3GPP TSG CT Plenary Meeting #28 **CP-050090**
1st – 3rd June 2005 Quebec, Canada.

Source: TSG CT WG4

Title: Corrections on Subscriber Certificates

Agenda item: 9.3

Document for: APPROVAL

Doc-2nd-Level	Spec	CR #	Rev	Rel	Tdoc Title	CAT	C_Version
C4-050583	29.109	015		Rel-6	XML extensibility	F	6.2.0
C4-050728	29.109	016	1	Rel-6	Remove BSF from visited network	F	6.2.0

3GPP TSG-CT WG4 Meeting #27 **C4-050583**
Cancun, MEXICO. 25th to 29th April 2005.

CR-Form-v7.1

CHANGE REQUEST

⌘ **29.109** **CR** **015** ⌘ **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:	⌘	XML extensibility
Source:	⌘	Siemens, Nokia
Work item code:	⌘	TEI6
Date:	⌘	11/04/2005
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:	⌘	To assure compatibility with future extensions of the XML-Schema in Annex A
Summary of change:	⌘	Add any-tags to the XML-schema in annex A
Consequences if not approved:	⌘	compatible extensibility in future releases is made difficult.

Clauses affected:	⌘	Annex A			
Other specs affected:	⌘	**Y**	**N**		
			X	Other core specifications	⌘
			X	Test specifications	
			X	O&M Specifications	
Other comments:	⌘	see also N4-020674			

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.

Annex A (normative): GBA-UserSecSettings XML definition

This annex contains the XML schema definition for an XML document carrying the GBA User Security Settings inside GBA-UserSecSettings AVP in Zh and Zn interface.

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema targetNamespace="guss-schema-of-3gpp-gaa"
    xmlns:tns="guss-schema-of-3gpp-gaa"
    xmlns:xs="http://www.w3.org/2001/XMLSchema"
    elementFormDefault="qualified"
    attributeFormDefault="unqualified">

  <!-- This import brings in the XML language attribute xml:lang-->
  <xs:import namespace="http://www.w3.org/XML/1998/namespace"
      schemaLocation="http://www.w3.org/2001/xml.xsd"/>

  <!-- The whole user's GBA specific data set  -->
  <xs:complexType name="guss">
    <xs:sequence>
       <xs:element ref="bsfInfo" minOccurs="0"/>
       <xs:element ref="ussList"/>
       <xs:any processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
    <xs:attribute name="id" type="xs:string"/>
  </xs:complexType>

  <!-- BSF specific information element -->
  <xs:complexType name="bsfInfo">
    <xs:sequence>
      <xs:element name="uiccType"  type="xs:string"  minOccurs="0" />
      <xs:element name="lifeTime"  type="xs:integer" minOccurs="0" />
       <xs:any processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
  </xs:complexType>

  <!--List of all users individual User Security Settings -->
  <xs:complexType name="ussList">
    <xs:sequence minOccurs="0" maxOccurs="unbounded">
       <xs:element ref="uss"/>
       <xs:any processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
  </xs:complexType>

  <!-- User Security Setting data -->
  <xs:complexType name="uss">
    <xs:sequence>
      <xs:element ref="uids"/>
      <xs:element name="flags"/>
      <xs:any processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
    <xs:attribute name="id"   use="required" type="xs:string"/>
    <xs:attribute name="type" use="required" type="xs:int"/>
    <xs:attribute name="nafGroup" use="optional" type="xs:string"/>
  </xs:complexType>

  <!-- User Public Identities for authentication -->
  <xs:complexType name="uids">
    <xs:sequence minOccurs="1" maxOccurs="unbounded">
```

```
      <xs:element name="uid"  type="xs:string"/>
      <xs:any processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
  </xs:complexType>

  <!-- GAA Application type specific Authorization flag codes -->
  <xs:complexType name="flags">
    <xs:sequence minOccurs="0" maxOccurs="unbounded">
      <xs:element name="flag"  type="xs:int"/>
      <xs:any processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
  </xs:complexType>

</xs:schema>
```

Note that the <xs:any> elements within the complex types allow for compatible extensions in future releases.

The values are:

- The value of the attribute “id” in the element “guss” is the the same as user’s IM Private Identity (IMPI) used in User-Name AVP.
- The value of the attribute “id” in the element “uss” is the same as service identifier (GSID) used in GAA-Service-Identifier AVP.
- The value of the element "uiccType" in the element "bsfInfo" is:
  GBA to indicate the basic case, or
  GBA_U to indicate that generation of UICC_Ks is also required in the BSF.
  The default value is GBA.
- The value of the element "lifeTime" in the element "bsfInfo" indicates a user specific key lifetime (duration in seconds). If the lifeTime element is missing the default value in the BSF is used.
- The value of attribute "type" in the element "uss" is GAA service type code defined in annex B.
- The value of attribute “nafGroup” in the element “uss” is an operator internal group designator for a NAF group the USS is valid for. If this attribute is missing then only the attribute “id” is used for selection of this element.
- Values of the element "uid" are user’s public authentication identities from the HSS.
- Values of element “flag” are user’s authorization flag codes from the HSS for GAA service type indicated in the type attribute in the parent uss element. If an authorization flag exist the NAF have permission to give the corresponding service, otherwise not

In the following illustrative example the values are italised and underlined. The content of one User Security Setting tag is boxed.

