3GPP TSG CT Meeting #28 **CP-050066**
1st – 3rd June 2005. Quebec, CANADA.

Source: **TSG CT WG1**

Title: **CRs on Rel-6 WI "SEC1-SC" for TS 24.109**

Agenda item: **9.3**

Document for: **APPROVAL**

This document contains 4 **CRs for Rel-6 WI "SEC1-SC"**, that have been agreed by TSG CT WG1 meeting #38 and forwarded to TSG CT Plenary meeting #28 for approval.

TDoc #	Tdoc Title	Spec	CR #	Rev	CAT	C_Version	WI	Rel
C1-050730	Format of lifetime values	24.109	13	1	F	6.2.0	SEC1-SC	Rel-6
C1-050731	User identify reference	24.109	15	1	F	6.2.0	SEC1-SC	Rel-6
C1-050609	Key material - Ks only	24.109	16		F	6.2.0	SEC1-SC	Rel-6
C1-050807	Usage of Ks_int_NAF	24.109	17	1	F	6.2.0	SEC1-SC	Rel-6

3GPP TSG-CT1 Meeting #38
Cancun, Mexico, 25-29 April 2005

Tdoc C1-050609

CR-Form-v7.1

CHANGE REQUEST

⌘ **24.109** **CR** **16** ⌘ **rev** **-** ⌘ Current version: **6.2.0** ⌘

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

Proposed change affects: UICC apps⌘ ☐ ME ☐ Radio Access Network ☐ Core Network ☒

Title:	⌘	Key material – Ks only
Source:	⌘	Nokia
Work item code:	⌘	SEC1-SC
Date:	⌘	16/04/2005
Category:	⌘	**F**
Release:	⌘	Rel-6

Use one of the following categories:
F *(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:

Ph2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*
Rel-7	*(Release 7)*

Reason for change:	⌘	SA3 agreed to optimize key derivation procedures (Ks_int_NAF and Ks_ext_NAF can be directly derived from Ks).
Summary of change:	⌘	Ks_int_NAF/Ks_ext_NAF are derived directly from Ks.
Consequences if not approved:	⌘	Misalignment with TS 33.220

Clauses affected:	⌘	5.2.2, A.3, B.2.1, D.2, E.2.1, F.2.1

Other specs affected: ⌘	Y	N		⌘
		X	Other core specifications	
		X	Test specifications	
		X	O&M Specifications	

Other comments: ⌘

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm.
Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be

downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

5.2.2 Authentication procedure

5.2.2.1 General

HTTP Digest authentication [9] shall be used with previously bootstrapped security association as follows:

- the "username" parameter shall be the bootstrapping transaction identifier;
- the password used in the digest calculations shall be the NAF specific key material (Ks_NAF) in the case of GBA_ME, and the NAF specific external key material (Ks_ext_NAF) in the case of GBA_U. The NAF specific key material (Ks_NAF or Ks_ext_NAF) is Base64 encoded as specified in RFC 3548 [10]; and

NOTE 1: The NAF specific key material (Ks_NAF or Ks_ext_NAF) is derived from the key material (Ks ~~or Ks_ext~~) using key derivation function as specified in 3GPP TS 33.220 [1].

NOTE 2: The NAF specific internal key material (Ks_int_NAF) in the case of GBA_U shall not be used with HTTP Digest authentication.

- the "realm" parameter shall contain two parts delimited by "@" sign. The first part is a constant string "3GPP-bootstrapping", and the latter part shall be the FQDN of the NAF (e.g. "3GPP-bootstrapping@naf1.operator.com").

Both the UE and the NAF shall verify upon receiving each of the HTTP responses and HTTP requests that the second part of the realm attribute is equal to the FQDN of the NAF.

An example flow of a successful HTTP Digest authentication procedure can be found in clause B.3.

---------- NEXT CHANGE ----------

A.3 Signalling flows demonstrating a successful bootstrapping procedure

The overall bootstrapping procedure in successful case is presented in figure A.3-1. The bootstrapping Zh interface performs the retrieval of an authentication vector by BSF from the HSS. The procedure corresponds to the step 2 in figure A.3-1.

This clause specifies in detail the format of the bootstrapping procedure that is further utilized by various applications. It contains the AKA authentication procedure with BSF, and later the bootstrapping key material generation procedure.

