3GPP TSG SA WG3 Security — S3#21b **S3z020004**

31st January - 1st February, 2002

Antwerp, Belgium

CR-Form-v3

CHANGE REQUEST

⌘ **TS 33.203 CR** ⌘ rev **1** ⌘ Current version: **v1.0.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: ⌘ (U)SIM **X** ME/UE **X** Radio Access Network **X** Core Network **X**

Title:	⌘	Incorporation of Integration Guidelines for R5 into TS33.203
Source:	⌘	BT Group
Work item code:	⌘	***Date:*** ⌘ 2002-01-21
Category:	⌘	**F** ***Release:*** ⌘ REL-5

Use one of the following categories:
- ***F*** *(essential correction)*
- ***A*** *(corresponds to a correction in an earlier release)*
- ***B*** *(Addition of feature),*
- ***C*** *(Functional modification of feature)*
- ***D*** *(Editorial modification)*

Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
REL-4	*(Release 4)*
REL-5	*(Release 5)*

Reason for change:	⌘	As it has been agreed that there will not be a separate Integration Guidelines document for R5, the equivalent information needs to be added to TS 33.203
Summary of change:	⌘	New annex G added based on text from TS33.103
Consequences if not approved:	⌘	No integration guidelines for R5 approved, making it difficult to determine R5 impact on existing and new network elements and terminals.

Clauses affected:	⌘	New Annex G
Other specs affected:	⌘	☐ Other core specifications ⌘ ☐ Test specifications ☐ O&M Specifications
Other comments:	⌘	

**** Modified section - Add

Annex G

This Annex defines how elements of the IMS -security architecture are to be integrated into the following entities of the system architecture.

G.1 ISIM

G.2 User equipment

G.3 Serving Call State Control Function (S-CSCF)

G.4 Proxy Call State Control Function in Visited Network (VP-CSCF)

G.5 Proxy Call State Control Function in Home Network (HP-CSCF)

G.7 Interrogating Call State Control Function (I-CSCF)

G.7 Home Subscriber Server (HSS)

The structure of this annex is a series of tables, which describe the security information and cryptographic functions to be stored in the above entities of the 3G system.

For security information, this is in terms of multiplicity, lifetime, parameter length and whether mandatory or optional.

For the cryptographic functions, the tables also include an indication of whether the implementation needs to be standardised or can be proprietary

G.1 ISIM

G.1.1 Authentication Key Agreement and Registration

The ISIM shall support the UMTS mechanism for Authentication Key Agreement and Registration described in 6.1 of 3G TS 33.203.

The following data elements need to be stored on the ISIM:

a) K_{IM}: a permanent secret key;

b) SQN_{ISIM}: a counter that is equal to the highest sequence number SQN in an AUTN parameter accepted by the user;

c) $RAND_{ISIM}$: the random challenge which was received together with the last AUTN parameter accepted by the user. It is used to calculate the re-synchronisation message together with the highest accepted sequence number (SQN_{ISIM});

d) KSI_{IM}: key set identifier;

e) $THRESHOLD_{IM}$: a threshold defined by the HE to trigger re-authentication and to control the cipher key lifetime;

f) CK_{IM} the IMS signalling cipher key established as part of authentication;

g) IK_{IM} the IMS signalling integrity key established as part of authentication;

h) AMF_{IM}: A 16-bit field used Authentication Management.

Table 1 provides an overview of the data elements stored on the ISIM to support Authentication Key Agreement and Registration.

Table 1: ISIM – Authentication Key Agreement and Registration – Data elements

Symbol	Description	Multiplicity	Lifetime	Length	Mandatory / Optional
IMPI	Private Identity	1	Permanent		Mandatory
IMPU	Public Identities	n	Updated during registration		Mandatory
DN_{HOME}	Home Network Domain Name	1	Permanent		Mandatory
K_{IM}	Permanent secret key	1 (note 1)	Permanent	128 bits	Mandatory
SQN_{ISIM}	Highest previously accepted sequence number counter	1	Updated when AKA protocol is executed	48 bits	Mandatory
SQN_{ISIM} [ ] array	array of last accepted sequence number	1	Updated when AKA protocol is executed	at least 32 entries	Optional
$RAND_{ISIM}$	Random challenge received by the user.	1	Updated when AKA protocol is executed	128 bits	Mandatory
KSI_{IM}	Key set identifier	2 (note 2)	Updated when AKA protocol is executed	3 bits	Mandatory
$THRESHOLD_{IM}$	Threshold value for cipher key	1	Permanent	24 bits	Mandatory
CK_{IM}	Cipher key	2 (note 2)	Updated when AKA protocol is executed	128 bits	Mandatory
IK_{IM}	Integrity key	2 (note 2)	Updated when AKA protocol is executed	128 bits	Mandatory
AMF_{IM}	Authentication Management Field (indicates the algorithm and key in use)	1	Updated when AKA protocol is executed	16 bits	Mandatory

