3GPP
TSG-T meeting #4
Miami, Florida / USA, 17-18 June 1999

Document TSGT#4(99)143

Source: **3GPP_TSG_SA_WG3**
Blanchard Colin[SMTP:colin.blanchard@BT.COM]

Title: **Revised version of 3G Security: Integration Guidelines**

Agenda item: **5.1**

Document for: **Information**

3rd Generation Partnership Project;
Technical Specification Group Services and System Aspects;
3G Security;
Integration Guidelines
3G TS ___ V 0.0.2

Reference
DTS/TSGS-_____

Keywords
Security, Authentication and Key Agreement, Security Information Stored, Location of Security Functions, Parameter Lengths

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 document has been drafted by 3GPP TSG-SA WG 3, i.e., the Workgroup devoted to “Security” issues, within the Technical Specification Group devoted to “System Aspects”.

1 Scope

This technical specification defines how elements of the security architecture are to be integrated into the following entities of the system architecture.

- Home Environment Authentication Center (HE/AuC)
- Serving Network Visited Location Register (SN/VLR)
- Radio Node Controller (RNC)
- Mobile station User Identity Module (UIM)
- Mobile Equipment (ME)

This specification is derived from 3G "Security architecture".

The structure of this technical specification is as follows:

Clause 5 lists the security information to be stored in the above entities of the 3G system in terms of Static information and Dynamic information.

Clause 6 defines the external specification of the security-related algorithms in terms of input and output parameters, and the parameter lengths.

The equivalent information for the alternative Temporary Key proposal is included in an appendix to this document

2 References

References may be made to:

a) specific versions of publications (identified by date of publication, edition number, version number, etc.), in which case, subsequent revisions to the referenced document do not apply; or

b) all versions up to and including the identified version (identified by “up to and including” before the version identity); or

c) all versions subsequent to and including the identified version (identified by “onwards” following the version identity); or

d) publications without mention of a specific version, in which case the latest version applies.

A non-specific reference to an ETS shall also be taken to refer to later versions published as an EN with the same number.

2.1 Normative references

[1] TR S3.03 Security Architecture

2.2 Informative references

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the following definitions apply:

Confidentiality: The property that information is not made available or disclosed to unauthorised individuals, entities or processes.
Data integrity: The property that data has not been altered in an unauthorised manner.
Data origin authentication: The corroboration that the source of data received is as claimed.
Entity authentication: The provision of assurance of the claimed identity of an entity.
Key freshness: A key is fresh if it can be guaranteed to be new, as opposed to an old key being reused through actions of either an adversary or authorised party.

3.2 Symbols

For the purposes of the present document, the following symbols apply:

||	Concatenation
⊕	Exclusive or
f1	Message authentication function used to compute MAC
f2	Message authentication function used to compute RES and XRES
f3	Key generating function used to compute CK
f4	Key generating function used to compute IK
f5	Key generating function used to compute AK
f6	Encryption function used to encrypt the IMUI
f7	Decryption function used to decrypt the IMUI ($=f6^{-1}$)
K	Long-term secret key shared between the USIM and the AuC

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

3GMS	Third Generation Mobile Communication System
AK	Anonymity key
AUTN	Authentication token
AV	Authentication vector
CK	Cipher key
CS	Circuit switched
HE	Home Environment
HLR	Home Location Register
IK	Integrity key
IMUI	International Mobile User Identity
KSI	Key Set Identifier
KSS	Key Stream Segment
LAI	Location Area Identity
MAC	Message Authentication Code
MAC	The message authentication code included in AUTN, computed using f1
MS	Mobile Station
MSC	Mobile Services Switching Centre
MT	Mobile Termination
PS	Packet switched
TE	Terminal Equipment
TMUI	Temporary Mobile User Identity
RAND	Random challenge
SEQ	Sequence number
SN	Serving network
TMUI	Temporary Mobile User Identity

UEA	UMTS Encryption Algorithm
UIA	UMTS Integrity Algorithm
UN	User Name
USIM	User Services Identity Module
VLR	Visited Location Register
XRES	Expected response
XUR	Expected User Response

