serving PLMN.

In order to avoid CK/IK exposure in UTRAN, K_{RNC} are derived from CK and IK in SGSN+ or MSC/VLR+.

Regarding why CK_U and IK_U are derived by SRNC+, the following reasons are proposed. 1) There is a requirement that the key derivations make the keys depend on the algorithm identifiers. And in UMTS UIA and UEA are finally decided by SRNC+. 2) It shall be possible to update keys at intra-UTRAN handovers (SRNC+/Node B mobility), and in an enhanced SRNC relocation procedure SRNC+ communicates with Target RNC+ directly, so if RNC+ has the ability to derive CK_U and IK_U, it would benefit key update during SRNC handover.

In order to provide fresh RAN keys at every Idle to Active transition, a DL COUNT is managed by CNN+ and ME+ respectively every time and is used to derive K_{RNC} together with IK/CK.

FRESH is used to ensure different derivations of IK_U and CK_U under the same K_{RNC} and algorithm identity among different RNCs+ (especially for SRNC relocation procedure).

The FRESH is included in the derivation of IK_U and CK_U to align the KDF input with the KDF input used to derive IK_U and CK_U at SRNS relocations.

In accordance with these reasons above, K_{RNC} are transferred from SGSN+ or MSC/VLR+ to SRNC+. And SRNC+ derives CK_U and IK_U based on K_{RNC}.

5.1.3.2 Context transfers

5.1.3.2.1 General

As the discussion in clause 5.3.2 is applicable to both the CS and the PS case, the generic term Core Network Node (CNN) will be used to denote a SGSN in the PS case and a MSC/VLR in the CS case. Similarly, the term (CNN+) will be used to denote a Core Network Node (a SGSN or MSC/VLR) that is aware of UTRAN KH.

At SGSN+ to SGSN(*) relocation, the source node shall send mapping legacy keys (IK_L, CK_L) and the enhanced keys materia {K_{RNC}*, NCC} and {IK, CK} to the target node. Because the source node may not know whether the target one is enhanced or not, in order to avoid (IK, CK) exposure in RAN if the target node isn't updated, (IK, CK) are transferred in a new defined IE which is only recognized by the updated target node, and (IK_L, CK_L) shall be carried in the original IE of IK and CK. If the target node isn't updated, it shall regard IK_L as IK and CK_L as CK; while if the target node is updated, it can recognize {K_{RNC}*, NCC} and (IK, CK).

As noted, the ME+ needs also to be able to detect when a handover from SGSN+ to SGSN occurs. Here, there may not be a new SECURITY MODE COMMAND issued by the target SGSN+, but an SGSN+ (when serving a ME+) could add a new IE in the RAU ACCEPT message to the ME+. Thus, the absence of this IE will tell the ME+ if it is ever handed over to a legacy SGSN. Since the network from now on may no longer have access to the underlying (CK, IK) and K_{RNC}*, the ME+ should make a note that (CK, IK) and K_{RNC}* are "expired" and that any further handover will be based (only) on (CK_L, IK_L).

5.1.3.2.2 Inter CNN+ context transfer

As noted above, a source SGSN+ always includes {K_{RNC}*, NCC}, (CK, IK) (CK_L, IK_L) and DL COUNT in the handover signaling. The SGSN+ also indicates whether the ME supports UTRAN KH.

5.1.3.2.3 CNN+ to CNN context transfer

The source SGSN+ sends (CK, IK), {K_{RNC}*, NCC}, (CK_L, IK_L) and DL COUNT. The source also includes whether the ME supports UTRAN KH or not. The target SGSN ignores the IEs containing the (CK, IK), {K_{RNC}*, NCC}, DL COUNT and the indication of the UTRAN KH capability of the ME.

5.1.3.2.4 CNN to CNN+ context transfer

At handover from SGSN to SGSN+, the SGSN will act according to TS 33.102 [3] and the target SGSN+ can observe the absence of K_{RNC}*. An issue however is that the context in the SGSN has been used to directly protect the UTRAN signaling and the user plane. This has to be taken into account in the further handling of the context and when it is transferred to a SGSN+. From a security point of view there is no advantage in generating a new K_{RNC} from the existing security context (i.e. CK, IK) in the SGSN+. Note also that the source SGSN is not aware of UTRAN KH, and may therefore not be able to inform the target SGSN+ about the new ME capability (this depends on if the UTRAN KH capability is included in the MS capability IE or if it is introduced in a separate IE). Therefore, the target SGSN+ may need to assume that the ME does not support the UTRAN KH which also implies that direct usage of (CK, IK) is the most straightforward solution when the UE is in Active mode. In case of Idle mode mobility, the ME could include the

UTRAN KH capability indication in the RAU Request, and the new SGSN+ could in this case gain knowledge of the support for UTRAN KH in the ME at this point.

5.1.3.2.5 Inter CNN context transfer

This is performed according to TS 33.102 [3].

5.1.3.3 SRNS relocation

5.1.3.3.1 General

Since UTRAN has an anchor in the Serving RNC, and the encryption/decryption and integrity protection is implemented in the SRNC, only when the SRNC is relocated, there is a possibility to update keys.

There are two main types of SRNS relocation to consider:

- SRNS relocation with UE involvement
- SRNS relocation without UE involvement

Combined hard handover and SRNS relocation belongs to SRNS relocation with UE involvement. While Combined CELL/URA updated and SRNS relocation belongs either SRNS relocation with UE involvement or SRNS relocation without UE involvement.

For combined CELL/URA updated and SRNS relocation with UE involvement, the procedure is just the same as combined hard handover and SRNS relocation with UE involvement.

5.1.3.3.2 SRNS relocation with UE involvement

5.1.3.3.2.1 SRNC relocation key chaining

During SRNC Relocation preparation procedure, because Serving RNC may not know whether the target RNC supports KH or not, there is a need to provide legacy support.

In this procedure, two sets of keys are transmitted to the target RNC: one is the mapping keys CK'/IK', the other is the enhanced keys. If the target RNC does not support KH, it cannot recognize the enhanced keys. So it will ignore this IE, and the mapping keys CK'/IK' are used. If the target RNC supports KH, it notices that the enhanced keys are present, so it will ignore the mapping keys, and derive the enhanced IK_U/CK_U.

The general principle of enhanced key handling at SRNC relocation is depicted in Figure 5.1.3.3.1-1.

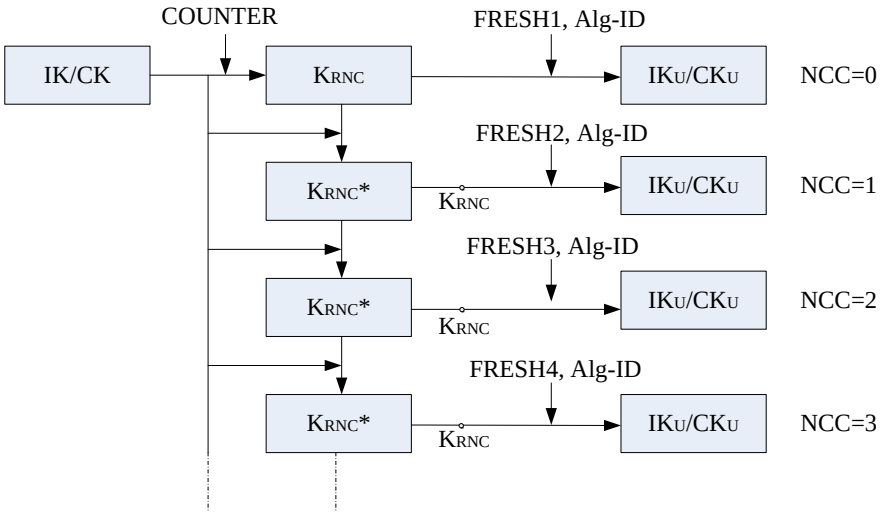

Figure 5.1.3.3.1-1 Model for the SRNC relocation key chaining

The following is an outline of the key handling model to clarify the intended structure of the key derivations.

Whenever an initial security context needs to be established between ME+ and SRNC+, SGSN+ and the ME+ shall derive a K_{RNC} and a K_{RNC}*. The K_{RNC} and K_{RNC}* are derived from the IK/CK. A Next-hop Chaining Counter (NCC) is associated with each K_{RNC}*. At initial setup, the K_{RNC} is derived directly from IK/CK, and is then considered to be associated with a virtual K_{RNC}* parameter with NCC value equal to zero. At initial setup, the derived K_{RNC}* value is associated with the NCC value one. K_{RNC} and {K_{RNC}*, NCC} are transmitted to SRNC during SMC procedure at initial attachment.

NOTE: Since the SGSN+ sends the {K_{RNC}*,NCC} value to SRNC at the initial attachment, the K_{RNC}* value associated with the NCC value one can be used in the next SRNC relocation or the next intra-SRNC relocation.

The ME+ and the RNC+ use the IK_U/CK_U derived from K_{RNC} to secure the communication between each other. On SRNC relocation, the basis for the K_{RNC} that will be used between the ME+ and the target RNC+, called K_{RNC}*, is derived from the IK/CK and old K_{RNC}*. On SRNC relocation the target RNC derives IK_U/CK_U based on the K_{RNC} and the FRESH generated by the target RNC, together with the algorithm ID, which is just the same as initial attachment.

As K_{RNC}* parameters are only computable by the ME+ and the SGSN+, it is arranged so that K_{RNC}* parameters are provided to SRNC from the SGSN+ in such a way that forward security can be achieved.

5.1.3.3.2.2 Network handling

5.1.3.3.2.2.1 Enhanced SRNS relocation procedure

During SRNS relocation the source RNC+ shall forward the {K_{RNC}*, NCC} pair to the target RNC+. The target RNC+ shall use the received K_{RNC}* directly as K_{RNC} to be used with the UE. The target RNC+ shall generate a parameter FRESH, and derive IK_U/CK_U Based on K_{RNC}, FRESH and algorithm ID. The target RNC+ shall include the received NCC into the prepared Target RNC to Source RNC Transparent Container, which is sent back to the source RNC+ and forwarded to the UE by source RNC+.

When the target RNC+ has completed the SRNC relocation signaling with the ME+, it shall send a Enhanced Relocation Complete Request message to the SGSN+. Upon reception of the Enhanced Relocation Complete Request, the SGSN+ shall increase its locally kept NCC value by one and compute a new fresh K_{RNC}* by using the IK/CK and its locally kept K_{RNC}* value as input to the function. The SGSN+ shall then send the newly computed {K_{RNC}*, NCC} pair to the target RNC+ in the Enahcned Relocation Complete Response message. The target RNC+ shall store the received {K_{RNC}*, NCC} pair for further SRNC relocation and remove other existing unused stored {K_{RNC}*, NCC} pairs if any.

NOTE: The newly computed {K_{RNC}*, NCC} can only be used to provide keying material for the next SRNC relocation procedure. Thus, for SRNC relocation key separation happens only after two hops because the source RNC+ knows the target RNC+ keys. The target RNC+ can immediately initiate an intra-cell handover to take the new K_{RNC}* into use once the new K_{RNC}* has arrived in the Relocation Complete Response.

5.1.3.3.2.2.2 SRNS relocation procedure

Upon reception of the Relocation Required message the source SGSN+ shall increase its locally kept NCC value by one and compute a fresh K_{RNC}* from its stored IK/CK and old K_{RNC}*. The source SGSN+ shall store that fresh {K_{RNC}*, NCC} pair and send it to the target SGSN+ in the Forward Relocation Request message.

The target SGSN+ shall store {K_{RNC}*, NCC} pair received from the source SGSN+.

The target SGSN+ shall then send the received {K_{RNC}*, NCC} pair to the target RNC+ within the Relocation Request message. Upon receipt of the Relocation Request from the target SGSN+, The target RNC+ shall use the received K_{RNC}* directly as K_{RNC} to be used with the UE. The target RNC+ shall generate a parameter FRESH, and derive IK_U/CK_U Based on K_{RNC}, FRESH and algorithm ID. The target RNC+ shall include the received NCC into the prepared Target to Source RNC Transparent Container, which is sent back to the source RNC+ and forwarded to the ME+ by source RNC+.

NOTE: The source SGSN+ may be the same as the target SGSN+ in the description in this subclause. If so the single SGSN+ performs the roles of both the source and target SGSN+, i.e. the SGSN+ calculates and stores the fresh {K_{RNC}*, NCC} pair and sends it to the target RNC+.

5.1.3.3.2.3 Intra-SRNS relocation

When the SRNC+ decides to perform an intra-SRNS relocation it shall generated a new FRESH, and use the K_{RNC}* as the K_{RNC}. The SRNC shall derive IKU/CKU using the new FRESH, algorithm ID, and the current K_{RNC}. The SRNC shall send the NCC corresponding to K_{RNC}* to ME+ in Physical Channel Reconfiguration message or UTRAN Mobility Information message.

5.1.3.3.3 ME handling

If the NCC value the ME+ received in the Physical Channel Reconfiguration message or UTRAN Mobility Information message from target RNC+ is equal to the NCC value stored in the ME+, the ME+ shall directly use the K_{RNC}* as K_{RNC} to derive CK_U/IK_U.

If the ME+ received an NCC value that was different from the NCC associated with the currently active K_{RNC}, the ME+ shall first synchronize the locally kept K_{RNC}* parameter iteratively, and increasing the NCC value until it matches the NCC value received from the source RNC+. When the NCC values match, the ME+ shall use the K_{RNC}* as K_{RNC} to compute the IK_U/CK_U.

5.1.3.3.4 SRNS relocation without UE involvement

For combined CELL/URA updated and SRNS relocation without ME+ involvement, the first Downlink message is target RNC(*) sending to ME+. This first DL message should be integrity protected and ciphered, while it is carrying target RNC(*)'s security capability. Since ME+ does not know whether target RNC(*) supports UTRAN KH or not before de-ciphering this message, and there are two different keys (the enhanced keys IK_U/CK_U and the legacy keys IK'/CK') in ME+. The result of this is that the ME+ does not know which key should be used to de-cipher this message. One solution is to try both keys. But it seems that it is not an optimized solution.

Here a solution is proposed to resolve this problem.

During SRNS relocation without UE involvement, a legacy SRNC relocation procedure is performed first, in which source RNC+ should send the keys currently used directly to target RNC+, i.e. the keys during this SRNC relocation procedure are not updated. While the operation of SGSN+ is the same as the one's in SRNS relocation with UE involvement, i.e., SGSN+ shall also derive new K_{RNC}*. The benefit is that SGSN+ does not need to know whether it is a SRNS relocation without UE involvement or not.

After the SRNC relocation is finished, an intra-SRNC relocation is performed. During this intra-SRNC relocation procedure, new IK_U and CK_U are derived just the same as in the SRNS relocation with UE involvement, except that the target RNC+ and the source RNC+ are the same one.

5.1.3.3.5 Using Enhanced SRNS Relocation

One example of hard handover using enhanced SRNS relocation procedure is showed below.