NOTE 1: HE policy may dictate more than one, the active key signalled using the AMF function.
NOTE 2: one for each IMS domain.

C W Blanchard 21/01/02 1 1. How many IMS domains are allowed

2 Relationship of $CK_{IM\ to}$ CK_{IM_in}. etc is unclear

The following cryptographic functions need to be implemented on the ISIM:

- f1: a message authentication function for IMS authentication;
- f1*: a message authentication function for support to re-synchronisation;
- f2: a message authentication function for user authentication;
- f3: a key generating function to derive the cipher key;
- f4: a key generating function to derive the integrity key;
- f5: a key generating function to derive the anonymity key (AK_{IM}) for normal operation;
- f5*: a key generating function to derive the anonymity key for re-synchronisation;

Table 2 provides a summary of the cryptographic functions implemented on the ISIM to support Authentication Key Agreement and Registration

Table 2: ISIM – Authentication Key Agreement and Registration – Cryptographic functions

Symbol	Description	Multiplicity	Lifetime	Standardised / Proprietary	Mandatory / Optional
f1	IMS authentication function	1	Permanent	Proprietary	Mandatory
f1*	IMS Message authentication function for synchronisation	1	Permanent	Proprietary	Mandatory
f2	User authentication function	1	Permanent	Proprietary	Mandatory
f3	Cipher key generating function	1	Permanent	Proprietary	Mandatory
f4	Integrity key generating function	1	Permanent	Proprietary	Mandatory
f5	Anonymity key generating function (for normal operation)	1	Permanent	Proprietary	Optional
f5*	Anonymity key generating function (for re-synchronisation)	1	Permanent	Proprietary	Optional

G.2 User equipment

G.2.1 Data confidentiality

The UE shall support the UMTS mechanism for confidentiality of user and signalling data described in 5.1.3 of 3G TS 33.203.

Table 3 provides an overview of the data elements stored on the UE to support the mechanism for data confidentiality:

Table 3: UE – Data Confidentiality – Data elements

Symbol	Description	Multiplicity	Lifetime	Length	Mandatory / Optional
UEA_{IM}	Selected ciphering capability	1 per UE	Updated at connection establishment	4 bits	Optional
CK_{IM_in}.	Encryption key for the SA inbound from the P-CSCF	1 per user	Updated when AKA protocol is executed	128 bits	Optional
CK_{IM_out}	Encryption key for the SA outbound from the P-CSCF	1 per user	Updated when AKA protocol is executed	128 bits	Optional

Table 4 provides an overview of the cryptographic functions implemented on the UE to support the mechanism for data confidentiality.

Table 4: UE – Data Confidentiality – Cryptographic functions

Symbol	Description	Multiplicity	Lifetime	Standardised / Proprietary	Mandatory / Optional
f20	IMS signaling encryption function	1-16	Permanent	Standardised	Optional
h1	Encryption key derivation functions	1	Permanent	Standardised	Optional
h2	Encryption key derivation functions	1	Permanent	Standardised	Optional

G.2.2 Data integrity

The UE shall support the UMTS mechanism for integrity of signalling data described in 5.1.4 of 3G TS 33.203.

Table 5 provides an overview of the data elements stored on the UE to support the mechanism for data confidentiality:

Table 5: UE – Data Integrity – Data elements

Symbol	Description	Multiplicity	Lifetime	Length	Mandatory / Optional
SA1	Security association for traffic from UE to P-CSCF	1	According to SA_lifetime		Mandatory
SA2	Security association for traffic from P-CSCF to UE	1	According to SA_lifetime		Mandatory
UIA_{IM}	Selected ciphering capability	1 per UE	Updated at connection establishment	4 bits	Mandatory
SA-ID	ID used to uniquely identify the SA at the receiving side.	1	According to SA_lifetime		Mandatory
SA11	Security association for traffic from UE to P-CSCF during re registration	1	According to SA_lifetime		Mandatory
SA12	Security association for traffic from P-CSCF to UE during re registration	1	According to SA_lifetime		Mandatory
SA_lifetime	Lifetime of the SA between the UE and the P-CSCF	1	As IMS Home Operator Policy		Mandatory
IK_{IM_in}.	integrity key for the SA inbound from the P-CSCF	1 per mode	Updated by the execution of the AKA protocol	128 bits	Mandatory
$IK_{IM\_out.}$	The integrity key for the SA outbound from the P-CSCF	1 per mode	Updated by the execution of the AKA protocol	128 bits	Mandatory

Table 6 provides an overview of the cryptographic functions implemented in the UE:

Table 6: UE – Data Integrity – Cryptographic functions

Symbol	Description	Multiplicity	Lifetime	Standardised / Proprietary	Mandatory / Optional
f21	IMS signaling data integrity function	1-16	Permanent	Standardised	One at least is mandatory
h1	integrity key derivation function	1	Permanent	Standardised	Mandatory
h2	integrity key derivation functions	1	Permanent	Standardised	Mandatory

G.3 Serving Call State Control Function (S-CSCF)

Table 7 provides an overview of the cryptographic functions implemented in the S-CSCF

Table 7: S-CSCF – Data Integrity – Cryptographic functions

Symbol	Description	Multiplicity	Lifetime	Standardised / Proprietary	Mandatory / Optional

(None identified)

G.3.1 Authentication Key Agreement and Registration

The S-CSCF shall support the UMTS mechanism for Authentication Key Agreement and Registration described in 6.1 of 3G TS 33.203.

The following data elements need to be stored in the S-CSCF

a) AV: Authentication vectors;

Table 8 provides an overview of the composition of an authentication vector

Table 8: Composition of an authentication vector

Symbol	Description	Multiplicity	Length
$RAND_{IM}$	IMS challenge	1	128
$XRES_{IM}$	Expected response	1	32-128
CK_{IM}	Cipher key	1	128
IK_{IM}	Integrity key	1	128
AUTN	Authentication token	1 that consists of:	128
SQN_{IM} or $SQN_{IM} \oplus AK_{IM}$	Sequence number or Concealed sequence number	1 per AUTN	48
AMF_{IM}	Authentication Management Field	1 per AUTN	16
MAC-A	Message authentication code for IMS authentication	1 per AUTN	64

b) KSI: Key set identifier;

c) CK: Cipher key;

d) IK: Integrity key;

Table 9 provides an overview of the data elements stored in the S-CSCF support authentication and key agreement.

Table 9: S-CSCF – Authentication Key Agreement and Registration – Data elements

Symbol	Description	Multiplicity	Lifetime	Length	Mandatory / Optional
Profile	Subscriber profile	1 per user	As IMS Home Operator Policy		Mandatory
Registration_flag	Registration Flag	1 per user	Registration Period	1 bit	Mandatory
Registration_timer	Registration timer value	1 per user	As IMS Home Operator Policy		Mandatory
SA_lifetime	Lifetime of the SA between the UE and the P-CSCF	1 per user	As IMS Home Operator Policy		Mandatory
UMTS AV	UMTS Authentication vectors	several per user, SN dependent	Depends on many things	528-640	Mandatory
KSI	Key set identifier	1 per user	Updated when AKA protocol is executed	3 bits	Mandatory
CK	Cipher key	1 per user	Updated when AKA protocol is executed	128 bits	Mandatory
IK	Integrity key	1 per user	Updated when AKA protocol is executed	128 bits	Mandatory
IMPU	Public Identity	n	Updated at registration		Mandatory

G.4 Proxy Call State Control Function in Visited Network (VP-CSCF)

G.4.1 Data confidentiality

The VP-CSCF shall store the following data elements:

Table 10: VP-CSCF – Data Confidentiality – Data elements

Symbol	Description	Multiplicity	Lifetime	Length	Mandatory / Optional
CK_{IM_in}.	Encryption key for the SA inbound from the P-CSCF	1 per user	Updated when AKA protocol is executed	128 bits	Mandatory
CK_{IM_out}	Encryption key for the SA outbound from the P-CSCF	1 per user	Updated when AKA protocol is executed	128 bits	Mandatory