4 Overview of the security architecture

4.1 Overview of the complete 3G security architecture.

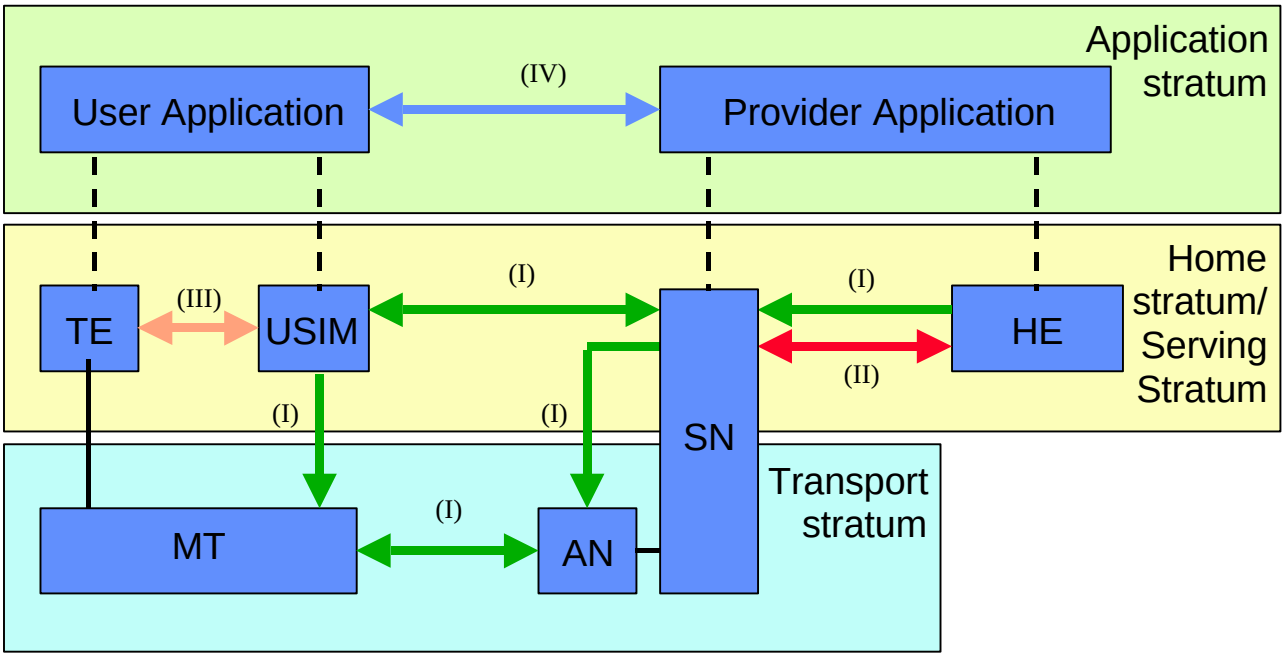

Figure 1 : Overview of the security architecture

Five security feature groups are defined. Each of these feature groups meets certain threats, accomplishes certain security objectives:

- **Network access security (I):** the set of security features that provide users with secure access to 3G services, and which in particular protect against attacks on the (radio) access link;
- **Network domain security (II):** the set of security features that enable nodes in the provider domain to securely exchange signalling data, and protect against attacks on the wireline network;
- **User domain security (III):** the set of security features that secure access to mobile stations
- **Application domain security (IV):** the set of security features that enable applications in the user and in the provider domain to securely exchange messages.

Visibility and configurability of security (V): the set of features that enables the user to inform himself whether a security features is in operation or not and whether the use and provision of services should depend on the security feature.

4.2 Overview of Authentication and Key Agreement Mechanism

Upon receipt of a request from the SN/VLR, the HE/AuC sends an ordered array of *n* authentication vectors (the equivalent of a GSM "triplet") to the SN/VLR.

When the SN/VLR initiates an authentication and key agreement, it selects the next authentication vector from the array and sends the parameters RAND and AUTN to the user. The USIM checks whether AUTN can be accepted and, if so, produces a response RES which is sent back to the SN/VLR. The USIM also computes CK and IK. The SN/VLR compares the received RES with XRES. If they match the SN/VLR considers the authentication and key agreement exchange to be successfully completed.