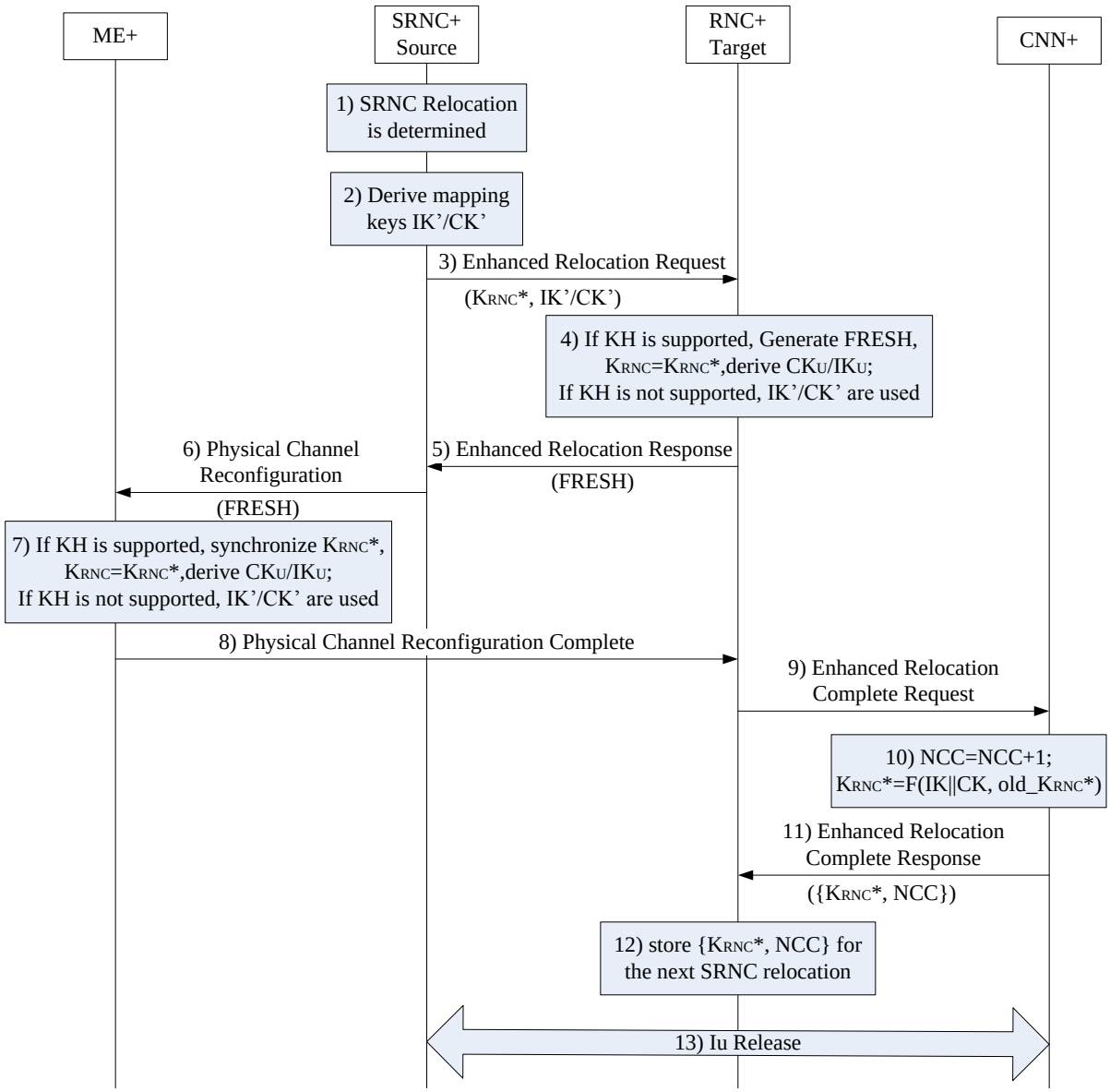

Figure 5.1.3.3.3-1: Hard Handover with switching in the CN+ using Enhanced SRNS Relocation (DCH state)

1. Serving RNC+ makes the decision to perform the Hard Handover via Iur interface. Serving RNC+ also decides into which RNC+ (Target RNC+) the Serving RNC+ functionality is to be relocated.

2. SRNC+ does not know whether the target RNC support KH or not, it derives the mapping keys CK'/IK' (The derivation for CK'/IK' is FFS).

3. SRNC+ sends Enhanced Relocation Request message to a neighboring RNC(*) (Target RNC(*)). In this message a Source RNC To Target RNC Transparent Container is included, which carries ME+ capability, the mapping keys IK'/CK', { K_{RNC}*, NCC }.

4. Target RNC+ decides to accept the request and allocates radio resources for the RRC connection and the Radio Link. If the target RNC does not support KH, it cannot recognize K_{RNC}* and ignore this IE. So the mapping keys IK'/CK' are used.

   If the target RNC supports KH, it notices that K_{RNC}* is present. It shall regard K_{RNC}* as K_{RNC}, and generates a new FRESH and derives new CKU/IKU based on the new FRESH (ie., IKU = H2(K_{RNC}, FRESH, int-alg-ID), CKU = H3(K_{RNC}, FRESH, enc-alg-ID)).

5. Target RNC+ replies an RNSAP **Enhanced Relocation Response** containing RRC Reconfiguration message in RRC Container to be sent to ME+ via the Source RNC+, in which FRESH and NCC are included.

6. The SRNC+ sends ME+ **Physical Channel ReConfiguration** message.

7. If KH is not supported in the target RNC, the mapping keys CK'/IK' are derived and used.

   If KH is supported in the target RNC, ME+ shall synchronize the locally kept K_{RNC}* parameter, and regard K_{RNC}* as K_{RNC}. ME+ shall derive CKU/IKU in the same way as target RNC+.

8. When the RRC connection is established with the target RNC+ and necessary radio resources have been allocated the ME+ sends RRC message **Physical Channel Reconfiguration Complete** to the target RNC+. This message is protected by the new CKU/IKU.

9. Target RNC+ sends the **RANAP Enhanced Relocation Complete Request** message to the CNN+, indicating that relocation is happened on the ME+.

10. SGSN+ shall increase NCC, and compute a new K_{RNC}*(eg., K_{RNC}*=F4(IK||CK, old_ K_{RNC}*)).

11. SGSN+ configures the necessary Iu resources for the Target RNC+ and acknowledges with "**RANAP Enhanced Relocation Complete Response**" message to the Target RNC+, including {K_{RNC}*,NCC}.

12. The target RNC+ shall store the received {K_{RNC}*,NCC} for the next SRNC relocation.

13. CNN+ initiates release of the resources in the source RNC+.

5.1.3.4 Idle mode mobility

When ME+ enters Idle mode, SRNC+ and ME+ shall delete CK_U and IK_U, and SGSN+ and ME+ shall delete the chained keys.

When ME+ goes from Idle mode to active mode, if needed, a Security Mode Command procedure is performed after the RRC connection is setup. During the SMC procedure, fresh CK_U and IK_U are established in the network and ME+ respectively, just the same as in the initial attach procedure.

5.1.3.5 Inter SGSN(*)/MME AV transfers

Since there is no special handling of AVs necessary for supporting the UTRAN KH, AV transfers between SGSN(*) shall be according to TS 33.102 [3], and AV transfers of AVs between SGSN(*) and MME shall be according to TS 33.401 [4].

5.1.4 Inter-working with GERAN procedures

5.1.4.1 General

When interworking with GERAN, HSPA+ system should be compatible with GERAN system. All the key materials that will be used later should be derived in HSPA+ system.

SGSN+/RNC+ should derives enhanced UMTS cipher/integrity keys CK_U and IK_U based on CK and IK

- SGSN+ derives K_{RNC} from UMTS cipher/integrity keys CK and IK, which are then forwarded to the target RNC+.

- The RNC+ derives enhanced UMTS cipher/integrity keys CK_U and IK_U from K_{RNC}.

5.1.4.2 Attach, RAU and Service Requests

An SGSN receiving such an initial layer 3 message may need to fetch the UE context from another SGSN.

When the new SGSN+ requests the UE context from the old SGSN, the old SGSN pass the GSM cipher key Kc to the new SGSN+, SGSN+ derives UMTS cipher/integrity keys CK and IK from the GSM cipher key Kc, and SGSN+ derives K_{RNC} from CK, IK and the fresh parameter, which are then forwarded to the target RNC+. The RNC+ derives enhanced UMTS cipher/integrity keys CK_U and IK_U from K_{RNC} as described in clause 5.1.3.1.

When the new SGSN requests the UE context from the old SGSN+, the old SGSN+ derives GSM cipher key Kc based on CK and IK, and pass the Kc to the new SGSN just the same as described in TS 33.102 [3].

5.1.4.3 Handovers

5.1.4.3.1 Handover from GERAN to enhanced UTRAN

In case of an intersystem change to an enhanced UTRAN controlled by the same or another SGSN, (i.e. enhanced SGSN or SGSN+), the IK and CK derivations are the same as TS 33.102 [3] defined. After SGSN+ gets IK/CK, it derives K_{RNC} from CK, IK and the fresh parameter, which are then forwarded to the target RNC+. The RNC+ derives enhanced UMTS cipher/integrity keys CK_U and IK_U from K_{RNC} as described in clause 5.1.3.1.

ME+ shall operate the same as the target network to derive IK_U/CK_U after it receives the HO Command message which indicates the target RNC supports the enhanced security.

5.1.4.3.2 Handover from enhanced UTRAN to GERAN

In case of an intersystem change to a GERAN controlled by the same or another SGSN, (i.e. enhanced SGSN or SGSN+), all the operations are just the same as described in TS 33.102 [3].

5.1.5 Inter-working with E-UTRAN

5.1.5.1 RAU and TAU Procedure

5.1.5.1.1 RAU procedures in UTRAN

The behaviour of SGSN+ is just the same as specified in TS 33.401 [4]. If Mapped context is used, target SGSN+ and ME+ shall derive and store K_{RNC} based on the mapping IK'/CK' individually.

5.1.5.1.2 TAU procedures in E-UTRAN

The behaviour of SGSN+ and ME+ is just the same as specified in TS 33.401 [4].

5.1.5.2 Handover procedure

5.1.5.2.1 Handovers from E-UTRAN to UTRAN

The behaviour of SGSN(*) is just the same as specified in TS 33.401 [4]. ME+ and MME shall derive a confidentiality key CK', and an integrity key IK' from the K_{ASME}. MME shall send CK' and IK' to the target SGSN(*). If the target SGSN supports the enhanced security, it shall regard the received CK'/IK' as CK/IK, and then derive K_{RNC} based on CK/IK. K_{RNC} should be transmitted to the target RNC+ carried by Relocation Request message. The target RNC+ shall derive CK_U/IK_U based on K_{RNC} and the selected security algorithm and new FRESH, which is generated by the target RNC+.

ME+ shall operate the same as the target network to derive IK_U/CK_U after it receives the HO from E-UTRAN Command message which indicates the target RNC+ supports the enhanced security.

5.1.5.2.2 Handovers from UTRAN to E-UTRAN

The behaviour of SGSN+ and ME+ is just the same as specified in TS 33.401 [4].

5.1.6 Summary of changes to messages

5.1.6.1 General

The following sub-clauses list the changes to existing messages that are needed to support the solution 1.

5.1.6.2 Changes to TS 24.008

The following messages or IEs in TS 24.008 [5] require a change to support solution 1.

Attach request

An indication that a ME+ supports enhanced security context functionality.

RAU Request

An indication that a ME+ supports enhanced security context functionality.

RAU Accept

An indication that the target SGSN+ after an intra-UTRAN handover or a handover to UTRAN supports the enhanced security context.

5.1.6.3 Changes to TS 24.301

The following messages or IEs in TS 24.301 [6] require a change to support solution 1.

Attach request

An indication that a ME+ supports enhanced security context functionality.

Tracking area update request

An indication that a ME+ supports enhanced security context functionality.

Editor's note: It should be clarified whether this indication is transparent to a legacy MME.

5.1.6.4 Changes to TS 29.060

The following messages or IEs in TS 29.060[7] require a change to support solution 1.

SGSN Context Response message

An SGSN+ includes {K_{RNC}*, NCC}, {IK, CK} and DL COUNT if the security context being used is an enhanced one.

Forward Relocation Request

An indication that a ME+ supports enhanced security context functionality.

{K_{RNC}*, NCC} used to derive the enhanced keys IK_U/CK_U during SRNS relocation.

Forward Relocation Response

An indication that the target RNC+ supports enhanced security context functionality.

A NCC used to synchronize key derivation between the target network and the ME+.

A fresh parameter (eg., NONCE) sent to ME+ used to derive K_{RNC} when UE+ moves from E-UTRAN to UTRAN supporting UTRAN KH.

5.1.6.5 Changes to TS 29.274

The following messages or IEs in TS 29.274 [8] require a change to support solution 1.

Forward Relocation Request

An indication that a ME+ supports enhanced security context functionality.

{K_{RNC}*, NCC} used to derive the enhanced keys IK_U/CK_U during SRNS relocation.

Forward Relocation Response

An indication that the target RNC+ supports enhanced security context functionality.

A NCC used to synchronize key derivation between the target network and the ME+.

A fresh parameter (eg., NONCE) sent to ME+ used to derive K_{RNC} when UE+ moves from E-UTRAN to UTRAN supporting UTRAN KH.

5.1.6.6 Changes to TS 25.413

The following messages or IEs in TS 25.413 [9] require a change to support solution 1.

SECURITY MODE COMMAND

An indication whether or not the SGSN(*) supports the enhanced security.

UE UTRAN KH capability received in the first L3 message sent by UE.

A K_{RNC} used to derive the enhanced keys IK_U/CK_U.

{K_{RNC}*, NCC} pair used to derive the next hop enhanced keys IK_U/CK_U during SRNS relocation.

A COUNT sent to UE+ used to derive K_{RNC}.

Relocation Required

An indication whether or not the ME(*) supports the enhanced security.

Relocation Request

An indication whether or not the ME(*) supports the enhanced security.

{K_{RNC}*, NCC} used to derive the next hop enhanced keys IK_U/CK_U during SRNS relocation.

K_{RNC} used when ME+ moves from E-UTRAN to UTRAN supporting UTRAN KH.

A fresh parameter (eg., NONCE) sent to ME+ used to derive K_{RNC} when ME+ moves from E-UTRAN to UTRAN supporting UTRAN KH.

Relocation Request Acknowledge/Relocation Command

An indication to ME whether or not the target RNC supports the enhanced security.

A NCC used to synchronize key derivation between the target network and the ME+.

A fresh parameter (eg., NONCE) sent to ME+ used to derive K_{RNC} when UE+ moves from E-UTRAN to UTRAN supporting UTRAN KH.

Enhanced Relocation Complete Response

{K_{RNC}*, NCC} pair used to derive the next hop enhanced keys IK_U/CK_U during next SRNS relocation.

5.1.6.7 Changes to TS 25.423

The following messages or IEs in TS 25.423 [13] require a change to support solution 1.

Enhanced Relocation Request

An indication whether or not the ME(*) supports the enhanced security.

{K_{RNC}*, NCC} used to derive the next hop enhanced keys IK_U/CK_U during SRNS relocation.

Enhanced Relocation Response

An indication to UE whether or not the target RNC(*) supports the enhanced security.

A NCC used to synchronize key derivation between the target network and the ME+.

5.1.6.8 Changes to TS 25.331

The following messages or IEs in TS 25.331 [10] require a change to support solution 1.

SECURITY MODE COMMAND

An indication whether or not the network (SGSN(*) and SRNC(*)) supports the enhanced security.

UE UTRAN KH capability received in the first L3 message sent by ME+.

A K_{RNC} used to derive the enhanced keys IK_U/CK_U.

{K_{RNC}*, NCC} pair used to derive the next hop enhanced keys IK_U/CK_U during SRNS relocation.

A COUNT sent to ME+ used to derive K_{RNC}.

Physical Channel Reconfiguration/UTRAN Mobility Information/Cell Update Confirm/URA Update Confirm

An indication whether or not the target network (SGSN(*) and SRNC(*)) supports the enhanced security.

A NCC used to synchronize key derivation between the target network and the ME+.

Physical Channel Reconfiguration Complete/UTRAN Mobility Information Confirm

An indication whether or not the ME(*) supports the enhanced security.

Handover to UTRAN Command

A fresh parameter (eg., NONCE) sent to UE+ used to derive K_{RNC} when ME+ moves from GERAN to UTRAN supporting UTRAN KH.

An indication whether or not the target network (SGSN(*) and SRNC(*)) supports the enhanced security.

5.1.6.9 Changes to TS 36.413

The following messages or IEs in TS 36.413 [14] require a change to support solution 1.

Handover Command

A fresh parameter (eg., NONCE) sent to ME+ used to derive K_{RNC} when ME+ moves from E-UTRAN to UTRAN supporting UTRAN KH.

An indication whether or not the target network (SGSN(*) and SRNC(*)) supports the enhanced security.

5.1.6.10 Changes to TS 36.331

The following messages or IEs in TS 36.331 [15] require a change to support solution 1.

MobilityFromEUTRACommand

A fresh parameter (eg., NONCE) sent to ME+ used to derive K_{RNC} when ME+ moves from E-UTRAN to UTRAN supporting UTRAN KH.

An indication whether or not the target network (SGSN(*) and SRNC(*)) supports the enhanced security.

5.2 Proposed solution 2

5.2.1 General

The aim of this solution is to give a method of providing CN and RAN level key separation including fresh RAN keys for each Idle to Active transition. The goals of this solution are to enable these security features in the following manner, such that:

- Only CN nodes need to be upgraded, i.e. no changes to RNC are necessary
- CN nodes can be upgraded one at a time and the security benefit are realised until the UE moves to a non-upgraded CN node

- When the UE moves to a legacy node, the keys that will be used subsequently will not affect the security of previous sessions.