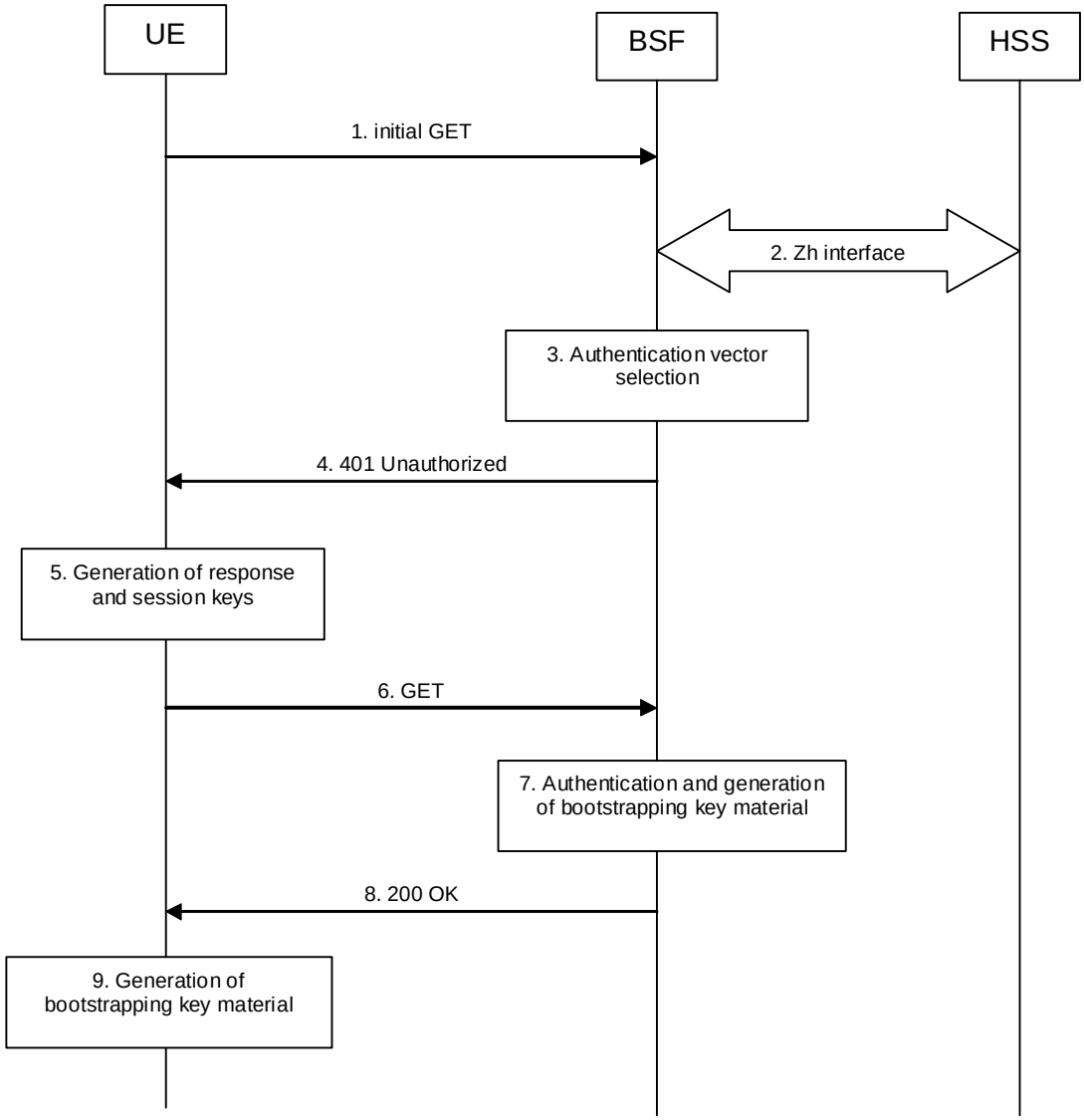

Figure A.3-1: Bootstrapping signalling

1. **Initial GET request (UE to BSF) - see example in table A.3-1**

   The purpose of this message is to initiate bootstrapping procedure between the UE and BSF. The UE sends an HTTP request containing the private user identity towards its home BSF.

Table A.3-1: Initial GET request (UE to BSF)

```
GET / HTTP/1.1
Host: registrar.home1.net:9999
User-Agent: Bootstrapping Client Agent; Release-6
Date: Thu, 08 Jan 2004 10:13:17 GMT
Accept: */*
Referer: http://pki-portal.home1.net:2311/pkip/enroll
Authorization: Digest username="user1_private@home1.net", realm="registrar.home1.net", nonce="",
uri="/", response=""
```

Request-URI: The Request-URI (the URI that follows the method name, "GET", in the first line) indicates the resource indication of this GET request. For bootstrapping server, this is by default "/".

Host: Specifies the Internet host and port number of the BSF server, obtained from the original URI given by referring resource.

User-Agent: Contains information about the user agent originating the request.

Date: Represents the date and time at which the message was originated.

Accept: Media types which are acceptable for the response.

Referer: Allows the user agent to specify the address (URI) of the resource from which the bootstrapping procedure was initiated.

Authorization: It carries authentication information. The private user identity (user1_private@home1.net) is carried in the username field of the Digest AKA protocol. The "uri" parameter (directive) contains the same value as the Request-URI. The ”realm” parameter (directive) contains the network name where the username is authenticated. The Request-URI and the "realm" parameter (directive) value are obtained from the same field in the USIM and therefore, are identical. In this example, it is assumed that a new UICC card was just inserted into the terminal, and there is no other cached information to send. Therefore, "nonce" and "response" parameters (directives) are empty.

2. **Zh: Authentication procedure**

BSF retrieves the corresponding AVs from the HSS.

For detailed signalling flows see 3GPP TS 29.109 [3].

Table A.3-2: BSF authentication information procedure (BSF to HSS)

Message source and destination	Zh Information element name	Information Source in GET	Description
BSF to HSS	Private User Identity	Authorization:	The Private User Identity is encoded in the username field according to the Authorization protocol.