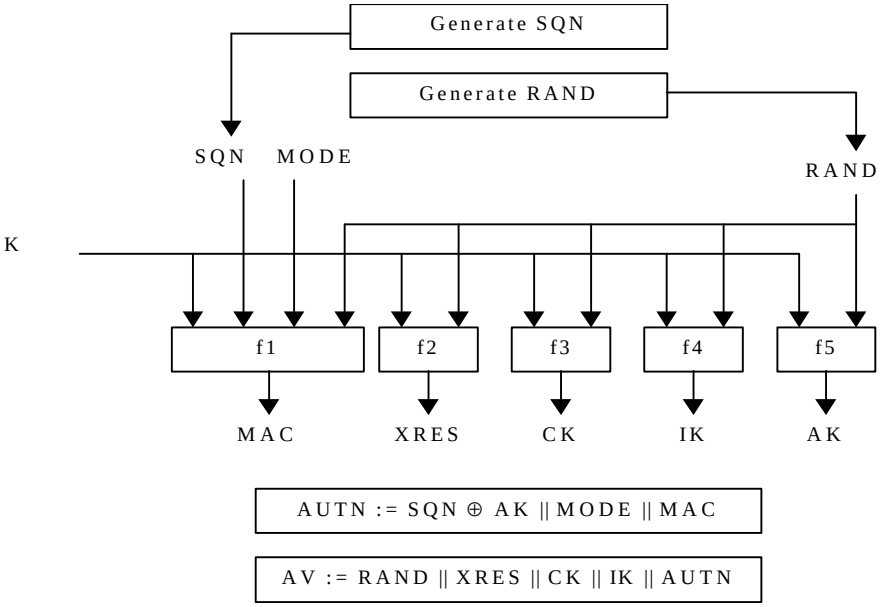

Figure 2: Generation of an authentication vector

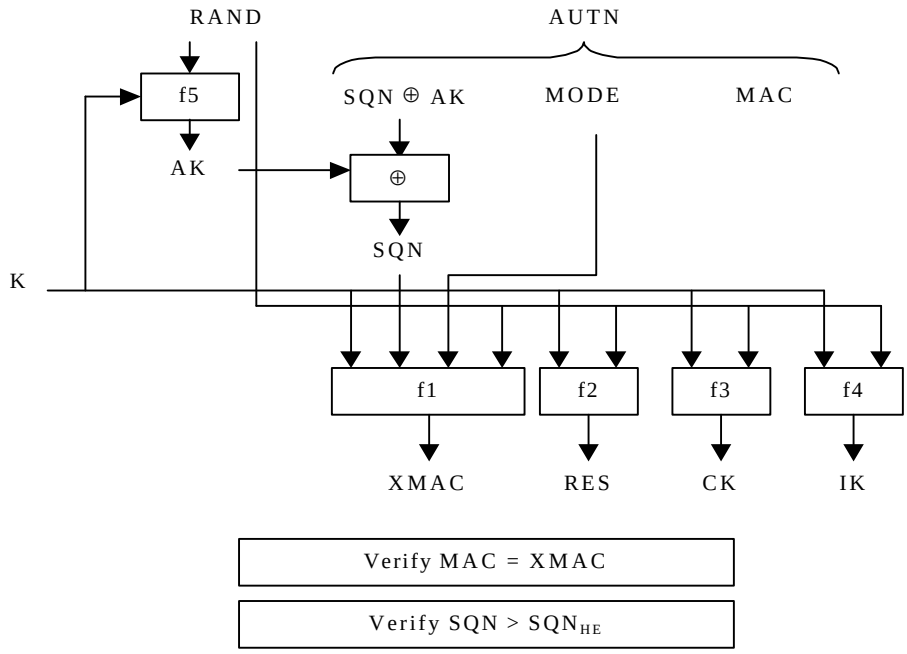

Figure 3: User authentication function in the USIM

5 Security Information Stored

5.1 Information common to Sequence Number and Temporary Key Mechanism

This Clause lists the security information to be stored in the relevant entities of the 3G system in terms of Static information and Dynamic information and relates to the preferred sequence number mechanism, the alternative temporary key mechanism is detailed in the Appendix. However, sections 5.1 contains information, which is common to both mechanisms.

Notes on tables

Parameter Lengths: The length of the parameters is given to allow estimates of the message sizes on the air interface to be determined and the maximum width for algorithm design. The effective key length used will be determined by national policy.

Lifetimes: The entry in the tables for parameter lifetime is defined in the table below

ref.	**Definition**
a	For the life of the equipment
b	Changed automatically at each new registration
c	Changed automatically at each new call
d	Lifetime dependent on Home Environment policy
e	Lifetime dependent on Serving Node policy
f	Lifetime dependent on User Policy
g	Lifetime Dependent on Manufacturer Policy

Identities: These are shown in the tables, but unless TSG SA WG3 have a specific security issue with the length uniqueness etc there are shown in Italics as these are defined in other TSG working groups. For example

IMUI	** 96 bits?*

5.1.1 Home Environment Authentication Center HE/AuC

Name	**Symbol**	**Parameter Length (actual or min-max)**	**Lifetime**
Long Term Secret Key	K	128 bits	a
User 1 permanent identity	*IMUI*	*	
User n permanent identity	*IMUI*	*	
Optional Enhanced user identity confidentiality			
Home Environment Id	He_id	32 bit	a
user 1			
Group Key	GK	128 bits	a
Group Identity	GI	32 bits	d
Sequence for UIC	SEQ_UIC	32 bits	c
Encrypted IMUI	EMUI	128 bit	c
user n			
Group Key	GK	128 bits	a
Group Identity	GI	32 bits	d
Sequence for UIC	SEQ_UIC	32 bits	c
Encrypted IMUI	EMUI	128 bit	c
Network Domain Security			
Network's own Private Key	PVTK	2048 bits	d,e
PKR_1 Public Key for network #1	$PUBK_1$	2048 bits	d,e
PKR_n Public Key for network #n	$PUBK_n$	2048 bits	d,e
Symmetric Send Key #i for sending data from X to Y	$KS_{XY}(i)$	128 bits	d,e
Symmetric Send Key #j for sending data from Y to X	KS_{YX} (j)	128 bits	d,e
Session key Sequence Number (for sending data from X to Y)	I	32 – 64 bits	d,e
Session key Sequence Number (for sending data from Y to X)	j	32 – 64 bits	d,e
Unpredictable Random Value generated by X	RND_X	128 bits	c
Unpredictable Random Value generated by Y	RND_y	128 bits	c