One consequence of the 2nd design feature above is that is possible to have variants of solution 2 where none, some or all of the E-UTRAN related enhancements are specified. The benefit of each of these changes should be analysed before being accepted into a final design that is specified in normative specifications. The benefit of the E-UTRAN enhancements is to provide the better security without having to run AKA at all inter-system changes (e.g. in UTRAN/GERAN an enhanced security context and in E-UTRAN a security context where K_{ASME} is calculated from keys that haven't been exposed outside the core network).

If is desired to have a variant of solution 2 that includes no changes to E-UTRAN then the functionality in sub-clause 5.2.2.3 and the message changes in sub-clauses 5.2.3.4.3 and sub-clauses 5.2.3.4.5 can be omitted. Omitting these has no effect on the UTRAN/GERAN functionality and message changes.

This solution is not intended to preclude the inclusion of RAN level security enhancements for which IK_S and CK_S could be used as the base keys.

5.2.2 Overview of the solution

The solution defines an enhanced security context (see below) that will be used by the UE and CNN whenever possible. Once the ME moves to an CNN that does not support the enhanced security context, both the UE and legacy SGSN will fall back to a legacy security context as described in the following clauses. The calculation of Kc and Kc_{128} and the handling of START parameters are not changed by this solution.

The enhanced security context contains the following parameters:

- KSI = 3-bit Key Set Identifier that is used exactly as in legacy UTRAN
- K_{ASMEU} = 256-bit root key for the enhanced security context that is calculated from CK and IK at an AKA in UTRAN/GERAN or from K_{ASME} when interworking with E-UTRAN (the exact KDF is FFS)
- COUNT = 16-bit counter that is used to ensure that fresh keys can be calculated at every Idle to Active transition

From these basic parameters, two different sets of CK and IK will be calculated

- CK_S and IK_S which are calculated as follows CK_S $||IK_S$ = KDF(K_{ASMEU}, COUNT)
- CK_L and IK_L which are calculated as follows CK_L || IK_L = KDF (K_{ASMEU}, fixed values)

The basic use of the enhanced security context is as follows with any exceptions given in the detailed procedures. The first pair, CK_S and IK_S, are passed to the RNC at every Idle to Active transitions by an CNN + when the ME is aware it is communicating with a CNN+ and are used to protect that session. These keys need to be stored in ME and CNN during the session. These keys will become the key used in a legacy security context if the ME moves to an CNN while in connected mode that does not support the enhanced security context. The second set, CK_L and IK_L, are passed from an CNN+ at Idle mode mobility and become the keys used in a legacy context if the new CNN does not support the enhanced security context.

5.2.3 Proposed PS solution

5.2.3.1 Intra-UTRAN procedures

5.2.3.1.1 General

This following sub-clause covers the changes needed to various procedures inside UTRAN to support the enhanced security context.

5.2.3.1.2 AKA

Before running an AKA, an SGSN+ will be aware of whether the ME supports the enhanced security context or not. This is because the ME+ will have signalled its support in the initial layer 3 message (see clause 5.2.3.1.3.1). If both SGSN and UE support the enhanced security context when the SGSN sends the Authentication and Ciphering Request

message carrying the AKA challenge it shall include an indication to the ME that the ME shall create an enhanced security context from this AKA run.

As a result of this message both the ME and SGSN shall create an enhanced security context and set COUNT = 1. In addition they shall both calculate CK_S and IK_S using the new K_{ASMEU} and COUNT = 0 for any subsequent security mode procedure or inter-RAT handovers. The SGSN shall delete any previously stored security context. The ME shall delete any previously stored security context once that context is no longer in use to protect traffic.

NOTE: In case when UE and SGSN+ both support the enhanced security context and the enhanced security context is available as a result of UE+ mobility from one SGSN+ to another SGSN+, a new AKA run is not necessary.

5.2.3.1.3 Attach, RAU and Service Requests

5.2.3.1.3.1 Initial message

In all Attach Request and RAU Request messages, an ME+ shall signal it support of the enhanced UTRAN security context to the SGSN. In addition in all the initial layer 3 messages, if the security context indicated in the KSI signalled by the ME+ is an enhanced one, the ME+ shall include the current value of COUNT in the message and also increase the stored COUNT by 1. The UE needs to remember the sent value of COUNT as this may be used to calculate a CK_S and IK_S pair subsequently.

An SGSN receiving such a message may need to fetch the ME context from another SGSN (see clause 5.2.3.1.3.2) before initiating the security mode procedure (see clause 5.2.3.1.3.3).

5.2.3.1.3.2 Transfer of security context between SGSN

In the case when one SGSN needs to fetch the UE context from another one, i.e. Attaches and RAUs involving a change of SGSN, the new SGSN requests the UE context from the old SGSN exactly as before.

An old SGSN+ that holds an enhanced security context does the following:

- calculates CK_L and IK_L (as described in clause 5.2.2) and include these in the existing IEs that are used to carry CK and IK currently.
- sends the K_{ASEMU} and COUNT to the new SGSN as well.

A legacy SGSN receiving the above message will use CK_L and IK_L as a legacy security context. An SGSN+ will be able to either use the enhanced security context with the UE or fallback to a legacy context with CK_L and IK_L as the keys.

The procedures on initiating a security mode command are described in the next clause.

5.2.3.1.3.3 Security mode command procedure

An SGSN+ that receives a message from a ME+ including a COUNT value and holds the enhanced security context for the ME+ does the following:

- it checks whether the received COUNT is greater than or equal to the stored COUNT
- if so it sets the stored COUNT equal to the received COUNT + 1 and calculates CK_S and IK_S from K_{ASMEU} and the received COUNT value
- if not, the error case behaviour is FFS.

A legacy SGSN will just ignore the COUNT value and use the CK_L and IK_L received from the old SGSN as keys.

The SGSN will then initiate the security mode procedure and pass either CK_L and IK_L or CK_S and IK_S to the RNC depending on the situation above. The RNC will then send the security mode command message to the ME(*) using the keys it received.

A ME+ that holds an enhanced security context may not be sure whether IK_L or IK_S has been sent to the RNC in the case that some Idle mode mobility may have happened from a SGSN+. In such a case, the ME+ checks the security mode command message integrity with both IK_S and IK_L. If IK_S works, then ME+ uses the enhanced security context. If

IK_L works then the ME+ shall transform the enhanced security context into a legacy one with CK_L and IK_L as the keys. If the integrity check fails with both keys IK_S and IK_L, the ME+ rejects the security mode command.

An RNC+ could be used to avoid the ME+ needing to check integrity of the security mode command with two different integrity keys. This enhancement is not necessary to realise the security benefits of an enhanced security context but may be worth including. In particular if RNC functionality is enhanced to provide RAN level security gains. The enhancement would work as follows. When the SGSN+ triggers the security mode procedure using keys derived from an enhanced security context, it includes an indication in the RANAP message that enhanced keys are being used or not. The RNC+ would include a similar indication in the RRC message, which the ME+ would then use to determine which integrity key to try. Legacy RNCs or MEs would ignore such an indication.

5.2.3.1.4 Intra-UTRAN handovers

An ME+ that is using an enhanced security context with an SGSN+ may be moved in connected mode to another SGSN.

In this case the SGSN+ includes CK_S and IK_S in the legacy CK and IK IEs and also includes K_{ASMEU} and COUNT in the transfer of the UE context to the target SGSN.

A legacy SGSN receiving such a message would treat the ME(*) as though it had a legacy context with CK_S and IK_S as keys.

An SGSN+ continues to use the enhanced security context and signals that it wishes to continue to so in the RAU Accept message that follows the RAU Request message that will be sent if the handover caused a change of SGSNs (as RA will have changed).

An ME+ that does not receive the expected RAU Accept message before it goes into Idle will delete the enhanced security context. An ME+ that receives the RAU Accept with no indication to continue using the enhanced security context will fallback to a legacy context with CK_S and IK_S as keys. If the ME+ receives the indication then it continues to use the enhanced security context.

5.2.3.2 Inter-working with GERAN procedures

5.2.3.2.1 General

The procedures for interworking with GERAN are nearly identical to the intra-UTRAN procedures with two exceptions. Firstly at Idle mode mobility from UTRAN/GERAN to GERAN to a new SGSN, it is necessary to signal whether the ME shall use legacy or session keys as a RAU Complete can be protected. This is achieved by sending an Authentication and Ciphering Command using the new indication that was included for UTRAN. Doing this ensures that there is a fresh RAN level key available if the ME is handed back into UTRAN after Idle mode mobility to GERAN. Secondly at handover from UTRAN to GERAN, the IK_S and CK_S are changed in order to ensure that if the ME is handed back to UTRAN after a transition to Idle mode and then Active mode again in GERAN there are fresh RAN level keys available. The new CK_S and IK_S are derived from K_{ASMEU} using the current CK_S and IK_S and the fact that this key derivation has occurred is signalled in handover signalling.

5.2.3.2.2 AKA

The same changes as for UTRAN are needed (see clause 5.2.3.1.2). Both the SGSN+ and ME+ shall calculate Kc from the CK_S and IK_S using the normal functions.

5.2.3.2.3 Attach, RAU and Service Requests

The same changes as for UTRAN (see clause 5.2.3.1.3), except a new SGSN that supports the enhanced security shall initiate an Authentication and ciphering request message to inform the ME+ of its use of the enhanced security context. Both the SGSN+ and ME+ shall calculate Kc from the CK_S and IK_S using the normal functions.

5.2.3.2.4 Handovers

5.2.3.2.4.1 Handover from GERAN to UTRAN

This context transfer follows the behaviour as in clause 5.2.3.1.4. The SGSN will pass IK_S and CK_S to the RNC and these will be used for security after the handover.

An SGSN+ and ME+ will act in the subsequent RAU procedure as described in clause 5.2.3.1.4.

5.2.3.2.4.2 Handover from UTRAN to GERAN

The context transfer follows the behaviour as in clause 5.2.3.1.4.

An SGSN+ receiving an enhanced context does the following

- Calculates a new CK_S and IK_S from K_{ASMEU} and the received CK_S and IK_S
- Inform the ME+ that its support the enhanced security context and has performed the above key derivation by setting one bit of the NAS Container for PS HO IE (see TS 24.008) [5]

An ME+ receiving a NAS Container for PS HO IE with the relevant bit set continues to use the enhanced security context and performs the same update of CK_S and IK_S as the SGSN+.

Otherwise the ME+ falls back to a legacy security context with original CK_S and IK_S as the keys for the secruity context.

The Kc to be used between the SGSN and ME+ is calculated form CK_S and IK_S using the normal functions.

5.2.3.3 Inter-working with E-UTRAN procedures

5.2.3.3.1 General

If a solution with no E-UTRAN changes is desired, then the functionality in subclaue 5.2.3.3 shall be omitted.

This following sub-clause covers the changes needed to various procedures to interwork with E-UTRAN to support the enhanced security context. The only significant difference from the intra-UTRAN procedures is during handover to E-UTRAN, the MME signals its capability to the ME in order to inform the ME whether to use the legacy method of generating K_{ASME} or to generate K_{ASME} from K_{ASMEU}.

The other notable functionality is that when an MME+ that is working with a ME+ passes the security context to an SGSN (in both Idle mode mobility and Active mode), the MME calculates a fresh K_{ASMEU} and sends COUNT = 0. This mimics the SGSN+ behaviour as far as the target SGSN is concerned.

5.2.3.3.2 EPS AKA

No changes are needed.

5.2.3.3.3 Idle mobility

5.2.3.3.3.1 Attach and TAU procedures in EPS

In Attach and TAU Requests, the ME+ shall signal its support of the enhanced security context. This means that an MME+ is aware of the ME's capabilities and can act appropriately when sending the ME's context to an SGSN during either Idle mode mobility or handover.

At Idle mode mobility between MMEs, if the current EPS NAS security context is an enhanced mapped one, i.e. it was created from an enhanced UTRAN security context, the old MME indicates this to the new MME.

In the case, an enhanced MME receives a K_{ASMEU} from an SGSN in Idle mode mobility from UTRAN/GERAN to E-UTRAN, it shall use K_{ASMEU} along with the exchanged nonces instead of the CK_L and IK_L (the keys received in the legacy IEs) to calculate K_{ASME}. In this case it shall signal to the ME that it has used K_{ASMEU} to calculate K_{ASME} in the

NAS Security Mode Command that creates the mapped context. The MME+ shall also remember that this Mapped EPS security context is an enhanced one.

An enhanced ME that receives such an indication in the NAS Security Mode Command shall use K_{ASMEU} to calculate K_{ASME}. The ME+ remembers that this mapped EPS NAS security context is an enhanced one.

5.2.3.3.3.2 Attach and RAU procedures in UTRAN/GERAN when TIN = 'GUTI'

The behaviour here is identical to that described in clause 5.2.3.1.3 with an MME+ acting like an SGSN+ except the following when the current EPS NAS security context is either a native or an enhanced mapped one

- The ME+ includes a COUNT = 0 in the initial message
- An MME+ that knows the ME(*) supports the enhanced security context calculates K_{ASMEU} from K_{ASME} and the same inputs as are used to calculate CK' and IK' except that the KDF is different. It sends K_{ASMEU} and COUNT = 0 to the SGSN.
- The ME+ tries IK_S (calculated from K_{ASMEU} with a COUNT of 0) and IK' to check the integrity protection of a subsequent security mode command.

5.2.3.3.4 Handovers

5.2.3.3.4.1 Intra-E-UTRAN S1 handovers

A source MME+ informs the target MME that the ME(*) supports the enhanced security context. This is to ensure a target MME+ is aware of the ME capabilities in case of a handover before the subsequent TAU Request.

The source MME+ also informs the target MME if the current EPS NAS security context is an enhanced mapped one.

5.2.3.3.4.2 Handovers from E-UTRAN to UTRAN/GERAN

This follows the behaviour as in clause 5.2.3.1.4, except that an MME+ that is handing a ME+ over to an SGSN does the following when the current EPS NAS security context is either a native or an enhanced mapped:

- The MME+ calculates a K_{ASMEU} from K_{ASME} and the same input parameters as used for calculating CK' and IK' except the KDF is different. It passes K_{ASMEU} and COUNT = 0 over to the SGSN.

In UTRAN, the SGSN will pass IK_S and CK_S to the RNC and these will be used for security after the handover. An SGSN+ and ME+ will act in the subsequent RAU procedure as described in clause 5.2.3.1.4.

In GERAN, the SGSN+ and ME+ then acts as in a UTRAN to GERAN handover (see clause 5.2.3.2.4.2).

5.2.3.3.4.3 Handover from GERAN/UTRAN to E-UTRAN

A source SGSN+ transfer the security context to the MME as described in clause 5.2.1.3

A target MME+ receiving the K_{ASMEU} and COUNT behaves as follows

- Calculates a new K_{ASME} and the received K_{ASMEU} using IK_S and CK_S as inputs to ensure a fresh K_{ASME}
- Informs the ME+ that its supports the enhanced security context and has performed the above key derivation by setting one bit of the NAS Security parameters to E-UTRA IE (see TS 24.301 [6])

An ME+ receiving NAS Security parameters to E-UTRA IE with the relevant bit set uses the new calculation for K_{ASME}. The ME+ remembers that this mapped EPS NAS security context is an enhanced one. Otherwise the ME+ falls back to a legacy security context with K_{ASME} calculated as in legacy situation.

5.2.3.3.5 Analysis of the benefits of inter-working with E-UTRAN

It has been noted in subclause 5.2.1, that all, some or none of the inter-working with E-UTRAN enhancements could be included in a chosen UTRAN KH solution. In this subclause, the benefits of the various interworking with E-UTRAN procedures that have been proposed for solution 2 are analysed. As further noted in subclause 5.2.1, the benefits have to

be weighed against the complexity of their implementation and deployment before being accepted into a final design that is specified in normative specifications.