Table 11 provides an overview of the cryptographic functions implemented in the VP-CSCF to support the mechanism for data confidentiality:

Table11: VP-CSCF – Data confidentiality – Cryptographic functions

Symbol	Description	Multiplicity	Lifetime	Standardised / Proprietary	Mandatory / Optional
f20	IMS signalling encryption function	1-16	Permanent	Standardised	One at least is mandatory
h1	Encryption key derivation function	1	Permanent	Standardised	Mandatory
h2	Encryption key derivation functions	1	Permanent	Standardised	Mandatory

G.4.2 Data integrity

The VP-CSCF shall support the UMTS mechanism for data integrity of signalling data described in 5.1.4 of 3G TS 33.203.

Table 12 provides an overview of the data elements stored on the VP-CSCF to support the mechanism for data confidentiality:

Table12: VP-CSCF – Data Integrity – Data elements

Symbol	Description	Multiplicity	Lifetime	Length	Mandatory / Optional
SA-ID	ID used to uniquely identify the SA at the receiving side.	1	According to SA_lifetime		Mandatory
SA11	Security association for traffic from UE to P-CSCF during re registration	1	According to SA_lifetime		Mandatory
SA12	Security association for traffic from P-CSCF to UE during re registration	1	According to SA_lifetime		Mandatory
SA lifetime	Lifetime of the SA between the UE and the P-CSCF	1	As IMS Home Operator Policy		Mandatory
IK_{IM_in}.	integrity key for the SA inbound from the P-CSCF	1 per mode	Updated by the execution of the AKA protocol	128 bits	Mandatory
$IK_{IM\_out.}$	The integrity key for the SA outbound from the P-CSCF	1 per mode	Updated by the execution of the AKA protocol	128 bits	Mandatory

Table 13 provides an overview of the cryptographic functions implemented in the VP-CSCF

Table 13: VP-CSCF – Data Integrity – Cryptographic functions

Symbol	Description	Multiplicity	Lifetime	Standardised / Proprietary	Mandatory / Optional
f21	IMS signalling data integrity function	1-16	Permanent	Standardised	One at least is mandatory
h1	integrity key derivation function	1	Permanent	Standardised	Mandatory
h2	integrity key derivation functions	1	Permanent	Standardised	Mandatory

G.5 Proxy Call State Control Function in Home Network (HP-CSCF)

G.5.1 Data confidentiality

The HP-CSCF shall store the following data elements:

Table 14: HP-CSCF – Data Confidentiality – Data elements

Symbol	Description	Multiplicity	Lifetime	Length	Mandatory / Optional
CK_{IM_in}.	Encryption key for the SA inbound from the P-CSCF	1 per user	Updated when AKA protocol is executed	128 bits	Mandatory
CK_{IM_out}	Encryption key for the SA outbound from the P-CSCF	1 per user	Updated when AKA protocol is executed	128 bits	Mandatory

Table 15 provides an overview of the cryptographic functions implemented in the HP-CSCF to support the mechanism for data confidentiality:

Table15: HP-CSCF – Data confidentiality – Cryptographic functions

Symbol	Description	Multiplicity	Lifetime	Standardised / Proprietary	Mandatory / Optional
f20	IMS signalling encryption function	1-16	Permanent	Standardised	One at least is mandatory
h1	Encryption key derivation function	1	Permanent	Standardised	Mandatory
h2	Encryption key derivation functions	1	Permanent	Standardised	Mandatory

G.5.2 Data integrity

The HP-CSCF shall support the UMTS mechanism for data integrity of signalling data described in 5.1.4 of 3G TS 33.203.

Table 16 provides an overview of the data elements stored on the HP-CSCF to support the mechanism for data confidentiality:

Table16: HP-CSCF – Data Integrity – Data elements

Symbol	Description	Multiplicity	Lifetime	Length	Mandatory / Optional
SA-ID	ID used to uniquely identify the SA at the receiving side.	1	According to SA_lifetime		Mandatory
SA11	Security association for traffic from UE to P-CSCF during re registration	1	According to SA_lifetime		Mandatory
SA12	Security association for traffic from P-CSCF to UE during re registration	1	According to SA_lifetime		Mandatory
SA lifetime	Lifetime of the SA between the UE and the P-CSCF	1	As IMS Home Operator Policy		Mandatory
IK_{IM_in}.	integrity key for the SA inbound from the P-CSCF	1 per mode	Updated by the execution of the AKA protocol	128 bits	Mandatory
$IK_{IM\_out.}$	The integrity key for the SA outbound from the P-CSCF	1 per mode	Updated by the execution of the AKA protocol	128 bits	Mandatory