Name	Symbol	Parameter Length (actual or min-max)	Lifetime
Time Variant Parameter	TVP	64 bits	c
Network Operator Identifier A, B	X, Y	32 bits	a
Network-Wide User Traffic Confidentiality			
Access link cipher key (traffic)	Ka	128 bits	c
Access link cipher key (signaling)	Ka'	128 bits	c
Received access link cipher key	Kb	128 bits	c
Received access link cipher key (signaling)	Kb'	128 bits	c
NWUTC Session key	K_S	128 bits	c

5.1.2 Serving Node Visited Location Register SN/VLR

Name	Symbol	Parameter Length (actual or min-max)	Lifetime
Registered User1 Permanent Identity	*IMUI*		
Registered User1 Old Temporary Identity	$TMUI_o$	*	
Registered User1 New Temporary Identity	$TMUI_n$	*	
Optional Enhanced user identity confidentiality for user 1			
Encrypted IMUI	EMUI	128 bit	c
Home Environment Id	He_id	32 bit	a
Group Identity	GI	32 bits	d
Registered User n Permanent Identity	*IMUI*		
Registered User n Old Temporary Identity	$TMUI_o$	*	
Registered User n New Temporary Identity	$TMUI_n$	*	
Optional Enhanced user identity confidentiality for user n			
Encrypted IMUI	EMUI	128 bit	c
Home Environment Id	He_id	32 bit	a
Group Identity	GI	32 bits	d

Name	Symbol	Parameter Length (actual or min-max)	Lifetime
Network Domain Security			
Symmetric Send Key #i for sending data from X to Y	$KS_{XY}(i)$	128 bits	d,e
Symmetric Send Key #j for sending data from Y to X	KS_{YX} (j)	128 bits	d,e
Network-Wide User Traffic Confidentiality			
Access link cipher key (traffic)	Ka	128 bits	c
Access link cipher key (signaling)	Ka'	128 bits	c
Received access link cipher key	Kb	128 bits	c
Received access link cipher key (signaling)	Kb'	128 bits	c

5.1.3 Radio Node Controller RNC

Name	Symbol	Parameter Length (actual or min-max)	Lifetime
Cipher Key – Circuit switched	CK_{CS}	128 bits	c
Cipher Key – Packet switched	CK_{PS}	128 bits	c
Integrity key	IK	128 bits	c
Access link cipher key (traffic)	Ka	128 bits	**c**
Access link cipher key (signaling)	Ka'	128 bits	**c**
Received access link cipher key	Kb	128 bits	c
Received access link cipher key (signaling)	Kb'	128 bits	c

5.1.3 Mobile Equipment user Identify Module USIM

Name	**Symbol**	**Parameter Length actual or min-max**	Lifetime
Long Term Secret Key	K	128 bits	a
User Permanent Individual Identity	*IMUI*	*****	
Registered User Old Temporary Identity	$TMUI_o$	*	
Registered User New Temporary Identity	$TMUI_n$	*	
Optional Enhanced user identity confidentiality			
Home Environment Id	He_id	32 bits	a
Group Key	GK	128 bits	a
Group Identity	GI	32 bits	d
Sequence for UIC	SEQ_UIC	32 bits	c
Encrypted IMUI	EMUI	128 bits	c
Cipher Key – Circuit switched	CK_{CS}	128 bits	c
Cipher Key – Packet switched	CK_{PS}	128 bits	c
Integrity Key	IK	128 bits	c
Key set identifier	KSI	32 bits	c
Cipher Key Lifetime	$LIFE_{CKCS}$	32 bits	d
Integrity Key Lifetime	$LIFE_{IKCS}$	32 bits	d
Cipher Key Use Counter – Circuit switched	USE_{CKCS}	32 bits	a
Integrity Key Use Counter – Circuit switched	USE_{IKCS}	32 bits	a
User-User authentication User Name 1	UN	32 bits	f
User Response	UR_{UN}	32 bits	f
Expected User Response	XUR_{UN}	32 bits	f
1st New User Response	$NUR1_{UN}$	32 bits	f
2nd New User Response	$NUR2_{UN}$	32 bits	f
User Authentication Failure Counter	$UUAFAIL_{UN}$	32 bits	a
User Authentication Failure limit	$UUAFLIM_{UN}$	32 bits	d
User Authentication Enable Status	$UUASTATE_{UN}$	1 bit	f
User Authentication Block	$UUABLOCK_{UN}$	1 bit	f