The UTRAN KH work proposes to introduce an enhanced type of security context to UTRAN (and possibly GERAN). The legacy interworking procedures could not create such a context on transition from E-UTRAN to UTRAN/GERAN as an SGSN+ is not aware whether the keys passed to it are derived for keys that have not been exposed outside the core network. Hence if an operator wishes to always use such a context for UTRAN KH-enhanced MEs it is necessary to run an AKA at every transition to UTRAN/GERAN. In addition to this AKA run, if an operator desires to always use a native context (see [4]) in E-UTRAN due to the fact that K_{ASME} is not exposed outside of the core network a further AKA may be required on transition to E-UTRAN. E-UTRAN however provides the concept of cached (native) EPS NAS security contexts, which was introduced to remove the need for AKAs in this particular case. If those contexts are used, there is no need to run an AKA at mobility from UTRAN/GERAN to E-UTRAN. It is however only possible to use a (cached) native EPS NAS security context if the UE comes back to the same MME where the context is stored. Therefore, if an operator opts to use UTRAN KH, there may be less reason to run an EPS AKA in E-UTRAN if the UE moves to a different MME and hence the number of EPS AKA runs in E-UTRAN could be reduced.

Without some enhancement to interworking with E-UTRAN (such an enhancement could be one that does not change EPS specifications), the introduction of UTRAN KH may increase (compared to before the operator decided to improve the security in UTRAN) the number AKA runs to due transitions between E-UTRAN and UTRAN/GERAN.

Editor's Note: Enhancements to interworking with E-UTRAN that do not change EPS specifications while not increasing the number of EPS AKA runs are ffs.

When transitioning from UTRAN/GERAN to E-UTRAN, the MME can be made aware that the K_{ASME} that results from the transition has been calculated from keys that have not been exposed outside the core network and the MME could then skip running EPS-AKA. To achieve this some changes are required to the MME to enable such functionality. A similar argument holds for the transition to UTRAN/GERAN in that the MME could have some new functionality to inform the SGSN that the keys it is being sent have been generated from keys that have not been exposed out side the CN.

These interworking features are provided in the proposed solution 2 by the message changes to TS 24.301 given in subclause 5.2.4.3 and the associated functionality, i.e. all of subclause 5.2.3.3.3.1 except the 2nd paragraph, all of subclause 5.2.3.3.3.2, all of subclause 5.2.3.3.4.2 and all of subclause 5.2.3.3.4.3.

The final message changes and associated functionality deal with the cases of MME and ensuring the new MME has the necessary information.

The 'indication that a ME+ supports enhanced security context' in the Forward Relocation Request message ensures a target MME + is aware of the ME capabilities for any handovers to UTRAN/GERAN before any TAU Request.

The 'indication that the current mapped context is an enhanced one' in the Forward Relocation Request and Context Response message ensure that the new MME is aware of enhanced mapped and hence could be used to create an enhanced UTRAN security context at a subsequent transition to UTRAN/GERAN.

5.2.3.4 Summary of changes to messages for PS

5.2.3.4.1 General

The following sub-clauses list the changes to existing messages that are needed to support the solution 2 for PS.

5.2.3.4.2 Changes to TS 24.008

The following messages or IEs in TS 24.008 [5] that require a change to support solution 2.

Authentication and ciphering request message

An indication to the ME+ that it shall use an enhanced security context

Attach request message

An indication that a ME+ supports enhanced security context functionality

The COUNT value when the ME+ is using an enhanced security context

RAU Request message

An indication that a ME+ supports enhanced security context functionality

The COUNT value when the ME+ is using an enhanced security context

Service Request message

The COUNT value when the ME+ is using an enhanced security context

RAU Accept message

An indication that the target SGSN+ after an intra-UTRAN handover or a handover to UTRAN supports the enhanced security context

NAS Container for PS HO IE

One bit of this is set to inform the ME+ that the SGSN+ has performed a non-legacy key derivation

5.2.3.4.3 Changes to TS 24.301

If a solution with no E-UTRAN changes is desired, then the message changes in this subclause shall be omitted.

The following messages or IEs in TS 24.301[6] that require a change to support solution 2.

Attach request message

An indication that a ME+ supports enhanced security context functionality

Tracking area update request message

An indication that a ME+ supports enhanced security context functionality

NAS Security Mode Command message

An indication the MME used K_{ASMEU} to calculate K_{ASME} when creating this mapped security context

NAS Security parameters to E-UTRA IE

One bit of this is set to inform the ME+ that the MME+ has performed a non-legacy key derivation.

5.2.3.4.4 Changes to TS 29.060

The following messages or IEs in TS 29.060 [7] that require a change to support solution 2.

Context Response message

An SGSN+ includes K_{ASMEU} if the security context being used is an enhanced one

An SGSN+ includes COUNT if the security context being used is an enhanced one

Forward Relocation Request message

An SGSN+ includes K_{ASMEU} if the security context being used is an enhanced one

An SGSN+ includes COUNT if the security context being used is an enhanced one

5.2.3.4.5 Changes to TS 29.274

If a solution with no E-UTRAN changes is desired, then the message changes in this subclause shall be omitted.

The following messages or IEs in TS 29.274 [8] that require a change to support solution 2.

Forward Relocation Request message

An indication that a ME+ supports enhanced security context functionality

An indication that the current mapped EPS NAS security context is an enhanced one

Context Response message

An indication that the current mapped EPS NAS security context is an enhanced one

5.2.3.4.6 Changes to TS 25.413

The following messages or IEs in TS 25.413 [9] that require a change to support solution 2.

SECURITY MODE COMMAND message

An indication whether or not the SGSN+ has used an enhanced security key derivation to get the keys

5.2.3.4.7 Changes to TS 25.331

The following messages or IEs in TS 25.331 [10] that require a change to support solution 2.

SECURITY MODE COMMAND message

An indication whether or not the SGSN+ has used an enhanced security key derivation to get the keys

5.2.4 CS related procedures

5.2.4.1 Intra-UTRAN procedures

5.2.4.1.1 General

This following sub-clause covers the changes needed to various procedures inside UTRAN to support the enhanced security context.

5.2.4.1.2 AKA

Before running an AKA, an MSC+ will be aware of whether the ME(*) supports the enhanced security context or not. This is because the ME+ will have signalled its support in the initial layer 3 message (see subclause 5.2.4.1.3.1). If both the MSC and ME support the enhanced security context when the MSC sends the Authentication Request message carrying the AKA challenge it shall include an indication to the ME+ that the ME+ shall create an enhanced security context from this AKA run.

As a result of this message both the ME+ and MSC+ shall create an enhanced security context and set COUNT = 1. In addition they shall both calculate CK_S and IK_S using the new K_{ASMEU} and COUNT = 0 for any subsequent security mode procedure. The MSC+ and ME+ shall keep any previous security context if it already been used to protect traffic.

5.2.4.1.3 Initial message and subsequent procedures

5.2.4.1.3.1 Initial message

In all initial message that may involve a change of MSC (e.g. Location Updating Request), an ME+ shall signal it support of the enhanced UTRAN security context to the MSC. In addition in all the initial layer 3 messages, if the security context indicated in the KSI signalled by the ME+ is an enhanced one, the ME+ shall include the current value of COUNT in the message and also increase the stored COUNT by 1. The ME needs to remember the sent value of COUNT as this may be used to calculate a CK_S and IK_S pair subsequently.

An MSC receiving such a message may need to fetch the UE context from another MSC (see clause 5.2.4.1.3.2) before initiating the security mode procedure (see clause 5.2.4.1.3.3).

5.2.4.1.3.2 Transfer of security context between MSCs

This follows the PS case with SGSN being replaced with MSC (see subclause 5.2.3.1.2.2).

5.2.4.1.3.3 Security mode command procedure

This follows the PS case with SGSN being changed to MSC (see subclause 5.2.3.1.2.3)

5.2.4.1.4 Intra-UTRAN handovers

There is no special behaviour.

5.2.4.2 GERAN interworking procedures

5.2.4.2.1 General

This proposal for GERAN inter-working with UTRAN follows the UTRAN procedures with the following exception. When the ME+ sends a Location Updating request that potentially changes MSC, the ME+ will be unsure of the (possibly new) MSCs support for enhanced UTRAN security context. For this reason when the ME could possibly change MSC (e.g. needs to send a non-periodic Location Updating Request), the ME+ does not include a COUNT value in the message. Both the ME and MSC use CK_L and IK_L for the security for this Idle to active transition. The MSC informs the ME whether it considers the current security context to be enhanced in the Location Updating Accept message. Furthermore if the ME+ is subsequently as part of this active session is handed over to UTRAN, then the ME defaults to a legacy context with CK_L and IK_L as the keys. This ensures that the same keys are not used for two active session in UTRAN while the ME and network believe they are using an enhanced security context.

5.2.4.2.2 Initial message and subsequent procedures

5.2.4.2.2.1 Initial message with possible MSC change

In all initial layer 3 messages that may involve a change of MSC (e.g. Location Updating Request), an ME+ shall signal its support of the enhanced UTRAN security context to the MSC.

The new MSC fetches the security context from the old MSC as described in subclause 5.2.4.1.3.2. The MSC and ME shall use CK_L and IK_L as the keys for this active session and calculate any GERAN keys from these using the normal functions.

The new MSC signals whether the security context it is using is an enhanced one in the Location Updating Accept message. If the ME does not receive the indication that the current context is an enhanced one, the ME shall fallback to a legacy context with CK_L and IK_L as keys.

Furthermore if the ME is handed over to UTRAN while using CK_L and IK_L as the keys, it shall fall back to a legacy context with CK_L and IK_L as keys.

5.2.4.2.2.2 Initial message without possible MSC change

In all the initial layer 3 messages when the ME+ know the MSC cannot change, if the security context indicated in the KSI signalled by the ME+ is an enhanced one the ME+ shall include the current value of COUNT in the message and also increase the stored COUNT by 1. The UE needs to remember the sent value of COUNT as this may be used to calculate a CK_S and IK_S pair subsequently.

The MSC shall check the value of COUNT as described in subclause 5.2.3.1.2.3 and if it is acceptable calculate CK_S and IK_S. Both the ME and MSC shall calculate the relevant GERAN keys from these.

5.2.4.3 Summary of changes to messages for CS domain

5.2.4.3.1 General

The following sub-clauses list the changes to existing messages that are needed to support the solution 2 for the CS domain that are in addition to the PS changes.

5.2.4.3.2 Changes to TS 24.008

The following messages or IEs in TS 24.008 [5] that require a change to support solution 2.

Authentication request message

An indication to the ME+ that it shall use an enhanced security context

Location updating request message

An indication that a ME+ supports enhanced security context functionality

The COUNT value when the ME+ is using an enhanced security context

CM re-establishment request

The COUNT value when the ME+ is using an enhanced security context

CM Service Request message

The COUNT value when the ME+ is using an enhanced security context

Location updating response message

An indication that the current security context is an enhanced one

5.2.4.3.3 Changes to TS 44.018

The following messages or IEs in TS 44.018 [17] that require a change to support solution 2.

Paging response

The COUNT value when the ME+ is using an enhanced security context

5.2.4.3.4 Changes to TS 29.002

The following messages or IEs in TS 29.002 [16] that require a change to support solution 2.

MAP_SEND_IDENTIFICATION service

A previous MSC+ includes K_{ASMEU} if the security context being used is an enhanced one

A previous MSC+ includes COUNT if the security context being used is an enhanced one

5.3 Proposed solution 3

5.3.1 General

Solution 3 can be seen as an add-on to Solution 2 in the sense that Solution 3 provides key derivations at SRNS relocations similar to X2-handovers in LTE (except that the concept of an NH value is not used for simplicity).

MMEs and legacy SGSNs must be expected to operate according to currently specified procedures/working assumptions. New processing and signaling can thus only be introduced in the HSS, SGSN+, MSC/VLR+ and ME+.

The following clauses give an outline of the signaling principles. Details and deeper rationale/analysis is elaborated in subsequent clauses.

5.3.2 Key handling and capability negotiation

5.3.2.1 General

An important aspect, apart from the actual key derivations done in the chaining, is to ensure that network and ME can interoperate and are aware of whether to use the UTRAN KH or not. This in turn implies that it is necessary to signal UTRAN KH capabilities between the ME(*) and network and between nodes in the network.

The term "chaining" is here used to mean that the source node derives a new set of keys from the currently used ones and pass the derived keys to the target node. The intention is to achieve backward security in a simple fashion. This is the same behaviour as used in LTE at X2 handovers when no NH value is accessible.

5.3.2.2 Initial NAS procedures

This handling works as described for Solution 2 in clause 5.2.1.2.

5.3.2.3 Key derivations and capability indication at intra-UTRAN mobility with SRNS relocation

The normal strategy for transferring ME capabilities from the source RNC to the target RNC is to include these in the source to target transparent container. So it seems natural to include the enhanced keying capability in this container. However, the current specs do not seem to guarantee that a legacy source RNC includes an IE that it does not understand to the target RNC. The situation is similar to the case of EPS security capabilities sent to a legacy SGSN and then not forwarded to an MME. Because of this it cannot be assumed that the target RNC will get the information about whether the ME is updated or not from the source RNC. Consequences of this are:

1. The ME must be the entity to supply the target RNC with information about whether it is updated or not,
2. Since the target RNC does not know if the ME is updated or not it must behave the same way towards all UEs until the target RNC is unformed by the ME whether the UE is updated or not.

Before the SRNS relocation is started the ME knows if it is connected to a legacy RNC or an updated RNC and vice versa. After the SRNS relocation is completed, the same property holds.

The following simple rules are applied:

ME: If the source RNC is updated, then the ME+ chains the CK_U/IK_U before communicating with the target RNC. Inform the target RNC about if the ME is updated by including an IE in the first uplink message to the target RNC indicating this. Deduce from the first downlink message from the target RNC if it is updated or not based on the presence of a corresponding IE.

Source RNC: If the ME is updated, then chain CK_U/IK_U before sending them to the target RNC otherwise behave as a legacy RNC and forward the keys used in the source cell unmodified.

Target RNC: Use the keys received from the source RNC to communicate with the ME. Inform the ME about if the target RNC is updated by including an IE in the first downlink message to the UE indicating this. Deduce from the first uplink message from the UE if it is updated or not based on the presence of a corresponding IE.

The only exception to these rules is if it is an SRNS relocation without UE involvement, in which case the UE and target RNC use the same CK_U/IK_U as in the source cell (the explanation of this can be found in the analysis below).

Below is a list of all combinations of updated/legacy ME/source RNC/target RNC and how each node behaves w.r.t. key derivations and transferring of the enhanced UTRAN KH capabilities at all three types of SRNS relocation: SRNS relocation without UE involvement, combined hard handover and SRNS relocation and combined cell/URA update and SRNS relocation.

The list below gives a detailed check that interworking with legacy RNCs/MEs is fully functional. References to message numbers refer to Figures 39, 42 and 43 of TS 23.060 [11].

A.1 ME is updated

A.1.1 Source RNC is updated

A.1.1.1 Target RNC is updated

Combined hard handover and SRNS relocation:

- ME knows source RNC is updated so the ME+ chains the currently used keys before contacting the target RNC.
- The source RNC knows that the ME is updated and chains the currently used keys before giving them to the target RNC.
- The ME and the target RNC use the chained keys when communicating.

- The ME informs the target about that it is capable of the enhanced UTRAN KH in the uplink RRC message 8.
- The target RNC informs the ME about that it is capable of the enhanced UTRAN KH in the downlink RRC message 8.

Combined CELL/URA update and SRNS relocation:

- ME knows source RNC is updated so the ME chains the currently used keys before contacting the target RNC (just after sending the CELL/URA update message).
- The source RNC knows that the ME is updated and chains the currently used keys before giving them to the target RNC.
- The ME and the target RNC uses the chained keys when communicating.
- The ME informs the target about that it is capable of the enhanced UTRAN KH in the UTRAN Mobility Information Confirm (uplink message 10).
- The target RNC informs the ME about that it is capable of the enhanced UTRAN KH in the Cell update confirm/URA update confirm message (downlink message 10).

