3GPP TSG CN Plenary Meeting #25 **NP-040415**
8th – 10th August 2004 Palm Springs, US.

Source: TSG CN WG4

Title: Corrections on Rel-6 Subscriber certificates

Agenda item: 9.22

Document for: APPROVAL

Spec	CR	Rev	Doc-2nd-Level N4-04	Phase	Subject	Cat	Ver_C
23.008	133	3	1205	Rel-6	GAA Domain Data Structure	B	6.2.0

3GPP TSG-CN WG4 Meeting #24 ***N4-041205***

Sophia Antipolis, France. 16th to 20th August 2004.

CR-Form-v7.1

CHANGE REQUEST

⌘	**23.008**	**CR**	**133**	⌘**rev**	**3**	⌘	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:	⌘	GAA Domain Data Structure		
Source:	⌘	CN4		
Work item code:	⌘	SEC1-SC	***Date:*** ⌘	2004-08-20
Category:	⌘	**B**	***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:	⌘	Generic Authentication Architecture (GAA) system requires permanent storage for User Security Settings.
Summary of change:	⌘	The definition of data structures of GAA is added.
Consequences if not approved:	⌘	Missing definition of the GAA data in the specification.

Clauses affected:	⌘	0.1, 1.3, 3.1.1 3.X (added), 5.3				
		Y	**N**			
Other specs affected:	⌘		**X**	Other core specifications	⌘	-
			X	Test specifications		
			X	O&M Specifications		
Other comments:	⌘	In Rev1 the Key lifetime definition has been clarified in clause 3A.4.1.				

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.

**** First modified section ****

0.1 References

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

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

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

[2] 3GPP TS 22.002: "Circuit Bearer Services (BS) supported by a Public Land Mobile Network (PLMN)".

[3] 3GPP TS 22.003: "Circuit Teleservices supported by a Public Land Mobile Network (PLMN)".

[4] 3GPP TS 22.004: "General on supplementary services".

[5] 3GPP TS 23.003: "Numbering, addressing and identification".

[6] 3GPP TS 23.007: "Restoration procedures".

[7] 3GPP TS 23.009: "Handover procedures".

[8] 3GPP TS 23.012: "Location Management Procedures".

[9] 3GPP TS 23.015: "Technical realization of Operator Determined Barring (ODB)".

[10] 3GPP TS 23.040: "Technical realization of the Short Message Service (SMS)".

[11] 3GPP TS 22.060: "General Packet Radio Service (GPRS); Service description; Stage 1".

[12] 3GPP TS 23.067: "Enhanced Multi-Level Precedence and Preemption service (EMLPP); Stage 2".

[13] 3GPP TS 23.078: "Customised Applications for Mobile network Enhanced Logic (CAMEL); Stage 2".

[14] 3GPP TS 23.081: "Line identification supplementary services; Stage 2".

[15] 3GPP TS 23.082: "Call Forwarding (CF) Supplementary Services; Stage 2".

[16] 3GPP TS 23.083: "Call Waiting (CW) and Call Hold (HOLD) Supplementary Services; Stage 2".

[17] 3GPP TS 23.084: "Multi Party (MPTY) Supplementary Service; Stage 2".

[18] 3GPP TS 23.085: "Closed User Group (CUG) Supplementary Service; Stage 2".

[19] 3GPP TS 23.086: "Advice of Charge (AoC) Supplementary Service; Stage 2".

[20] 3GPP TS 23.088: "Call Barring (CB) Supplementary Service; Stage 2".

[21] 3GPP TS 23.060: "General Packet Radio Service (GPRS); Service Description; Stage 2".

[22] 3GPP TS 23.078: "Customised Applications for Mobile network Enhanced Logic (CAMEL); Stage 2".

[23] 3GPP TS 23.090: "Unstructured Supplementary Service Data (USSD); Stage 2".

[24] 3GPP TS 23.116: "Super-Charger Technical Realization; Stage 2."

[25] 3GPP TS 23.135: "Multicall supplementary service; Stage 2"

[26] 3GPP TS 24.008: "Mobile radio interface Layer 3 specification; Core network protocols; Stage 3".

[27] 3GPP TS 29.002: "Mobile Application Part (MAP) specification".

[28] 3GPP TS 29.007: "General requirements on interworking between the Public Land Mobile Network (PLMN) and the Integrated Services Digital Network (ISDN) or Public Switched Telephone Network (PSTN)".

[29] 3GPP TS 29.060: "General Packet Radio Service (GPRS); GPRS Tunnelling Protocol (GTP) across the Gn and Gp interface".

[30] 3GPP TS 42.032: "Digital cellular telecommunications system (Phase 2+); Immediate Service Termination (IST) Service description - Stage 1".

[31] 3GPP TS 43.020: "Digital cellular telecommunications system (Phase 2+); Security-related network functions".