Name	Symbol	Parameter Length (actual or min-max)	Lifetime
Terminal Lock User Name 1	UN1	32 bits	f
Terminal Lock User Name 2	UN2	32 bits	f
Terminal- USIM Lock Password	V1	32 bits	f
Lock Disable Password	V2	32 bits	f
Lock Enable/Disable Failure Counter	LOCKFAIL	32 bits	a
Terminal Lock Counter	LOCKCOUNT	32 bits	a
Lock Enable/Disable Failure Counter Limit	LOCKEDFLIM	32 bits	d
Terminal Lock Failure Counter Limit	LOCKFLIM	32 bits	d
Terminal Lock Enable Status	LOCKSTATE	1 bit	f
Terminal Lock	LOCK	1 bit	f

5.1.4 Mobile Equipment ME

Name	Symbol	Parameter Length (actual or min-max)	Lifetime
Terminal- USIM Lock Password	XV1	32 bits	f
Lock Disable Password	XV2	32 bits	f
Cipher Key Circuit Switched	CK_{CS}	128 bits	c
Cipher Key Packet Switched	CK_{PS}	128 bits	c
Integrity Key	IK	128 bits	c
Access link cipher key (traffic)	Ka	128 bits	**c**
Received access link cipher key	Kb	128 bits	c
NWUTC Session key	K_S	128 bits	c

5.2 Sequence Number Mechanism

5.2.1 Home Environment Authentication Center HE/AuC

Name	**Symbol**	**Parameter Length (actual or min-max)**	**Lifetime**
Sequence Number	SQN	32-64 bits	d
Anonymity Key	AK	32-64 bits	d
Message Authentication Code	MAC	64 bits	
AV1 Random Number	RAND	128 bits	c
Expected Response	XRES	64 bits	c
Cipher Key	CK	128 bits	c
Integrity Key	IK	128 bits	c
Authentication Token	AUTN	97- 129 bits	c
AVn Random Number	RAND	128 bits	c
Expected Response	XRES	64 bits	c
Cipher Key	CK	128 bits	c
Integrity Key	IK	128 bits	c
Authentication Token	AUTN	97- 129 bits	c
Key set identifier	KSI	32 bits	d
Message authentication Code	MAC	64 bits	c
Anonymity Key	AK	32-64 bits	c
Mode	MODE	1 bit	c
Option 1			
User 1 Counter- Circuit switched	$SQN_{HE/CS}$	32 bits	d
User 1 Counter – Packet switched	$SQN_{HE/PS}$	32 bits	d
User n Counter- Circuit switched	$SQN_{HE/CS}$	32 bits	d
User n Counter – Packet switched	$SQN_{HE/PS}$	32 bits	d
Option 2			
Global Counter	SQN_{he}	32 bits	d

The Authentication center will store 10 Authentication vectors

5.2.2 Serving Node Visited Location Register SN/VLR

Name	Symbol	Parameter Length (actual or min-max)	Lifetime
AV1 Random Number	RAND	128 bits	c
Expected Response	XRES	64 bits	c
Cipher Key	CK	128 bits	c
Integrity Key	IK	128 bits	c
Authentication Token	AUTN	97-129 bits	c
AVn Random Number	RAND	128 bits	c
Expected Response	XRES	64 bits	c
Cipher Key	CK	128 bits	c
Integrity Key	IK	128 bits	c
Authentication Token	AUTN	97 –129 bits	c

5.2.3 Radio Node Controller RNC

Name	Symbol	Parameter Length (actual or min-max)	Lifetime
See Common items section 5.1			

5.2.4 Mobile Equipment user identity Module USIM

Name	Symbol	Parameter Length (actual or min-max)	Lifetime
Received Random Number	RAND	128 bits	c
Received Authentication Token	AUTN	97–129 bits	c
Computed Anonymity Key	AK	32-64 bits	c
Computed Message authentication Code	XMAC	64 bits	c
Retrieved Sequence Number	SQN	32-64 bits	c
Computed Response	RES	32-64 bits	c
- and common items – section 5.1			
Option 1			
Counter- Circuit switched	$SQN_{MS/CS}$	32 bits	d
Counter – Packet switched	$SQN_{MS/PS}$	32 bits	d
Option 2			
Sequence Number Window- Circuit switched	$SQN_{MS/CS}$ - W	10	c
Sequence Number Window- Packet switched	$SQN_{MS/PS}$ - W	10	c
Option 3			
Sequence Number List – Circuit switched	$LIST_{SQNCS}$	10	c
Sequence Number List – Packet switched	$LIST_{SQNPS}$	10	c

5.2.5 Mobile Equipment ME

Name	Symbol	Parameter Length (actual or min-max)	Lifetime
See common items – section 5.1			