SRNS relocation without ME involvement:

- In this case the ME is informed about the event from the target RNC in the RAN mobility information message (downlink message 10). This message is security protected, and hence the target RNC needs keys to protect the message. Providing the target RNC with the keys used in the source cell defeats the purpose to use any form of key separation between RNCs. This means that whatever keys are to be used by the target RNC, they should be chained. A solution to this problem is that the source RNC, before performing the SRNS relocation to the target RNC, performs an intra-SRNS relocation. The source RNC then gives the currently used keys to the target RNC. This chains the keys and only the data transmitted between the intra-SRNS relocation and the real SRNS relocation is exposed to the target RNC. An SRNS relocation without ME involvement is not time critical (as the hard handover case is).
- The ME knows that the source RNC is updated and behaves as described above. Therefore the ME will chain its keys correspondingly.
- The target RNC informs the ME about that it is capable of the enhanced UTRAN KH in the RAN Mobility Information message (downlink message 10).
- The ME informs the target about that it is capable of the enhanced UTRAN KH in the RAN Mobility Information Confirm (uplink message 10).

A.1.1.2 Target RNC is not updated

Combined hard handover and SRNS relocation:

- ME knows source RNC is updated so the ME chains the currently used keys before contacting the target RNC.
- The source RNC knows that the ME is updated and chains the currently used keys before giving them to the target RNC.
- The ME and the target RNC uses the chained keys when communicating.
- The ME informs the target RNC about that it is capable of the enhanced UTRAN KH in the uplink RRC message 8. The target RNC is not updated, so it does not understand this new IE and discards it.
- From the downlink RRC message 8, the ME deduces from the lack of the IE containing the RNC enhanced UTRAN KH, that the target RNC is a legacy RNC (otherwise the target RNC would have included such an IE).

Combined CELL/URA update and SRNS relocation:

- ME knows source RNC is updated so the ME chains the currently used keys before contacting the target RNC (just after sending the CELL/URA update message).

- The source RNC knows that the ME is updated and chains the currently used keys before giving them to the target RNC.
- The ME and the target RNC uses the chained keys when communicating.
- The ME informs the target about that it is capable of the enhanced UTRAN KH in the UTRAN Mobility Information Confirm (uplink message 10).
- From the Cell update confirm/URA update confirm message (downlink message 10), the ME deduces from the lack of the IE containing the RNC enhanced UTRAN KH, that the target RNC is a legacy RNC (otherwise the target RNC would have included such an IE).

SRNS relocation without ME involvement:

- The key derivations are done exactly in the same way as if the target RNC was updated.
- From the RAN Mobility Information message (downlink message 10), the ME deduces from the lack of the IE containing the RNC enhanced UTRAN KH, that the target RNC is a legacy RNC (otherwise the target RNC would have included such an IE).
- The ME informs the target about that it is capable of the enhanced UTRAN KH in the RAN Mobility Information Confirm (uplink message 10).

A.1.2 Source RNC is not updated

A.1.2.1 Target RNC is updated

Combined hard handover and SRNS relocation:

- The source RNC behaves like any legacy RNC and just forwards the CK/IK used for the air interface protection to the target RNC as they are.
- ME knows source RNC is legacy so the ME uses the same CK/IK with the target RNC as with the source RNC.
- The ME and the target RNC uses the same keys as was used in the source RNC when communicating.
- The ME informs the target about that it is capable of the enhanced UTRAN KH in the uplink RRC message 8.
- The target RNC informs the ME about that it is capable of the enhanced UTRAN KH in the downlink RRC message 8.

Combined CELL/URA update and SRNS relocation:

- The key handling is exactly as for the combined hard handover and SRNS relocation case above.
- The ME informs the target about that it is capable of the enhanced UTRAN KH in the UTRAN Mobility Information Confirm (uplink message 10).
- The target RNC informs the ME about that it is capable of the enhanced UTRAN KH in the Cell update confirm/URA update confirm message (downlink message 10).

SRNS relocation without ME involvement:

- The key handling is exactly as for the combined hard handover and SRNS relocation case above.
- The target RNC informs the ME about that it is capable of the enhanced UTRAN KH in the RAN Mobility Information message (downlink message 10).
- The ME informs the target about that it is capable of the enhanced UTRAN KH in the RAN Mobility Information Confirm (uplink message 10).

A.1.2.2 Target RNC is not updated

Combined hard handover and SRNS relocation:

- The key handling is exactly the same as in the case the target RNC was updated above (see clause A.1.2.1).

- The way the ME and target RNC learns about if their peer is updated or legacy is exactly as in the case where the source RNC is updated and the target RNC is not updated above (see clause A.1.1.2).

Combined CELL/URA update and SRNS relocation:

- The key handling is exactly as for the combined hard handover and SRNS relocation case above.

- The way the ME and target RNC learns about if their peer is updated or legacy is exactly as in the case where the source RNC is updated and the target RNC is not updated above (see clause A.1.1.2).

SRNS relocation without ME involvement:

- The key handling is exactly as for the combined hard handover and SRNS relocation case above.

- The way the ME and target RNC learns about if their peer is updated or legacy is exactly as in the case where the source RNC is updated and the target RNC is not updated above (see clause A.1.1.2).

A.2 ME is not updated

A.2.1 Source RNC is updated

A.2.1.1 Target RNC is updated

Combined hard handover and SRNS relocation:

- ME is legacy and hence behaves as if the enhanced key hierarchy did not exist.

- Since the source RNC is updated and knows that the ME is legacy, the source RNC behaves like any legacy RNC and just forwards the CK/IK used for the air interface protection to the target RNC as they are.

- The ME and the target RNC uses the same keys as was used in the source RNC when communicating.

- From the uplink RRC message 8, the updated target RNC deduces that the ME is a legacy ME since the ME did not include an IE about its enhanced UTRAN KH capabilities.

- The target RNC informs the ME about that it is capable of the enhanced UTRAN KH in the downlink RRC message 8. Since the ME is legacy, it will discard this unknown IE.

Combined CELL/URA update and SRNS relocation:

- The key handling is exactly as described in the combined hard handover and SRNS relocation case above.

- From the UTRAN Mobility Information Confirm (uplink message 10), the updated target RNC deduces that the ME is a legacy ME since the ME did not include an IE about its enhanced UTRAN KH capabilities.

- The target RNC informs the ME about that it is capable of the enhanced UTRAN KH in the Cell update confirm/URA update confirm message (downlink message 10). Since the ME is legacy, it will discard this unknown IE.

SRNS relocation without ME involvement:

- The key handling is exactly as described in the combined hard handover and SRNS relocation case above.

- The target RNC informs the ME about that it is capable of the enhanced UTRAN KH in the RAN Mobility Information message (downlink message 10). Since the ME is legacy, it will discard this unknown IE.

- From the RAN Mobility Information Confirm (uplink message 10), the updated target RNC deduces that the ME is a legacy ME since the ME did not include an IE about its enhanced UTRAN KH capabilities.

A.2.1.2 Target RNC is not updated

Combined hard handover and SRNS relocation:

- The key handling is exactly the same as in the case combined hard handover and SRNS relocation when the target RNC is updated.
- Neither the target RNC nor the ME is updated, so nothing regarding the enhanced UTRAN KH is signalled.

Combined CELL/URA update and SRNS relocation:

- The key handling is exactly as described in the combined hard handover and SRNS relocation case above.
- Neither the target RNC nor the ME is updated, so nothing regarding the enhanced UTRAN KH is signalled.

SRNS relocation without ME involvement:

- The key handling is exactly as described in the combined hard handover and SRNS relocation case above.
- Neither the target RNC nor the ME is updated, so nothing regarding the enhanced UTRAN KH is signalled.

A.2.2 Source RNC is not updated

A.2.2.1 Target RNC is updated

- Key handling is performed exactly as in the current (legacy) UTRAN specifications for all cases.
- The target RNC can deduce from the lack of the enhanced UTRAN KH IE in the RAN Mobility Information Confirm (uplink message 10)/UTRAN Mobility Information Confirm (uplink message 10)/uplink RRC message 8 that the ME is not updated. The ME is not updated and discards any IE containing the corresponding information from the updated target RNC.

A.2.2.2 Target RNC is not updated

- Key handling is performed exactly as in the current (legacy) UTRAN specifications for all cases.
- None of the nodes are aware of the enhanced UTRAN KH and behaves exactly as legacy UTRAN nodes.

5.3.2.4 Capability indication at IRAT mobility

This is handled as described for Solution 2 in clause 5.2.3.

5.3.3 Summary of changes to messages

5.3.3.1 General

Solution 3 deals with horizontal key derivations and can be seen as an add-on to Solution 2, which deals with vertical key derivations. The following sub-clauses list the changes to existing messages that are needed to support the Solution 3 in addition to the ones needed to support Solution 2.

Editor's note: It must be checked if other messages are affected in case of IRAT mobility.

5.3.3.2 Changes to TS 25.331 RRC

The following messages or IEs in TS 25.331 [10] that require a change to support solution 3.

Physical Channel Reconfiguration Complete

A ME+ includes its capability to perform UTRAN key management enhancements in the message at combined hard handover and SRNS relocation.

RAN Mobility Information

A target RNC+ includes its capability to perform UTRAN key management enhancements in the message at SRNS relocation without ME involvement.

RAN Mobility Information Confirm

A ME+ includes its capability to perform UTRAN key management enhancements in the message at combined CELL/URA update and SRNS relocation.

Cell Update Confirm/URA Update Confirm

An RNC+ includes its capability to perform UTRAN key management enhancements in the message at combined CELL/URA update and SRNS relocation.

5.3.3.3 Changes to TS 25.413 RANAP

The following messages or IEs in TS 25.413 [9] that require a change to support solution 3.

Target RNC to Source RNC Transparent Container

A target RNC+ includes its capability to perform UTRAN key management enhancements in the container whish is transparently sent to the source RNC(+). A source RNC+ includes the target RNCs capability to perform UTRAN key management enhancements in the Physical Channel Reconfiguration as normal.

5.4 Proposed solution 4

5.4.1 General

This solution is based on key hierarchy solution 2. It can be seen as an add-on to Solution 2 in the sense that Solution 4 provides forward security based key derivations at SRNS relocations similar to X2/S1 handovers in E-UTRAN. Compared to solution 1, this solution deletes algorithm ID binding with key derivation, and thus the complexity is reduced greatly. So we can call this simplified forward security based solution.

Figure 5.4.1-1 shows the dependencies between the keys at initial setup (i.e., when the ME goes to Active mode), and at combined hard handover and SRNS relocation as well as combined cell/URA updated and SRNS relocation.

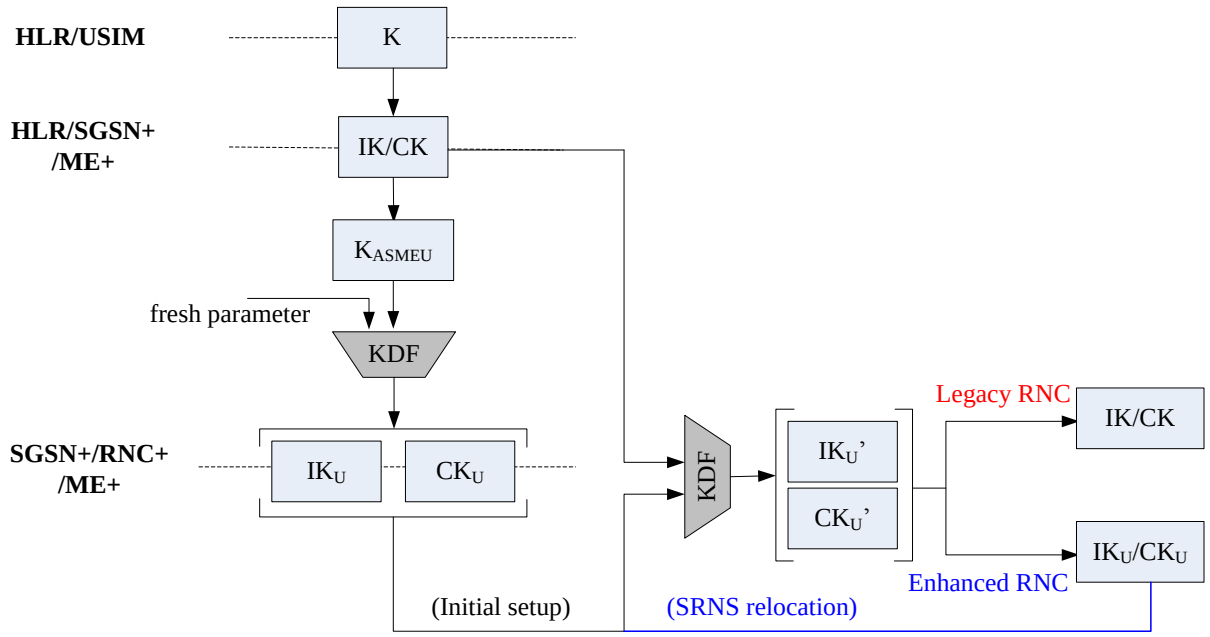

Figure 5.4.1-1: Key distribution and key derivation scheme for UTRAN Key hierarchy

(IK_U, CK_U) and (IK_U', CK_U') shall be transmitted to SRNC+ at the intial connetion setup. The first pair (IK_U, CK_U) is used to protect the communication under the current SRNC+. The second pair (IK_U', CK_U') is used as the keys after the next SRNS relocation performs. When SRNC relocation occurs, (IK_U', CK_U') are transmitted to the target RNC(*). If target RNC is not updated, it will regard IK_U'/ CK_U' as legacy IK/CK. And if target RNC is updated, it will regard IK_U'/ CK_U' as IKu/CK_U.NOTE: In this solution, because the integrity key and ciphering key in CNN+ are always the same

with the ones in RNC+, it is not necessary to differentiate them as solution 3. IK_U is corresponding to IK_S in solution 2, and CK_U is corresponding to CK_S in solution 2.

5.4.2 Forward security based SRNS relocation with UE involvement

5.4.2.1 Key chaining

The general principle of enhanced key handling at SRNC relocation is depicted in Figure 5.4.2.1-1.

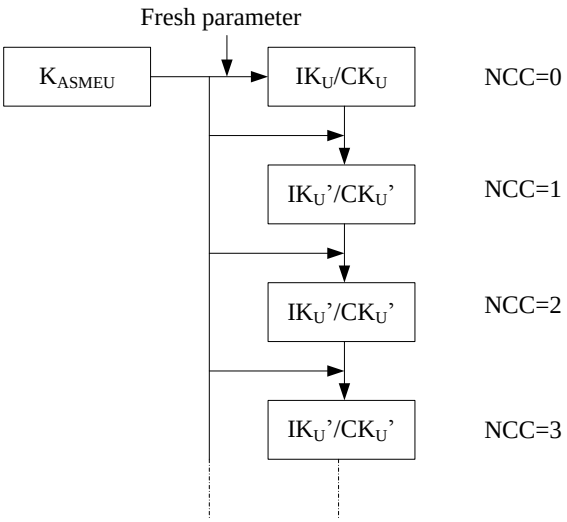

Figure 5.4.2.1-1A simplified model for the SRNC relocation key chaining

The following is an outline of the key handling model to clarify the intended structure of the key derivations during SRNS relocation with UE involvement.

Whenever an initial security context needs to be established between ME+ and SRNC+, SGSN+ and the ME+ shall derive IK_U/CK_U and IK_U'/CK_U', which are both derived from the IK/CK. A Next-hop Chaining Counter (NCC) is associated with each IK_U'/CK_U'. At initial setup, the IK_U/CK_U is derived directly from IK/CK, and is then considered to be associated with a virtual IK_U'/CK_U' parameter with NCC value equal to zero. At initial setup, the derived IK_U'/CK_U' value is associated with the NCC value one. IK_U/CK_U and { IK_U', CK_U', NCC} are transmitted to SRNC+ during SMC procedure at initial attachment.

NOTE: Since the SGSN+ sends the { IK_U', CK_U', NCC} value to SRNC+ at the initial attachment, the IK_U'/CK_U' value associated with the NCC value one can be used in the next SRNC relocation or the next intra-SRNC relocation.

The ME+ and the SRNC+ use the IK_U/CK_U derived from IK/CK to secure the communication between each other. On SRNC relocation, IK_U'/CK_U' are derived from the IK/CK and the old IK_U'/CK_U'.

As IK_U'/CK_U' are only computable by the ME+ and the SGSN+, it is arranged so that IK_U'/CK_U' are provided to SRNC from the SGSN+ in such a way that forward security can be achieved.