3. **Authentication vector selection**

The BSF selects an authentication vector for use in the authentication challenge. For detailed description of the authentication vector, see 3GPP TS 33.203 [21].

NOTE 1: The authentication vector can be of the form as in 3GPP TS 33.203 [21] (if IMS AKA is the selected authentication scheme):

- $AV = RAND_n||AUTN_n||XRES_n||CK_n||IK_n$ where:
  - RAND: random number used to generate the XRES, CK, IK, and part of the AUTN. It is also used to generate the RES at the UE.
  - AUTN: Authentication token (including MAC and SQN); 128 bit value generated by the HSS.
  - XRES: Expected (correct) result from the UE.
  - CK: Cipher key (optional).
  - IK: Integrity key.

4. **401 Unauthorized response (BSF to UE) - see example in table A.3-3**

BSF forwards the challenge to the UE in HTTP 401 Unauthorized response (without the CK, IK and XRES). This is to demand the UE to authenticate itself. The challenge contains RAND and AUTN that are populated in nonce field according to RFC 3310 [6].

Table A.3-3: 401 Unauthorized response (BSF to UE)

```
HTTP/1.1 401 Unauthorized
Server: Bootstrapping Server; Release-6
Date: Thu, 08 Jan 2004 10:13:17 GMT
WWW-Authenticate: Digest realm="registrar.home1.net", nonce= base64(RAND + AUTN + server specific
data), algorithm=AKAv1-MD5, qop="auth-int"
```

Server: Contains information about the software used by the origin server (BSF).

Date: Represents the date and time at which the message was originated.

WWW-Authenticate: The BSF challenges the user. The nonce includes the quoted string, base64 encoded value of the concatenation of the AKA RAND, AKA AUTN and server specific data.

NOTE 2: The actual nonce value in the WWW-Authenticate header field is encoded in base64, and it can look like: nonce="A34Cm+Fva37UYWpGNB34JP".

5. **Generation of response and session keys at UE**

Upon receiving the Unauthorized response, the UE extracts the MAC and the SQN from the AUTN. The UE calculates the XMAC and checks that XMAC matches the received MAC and that the SQN is in the correct range. If both these checks are successful the UE calculates the authentication challenge response (using RES and other parameters as defined in RFC 3310 [6]), and also computes the session keys IK and CK. The authentication challenge response is put into the Authorization header and sent back to the BSF in the GET request.

6. **GET request (UE to BSF) - see example in table A.3-4**

The UE sends an HTTP GET request again, with the RES, which is used for response calculation, to the BSF.

Table A.3-4: GET request (UE to BSF)

```
GET / HTTP/1.1
Host: registrar.home1.net:9999
User-Agent: Bootstrapping Client Agent; Release-6
Date: Thu, 08 Jan 2004 10:13:18 GMT
Accept: */*
Referer: http://pki-portal.home1.net:2311/pkip/enroll
Authorization: Digest username="user1_private@home1.net", realm="registrar.home1.net",
nonce=base64(RAND + AUTN + server specific data), uri="/", qop=auth-int, nc=00000001,
cnonce="6629fae49393a05397450978507c4ef1", response="6629fae49393a05397450978507c4ef1",
opaque="5ccc069c403ebaf9f0171e9517f30e41", algorithm=AKAv1-MD5
```

Authorization: This carries the response to the authentication challenge received in step 4 along with the private user identity, the realm, the nonce, the URI, the qop, the NC, the cnonce, the response, the opaque, and the algorithm.

7. **Authentication and generation of key material at BSF**

Upon receiving an integrity protected GET request carrying the authentication challenge response, the BSF checks that the expected response (calculated by the BSF using XRES and other parameter as defined in RFC 3310 [6]) matches the received challenge response. If the check is successful then the user has been authenticated and the private user identity is registered in the BSF.

The BSF generates the bootstrapping transaction identifier (B-TID) for the IMPI and stores the tuple <B-TID,IMPI,CK,IK>.

For detailed bootstrapping key material generation procedure see 3GPP TS 33.220 [1].

8. **200 OK response (BSF to UE) - see example in table A.3-5**

The BSF sends 200 OK response to the UE to indicate the success of the authentication.

Table A.3-5: 200 OK response (BSF to UE)

```
HTTP/1.1 200 OK
Server: Bootstrapping Server; Release-6
Authentication-Info: qop=auth-int, rspauth="6629fae49394a05397450978507c4ef1",
cnonce="6629fae49393a05397450978507c4ef1", nc=00000001
Date:
Expires: Thu, 08 Jan 2004 10:23:17 GMT
Content-Type: application/vnd.3gpp.bsf+xml
Content-Length: (...)

<?xml version="1.0" encoding="UTF-8"?>
<BootstrappingInfo xmlns="uri:3gpp-gba">
  <btid>user@bsf.operator.com</btid>
```

```
  <lifetime>2004-05-28T13:20:00-05:00</lifetime>
</BootstrappingInfo>
```

Content-Type: Contains the media type of the entity body.

Content-Length: Indicates the size of the entity-body, in decimal number of OCTETs, sent to the recipient.