[32] 3GPP TS 43.035: "Digital cellular telecommunications system (Phase 2+); Immediate Service Termination (IST); Stage 2".

[33] 3GPP TS 43.068: "Digital cellular telecommunications system (Phase 2+); Voice Group Call Service (VGCS); Stage 2".

[34] 3GPP TS 43.069: "Digital cellular telecommunications system (Phase 2+); Voice Broadcast Service (VBS); Stage 2".

[35] 3GPP TS 23.071: "Location Services (LCS); Functional Description; Stage 2".

[36] GSM 12.03: "Digital cellular telecommunications system (Phase 2+) (GSM); Security management".

[37] GSM 12.08: "Digital cellular telecommunications system (Phase 2+) (GSM); Subscriber and equipment trace".

[38] ITU-T Recommendation Q.763: "Signalling System No. 7 - ISDN User Part formats and codes".

[39] ANSI T1.113: "Signalling System No7 (SS7); Integrated Services Digital Network (ISDN) User Part"

[40] 3GPP TS 32.005 "Telecommunication Management; Charging and billing; 3G call and event data for the Circuit Switched (CS) domain".

[41] 3GPP TS 32.015: "Telecommunication Management; Charging and billing; 3G call and event data for the Packet Switched (PS) domain".

[42] 3GPP TS 23.228: "IP Multimedia Subsystem (IMS); Stage 2".

[43] 3GPP TS 29.228: "IP Multimedia (IM) Subsystem Cx and Dx interfaces; Signalling flows and message contents".

[44] 3GPP TS 29.229: "Cx and Dx Interfaces based on the Diameter protocol; Protocol details".

[45] IETF RFC 3261: "SIP: Session Initiation Protocol".

[46] IETF RFC 2396: "Uniform Resource Identifiers (URI): Generic Syntax".

[47] Void

[48] IETF RFC 2486: "The Network Access Identifier".

[49] 3GPP TS 33.203: "3G security; Access security for IP-based services".

[50] 3GPP TS 23.002: "Network Architecture".

[51] draft-ietf-aaa-diameter-08.txt: "Diameter Base Protocol", work in progress".

[52] 3GPP TS 33.102: "3G Security; Security Architecture".

[53] 3GPP TS 23.218: "IP Multimedia (IM) session handling; IM call model; Stage 2".

[54] 3GPP TS 29.328: "IP Multimedia Subsystem (IMS) Sh interface signalling flows and message contents (Release 5)".

[55] 3GPP TS 23.278: "Customised Applications for Mobile network Enhanced Logic (CAMEL) - IP Multimedia System (IMS) interworking; Stage 2".

[56] 3GPP TS 23.271: "".

[57] 3GPP TS 23.221: " Architectural requirements ".

[xx1] 3GPP TS 33.220: “Generic Authentication Architecture (GAA);Generic bootstrapping architecture”.

[xx2] 3GPP TS 29.109 “Zh and Zn Interfaces based on the Diameter protocol; Protocol details”.

[xx3] IETF RFC 3548: "The Base16, Base32, and Base64 Data Encodings".

****** Second modified section ******

1.3 Subscriber data in functional units other than the HLR, the VLR, the SGSN, the GGSN, the GMLC, the SMLC and the LMU

The individual Subscriber Authentication Key Ki defined in 3GPP TS 43.020 [31] is stored in the Authentication Centre (AuC); it is also stored in the SIM and therefore available in the MS. Version numbers of algorithms A3 and A8 may also be stored in the AuC.

Bootstrapping Server Function (BSF) handles subscriber’s bootstrapping information after bootstrapping procedure in Generic Authentication Architecture (GAA) system. A bootstrapping procedure creates security association between an UE and a BSF. Using the stored user’s bootstrapping information and the security association the BSF can provide security services to network application functions (NAF) contacted by the UE. Functions of the BSF are defined in 3GPP TS 33.220 [xx1] and 3GPP TS 29.109 [xx2].

NOTE: It is for further study whether or not other types of functional units containing mobile subscriber parameters are to be included in this specification. Such units could include encryption key distribution centres, maintenance centres, etc...

****** Third modified section ******

3.1.1 Private User Identity

The Private User Identity is in the form of a Network Access Identifier (NAI), which is defined in RFC 2486 [48].

If the GAA bootstrapping is based on authentication data from the IM domain, the corresponding Private User Identity from the IM domain (IMPI) is used as it is. If the GAA bootstrapping is based on the authentication data from the CS/PS domain, a Private User Identity is derived from user's IMSI according 3GPP TS 23.003 [5] is used.

The Private User Identity is permanent subscriber data and is stored in HSS, ~~and in~~ S-CSCF and BSF.

**** Fourth modified section ****

3.X Data related to Generic Authentication Architecture

The Generic Authentication Architecture (GAA) is defined in 3GPP TS 33.220 [xx1] and 3GPP TS 29.109 [xx2]. For data related to GAA, see also the definition of Private User Identity in chapter 3.1.1.