5.4.2.2 Network handling

5.4.2.2.1 Enhanced SRNS relocation procedure

During SRNS relocation the source RNC+ shall forward the IK_U'/CK_U' to the target RNC(*). If the target RNC+ supports UTRAN KH, it shall use the received IK_U'/CK_U' directly as IK_U/CK_U to be used with the ME. The source RNC+ shall send NCC to the ME.

If the target RNC is a legacy one, it shall use the received keys directly as IK/CK to be used with the UE, just the same as the operation of TS 33.102 [3].

When the target RNC+ has completed the SRNC relocation signaling with the ME+, it shall send a Enhanced Relocation Complete Request message to the SGSN+. Upon reception of the Enhanced Relocation Complete Request, the SGSN+ shall increase its locally kept NCC value by one and compute a new fresh IK_U'/CK_U' by using the IK/CK and its locally kept IK_U'/CK_U' value as input to the function. The SGSN+ shall then send the newly computed { IK_U', CK_U', NCC} triple to the target RNC+ in the Enhanced Relocation Complete Response message. The target RNC+ shall store the received { IK_U', CK_U', NCC} triple for further SRNC relocation and remove other existing unused stored { IK_U', CK_U', NCC} triples if any.

NOTE: The newly computed { IK_U', CK_U', NCC} can only be used to provide keying material for the next SRNC relocation procedure. Thus, for SRNC relocation key separation happens only after two hops because the source RNC+ knows the target RNC+ keys. The target RNC+ can immediately initiate an intra-cell handover to take the new IK_U'/CK_U' into use once the new IK_U'/CK_U' has arrived in the Enhanced Relocation Complete Response.

5.4.2.2.2 SRNS relocation procedure

Considering backward compatibility, the source RNC+ shall send unused IK_U'/CK_U' (if there are unused IK_U'/CK_U') or its currently used IK_U/CK_U (if there are no unused IK_U'/CK_U') in the Source RNC to Target RNC Transparent Container to the target RNC just the same behaviour as in enhanced SRNS relocation procedure.

Upon reception of the Relocation Required message the source SGSN+ shall increase its locally kept NCC value by one and compute a fresh IK_U'/CK_U' from its stored IK/CK and old IK_U/CK_U. The source SGSN+ shall store that fresh keys and send them in legacy IK/CK IE and the corresponding NCC, together with K_{ASMEU} and COUNT to the target SGSN+ in the Forward Relocation Request message.

If the target SGSN is an enhanced one, it shall store IK_U'/CK_U', corresponding NCC, K_{ASMEU} and COUNT received from the source SGSN+. If the target SGSN is a legacy one, it should regard the received IK_U'/CK_U' as legacy IK/CK.

The target SGSN+ shall then send the received IK_U'/CK_U' to the target RNC+ within the Relocation Request message.

Upon receipt of the Relocation Request from the target SGSN(*), if the target RNC is an enhanced one, it shall regard the received IK_U'/CK_U' as IK_U/CK_U, and save the keys. The target RNC+ shall discard the received keys in Source RNC to Target RNC Transparent Container and remove any existing unused stored IK_U'/CK_U'. If the target RNC is a legacy one, it can only recognize the received keys in Source RNC to Target RNC Transparent Container. It shall regard the keys as legacy IK/CK, and save the keys.

The source SGSN+ shall forward NCC and the target RNC UTRAN KH capability to the source RNC+, which is included in the Relocation Command message.

Upon receipt of the Relocation Command from the source SGSN+, the source RNC+ knows if the target RNC(*) supports UTRAN KH. If the target RNC supports UTRAN KH, the source RNC+ shall distribute the NCC value sent by source SGSN+ to ME+. If the target RNC does not support UTRAN KH, the source RNC+ shall send the NCC value to ME+ which is corresponding to the keys sent to target RNC(*) in the transperant container.

NOTE: The source SGSN+ may be the same as the target SGSN+ in the description in this subclause. If so the single SGSN+ performs the roles of both the source and target SGSN+, i.e. the SGSN+ calculates and stores the fresh IK_U'/CK_U' and corresponding NCC and sends them to the target RNC+.

NOTE: One-hop forward security can be ensured in this SRNS relocation. Considering its complexity it could be seen as an optimization of SRNS relocation. If this enhancement is not used, the operations of source SGSN+ and target SGSN(*) are the same with the ones in solution 2 and solution 3.

5.4.2.3 ME handling

If the NCC value the ME+ received in the Physical Channel Reconfiguration message or UTRAN Mobility Information message from target RNC+ is equal to the NCC value stored in the ME+, the ME+ shall directly use the IK_U'/CK_U' as IK_U/CK_U.

If the ME+ received an NCC value that was different from the NCC associated with the currently active IK_U'/CK_U', the ME+ shall first synchronize the locally kept IK_U'/CK_U' parameter iteratively, and increasing the NCC value until it matches the NCC value received from the network. When the NCC values match, the ME+ shall use the IK_U'/CK_U' as IK_U/CK_U to protect the communication between the ME+ and the target RNC+.

5.4.2.4 Intra-SRNS relocation

When the SRNC+ decides to perform an intra-SRNS relocation it shall use the IK_U'/CK_U' as the IK_U/CK_U. The SRNC shall send the NCC corresponding to IK_U'/CK_U' to ME in Physical Channel Reconfiguration message or UTRAN Mobility Information message.

5.4.3 SRNS relocation without UE involvement

During SRNS relocation without UE involvement, a legacy SRNC relocation procedure is performed first, in which source RNC+ should send the keys currently used directly to target RNC(*), i.e. the keys during this SRNC relocation procedure are not updated. While the operation of SGSN+ is the same as the one's in SRNS relocation with UE involvement, i.e., SGSN+ shall also derive a new pair of IK_U'/CK_U'. The benefit is that SGSN+ does not need to know whether it is a SRNS relocation without UE involvement or not.

After the SRNC relocation is finished, if target RNC is an updated one, an intra-SRNC relocation is performed. During this intra-SRNC relocation procedure, new IK_U and CK_U are activated just the same as in the SRNS relocation with UE involvement, except that the target RNC+ and the source RNC+ are the same one.

5.4.4 Interworking with GERAN

When interworking with GERAN, UTRAN KH should be compatible with GERAN system. Not any changes shall be introduced by UTRAN KH.

When ME+ moves from GERAN to enhanced UTRAN(handover or Idle mobility) with SGSN changes, because source SGSN may not transfer UE UTRAN KH capability to target SGSN+, all the operation is just the same as TS 33.102 defined. After ME+ connects to the enhanced UTRAN, ME+ and the network have known each other's capability, the network can trigger an AKA and SMC procedure (or just a SMC procedure) to establish the enhanced security context. Whether AKA is run after IRAT mobility is independent of whether forward security is used or not.

When ME+ moves from GERAN to enhanced UTRAN (handover or Idle mobility) without SGSN change, if SGSN is an enhanced one, it can establish an enhanced security context directly from CK/IK which is derived from GSM cipher key Kc.

When ME+ moves from enhanced UTRAN to GERAN (handover or Idle mobility), all the operations are just the same as described in TS 33.102.

5.4.5 Interworking with E-UTRAN

When interworking with E-UTRAN, UTRAN KH should be compatible with E-UTRAN system. Not any changes shall be introduced by UTRAN KH.

When ME+ moves from E-UTRAN to enhanced UTRAN (handover or Idle mobility), because source MME may not transfer UE UTRAN KH capability to target SGSN+, all the operation is just the same as TS 33.401 defined. After ME+ connects to the enhanced UTRAN, ME+ and the network have known each other's capability, the network can trigger an AKA and SMC procedure (or just a SMC procedure) to establish the enhanced security. Whether AKA is run after IRAT mobility is independent of whether forward security is used or not.

When ME+ moves from enhanced UTRAN to E-UTRAN (handover or Idle mobility), all the operations are just the same as described in TS 33.401.

5.4.5 Summary of changes to messages

5.4.5.1 General

The following sub-clauses list the changes to existing messages that are needed to support the solution above.

5.4.5.2 Changes to TS 24.008

The following messages or IEs in TS 24.008 [5] require a change to support solution above.

Attach request

An indication that a ME+ supports enhanced security context functionality.

The COUNT value when the ME+ is using an enhanced security context.

RAU Request

An indication that a ME+ supports enhanced security context functionality.

The COUNT value when the ME+ is using an enhanced security context.

Service Request

The COUNT value when the ME+ is using an enhanced security context.

RAU Accept

An indication that the target SGSN+ after an intra-UTRAN handover or a handover to UTRAN supports the enhanced security context.

5.4.5.3 Changes to TS 29.060

The following messages or IEs in TS 29.060 [7] require a change to support solution above.

SGSN Context Response message

An SGSN+ includes K_{ASMEU} if the security context being used is an enhanced one.

An SGSN+ includes COUNT if the security context being used is an enhanced one.

Forward Relocation Request

An SGSN+ includes IK_U'/CK_U'and the corresponding NCC and K_{ASMEU} if the security context being used is an enhanced one. IK_U'/CK_U' are sent in legacy IK/CK IE.

5.4.5.4 Changes to TS 25.413

The following messages or IEs in TS 25.413 [9] require a change to support solution above.

SECURITY MODE COMMAND

An indication whether or not the SGSN(*) supports the enhanced security.

UE UTRAN KH capability received in the first L3 message sent by ME+.

{IK_U', CK_U', NCC} used when the next SRNS relocation.

Relocation Request

An SGSN+ includes IK_U'/CK_U' to target RNC+ if the security context being used is an enhanced one.

Source RNC to Target RNC Transparent Container IE

An indication whether or not the ME supports the enhanced security.

Source RNC+ includes IK_U'/CK_U' to target RNC+ if the security context being used is an enhanced one.

Target RNC to Source RNC Transparent Container IE

An indication to ME via source RNC+ whether or not the target RNC supports the enhanced security.

Relocation Command

A NCC used to synchronize key derivation between the target network and the ME+ during SRNS relocation.

5.4.5.5 Changes to TS 25.331

The following messages or IEs in TS 25.331 [10] require a change to support solution above.

SECURITY MODE COMMAND

An indication whether or not the network (SGSN(*) and SRNC(*)) supports the enhanced security.

UE UTRAN KH capability received in the first L3 message sent by ME+.{IK_U', CK_U', NCC} used when the next SRNS relocation.

Physical Channel Reconfiguration/UTRAN Mobility Information/Cell Update Confirm/URA Update Confirm

An indication whether or not the target network (SGSN+ and SRNC+) supports the enhanced security.

A NCC used to synchronization key derivation between the target network and the ME+ during SRNS relocation.

Physical Channel Reconfiguration Complete/UTRAN Mobility Information Confirm

An indication whether or not the ME(*) supports the enhanced security.

6 Comparison of proposed Solutions

6.1 Signalling aspects

6.1.1 Initial authentication / AV fetch

For all the four solutions, before running an AKA, an SGSN+ will be aware of whether the UE supports the enhanced security context or not.

For solution 1 and solution 4, there is not any change during AKA procedure. After AKA is successfully finished, if both UE and SGSN support UTRAN KH, SGSN+ shall notify UE to create an enhanced security context in SMC message.

For solution 2 and solution 3, if both SGSN and UE support the enhanced security context when the SGSN sends the Authentication and Ciphering Request message carrying the AKA challenge it shall include an indication to the UE that the UE shall create an enhanced security context from this AKA run.

6.1.2 Idle to Active transition

During Idle to Active transition, for solution 1 and 4, if both UE and SGSN support UKH, SGSN+ shall notify UE to create an enhanced security context in SMC message.

The following creating an enhanced security context procedure are the same for solutions 2, 3 and 4, except that for solution 4 SGSN+ should also generate IK_U'/CK_U' and corresponding NCC. The triple {IK_U', CK_U', NCC} shall be sent from SGSN+ to SRNC+ in SMC message. But this is not necessarily needed. If it is not transmitted to SRNC+ in SMC message, there is no forward security guarantee in the first SRNS relocation.

6.1.3 SRNS relocation and intra-UTRAN key-refresh

For solution 2, there is no key update during SRNS relocation. All the operations are the same as TS 33.102 defined.

For solution 3, in order to achieve backward security, the source RNC+ shall chain the keys and pass the chained keys to the target node in legacy IK/CK IE for combined hard handover and SRNS relocation, and combined CELL/URA update and SRNS relocation. As for SRNS relocation without UE involvement, the source RNC+, before performing

the SRNS relocation to the target RNC(*), performs an intra-SRNS relocation. The source RNC+ then gives the currently used keys to the target RNC(*).

For solution 4, after a successful enhanced SRNS relocation, SGSN+ shall increase its locally kept NCC value by one and compute a new fresh IK_U'/CK_U' by using the IK/CK and its locally kept IK_U'/CK_U' value as input. The SGSN+ shall then send the newly computed triple {IK_U', CK_U', NCC} to the target RNC+ in the Relocation Complete Response message. For the next SRNS relocation, the source RNC+ (i.e., the target RNC+ at last SRNS relocation) shall send the received IK_U'/CK_U'in legacy IK/CK IE and corresponding NCC to the target RNC+. The target RNC+ shall regard the received IK_U'/CK_U' as IK_U/CK_U.

For solution 4, during SRNS relocation with CNN+ involved, the source SGSN+ shall increase its locally kept NCC value by one and compute a fresh IK_U'/CK_U' from its stored IK/CK and old IK_U/CK_U. The source SGSN+ shall send the fresh IK_U'/CK_U' and corresponding NCC to the target RNC+ via the target SGSN+. The target RNC+ shall regard the received IK_U'/CK_U' as IK_U/CK_U.

Forward security and backward security can be ensured by the above way for solution 4.

During Intra-UTRAN handovers, the operations are the same for solution 2, 3 and 4, except that for solution 4 the source SGSN+ should also send the triple {IK_U', CK_U', NCC} to the target SGSN(*).

As described in clause 6.3 of this document, backwards compatibility can be achieved by all proposed solutions. In particular, there is no need to update macro RNCs if only backward compatibility is to be achieved. However, if the full benefits of solutions 1 and 4 are to be achieved enhancements of macro RNCs may be required. A macro RNC that is not enhanced and is connected to a collapsed RNC/NodeB will achieve the same level of security as if UTRAN KH is not used.

Even without any UTRAN KH, a macro RNC that allows SRNS relocation from a collapsed RNC/NodeB is vulnerable if an attacker has broken into the collapsed RNC/NodeB and captured the CK/IK there. There are several options to ensure that normal UTRAN security is re-established in this case. For example, the network can wait until the next Idle to Active transition the UE performs and run a new AKA then. However, this would mean giving up on the full benefits of forward security (as in solutions 1 and 4). (All solutions achieve the same effect without an AKA). If the SRNS relocation was done in Active mode and the network do not wish to wait until the next Idle to Active transition, an AKA followed by a key change on the fly can be run. However, this may lead to an undesirable load increase if the nu mber of such AKA runs becomes too large. If horizontal key derivations as used by Solutions 1, 3 and 4 are used, this is achieved even without an AKA and key change on-the-fly. Running AKA and possibly key change on-the-fly of course has a cost and an operator may chose to implement UTRAN KH also in macro RNCs if seen necessary. Since all solutions provide backwards compatibility, potential upgrades of macro RNCs could be done in selected problem areas.

6.2 Compatibility aspects

All the four solutions should consider backward compatibility.

At idle mobility, for all the 4 solutions an old SGSN+ that holds an enhanced security context shall calculate CK_L and IK_L and include these in the existing IEs that are used to carry CK and IK currently. A legacy SGSN receiving the above message will use CK_L and IK_L as a legacy CK and IK.

At intra-UTRAN handovers, for solution 2 and 3 the SGSN+ includes CK_S and IK_S in the legacy CK and IK IEs to the target SGSN. A legacy SGSN receiving such a message would treat the UE as though it had a legacy context with CK_S and IK_S as keys. An SGSN+ continues to use the enhanced security context. While for solution 1 and 4, the source SGSN+ always send CK_L and IK_L to the target SGSN(*) just the same as at idle mobility.

During SRNS relocation, for solution 1 two sets of keys are transmitted to the target RNC: the one is the mapping legacy keys CK_L /IK_L, the other is the enhanced keys K_{RNC}*. If the target RNC is a legacy one, it will only regard the mapping legacy keys CK_L /IK_L as CK/IK; if the target RNC is an enhance one, it will derive the enhanced IKU/CKU based on the received K_{RNC}*.