Authentication-Info: This carries the server authentication information. The header includes the "rspauth" parameter which is calculated as specified in RFC 2617 [9] using RES for response calculation as specified in RFC 3310 [6].

Expires: Gives the date/time after which the response is considered stale.

9. **Generation of key material at UE**

The key material Ks is generated in UE by concatenating CK and IK. The NAF specific key material (Ks_NAF ~~is derived from Ks~~ in the case of GBA_ME, or Ks_ext_NAF ~~is derived from Ks_ext~~ in the case of GBA_U) is derived from Ks, and used for securing the Ua interface. The UE stores the tuple <B-TID,Ks_NAF> or <B-TID,Ks_ext_NAF>.

For detailed bootstrapping key material generation procedure for NAF specific key (Ks_NAF or Ks_ext_NAF) see 3GPP TS 33.220 [1].

---------- NEXT CHANGE ----------

B.2.1 General

A bootstrapping session established using a bootstrapping procedure (cf. clause 4 and annex A) is used between a UE and a NAF. The BSF provides to the NAF a NAF specific key material (Ks_NAF or Ks_ext_NAF) which is derived from the key material (Ks ~~or Ks_ext~~). The NAF uses this key to authenticate and optionally secure (i.e. integrity protect and encrypt) the communications between it and the UE. The BSF will also provide the NAF the expiration time of the bootstrapping session. When the bootstrapping session becomes invalid the NAF will stop using the session, and indicate to the UE that bootstrapping session has expired and that new session needs to be established.

An example of the signalling flows of the authentication procedure using HTTP Digest authentication [9] is given in clause B.3.

---------- NEXT CHANGE ----------

D.2 Introduction

A bootstrapping session (established using a bootstrapping procedure, cf. clause 4 and annex A) is used between a UE and an authentication proxy (AP) that is functioning as a NAF. The BSF provides to the AP an AP specific key material (Ks_NAF or Ks_ext_NAF) which is derived from the key material (Ks ~~or Ks_ext~~). The AP uses this key to authenticate and optionally secure (i.e. integrity protect with HTTP Digest using "auth-int" qop option, or integrity protect and encrypt with PSK TLS) the communications between it and the UE. The BSF will also provide the AP the expiration time of the bootstrapping session. When the bootstrapping session becomes invalid the AP will stop using the session, and indicate to the UE that bootstrapping session has expired and that new session needs to be established.

The AP functions as a reverse proxy. After the AP has authenticated and optionally secured the communcation between it and the UE, the AP will forward the incoming HTTP requests from the UE to the correct appliation server (AS) behind the AP. There can be multiple application servers behind the AP.

NOTE: As consequence of the fact that the UE assumes it is communicating with the AS, not the AP, the AP might need to use different Ks_NAF keys per UE because (i) the UE will use the hostname of the AS (i.e., NAF_ID) when deriving the Ks_NAF key, (ii) the AP is doing virtual name based hosting, i.e., has reverse proxy functionality, and (iii) the UE can communicate through the AP with several ASes at the same time.

An example of the signalling flows of the authentication procedure between a UE, an AP, and an AS is given in clause D.3.

---------- NEXT CHANGE ----------

E.2.1 General

A bootstrapping session established using a bootstrapping procedure (cf., clause 4 and annex A) is used between a UE and a PKI portal. The BSF provides to the PKI portal a NAF specific key material (Ks_NAF or Ks_ext_NAF) which is derived from the key material (Ks ~~or Ks_ext~~). The PKI portal uses this key to authenticate and optionally secure (i.e. integrity protect and encrypt) the communications between it and the UE. The BSF will also provide the PKI portal the expiration time of the bootstrapping session.

---------- NEXT CHANGE ----------

F.2.1 General

A bootstrapping session established using a bootstrapping procedure (cf., clause 4 and annex A) is used between a UE and a NAF. The BSF provides to the NAF a NAF specific key material (Ks_NAF or Ks_ext_NAF) which is derived from the key material (Ks ~~or Ks_ext~~). The NAF uses this key to authenticate and optionally secure (i.e. integrity protect and encrypt) the communications between it and the UE. The BSF will also provide the NAF the expiration time of the bootstrapping session. When the bootstrapping session becomes invalid the NAF will stop using the session, and indicate to the UE that bootstrapping session has expired and that new session needs to be established.

An example of the signalling flows of the authentication procedure using PSK TLS [15] is given in clause F.3.

3GPP TSG-CT1 Meeting #38
Cancun, Mexico, 25-29 April 2005

Tdoc C1-05050730

CR-Form-v7.1

CHANGE REQUEST

⌘ **24.109** **CR** **013** ⌘ **rev** **1** ⌘ Current version: **6.2.0** ⌘

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

Proposed change affects: UICC apps⌘ ☐ ME ☐ Radio Access Network ☐ Core Network ☒

Title:	⌘	Format of lifetime values
Source:	⌘	Siemens
Work item code:	⌘	SEC1-SC
Date:	⌘	05/04/2005
Category:	⌘	**F**
Release:	⌘	Rel-6

Use one of the following categories:
F *(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:

Ph2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*
Rel-7	*(Release 7)*

Reason for change:	⌘	The current definition of lifetime only gives the format datetime but does not require the timezone within this format. Without a mandatory timezone indication there will be different interpretations of the value lifetime in the UE and on the Zn interface.
Summary of change:	⌘	Specified that values of lifetime must be expressed in UTC.
Consequences if not approved:	⌘	Interworking problems

Clauses affected:	⌘	3.2, Annex A.3, Annex C			
		Y	**N**		
Other specs affected:	⌘		**X**	Other core specifications	⌘
			X	Test specifications	
			X	O&M Specifications	
Other comments:	⌘				

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm.
Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

**** 1st change ****

3.2 Abbreviations

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

AKA	Authentication and Key Agreement
AP	Authentication Proxy
AS	Application Server
AUTN	Authentication Token
AUTS	Re-synchronisation Token
AV	Authentication Vector
BSF	BootStrapping Function
B-TID	Bootstrapping - Transaction IDentifier
CA	Certification Authority
CK	Confidentiality Key
DER	Distinquished Encoding Rules
FQDN	Fully Qualified Domain Name
GAA	Generic Authentication Architecture
GBA	Generic Bootstrapping Architecture
HSS	Home Subscriber System
IK	Integrity Key
IMPI	IP Multimedia Private Identity
IMPU	IP Multimedia PUblic identity
Ks	Key material
Ks_NAF	NAF specific key material
MAC	Message Authentication Code
NAF	Network Application Function
PKCS	Public-Key Cryptography Standards
PKI	Public Key Infrastructure
PSK	Pre-Shared Secret
RAND	RANDom challenge
RES	authentication Response
SQN	SeQuence Number
TLS	Transport Layer Security
UE	User Equipment
URI	Uniform Resource Identifier
URN	Uniform Resource Name
USIM	User Service Identity Module
UTC	Coordinated Universal Time
WIM	Wireless Identity Module
WPKI	Wireless PKI
WTLS	Wireless Transport Layer Security
XRES	Expected authentication response

**** next change ****

A.3 Signalling flows demonstrating a successful bootstrapping procedure

The overall bootstrapping procedure in successful case is presented in figure A.3-1. The bootstrapping Zh interface performs the retrieval of an authentication vector by BSF from the HSS. The procedure corresponds to the step 2 in figure A.3-1.

This clause specifies in detail the format of the bootstrapping procedure that is further utilized by various applications. It contains the AKA authentication procedure with BSF, and later the bootstrapping key material generation procedure.