```
<guss id="358500004836551@ims.mnc050.mcc358.3gppnetwork.org">
     <bsfInfo>
          <lifeTime>86400</lifeTime>
     </bsfInfo>
     <ussList>
          <uss id="1" type="1">
               <uids>
                    <uid>tel:358504836551</uid>
                    <uid>lauri.laitinen@nokia.com</uid>
                    …
               </uids>
               <flags>
                    <flag>1</flag>
                    …
               </flags>
          </uss>
          …
```

```
    </ussList>
</guss>
```

The above GAA User Security Settings example for user “358500004836551@ ims.mnc050.mcc358.3gppnetwork.org” defines that for PKI-Portal (GAA service type code is 1) services are allowed for user identities “tel:358504836551” and “lauri.laitinen@nokia.com” and authentication is allowed (flag 1 exists) but non-repudiation is not allowed (flag 2 is missing) to NAFs that provide the GAA service identified by "1" GAA Service Identifier. The BSF shall not generate UICC-Ks, because uiccType is missing. A special key lifetime defines that athe duration after which the key expires is 86400 seconds

3GPP TSG-CT WG4 Meeting #27 **C4-050728**
Cancun, MEXICO. 25th to 29th April 2005.

CR-Form-v7.1

CHANGE REQUEST

⌘ **29.109** **CR** **016** ⌘ **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:	⌘	Remove BSF from visited network
Source:	⌘	Siemens
Work item code:	⌘	TEI6
Date:	⌘	15/04/2005
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 have decided that the BSF shall be placed in subscriber's Home network (also in later releases). The visited NAF can extract the address of the BSF from the B-TID.
Summary of change:	⌘	remove the text referring to BSF in visited network and SLF and use B-TID to discover the correct BSF address
Consequences if not approved:	⌘	unaligned specifications

Clauses affected:	⌘	5.2			
Other specs affected:	⌘	Y	N	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 Protocol Zn between NAF and BSF

The requirements for Zn interface are defined in 3GPP TS 33.220 [5].