During SRNS relocation, for solution 2, 3 and 4 the source RNC+ shall send the currently used CK_S and IK_S (for solution 2) or the chained CK_U and IK_U (for solution 3) or the stored CK_U'and IK_U'(for solution 4) in the legacy CK and IK IE to the target RNC(*). If the target RNC is a legacy one, it shall regard the received keys as CK and IK; if the target RNC is an enhanced one, it shall regard the received keys as CK_S and IK_S (for solution 2) or CK_U and IK_U (for solution 3 and 4).

During SRNS relocation and SGSN relocation, UE UTRAN KH capability should be always transferred by the source RNC+/SGSN+ to the target RNC(*)/SGSN(*).

6.3 Security

Editor's note, should consider which security objectives that are obtained / not obtained in the different options.

6.3.1 Threats

6.3.1.1 Handover from a collapsed RNC and NodeB

The ME is connected to a collapsed RNC and NodeB. The ME is then handed over to a regular NodeB and keeps the RNC or an SRNS relocation happens at the same time

Threats 1: If the RNC stays the same, then an attacker breaking into the target NodeB gains nothing by the attack and an attacker breaking in to the source collapsed RNC/NodeB will still have access to all data no matter what is done.

Analysis: The only thing that helps is an SRNS relocation in combination with a forward security based key re-fresh.

Threats 2: Further, if there is an SRNS relocation, then the attacker could break in to the target RNC, but this is assumed to be located in a safe place according to the normal UTRAN trust model. An attacker who has broken into the source collapsed RNC/NodeB would have access to the keys used in both the source and the target RNC.

Analysis: For solution 3, because the keys used by the target RNC(*) is derived by the source RNC+, no matter how many times SRNS relocations perform, the attacker could always have access to the keys used by the source and the target RNC(*).

For solution 1 and 4, when UE performs general SRNS relocation with SGSN+ involved during preparation phase, because the keys materials used by the target RNC(*) is derived by SGSN+, even if the source RNC is broke into by the attacker, it is impossible to know the updated keys to this attacker. In this case, one-hop forward security can be ensured.

For solution 1and 4, when UE performs enhanced SRNS relocation without SGSN+ involved during preparation phase, because the keys materials used by the target RNC(*) is sent by the source RNC+, the attacker would have access to the keys used in both the source and the target RNC. But after two-hop SRNS relocations, or after one more intra-SRNS relocation, this risk could be eliminated. In this case, two-hop forward security can be ensured.

Threats 3: If there is an SGSN relocation, and the target SGSN is an legacy normal one, because the keys used by the target network have been exposed to the attacker who has broken into the source collapsed RNC, the attacker would have access to the keys used in the target RNC. Thus the security threats brought by present deployments of UTRAN with RNC functionality moved to HSPA NodeBs are introduced to the normal UTRAN network.

Analysis: The UTRAN key hierarchy introduced in this TR can solve this problem. All the four solutions provide a pair of legacy keys by the source SGSN+, which will be sent to the target SGSN during SGSN relocation. Because the legacy keys are not transmitted to the collapsed RNC, there is no possibility that the attacker could have access to the keys used by the target normal UMTS network.

Threats 4: The fourth case is that the ME is connected to a collapsed RNC and NodeB. The ME is then handed over to another collapsed RNC/NodeB. This implies that an SRNS relocation happens.

Analysis: In this situation, an attacker could have broken into either the source or the target collapsed RNC/NodeB and would then have access to the necessary keys to get hold of the user traffic both before and after the handover. No counter measure is completely effective here. Frequent/regular re-authentication and/or key refresh at Idle to Active mode transitions helps, but it does not help while the ME is active, e.g, during a CS session (note that most operators have a policy of authenticating one in n calls, where n is small, anyhow).

6.3.1.2 Handover from a separated RNC and NodeB

The ME is connected to a NodeB and the RNC is located in a safe location (e.g, in the core network) according to the regular UTRAN threat model. The ME is then handed over to a regular NodeB and keeps the RNC or an SRNS relocation happens at the same time.

By the regular UTRAN threat model, both the source and the target RNC are located in a safe place, so an attacker is assumed not to be able to break in there. Hence no additional security is required for this situation.

Threats 5: The other case is that the ME is connected to a NodeB and the RNC is located in a safe location according to the regular UTRAN threat model. The ME is then handed over to a collapsed RNC/NodeB. SRNS relocation happens by definition here.

Analysis: In this case, the attacker's only option is to break into the target collapsed RNC/NodeB. By doing so the attacker gets access to the keys necessary to get hold of the user plane data sent both before and after the handover.

For solution 1 and solution 3, because the keys used by the target RNC(*) is different from the one the source RNC+ used, even if the attacker breaks into the target RNC(*), it is impossible to know the keys used by the source RNC+. Thus one-hop backward security can be ensured.

For solution 4, when UE performs general SRNS relocation with SGSN+ involved during preparation phase, because the keys materials used by the target RNC(*) is different from the one the source RNC+ used, even if the target RNC is broke into by the attacker, it is impossible to know the keys used by the source RNC+. Thus one-hop backward security can be ensured.

For solution 4, when UE performs enhanced SRNS relocation after a general SRNS relocation with SGSN+ involved during preparation phase, because the source RNC+ has no updated keys, it can only sent the keys currently used to the target RNC(*). So the attacker would have access to the keys used in both the source and the target RNC.

6.3.2 Forward security analysis

6.3.2.1 Desired security properties

The following 4 desired security properties are proposed in TR 33.859:

Property 1: It shall be possible separate the CN and RAN level key and in particular it should be possible to provide fresh RAN keys at every Idle to Active transition.

Property 2: It shall be possible to update keys at intra-UTRAN handovers (e.g. SRNC mobility).
Rationale: Improved "backward" security in UTRAN.

Property 3: It shall be possible to make the key derivations depend on the algorithm identifiers.

Property 4: Any possible lapse in security in one access technology shall not compromise security of other accesses.

6.3.2.2 Analysis

The following table lists the comparison of the 3 proposed solutions in TR 33.859.

Table 1: Architecture Comparison

	Solution 1	Solution 2	Solution 3
Property 1	X	X	X
Property 2	X		X
Property 3	X		
Property 4	X	X	X
Forward security	X UE involved : 2-hop ; UE not involved:1-hop		
Backward security	X UE involved : 1-hop ; UE not involved:2-hop		X 1-hop
Complexity	high	low	middle

From the above table, property 2 (including forward security) and property 3 are the main important differences among the 3 solutions.

6.3.2.2.1 Algorithm ID binding

For property 3, there is some benefit to bind key derivation with algorithm identifiers. But it is not the critical one. Only when IK_U/CK_U are derived by the target RNC, this property can be satisfied. But because legacy RNC must be taken into account, when source RNC transmits the keys to target RNC during SRNC relocation preparation phase, it may not know whether target RNC supports the enhanced security or not. If target RNC supports the enhanced security, the enhanced keys CK_U/IK_U should be derived by the target RNC. Because only in this way IK_U/CK_U derivation can be bound with algorithm ID. While if target RNC does not support the enhanced security, it can only regard the received keys as legacy IK/CK. So if do like this, two set of keys must be sent to target RNC, the one is the enhanced keys which is used to derive IK_U/CK_U, the other is the legacy keys IK/CK. This operation obviously adds complexity.

Further more, during the SRNC relocation without ME involvement when ME receives the first DL message from target RNC, because there are two set of keys in the target RNC, ME can't know which key the target RNC uses to protect this message. So some special operation is needed. For example, some intra-SRNC relocation must be performed. This operation also adds complexity.

If we do not introduce the property 3, key update can be done by the source RNC. The source RNC only needs to send the updated keys to the target RNC, no matter the target RNC supports UTRAN KH or not. If the target RNC supports UTRAN KH, it can regard the received keys as IK_U/CK_U. While if the target RNC doesn't support UTRAN KH, it shall regard the received keys as legacy IK/CK. In either case, the operation is just the same to the target RNC. The complexity is greatly reduced. So we think we hadd better not introduce this property 3 considering complexity.

6.3.2.2.2 Key update and forward security

Present deployments of UTRAN with part of the RNC functionality, including user plane and signalling protection, moved to HSPA NodeBs present the same threat environment as encountered by E-UTRAN eNBs. In order to resist the security compromise resulting in one eNB controlled by an attacker, the solution of key update ensuring forward security (Solution 1) is proposed in E-UTRAN.

There have been a lot of analyses of why forward security should be introduced in E-UTRAN. In short, if an attacker has full control of the initial serving NodeB, all the NodeB keys are available to the attacker, as well as all the AS traffic passing through it is visible to the attacker. During SRNC relocation if the keys are directly derived by the source NodeB (source RNC), the attacker will know the keys used by the target NodeB (target RNC). Thus the attacker will always steal the keys from one handover to the next handover. There is no security guarantee if forward security is not used, which will lead to huge security threaten. All in all, forward security is necessary and essential for UTRAN KH.

An idea that ME can go Idle mode and then return to Active mode in order to get forward security is proposed. But the Idle ⇔ Active transition is not controlled by network. That is to mean, if ME has a long call or communicates with network during a handover, there is no opportunity to go to idle mode. The attacker would have the possibility to steal the keys used by UE. Anyway, it is uncontrolled by network for Idle ⇔ Active transition, so it is not appropriate to ensure forward security. Furthermore, forward security should be realized during handover, not by the Idle ⇔ Active transition.

Compared to the solution of key chaining, the solution ensuring forward security based on solution 1 in TR 33.859 is much more complicated. While complexity is an important factor for the implement of UTRAN KH, if there is a simpler way to realize forward security and not too much overhead is introduced, that could be a good selection.

6.4 Messages comparisons

Based on the analysis above, a comparison table is listed to show the changes of messages for last 3 solutions as below.

Editor's note: It is expected that the table below will be updated.

Table 6.4.1 Comparison table of changes to messages

Specifications	Messages	Solution 2	Solution 3	Solution 4
TS 24.008	**Authentication and ciphering request**	An indication to the UE that it shall use an enhanced security context.	Same with solution 2	
	Attach request	An indication that a UE+ supports enhanced security context functionality. The COUNT value when the UE+ is using an enhanced security context.	Same with solution 2	Same with solution 2
	RAU Request	An indication that a UE+ supports enhanced security context functionality. The COUNT value when the UE+ is using an enhanced security context.	Same with solution 2	Same with solution 2
	Service Request	The COUNT value when the UE+ is using an enhanced security context.	Same with solution 2	Same with solution 2
	RAU Accept	An indication that the target SGSN+ after an intra-UTRAN handover or a handover to UTRAN supports the enhanced security context.	Same with solution 2	Same with solution 2
	NAS Container for PS HO IE	One bit of this is set to inform the UE+ that the SGSN+ has performed a non-legacy key derivation.	Same with solution 2	
TS 29.060	**SGSN Context Response**	An SGSN+ includes K_{ASMEU} if the security context being used is an enhanced one An SGSN+ includes COUNT if the security context being used is an enhanced one	Same with solution 2	Same with solution 2.
	Forward Relocation Request	An SGSN+ includes K_{ASMEU} if the security context being used is an enhanced one. An SGSN+ includes COUNT if the security context being used is an enhanced one.	Same with solution 2	An SGSN+ includes IK_U'/CK_U', the corresponding NCC, and K_{ASMEU} if the security context being used is an enhanced one. An SGSN+ includes COUNT if the security context being used is an enhanced one. IK_U'/CK_U' are sent in legacy IK/CK IE, so there is no need to enhance this parameter.
TS 25.413	**SECURITY MODE COMMAND**	An indication whether or not the SGSN+ has used an enhanced security key derivation to get the keys	Same with solution 2. UE UTRAN KH capability received in the first L3 message sent by UE.	An indication whether or not the SGSN supports the enhanced security. {IK_U', CK_U', NCC}

				used when the next SRNS relocation.
	Relocation Request		Refer to **Source RNC to Target RNC Transparent Container IE**	An SGSN+ includes IK_U'/CK_U' to target RNC+ if the security context being used is an enhanced one.
	Source RNC to Target RNC Transparent Container IE			An indication whether or not the UE supports the enhanced security. Source RNC+ includes IK_U'/CK_U' to target RNC+ if the security context being used is an enhanced one. IK_U'/CK_U'are sent in legacy IK/CK IE.
	Target RNC to Source RNC Transparent Container		A target RNC+ includes its capability to perform UTRAN key management enhancements in the container which is transparently sent to the source RNC(+). A source RNC+ includes the target RNCs capability to perform UTRAN key management enhancements in the Physical Channel Reconfiguration as normal.	An indication to UE via source RNC+ whether or not the target RNC supports the enhanced security.
	Relocation Command			A NCC used to synchronize key derivation between the target network and the ME+ during SRNS relocation.
TS 25.331	**SECURITY MODE COMMAND**	An indication whether or not the SGSN+ has used an enhanced security key derivation to get the keys.	Same with solution 2 UE UTRAN KH capability received in the first L3 message sent by UE.	An indication whether or not the network (SGSN+ and SRNC+) supports the enhanced security. {IK_U', CK_U', NCC} used when the next SRNS relocation.
	Physical Channel Reconfiguration /UTRAN Mobility Information		A target RNC+ includes its capability to perform UTRAN key management enhancements in the message at SRNS relocation without UE involvement.	An indication whether or not the target network (SGSN+ and SRNC+) supports the enhanced security. A NCC used to synchronization key derivation between the target network and the UE during SRNS relocation.
	UTRAN Mobility Information Confirm / Physical Channel Reconfiguration		A UE+ includes its capability to perform UTRAN key management enhancements in the message at combined	An indication whether or not the UE supports the enhanced security.

	Complete		CELL/URA update and SRNS relocation.	
	Cell Update Confirm/URA Update Confirm		An RNC+ includes its capability to perform UTRAN key management enhancements in the message at combined CELL/URA update and SRNS relocation.	An indication whether or not the target network (SGSN+ and SRNC+) supports the enhanced security. A NCC used to synchronization key derivation between the target network and the UE during SRNS relocation.
TS 24.301	**Attach request**	An indication that a UE+ supports enhanced security context functionality	Same with solution 2	
	TAU request	An indication that a UE+ supports enhanced security context functionality.	Same with solution 2	
	NAS Security Mode Command	An indication the MME used K_{ASMEU} to calculate K_{ASME} when creating this mapped security context.	Same with solution 2	
	NAS Security parameters to E-UTRA IE	One bit of this is set to inform the UE+ that the MME+ has performed a non-legacy key derivation.	Same with solution 2	
TS 29.274	**Forward Relocation Request**	An indication that a UE+ supports enhanced security context functionality. An indication that the current mapped EPS NAS security context is an enhanced one	Same with solution 2	
	Context Response	An indication that the current mapped EPS NAS security context is an enhanced one	Same with solution 2	

The following analysis relates to the messages that are used to ensure that a fresh key is available at every idle to active transition:

Solutions 2 and 3 consider a wider set of uses cases, i.e. both GERAN and E-UTRAN interworking, so hence they affect more messages. In particular this applies to all the proposed changes to TS 24.301 and TS 29.274 from E-UTRAN interworking and the Authentication and ciphering request and NAS Container for PS HO IE for GERAN interworking. Hence any decision on solution needs to be taken after a decision on how widely to apply the functionality.

There are some differences between solution 2/3 and 4 in UTRAN. In solutions 2 and 3, the changes to the security mode command message in TS 25.331 and 25.413 are optional (see subclause 5.2.3.1.3.3) and hence no changes to the RNC are needed whereas in solution 4 changes to the RNC are mandatory (see for example subclause 6.1.1 where the SGSN+ shall notify the UE in a SMC message). The full impact of the different changes to the RAN in the various solutions depends not only on providing fresh keys at idle to active transitions but also on the decision on the amount of additional functionality (e.g. key update during SRNS relocation) that is needed.

7 Complexity versus benefit analysis

7.1 Threats, use cases and protection level

7.1.1 Use case: temporarily stationary user

Attack targeting an individual user:

In some use cases, a user will not move at all or move in such a limited way that he will remain attached to the same collapsed RNC/NodeB for an extended period of time. Here are a few examples:

- The user has no fixed access to a telecommunications network any more and entirely relies on mobile access. The number of such users is growing steadily. HSPA is particularly attractive as a DSL or cable replacement due to its high speed.
- Even when the user has fixed access he is likely to receive, or even make, many mobile calls while at home.
- Similarly, the user is likely to make and receive many mobile calls while at his permanent or temporary workplace. A temporary workplace could e.g. a business meeting location away from his office.
- When the user is at leisure he may pause to watch a movie or check his social network account while stationary, e.g. in a cafe.