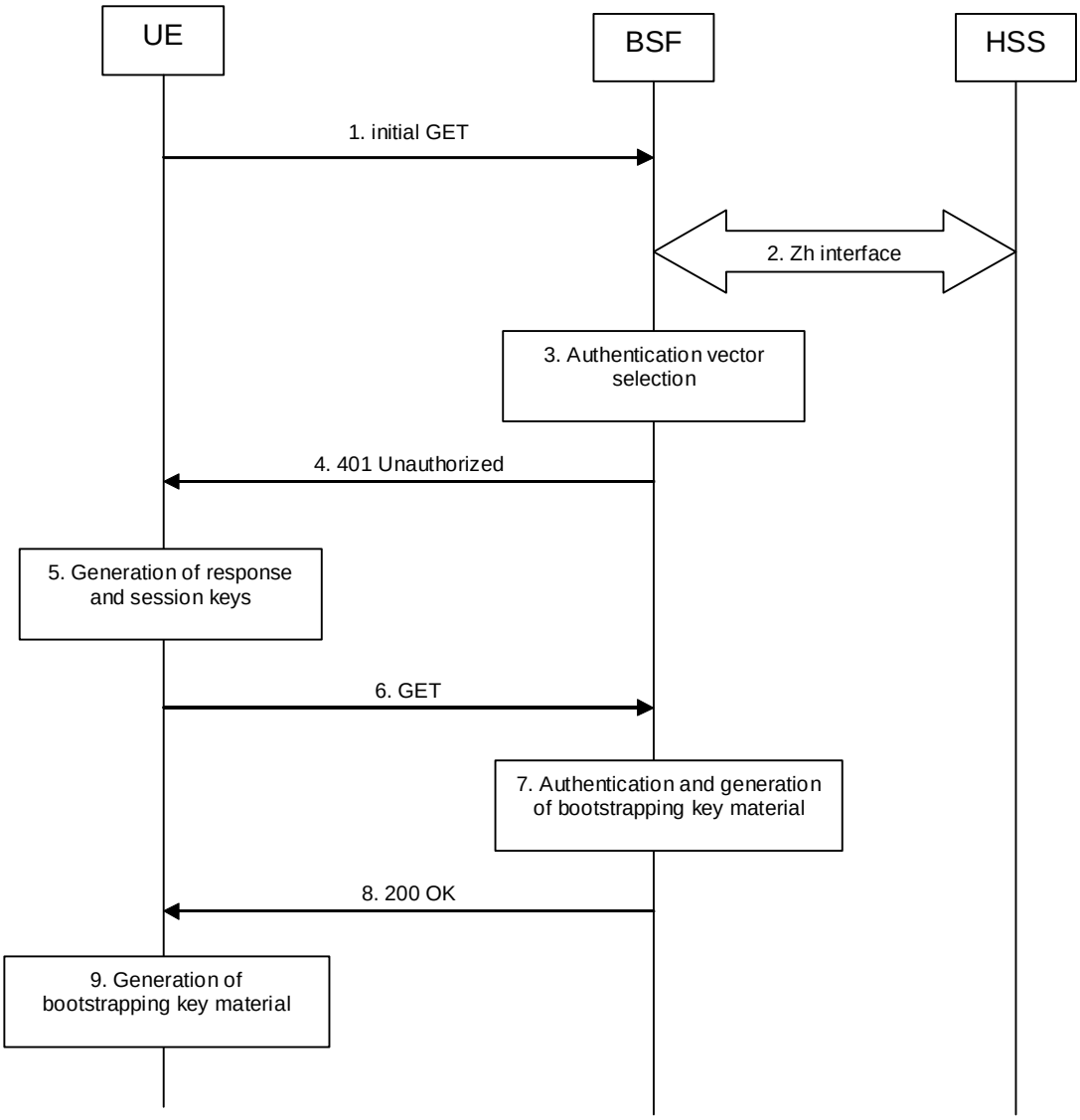

Figure A.3-1: Bootstrapping signalling

1. **Initial GET request (UE to BSF) - see example in table A.3-1**

   The purpose of this message is to initiate bootstrapping procedure between the UE and BSF. The UE sends an HTTP request containing the private user identity towards its home BSF.

Table A.3-1: Initial GET request (UE to BSF)

```
GET / HTTP/1.1
Host: registrar.home1.net:9999
User-Agent: Bootstrapping Client Agent; Release-6
Date: Thu, 08 Jan 2004 10:13:17 GMT
Accept: */*
Referer: http://pki-portal.home1.net:2311/pkip/enroll
Authorization: Digest username="user1_private@home1.net", realm="registrar.home1.net", nonce="",
uri="/", response=""
```

Request-URI: The Request-URI (the URI that follows the method name, "GET", in the first line) indicates the resource indication of this GET request. For bootstrapping server, this is by default "/".

Host: Specifies the Internet host and port number of the BSF server, obtained from the original URI given by referring resource.

User-Agent: Contains information about the user agent originating the request.

Date: Represents the date and time at which the message was originated.

Accept: Media types which are acceptable for the response.

Referer: Allows the user agent to specify the address (URI) of the resource from which the bootstrapping procedure was initiated.

Authorization: It carries authentication information. The private user identity (user1_private@home1.net) is carried in the username field of the Digest AKA protocol. The "uri" parameter (directive) contains the same value as the Request-URI. The ”realm” parameter (directive) contains the network name where the username is authenticated. The Request-URI and the "realm" parameter (directive) value are obtained from the same field in the USIM and therefore, are identical. In this example, it is assumed that a new UICC card was just inserted into the terminal, and there is no other cached information to send. Therefore, "nonce" and "response" parameters (directives) are empty.

2. **Zh: Authentication procedure**

   BSF retrieves the corresponding AVs from the HSS.

   For detailed signalling flows see 3GPP TS 29.109 [3].

Table A.3-2: BSF authentication information procedure (BSF to HSS)

Message source and destination	Zh Information element name	Information Source in GET	Description
BSF to HSS	Private User Identity	Authorization:	The Private User Identity is encoded in the username field according to the Authorization protocol.

3. **Authentication vector selection**

   The BSF selects an authentication vector for use in the authentication challenge. For detailed description of the authentication vector, see 3GPP TS 33.203 [21].

NOTE 1: The authentication vector can be of the form as in 3GPP TS 33.203 [21] (if IMS AKA is the selected authentication scheme):

- $AV = RAND_n||AUTN_n||XRES_n||CK_n||IK_n$ where:
  - RAND: random number used to generate the XRES, CK, IK, and part of the AUTN. It is also used to generate the RES at the UE.
  - AUTN: Authentication token (including MAC and SQN); 128 bit value generated by the HSS.
  - XRES: Expected (correct) result from the UE.
  - CK: Cipher key (optional).
  - IK: Integrity key.

4. **401 Unauthorized response (BSF to UE) - see example in table A.3-3**

   BSF forwards the challenge to the UE in HTTP 401 Unauthorized response (without the CK, IK and XRES). This is to demand the UE to authenticate itself. The challenge contains RAND and AUTN that are populated in nonce field according to RFC 3310 [6].

Table A.3-3: 401 Unauthorized response (BSF to UE)

```
HTTP/1.1 401 Unauthorized
Server: Bootstrapping Server; Release-6
Date: Thu, 08 Jan 2004 10:13:17 GMT
WWW-Authenticate: Digest realm="registrar.home1.net", nonce= base64(RAND + AUTN + server specific
data), algorithm=AKAv1-MD5, qop="auth-int"
```

Server: Contains information about the software used by the origin server (BSF).

Date: Represents the date and time at which the message was originated.

WWW-Authenticate: The BSF challenges the user. The nonce includes the quoted string, base64 encoded value of the concatenation of the AKA RAND, AKA AUTN and server specific data.

NOTE 2: The actual nonce value in the WWW-Authenticate header field is encoded in base64, and it can look like: nonce="A34Cm+Fva37UYWpGNB34JP".