The protocol Zn retrieves the key material and possibly user security settings data by NAF from BSF. After UE is authenticated with the BSF, every time the UE wants to interact with an NAF the following steps are executed as depicted in Figure 5.3. The basic procedure is:

A) The UE starts protocol Ua (see 3GPP TS 33.220 [5])

- In general, the UE and the NAF will not yet share the key(s) required to protect protocol Ua. If they already do, there is no need for the NAF to invoke protocol Zn.
- It is assumed that UE supplies sufficient information to NAF, i.e. the Bootstrapping Transaction Identifier (B-TID), to allow the NAF to retrieve specific key material (e.g. ME-Ks and UICC-Ks) from BSF.
- The UE derives the keys required to protect protocol Ua from the key material.

B) The NAF starts protocol Zn with BSF

- The NAF requests NAF specific key material corresponding to the information supplied by the UE to the NAF (i.e. the bootstrapping transaction identifier) in the start of protocol Ua.
- The BSF generates and supplies to the NAF the requested NAF specific key material, the expiry time , the bootstrapinfo creation time, and the appropriate User Security Settings defined for received application identifiers.

C) The NAF continues protocol Ua with the UE (see 3GPP TS 33.220~~1~~ [6])

Once the run of protocol Ua is completed the purpose of bootstrapping is fulfilled as it enabled UE and NAF to run protocol Ua in a secure way.

The common GAA application procedure is presented in Figure 5.3.

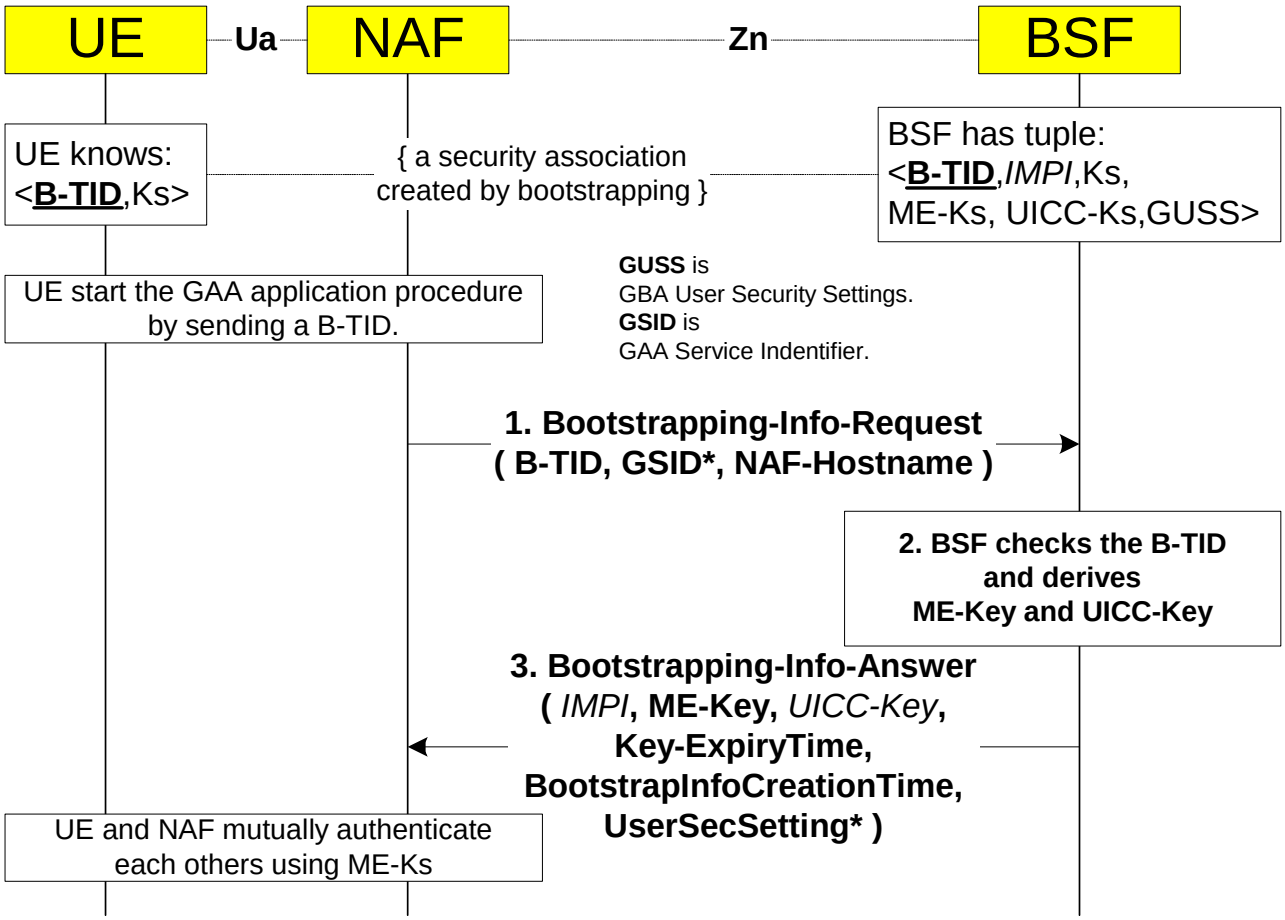

Figure 5.3: The GAA application procedure

The steps of the GAA application procedure in Figure 5.3 are:

Step 1

The NAF shall send a Bootstrapping-Info-Request message (BIR) to the BSF. The content of the message is given here in the same format as in 3GPP TS 29.229 [3]. The curly brackets indicate mandatory AVPs. The square brackets indicate optional AVP. The address refers to the Fully Qualified Host Name (FQDN).