Table 17 provides an overview of the cryptographic functions implemented in the HP-CSCF

Table 17: HP-CSCF – Data Integrity – Cryptographic functions

Symbol	Description	Multiplicity	Lifetime	Standardised / Proprietary	Mandatory / Optional
f21	IMS signalling integrity function	1-16	Permanent	Standardised	One at least is mandatory
h1	integrity key derivation function	1	Permanent	Standardised	Mandatory
h2	integrity key derivation functions	1	Permanent	Standardised	Mandatory

G.6 Interrogating Call State Control Function (I-CSCF)

G.6.1 Data confidentiality

The I-CSCF shall store the following data elements:

Table 18: I-CSCF – Data Confidentiality – Data elements

Symbol	Description	Multiplicity	Lifetime	Length	Mandatory / Optional
Key_hide	Key for hiding function	1	Permanent	Proprietary	Optional

Table 19 provides an overview of the cryptographic functions implemented in the I-CSCF to support the mechanism for data confidentiality:

Table 19: I-CSCF – Data confidentiality – Cryptographic functions

Symbol	Description	Multiplicity	Lifetime	Standardised / Proprietary	Mandatory / Optional
f22	Hiding function	1	Permanent	Proprietary	Optional

G.7 Home Subscriber Server (HSS)

G.7.1 Authentication Key Agreement and Registration

The HSS shall support the UMTS mechanism for Authentication Key Agreement and Registration described in 6.1 of 3G TS 33.203.

Table 20 provides an overview of the data elements stored on the HSS support authentication and key agreement.

Table 20: HSS – Authentication Key Agreement and Registration – Data elements

Symbol	Description	Multiplicity	Lifetime	Length	Mandatory / Optional
IMPI	Private Identity	1	Permanent		Mandatory
profile	Subscriber profile	1 per user	As IMS Home Operator Policy		Mandatory
Registration_flag	Registration Flag	1 per user	Registration Period	1 bit	Mandatory
S-CSCF_ID	S-CSCF name	1	As IMS Home Operator Policy		
K_{IM}	Permanent secret key	1	Permanent	128 bits	Mandatory
SQN_{HSS}	Sequence number counter	1	Updated when AVs are generated	48 bits	Mandatory
IM AV	UMTS Authentication vectors	HS option	Updated when AVs are generated	544-640 bits	Optional
IMPU	Implicitly Registered IMPU,s	n	Updated during registration		Mandatory

Table 21 shows how the construction of authentication token for synchronisation failure messages used to support authentication and key agreement.

Table 21: Composition of an authentication token for synchronisation failure messages

Symbol	Description	Multiplicity	Length
AUTS	Synchronisation Failure authentication token	that consists of:	112
SQN	Sequence number	1 per AUTS	48
MAC-S	Message authentication code for Synchronisation Failure messages	1 per AUTS	64

The following cryptographic functions need to be implemented in the HSS

- f1: a message authentication function for IMS authentication;
- f1*: a message authentication function for support to re-synchronisation;
- f2: a message authentication function for user authentication;
- f3: a key generating function to derive the cipher key;
- f4: a key generating function to derive the integrity key;
- f5: a key generating function to derive the anonymity key for normal operation;
- f5*: a key generating function to derive the anonymity key for re-synchronisation;

Table 22 provides a summary of the cryptographic functions implemented on the HSS support authentication and key agreement.

Table 22: HSS – Authentication Key Agreement and Registration – Cryptographic functions

Symbol	Description	Multiplicity	Lifetime	Standardised / Proprietary	Mandatory / Optional
f1	IMS authentication function	1	Permanent	Proprietary	Mandatory
f1*	Message authentication function for synchronisation	1	Permanent	Proprietary	Mandatory
f2	User authentication function	1	Permanent	Proprietary	Mandatory
f3	Cipher key generating function	1	Permanent	Proprietary	Optional
f4	Integrity key generating function	1	Permanent	Proprietary	Mandatory
f5	Anonymity key generating function (for normal operation)	1	Permanent	Proprietary	Optional
f5*	Anonymity key generating function (for re-synchronisation)	1	Permanent	Proprietary	Optional