5. **Generation of response and session keys at UE**

   Upon receiving the Unauthorized response, the UE extracts the MAC and the SQN from the AUTN. The UE calculates the XMAC and checks that XMAC matches the received MAC and that the SQN is in the correct range. If both these checks are successful the UE calculates the authentication challenge response (using RES and other parameters as defined in RFC 3310 [6]), and also computes the session keys IK and CK. The authentication challenge response is put into the Authorization header and sent back to the BSF in the GET request.

6. **GET request (UE to BSF) - see example in table A.3-4**

   The UE sends an HTTP GET request again, with the RES, which is used for response calculation, to the BSF.

Table A.3-4: GET request (UE to BSF)

```
GET / HTTP/1.1
Host: registrar.home1.net:9999
User-Agent: Bootstrapping Client Agent; Release-6
Date: Thu, 08 Jan 2004 10:13:18 GMT
Accept: */*
Referer: http://pki-portal.home1.net:2311/pkip/enroll
Authorization: Digest username="user1_private@home1.net", realm="registrar.home1.net",
nonce=base64(RAND + AUTN + server specific data), uri="/", qop=auth-int, nc=00000001,
cnonce="6629fae49393a05397450978507c4ef1", response="6629fae49393a05397450978507c4ef1",
opaque="5ccc069c403ebaf9f0171e9517f30e41", algorithm=AKAv1-MD5
```

Authorization: This carries the response to the authentication challenge received in step 4 along with the private user identity, the realm, the nonce, the URI, the qop, the NC, the cnonce, the response, the opaque, and the algorithm.

7. **Authentication and generation of key material at BSF**

   Upon receiving an integrity protected GET request carrying the authentication challenge response, the BSF checks that the expected response (calculated by the BSF using XRES and other parameter as defined in RFC 3310 [6]) matches the received challenge response. If the check is successful then the user has been authenticated and the private user identity is registered in the BSF.

   The BSF generates the bootstrapping transaction identifier (B-TID) for the IMPI and stores the tuple <B-TID,IMPI,CK,IK>.

   For detailed bootstrapping key material generation procedure see 3GPP TS 33.220 [1].

8. **200 OK response (BSF to UE) - see example in table A.3-5**

   The BSF sends 200 OK response to the UE to indicate the success of the authentication.

Table A.3-5: 200 OK response (BSF to UE)

```
HTTP/1.1 200 OK
Server: Bootstrapping Server; Release-6
Authentication-Info: qop=auth-int, rspauth="6629fae49394a05397450978507c4ef1",
cnonce="6629fae49393a05397450978507c4ef1", nc=00000001
Date:
Expires: Thu, 08 Jan 2004 10:23:17 GMT
Content-Type: application/vnd.3gpp.bsf+xml
Content-Length: (...)

<?xml version="1.0" encoding="UTF-8"?>
<BootstrappingInfo xmlns="uri:3gpp-gba">
  <btid>user@bsf.operator.com</btid>
  <lifetime>2004-05-28T13:20:00-05:00Z</lifetime>
</BootstrappingInfo>
```

Content-Type: Contains the media type of the entity body.

Content-Length: Indicates the size of the entity-body, in decimal number of OCTETs, sent to the recipient.

Authentication-Info: This carries the server authentication information. The header includes the "rspauth" parameter which is calculated as specified in RFC 2617 [9] using RES for response calculation as specified in RFC 3310 [6].

Expires: Gives the date/time after which the response is considered stale.

9. **Generation of key material at UE**

The key material Ks is generated in UE by concatenating CK and IK. The NAF specific key material Ks_NAF is derived from Ks in the case of GBA_ME, or Ks_ext_NAF is derived from Ks_ext in the case of GBA_U, and used for securing the Ua interface. The UE stores the tuple <B-TID,Ks_NAF> or <B-TID,Ks_ext_NAF>.

For detailed bootstrapping key material generation procedure for NAF specific key (Ks_NAF or Ks_ext_NAF) see 3GPP TS 33.220 [1].

**** next change ****

Annex C (normative): XML Schema Definition

C.1 Introduction

This annex contains the XML schema definition for an XML document carrying the bootstrapping transaction identifier (B-TID), the key lifetime, and possibly other server specific data.

The "lifetime" attribute shall indicate the expiry time of the key. The lifetime value shall be expressed in UTC form, indicated by a time zone designator "Z" immediately following the time portion of the value.

Editor's note: The content-type "application/vnd.3gpp.bsf+xml" needs to be registered with IANA.