6 Location of Security Functions

6.1 Sequence Number Mechanism

6.1.1 Home Environment Authentication Center HE/AuC

Name	Symbol	**Input Parameters**
Algorithms		
Message Authentication Function	F1	Input: K,SQN,RAND,MODE Output: MAC
Message Authentication Function	F2	Input: K,RAND Output: XRES
Cipher Key Generating Function	F3	Input: K,RAND Output: CK
Integrity Key Generating Function	F4	Input: K, RAND Output: IK
Anonymity Key Generating Function	F5	Input: K, RAND Output: AK
Identity Decryption Function	F7	Input: GK, EMUI Output: SEQ_UIC IMUI
Block Encryption Algorithm for Network Operators	BEANO	Input: KS_{XY}, Data Output: Encrypted data
Secure Hash Function	HASH	Input: Data Output: hashed data
Public Key encryption Function	E_PK(data)	Input: PK, data Output: edata
Public Key decryption Function	D_SK(edata)	Input: SK, edata Output: data

6.1.2 Serving Node Visited Location Register SN/VLR

Name	Symbol	**Input Parameters**
Algorithms		
Block Encryption Algorithm for Network Operators	BEANO	Input: KS_{XY}, Data Output: Encrypted data
Secure Hash Function	HASH	Input: Data Output: hashed data
Public Key encryption Function	E_PK(data)	Input: PK, data Output: edata
Public Key decryption Function	D_SK(edata)	Input: SK, edata Output: data

6.1.3 Radio Node Controller RNC

Name	Symbol	**Input Parameters**
Algorithms		
Encryption algorithm	UEA	Input: Count, Direction Bearer, Length, CK Output: Keystream
Integrity algorithm	UIA	Input: Message, Count, Fresh, IK Output: MAC

6.1.4 Mobile Equipment user identity Module USIM

Name	Symbol	**Input Parameters**
Algorithms		
Message Authentication Function	F1	Input: K,SQN,RAND, MODE Output: XMAC
Message Authentication Function	F2	Input: K,RAND Output: RES
Cipher Key Generating Function	F3	Input: K,RAND Output: CK
Integrity Key Generating Function	F4	Input:

		K,RAND Output: IK
Anonymity Key Generating Function	F5	Input: AK,SQNAK Output: SQN
Integrity algorithm	UIA	

6.1.5 Mobile Equipment ME

Name	Symbol	**Input Parameters**
Algorithms		
Encryption algorithm	UEA	Input: Count, Direction Bearer, Length, CK Output: Keystream
Integrity algorithm	UIA	Input: Message, Count, Fresh, IK Output: MAC
Network-wide user traffic confidentiality Algorithm	UNA	Input: IV, K_S Output: Keystream

Appendix 1 Temporary Key Mechanism

When the mobile first requests service from the SN/VLR, a random seed RSu created by the user (USIM or terminal) is included in the request message. The message including RSu is forwarded to the HE/AuC, which generates its own random challenge RSn. An authentication vector is returned to the SN/VLR. The vector contains {RSn, RES1, XRES2, KT}, where RES1 is the response to the user's challenge, XRES2 is the response to the network's challenge which is expected from the user, and KT is the temporary authentication key shared with the SN/VLR. The network's challenge RSn and the network authentication response RES1 are sent to the MS. If the MS verifies RES1, thereby authenticating the identity of the network, it responds with RES2 and generates the new temporary key KT. The SN/VLR then verifies that RES2 equals XRES2, thereby authenticating the identity of the USIM, and stores the new temporary key KT. Furthermore, both the USIM and the SN/VLR immediately use KT with the random seeds RSu and RSn to generate the first session keys CK and IK. This process is shown in Figure 4 below.

Figure 5 shows how the SN/VLR can offer secure service to the USIM without reference to the home system HE/AuC by using the temporary key KT.