```
< Bootstrapping-Info-Request> ::=<Diameter Header: 310, REQ, PXY, 16777220 >
                < Session-Id >
                { Vendor-Specific-Application-Id }
                { Origin-Host }                          ; Address of NAF
                { Origin-Realm }                         ; Realm of NAF
                { Destination-Realm }                    ; Realm of BSF
                [ Destination-Host ]                     ; Address of the BSF
                * [ GAA-Service-Identifier ]             ; Service identifiers
                { Transaction-Identifier }               ; B-TID
                { NAF-Hostname }                         ; FQDN of NAF as seen
                by UE
                [ GBA_U-Awareness-Indicator ]            ; GBA_U awareness of
                the NAF
                *[ AVP ]
                *[ Proxy-Info ]
                *[ Route-Record ]
```

The content of Vendor-Specific-Application-ID according [1] is:

```
<Vendor-Specific-Application-Id>::=<AVP header: 260>
                1*  [Vendor-Id]                          ; 3GPP is 10415
                0*1 {Auth-Application-Id}                ; 16777220
                0*1 {Acct-Application-Id}                ; Omitted
```

The Destination-Realm AVP is set to ~~the NAF~~subscriber's ~~default~~ BSF. The address of the BSF is extracted from the B-TID. ~~When determining the value of Destination-Host AVP in home network the NAF can use redirector function (SLF) to resolve the address of the BSF if needed (see 3GPP TS 29.229 [3]). The derivation of the Destination-Host in the visited network case is FSS in the later phases.~~

NOTE: In the case where the subscriber has contacted a NAF that is in a visited network, the NAF contacts~~.~~ the subscriber's home BSF through a Diameter-Proxy (D-Proxy) that is located in the same network as the NAF. The local BSF and the D-Proxy may be co-located. See 3GPP TS 33.220 [6].

~~—~~The NAF indicates the GAA services for which the information is retrieved by GAA-Service-Identifier AVPs. The Bootstrapping Transaction Identifier defines the earlier bootstrapping procedure execution.

Step 2

In the successful case the BSF has a tuple <B-TID,IMPI,Ks, ME-Ks,UICC-Ks,Key lifetime, Bootstrapinfo creation time, GBA-UserSecSettings> identified by Bootstrapping Transaction Identifier (B-TID). When the BSF receives the request it checks the existence and validity of the tuple for given B-TID. If checking fails the BSF sends an Answer message with Experimental-Result set to indicate the error type 5403. If the tuple for B-TID exists, but is expired, error type 5403 is also send to indicate needs for renewal of the boostrapping procedure. In successful case the Result-Code is set to 2xxx as defined in [1].

The BSF derives the key material for the ME (and possibly the key material for the UICC) according to the B-TID and packs them into ME-Key-Material AVP (and possible UICC-Key-Material AVP). The BSF select correct user's Security Settings according the request's GAA-Service-Identifier AVP to GBA-UserSecSettings AVP. If NAF grouping is used by the operator and there are one or more USSs corresponding to the requested GSID, then also the nafGroup attribute of USS is checked. If the NAF has sent a GAA-Service-Identifier that does not have corresponding user's security settings, and the BSF is locally configured to reject those requests from the NAF, then the error 5402 is raised. If the NAF has sent a GAA-Service-Identifierthat have corresponding user's security settings, but the BSF is locally configured to reject those from that NAF, then the error 5402 is raised too.

The NAF may be addressed from the UE with different FQDNs. The BSF shall check if this NAF-Hostname is allowed to be used for the NAF. If the NAF identified by its Origin-Host AVP is configured in the BSF not to be authorized to use the given NAF-Hostname, the BSF may raise the error situation 5402. The BSF may also be configured so that a certain NAF is not authorized to use a certain GAA-Service-Identifier. This situation may be also indicated by error code 5402.

Step 3

After that the BSF shall send a Bootstrapping-Info-Answer message (BIA) back to the NAF.

```
< Boostrapping-Info-Answer> ::= < Diameter Header: 310, PXY, 16777220 >
                < Session-Id >
                { Vendor-Specific-Application-Id }
                [ Result-Code ]
                [ Experimental-Result]
                { Origin-Host }                  ; Address of BSF
                { Origin-Realm }                 ; Realm of BSF
                [ User-Name ]                    ; IMPI
                [ ME-Key-Material ]              ; Required
                [ UICC-Key-Material ]            ; Conditional
                [ Key-ExpiryTime ]               ; Time of expiry
                [ BootstrapInfoCreationTime ]    ; Bootstrapinfo creation time
                [ GBA-UserSecSettings ]          ; Selected USSs
                *[ AVP ]
                *[ Proxy-Info ]
                *[ Route-Record ]
```

The BSF may or may not send the User-name AVP (IMPI) according its configuration.

The mandatory common key material with the ME (ME-Ks-naf) is sent in the ME-Key-Material AVP. The common key material with the UICC (UICC-Ks-naf) is optionally sent in the UICC-Key-Material AVP only if the “uiccType” tag in bsfInfo from the HSS is set to "GBA_U".

The Key-ExpiryTime AVP contains the expiry time of the Bootstrapping information in the BSF according its configuration. The expiry time is represented according the Diameter Time data format in seconds that have passed since 0h on January 1, 1900 UTC . If a special key lifetime value is given in the “lifeTime” tag inside the bsfInfo from the HSS in bootstraping procedure, it is used instead of the BSF default configuration value when the expiry time is calculated.

The BootstrapInfoCreationTime AVP contains the bootstrapinfo creation time, i.e., creation time of the Bootstrapping information in the BSF. The bootstrapinfo creation time is represented in seconds that have passed since January 1, 1900 00:00:00.000 UTC.

The BSF selects the appropriate User Security Settings (if any) to the GBA-UserSecSettings AVP from stored GAA-UserSecSettings in Bootstrapping information according the GBA-Service-Identifier AVPs in the request message.

The procedure in the NAF when the BIA is received is described in 3GPP TS 33.220 [5], 3GPP TS 33.222 [11] and optionally in GAA service type specific TSs.