Therefore, if an attacker wants to eavesdrop on the traffic of a particular victim then the RNC covering the home area or the workplace area of the user is an attractive target for an attacker. If the attacker wants to eavesdrop on random victims then the RNC covering popular leisure spots is an attractive target for an attacker.

As long as an attacker has control of the collapsed RNC/NodeB covering a temporarily stationary user changing keys (either via a UTRAN KH or a re-authentication) will not stop the attack. However, as soon as the temporarily stationary users move out of coverage of the collapsed RNC/NodeB under the attacker's control, security will be restored if a key change is performed such that the new key cannot be known to the compromised RNC/NB. Note that mere key chaining is not sufficient to lose the attacker. Key chaining would however stop the attacker from decrypting previously recorded traffic using the same key.

There is a case where changing the keys can help also while the temporarily stationary user remains in coverage of the collapsed RNC/NodeB which the attacker is interested in., This is the case when the attacker manages to gain control of the collapsed RNC/NodeB only for a brief period of time, and the UTRAN KH enhancement implies frequent change of keys available in the collapsed RNC/NodeB. But the first case where the attacker controls the collapsed RNC/NodeB for an extended period of time needs also to be taken into consideration when weighing the benefits against the benefits .

Conclusion: Changing keys (either via re-authentication or UTRAN KH) provides no protection for users connected to a collapsed RNC/NodeB which is under the control of an attacker for an extended period of time. However, as soon as the user leaves the area covered by the collapsed RNC/NodeB under the attacker's control, a change of keys such that the new key cannot be known to the compromised RNC/NB would restore the security for further communication. Note that mere key chaining is not sufficient to lose the attacker. Key chaining would however stop the attacker from decrypting previously recorded traffic using the same key.

Attack targeting a particular area:

Another type of attacker behaviour would be to eavesdrop on all users present in a particular area. The attacker can achieve this by breaking into a collapsed RNC/NodeB covering that area. The interest of the attacker would lie not so much in targeting a particular user, but getting to know the communication of all users visiting that particular area, for the purpose of gathering intelligence on e.g. a business or popular meeting point. The technical approach for performing the attack is similar to the attack on the individual user (cf. above in this clause 7.1.1), but the objective of the attack and the mobility patterns of the intercepted users may be quite different.

Conclusion: It is true that changing keys before or after moving in or out of coverage of the collapsed RNC/NodeB under the attacker's control will result in that the attacker can no longer get access to any traffic protected by those keys. But as it is the attacker’s objective to monitor traffic in a certain area and not to follow a user around and intercept his traffic while he is moving the attacker’s objective cannot be thwarted by changing the keys. Any data transmitted while

the user is connected to the collapsed RNC/NodeB will be available to the attacker (just as described in the first part of clause 7.1.1).

7.1.2 Use case: mobile users

7.1.2.1 Description

A very common mobility pattern, is that a user moves around in a city (e.g., by car, by bus or by foot), walks in and out of malls, cafés, work place, home etc during the day. As a result the user is handed over (or moves in Idle mode) between different base stations and RNCs (possibly even changing RAT, e.g., if only GERAN coverage exists).

Typically the user picks up the phone to check social media sites, news, the weather etc from time to time. These checks can be very short, ranging from seconds to a few minutes. Further, the user may have one or more apps which receives data from the network or polls the network for data as the user is on the move. Examples of such data are presence information of friends, location based service data (such as stores in the vicinity that are carrying an item on the user's wish list), and pollen reports. The user may also make CS calls on the go.

7.1.2.2 Attacker behaviour

If an attacker wants to eavesdrop on such a user, the attacker can break into a collapsed RNC/NodeB which the user connects to (e.g., one located in a place which the attacker knows the user frequents, like the home or work place of the user). Another possibility is that the attacker knows about a weakness in the encryption algorithms UEA and obtains the CK using that. But we would like to note that no signs of weakness of an encryption algorithm UEA have become known, nor are any problems with the key lengths to be expected any time soon. Once the attacker gets hold of the CK/IK of the user, the attacker can start eavesdropping on the data of such a user on the air interface and follow the user around.

Since the CK/IK remains the same until the next AKA run, the attacker will have access to the user data until then.

7.1.2.3 Countermeasures

Increasing the frequency of AKA runs would limit the amount of data the attacker gets access to. This also increases the load on the network, authentication vector consumption and, if tied to events, e.g., every call setup, a delay in accessing those services is added.

Changing keys for every Idle/Active transition using a UTRAN KH will also result in that the attacker is cut out of the loop, but with the benefit of no additional signaling compared to an AKA run and lower consumption of authentication vectors. As long as the user stays in Active mode, the attacker will however have access to the data. For example, if the user is constantly streaming Internet radio or has an ongoing CS call.

If key update is only a simple chaining without forward security ensured, even if the user moves out of that collapsed RNC/NodeB, the attacker could also derive the new updated key by just chaining the old key once. Only if key changes using a UTRAN KH with forward security are introduced at SRNS relocations and handovers as well, then even the users who move around in Active mode (e.g., streaming Internet radio or has an ongoing CS call) will also get rid of the attacker when relocated to a new RNC (it being collapsed into a NodeB or not).

7.1.2.4 Conclusion

For the typical user moving around, and an attacker who has once got access to CK/IK, there are two main cases to consider: the user is in Active mode for longer periods (e.g., listening to Internet radio or has a CS call ongoing) and the case where the user is mainly in Idle mode but goes to Active mode to get/send some data from time to time. In the first case the only countermeasure that helps to get rid of the attacker is to change keys at handovers and SRNS relocations. In the second case, changing keys using a more frequent AKA runs or changing keys using a UTRAN KH seem almost equivalent from security point of view. However, the increasing the frequency of AKA runs causes a higher load on the network, increases the authentication vector consumption and adds delay to bearer setup.

7.1.3 Theft of service

7.1.3.1 Threat

Theft of service includes making calls, sending SMSes and sending/receiving data without being charged for it. In the scope of this study it is relevant only to look at service theft by an attacker who has broken into a collapsed RNC/NodeB or has broken the ciphering/integrity algorithms and can inject data over the air interface. Other options may be at an attacker's disposal, but since a UTRAN KH would not protect against them they are left out from this study.

7.1.3.2 Analysis

An attacker that has broken into a collapsed RNC/NodeB or home NodeB can use services making it look like any subscriber connected to the node. This results in that the legitimate subscriber can get charged for services he did not use or that the legitimate subscriber is implicated in potentially criminal activities against internet hosts.

If no subscribers are connected to the compromised node, the attacker may increase the signal strength of the node to attract terminals from a wider area. Doing so, however, increases the risk of detection of the compromised node, since it would disturb other NodeBs in the vicinity.

As soon as the subscriber moves to a node not controlled by the attacker, it is likely that the attacker will not be able to use that subscriber as a victim any longer. For instance, if the terminal sends a RAU/LAU in a different area, the attacker will not be able to maintain control. The attacker could of course send a spoofed RAU/LAU on behalf of the subscriber to fool the core network to believe the terminal was back in the attacker controlled node. This would however throw out the legitimate terminal.

In either of the above cases, if that happens too many times the operator will get sufficiently many complaints to investigate what is wrong with the collapsed RNC/NodeB the attacker is using.

Since a UTRAN KH does not, and never was intended to, protect against the case that the attacker has compromised the node the subscriber is currently connected to, it does not help when the user stays put.

7.1.4 CN and RAN level key separation

One implication of the legacy UTRAN key hierarchy is that the security properties of providing fresh keys for communication between the UE and network and the checking the presence of the UICC are effectively the same procedure, i.e. an AKA run. In the legacy UTRAN architecture this was not much of an issue as the keys used between the UE and network were known only to RNC and CN elements that were all assumed to be in secure locations.

This assumption can no longer be assumed to hold due to the introduction of collapsed RNCs, i.e. ones that are co-located with the Node B. A compromise of such an node would allow an attackers to not only get access to the UE's data during it current session but also allow an attacker to masquerade as the UE to both make and receive calls or get access to a UE's data during a later (or indeed previous if the encrypted data had been saved) session with the network. This situation would continue until a new AKA has been run (which has the effect of refreshing the keys). Without changes to the UTRAN keying, this may have the effect of increasing the frequency of AKA runs in order to achieve a good separation of security between different sessions and restrict the effect of a compromised collapsed RNC depending on a trade off between complexity and security.

The introduction of CN and RAN level key separation with a fresh key being delivered to the RAN at each idle-to-active transitions provides a strict limit on the amount that could be gained by an attacker that compromises a collapsed RNC, i.e. only data from the current session to each UE would be compromised and the attacker would not be able to make/receive subsequent calls. The frequency of AKA runs could then be determined by the desire of the operator to check the presence of the UICC rather than for (re-)keying purposes. Both solutions 1 and 2 give methods of providing this key separation that only require the addition/modification of a few IEs between the UE and serving network nodes. Furthermore solution 2 allows this to be done without effecting the RAN node. These improvements compare favourably with increasing the frequency of AKA runs which have the impact of increasing the signalling load throughout the network including that on the key central network elements (e.g. HSS/HLR) and also avoiding the delay in call set-up times that an AKA run entails.

7.2 Cost and complexity analysis

7.2.1 Target orientation

Platform security is a measure that affects only the entity that motivates the study of 3G security enhancements, that is, the collapsed RNC/NodeB. A UTRAN key hierarchy enhancement requires support at least by MEs and core network nodes (SGSNs and MSC/VLRs respectively), possibly also collapsed RNC/NodeBs and classical RNCs (depending on the proposed solution).

It is possible that UTRAN KH enhancements would have to be mandated for MEs from a certain release on as otherwise a reasonable penetration may be impossible to achieve even in the long run. This would then mean that the associated cost of UTRAN KH enhancements in the ME would have to be borne by operators and subscribers irrespective of whether they would ever make use of collapsed RNC/NodeBs. Operators not making use of collapsed RNC/NodeBs would not have to purchase any enhancements to network equipment, The reason for this is that the terminals needs to be prepared to deal with legacy networks anyhow, and hence the operators do not need to upgrade any of their network nodes. In addition, there is no reason to mandate the suppport or use of a UTRAN KH for classical UTRAN architectures. An operator who wants to make use of UTRAN KH will have to update SGSN/MSC and possibly collapsed and macro RNCs.

Conclusion: If UTRAN KH enhancements were mandated in a specifaction, operators who do not make use of collapsed RNC/NodeBs may have to help bearing the cost of the ME implementations even if they would not benefit from any enhanced security. They would, however, not have to help bearing the cost for any network equipment enhancements. An operator who wants to make use of UTRAN KH will have to update SGSN/MSC and possibly collapsed and macro RNCs.

7.2.2 Cost of countermeasures

Increasing the frequency of AKA runs results in a higher load in signaling, an increased consumption of authentication vectors, more frequent writes to the UICC, added delay in setting up services (e.g., call setup, if tied to that event). No equipment needs upgrading assuming the existing equipment can handle the increased load. Backwards compatibility is not an issue since nothing new is added.

Adding a UTRAN KH that allows changes of keys at Idle to Active transitions implies that the core network nodes and terminals require new functionality. New IEs can be piggy-backed on existing signaling. Backwards compatibility can be ensured.

Enhancing the UTRAN KH to allow also for key changes at SRNS relocation and handover requires that, in addition to core network nodes and terminals, new functionality is also implemented in RNC. The main difference between solutions 3 and 4 is that solution 4 provides both backward and forward security whereas solution 3 only provides backward security. The cost of adding also forward security is more complex handling in both core network nodes and RNCs. But forward security is the only proposed measure to get rid of the possibility for the attacker to continue the attack after the victim connects to a different RNC. Backward compatibility can be ensured for both solutions 3 and 4.

8 Conclusions

8.1 General

This clause collects and summarizes the conclusions from the comparison between the different proposals and from the cost vs. complexity analysis clauses.

8.2 Threats

8.2.1 General

This clause only discusses the threats and what security benefits a UTRAN KH may bring.

8.2.2 Privacy

Individual users will benefit from key changes at mobility between RNCs. This is especially true for collapsed RNC/NodeBs. An attacker who has compromised a (collapsed NodeB) RNC will not be able to get access to any significant amount of data from earlier/later RNCs. Depending on how the key change is implemented, the attacker will get more or less data. Some solutions make sure the attacker gets no data at all. These solutions have a bigger signalling load/complexity compared to the ones who only ensures that the attacker gets a small amount of data.

An attacker will of course be able to get access to all data that a user transmits or receives while connected to a RNC/NodeB under the attackers control even if a UTRAN KH is used. The study is made under the assumption that platform security is in place though.

8.2.3 Fraud

An attacker will be able to perform fraud even in the presence of UTRAN KH. The attacker could impersonate any UE connected to the compromised RNC/NodeB. If the user moves away, the attacker may choose another victim connected to the compromised RNC/NodeB. This does not work well for call fraud, but better for packet based services (the attacker may get problems with having to change his IP address when using another victim, but that may not be too annoying).

8.3 Differences between solutions

There are four proposed solutions for introducing a UTRAN KH in the present document. Each of these has parts that can be added or removed for additional or lesser functionality. This is analyzed and compared in exquisite detail in earlier clauses of the present document, and hence this clause will only give a high level comparison of the solutions w.r.t. their differences.

Solution 1 is similar to how the LTE key hierarchy is designed and maintained. One key difference is that key freshness at Idle to Active state transitions is provided using a counter sent from the network node (MSC or SGSN) to the terminal. No synchronization between the counter used in the CS domain and the counter used in PS domain is in place, which implies that the same counter value may be used more than once. This leads to security weaknesses. Should this be fixed, solution 1 still is not as mature as the other proposals. Solution 1 provides both forward and backward security at SRNS relocations.

Solution 2 only ensures fresh keys at Idle to Active state transitions. At SRNS relocations the ciphering and integrity keys remain the same. No forward or backward security is provided. Solution 2 alone has least impact on existing nodes and protocols of all the proposed solutions.

Solution 3 is an addition to Solution 2. That is to say, Solution 3 consists of Solution 2 at its core and adds additional functionality on top of this. Solution 3 provides backward security at SRNS relocations. This requires some further changes to the RNC and RANAP protocols. In comparison to Solution 4 it is more light-weight, but it does not provide forward security.

Solution 4 is also an addition on Solution 2. Solution 4 provides forward and backward security at SRNS relocations. This also requires some further changes to the RNC and RANAP protocols.

Figure 8.3-1 shows what degree of security the different solutions provide in relation to each other. Solution 1 and Solution 4 (attempt to) provide the same degree of security (fresh keys at Idle to Active transitions, backward and forward security). Solution 1 fails to provide fresh keys at Idle to Active state transitions in some cases and is hence shown as a separate box.

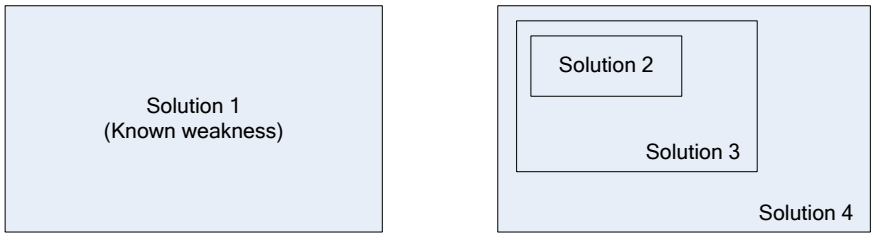

Figure 8.3-1 Security functionality provided by the solutions in comparison to each other.

In addition to showing how much functionality each soltion proposal provides, the sizes of the boxes in Figure 8.3-1 roughly represents the differences in complexity between the proposals.

Annex A:
Change history

Change history							
Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Old	New
2010-11	SA#50	SP-100736	--	--	Presentation to SA for Information	---	1.0.0
2011-11	SA#54	SP-110688	--	--	Presentation to SA for Approval	1.0.0	2.0.0
2012-01	--	--	--	--	Publication	2.0.0	11.0.0
2012-03	SA#55	SP-120035	1	1	UKM conclusions	11.0.0	11.1.0