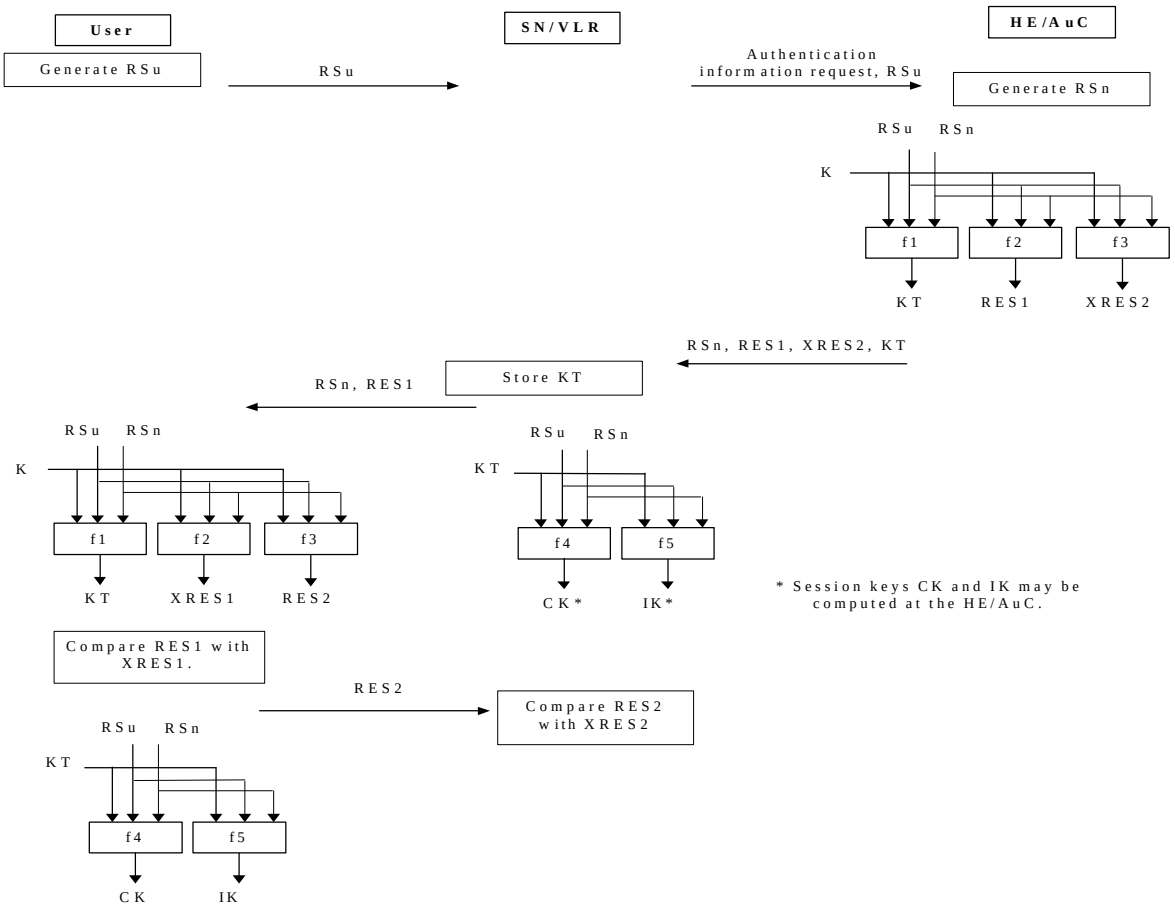

Figure 4: Temporary Key Generation Protocol

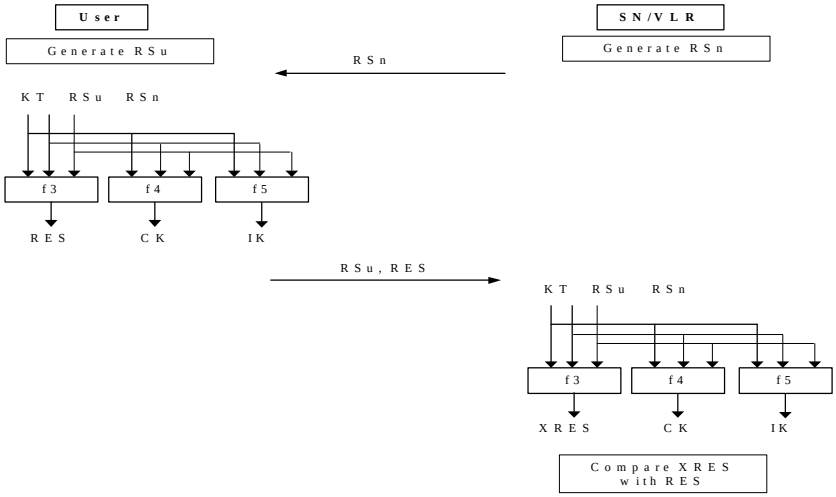

Figure 5. Locally authenticated session key agreement

A1 Security Information stored

A1.1 Home Environment Authentication Centre HE/AuC

Name	**Symbol**	**Parameter Length (actual or min-max)**	**Lifetime**
Dynamic Information			
Random Seed User	RS_U	128 bits	b
AV1Random Seed Network	RS_N	128 bits	b
Response to User Challenge RS_U	RES1	32-64 bits	b
Response to Nwk Challenge RS_N	XRES2	64 bits	b
Temporary Key	KT	128 bits	b
AVn Random Seed Network	RS_N	128 bits	b
Response to User Challenge RS_U	RES1	32-64 bits	b
Response to Nwk Challenge RS_N	XRES2	64 bits	b
Temporary Key	KT	128 bits	b
Fixed Initial Value	PAR1	TBD	a
Fixed Initial Value	PAR2	TBD	a
Fixed Initial Value	PAR3	TBD	a
Fixed Initial Value	PAR4	TBD	a
Fixed Initial Value	PAR5	TBD	a
- and common items – section 5.1			