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema targetNamespace="uri:3gpp-gba"
    xmlns:gba="uri:3gpp-gba"
    xmlns:xs="http://www.w3.org/2001/XMLSchema">

  <!-- definition of the root element containing B-TID and key lifetime -->
  <xs:complexType name="bootstrappingInfoType">
    <xs:sequence>
       <xs:element name="btid" type="xs:string"/>
       <xs:element name="lifetime" type="xs:dateTime"/>
    </xs:sequence>
  </xs:complexType>

  <!-- the root element -->
  <xs:element name="BootstrappingInfo" type="gba:bootstrappingInfoType"/>

</xs:schema>
```

3GPP TSG-CT1 Meeting #38
Cancun, Mexico, 25-29 April 2005

Tdoc C1-050731

CR-Form-v7.1

CHANGE REQUEST

⌘ **24.109** **CR** **15** ⌘ **rev** **1** ⌘ Current version: **6.2.0** ⌘

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

Proposed change affects: UICC apps⌘ ☐ ME ☐ Radio Access Network ☐ Core Network ☒

Title:	⌘	User identity reference
Source:	⌘	Nokia
Work item code:	⌘	SEC1-SC
Date:	⌘	27/04/2005
Category:	⌘	**F**
Release:	⌘	Rel-6

Use one of the following categories:
F *(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:

Ph2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*
Rel-7	*(Release 7)*

Reason for change:	⌘	The user identity related reference to TS 29.109 in chapter G.2 and G.3 does not describe the place of the type definition.
Summary of change:	⌘	Reference explained.
Consequences if not approved:	⌘	Unclear reference.

Clauses affected:	⌘	G.2, G.3

Other specs affected: ⌘	Y	N	
		X	Other core specifications
		X	Test specifications
		X	O&M Specifications

⌘

Other comments: ⌘

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm.
Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be

downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

G.2 X-3GPP-Intended-Identity extension-header

The "X-3GPP-Intended-Identity" header is used optionally by the UE to indicate the user identity intended to be used with the AS. It contains the user identity surrounded by quotation marks (").

Table G.2: Syntax of X-3GPP-Intended-Identity extension-header

```
X-3GPP-Intended-Identity = "X-3GPP-Intended-Identity" ":" DQUOTE identity DQUOTE
identity = *(%x20-21 / %x23-7E)
```

In the syntax definition the rule 'identity' refers to the user identity and it is defined as a string of printable characters and spaces but excluding quotation marks. The exact type definition for ~~user~~ 'identity' is done in TS 29.109 [3] as part of the User Security Setting definition (as the uid tag in the XML scheme definition).

G.3 X-3GPP-Asserted-Identity extension-header

Depending on the subscriber's GBA user security settings the "X-3GPP-Asserted-Identity" header is used by the AP to indicate an asserted identity or a list of identities to the AS. It contains a list of identities separated by comma (,) and each identity is surrounded by quotation marks (").

Table G.3: Syntax of X-3GPP-Asserted-Identity extension-header

```
X-3GPP-Asserted-Identity = "X-3GPP-Asserted-Identity" ":" identity-list
identity-list = DQUOTE identity DQUOTE *("," DQUOTE identity DQUOTE)
identity = *(%x20-21 / %x23-7E)
```

In the syntax definition the rule 'identity' refers to the user identity and it is defined as a string of printable characters and spaces but excluding quotation marks. The exact type definition for ~~user~~ 'identity' is done in TS 29.109 [3] as part of the User Security Setting definition (as the uid tag in the XML scheme definition).

3GPP TSG-CT1 #38
Cancun, Mexico, 25-29 April 2005

C1-050807

CR-Form-v7.1

CHANGE REQUEST

⌘ **24.109** **CR** **17** ⌘ **rev** **1** ⌘ Current version: **6.2.0** ⌘

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

Proposed change affects: UICC apps⌘ [X] ME [ ] Radio Access Network [ ] Core Network [X]

Title:	⌘	Usage of Ks_int_NAF
Source:	⌘	Axalto, Gemplus
Work item code:	⌘	SEC1-SC
Date:	⌘	29/04/2005
Category:	⌘	**F**
Release:	⌘	Rel-6

Use one of the following categories:
F *(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)*
Rel-6	*(Release 6)*
Rel-7	*(Release 7)*

Reason for change:	⌘	SA3 has identified a misallignement between TS 33.220 and TS 24.109 in TD S3-050289.
Summary of change:	⌘	Update TS 24.109 to mention explicitly that the usage of Ks_int_NAF is possible.
Consequences if not approved:	⌘	Misallignement between TS 33.220 and TS 24.109

Clauses affected:	⌘	5.1

	Y	N		
Other specs affected: ⌘		X	Other core specifications	⌘
		X	Test specifications	
		X	O&M Specifications	

Other comments:	⌘	

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

5.1 Introduction

The usage of bootstrapped security association i.e. B-TID and Ks_NAF (or Ks_ext_NAF or Ks_int_NAF) over Ua interface depends on the application protocol used between UE and NAF.

The Ua interface is used to supply the B-TID, generated during the bootstrapping procedure, to the network application function (NAF), and Zn interface is used by the NAF to retrieve the Ks_NAF or Ks_ext_NAF or Ks_int_NAF from BSF. The default is the use of Ks_(ext)_NAF, but the usage of Ks_int_NAF in Ua interface is possible. The Ua interface depends on type of NAF. The Zn interface is defined in 3GPP TS 29.109 [3]. This clause describes how B-TID and Ks_NAF or Ks_ext_NAF can be utilized ~~in general Ua usage~~, as specified in 3GPP TS 33.220 [1], and in the context of more specific Ua usage, as specified for deployment of HTTPS in 3GPP TS 33.222 [4A], or for a PKI portal in 3GPP TS 33.221 [4]).