A1.2 Serving Node Visited Location Register SN/VLR

Name	**Symbol**	**Parameter Length (actual or min-max)**	**Lifetime**
Dynamic Information			
Temporary Key	KT	128 bits	b
Random Seed User	RS_U	128 bits	b
Random Seed Network	RS_N	128 bits	b
Response to Users Challenge	RES1	32-64 bits	b
Response to Network Challenge	RES2	32-64 bits	b
Response to Network Challenge	XRES2	64 bits	b
Cipher Key	CK*	128 bits	b
Integrity Key	IK*	128 bits	b
Response to SN/VLR challenge (local)	RES	32-64 bits	b
Expected response to challenge	XRES	64 bits	b

* May be computed at HE/AuC

A1.3 Radio Node Controller RNC

Name	**Symbol**	**Parameter Length (actual or min-max)**	**Lifetime**
See common items – section 5.1			

A1.4 Mobile Equipment user identity Module USIM

Name	**Symbol**	**Parameter Length (actual or min-max)**	**Lifetime**
Dynamic Information			
Temporary Key	KT	128 bits	b
Random Seed User	RS_U	128 bits	b
Random Seed Network	RS_N	128 bits	b
Computed Response (local authent.)	RES	32-64 bits	b
Response to Users Challenge	RES1	32-64 bits	b
Response to Network Challenge	RES2	32-64 bits	b
Expected response from SN/VLR	XRES1	64 bits	b
- and common items – section 5.1			

A1.5 Mobile Equipment

Name	**Symbol**	**Parameter Length (actual or min-max)**	**Lifetime**
See common items – section 5.1			

A2 Location of Security Functions

A2.1 Home Environment Authentication Centre HE/AuC

Name	**Symbol**	**Input Parameters**
Algorithms		
Key Generating Function	F1	Input: K, RS_U, RS_N Output: KT
Message Authentication Function	F2	Input: K, RS_U, RS_N Output: RES1
Message Authentication Function	F3	Input: K, RS_U , RS_N Output: XRES1
Identity Decryption Function	F7	Input: GK, EMUI Output: SEQ_UIC IMUI
Block Encryption Algorithm for Network Operators	BEANO	Input: KS_{XY}, Data Output: Encrypted data
Secure Hash Function	HASH	Input: Data Output: hashed data
Public Key encryption Function	E_PK(data)	Input: PK, data Output: edata
Public Key decryption Function	D_SK(edata)	Input: SK, edata Output: data

A2.2 Serving Node Visited Location Register SN/VLR

Name	**Symbol**	**Input Parameters**
Algorithms		* May be computed at HE/AuC
Message Authentication Function (local authentication only)	F3	Input: KT, RS_U, RS_N Output: XRES
Cipher Key Generating Function	F4	Input: KT, RS_U, RS_N Output: CK*
Integrity Key Generating Function	F5	Input: KT, RS_U,RS_N Output: IK*
Block Encryption Algorithm for Network Operators	BEANO	Input: KS_{XY}, Data Output: Encrypted data
Secure Hash Function	HASH	Input: Data Output: hashed data
Public Key encryption Function	E_PK(data)	Input: PK, data Output: edata
Public Key decryption Function	D_SK(edata)	Input: SK, edata Output: data

A2.3 Radio Node Controller RNC

Name	**Symbol**	**Input Parameters**
Algorithms		
Encryption algorithm	UEA	Input: Count, Direction Bearer, Length, CK Output: Keystream
Integrity algorithm	UIA	Input: Message, Count, Fresh, IK Output: MAC

A2.4 Mobile Equipment user identity Module USIM

Name	**Symbol**	**Input Parameters**
Algorithms		
Key generating function	F1	Input: K, RS_U, RS_N Output: KT
Message Authentication Function	F2	Input: K, RS_U, RS_N Output: XRES1
Message Authentication Function	F3	Input: K, RS_U, RS_N Output: RES2
Message Authentication Function (for local authentication)	F3	Input: KT, RS_U, RS_N Output: RES
Cipher Key Generating Function	F4	Input: KT, RS_U, RS_N Output: CK
Integrity Key Generating Function	F5	Input: KT, RS_U RS_N Output: IK

A2.5 Mobile Equipment ME

Name	Symbol	**Input Parameters**
Algorithms		
Encryption algorithm	UEA	Input: Count, Direction Bearer, Length, CK Output: Keystream
Integrity algorithm	UIA	Input: Message, Count, Fresh, IK Output: MAC
Network-wide user traffic confidentiality Algorithm	UNA	Input: IV, K_S Output: Keystream

Appendix 2 Document history

Document history		
0.0.0	2nd May 1999	Initial draft: Rapporteur- Colin Blanchard
0.0.1	28th May 1999	After review at TSG SA WG3 #3 Bonn 11- 12th May 1999
0.0.2	11th June 1999	To incorporate comments from Takeshi Igarashi, Adam Berenzweig, Benno Tietz, Takeshi Chikazawa