3.X.1 GAA Application Type

The GAA Application Type is an enumerated integer, which is defined in 3GPP TS 29.109 [58].

The GAA Application Type is permanent subscriber data and is stored in the HSS, BSF and NAF.

3.X.2 GAA Service Identifier

The GAA Service Identifier (GSID) is an integer, which uniquely identifies a GAA Service. For example a set of NAFs belonging to a certain GAA Service Type and owned or managed by a certain operator may provide the same operator specific service and they may use the same GAA Service Identifier to identify their services to BSF. The owner of the user's home HSS may define different GAA Authorization flags and allowed Private User Identities for each GAA Service Identifiers separately.

The GAA Service Identifier is permanent subscriber data and is stored in the HSS, BSF and NAF.

3.X.3 GAA Service Subscription

The GAA Service Subscription (GSS) is uniquely identified by a combination of Private User Identities and GAA Service Identifier. GAA Service Subscription combines the user and the GAA Service together. No duplicates are allowed.

The User Security Setting is permanent subscriber data and is stored in the HSS, BSF and NAF.

3.X.4 User Public Identity

The User Public Identity (UID) is a freely defined string that can be used as user's public identity in a GAA application. A list of allowed User Public Identities is stored for each GAA Service Subscription. A User Public Identity may be connected to several GAA Service Subscription.

The User Public Identity is permanent subscriber data and is stored in the HSS, BSF and NAF.

3.X.5 GAA Authorization flag

The GAA Authorization flag is a GAA Application specific integer code, which authorizes a defined security operation in the GAA application. A list of allowed operations is stored for each GAA Service Subscription.

The GAA Authorization flag is concatenated from GAA Application Type code and GAA Application Type specific operation code in range 00-99. The value of a GAA Authorization flag is a sum of 100*(GAA-Application-Type

Code)+(GAA-Application-Type specific operation code). The values of GAA Authorization flags operation code can be therefore specified separately for each GAA application in their specifications.

The Authorization Flag is permanent subscriber data and is stored in the HSS, BSF and NAF.

3.X.6 Bootstrapping Transaction Identifier

The Bootstrapping Transaction Identifier (B-TID) identifies the security association between a BSF and a UE after a bootstrapping procedure in GAA. According [57] the B-TID value shall be also generated in format of NAI by taking the base64 encoded RAND value [xx3] and the BSF server name, i.e. base64 encoded (RAND)@BSF_servers_domain_name.

The Bootstrapping Transaction Identifier is temporary subscriber data and is stored in the BSF and NAF.

3.X.7 Key Lifetime

Key Lifetime is an integer which defines the expiry time of bootstrapping information in BSF in seconds passed since January 1, 1970 00:00:00.000 GMT.

The Key Lifetime is temporary subscriber data and is stored in the BSF and NAF.

****** Fifth modified section ******

5.3 IP Multimedia Service Data Storage

Table 5.3: Overview of data used for IP Multimedia services

PARAMETER	Subclause	HSS	S-CSCF	IM-SSF	AS	BSF	NAF	TYPE
Private User Identity	3.1.1	M	M		-	M		P
Public Identity	3.1.2	M	M		-			P
Barring Indication	3.1.3	M	M		-			P
List of authorized visited network identifiers	3.1.4	M	-		-			P
Registration Status	3.2.1	M	-		-			T
S-CSCF Name	3.2.2	M	-		-			T
Diameter Client Address of S-CSCF	3.2.3	M	-		-			T
Diameter Server Address of HSS	3.2.4	-	M	-	C			T
RAND, XRES, CK, IK and AUTN	3.3.1	M	C		-			T
Server Capabilities	3.4.1	C	C		-			P
Subscribed Media Profile Identifier	3.5.1	C	C		-			P
Initial Filter Criteria	3.5.2	C	C		-			P
Application Server Information	3.5.3	C	C	-	-			P
Service Indication	3.5.4	M	-		M			P
Primary Event Charging Function Name	3.7.1	C	C	-	-			P
Secondary Event Charging Function Name	3.7.2	C	C	-	-			P
Primary Charging Collection Function Name	3.7.3	M	M	-	-			P
Secondary Charging Collection Function Name	3.7.4	C	C	-	-			P
GsmSCF address for IM CSI	3.8.4	C	-		-			P
IM-SSF address for IM CSI	3.8.5	C	-		-			T
O-IM-CSI	3.8.1	C	-	C	-			P
VT-IM-CSI	3.8.2	C	-	C	-			P
D-IM-CSI	3.8.3	C	-	C	-			P
GsmSCF address for IM CSI	3.8.4	C	-	-	-			P
IM-SSF address for IM CSI	3.8.5	C	-	-	-			T
GAA Application Type	3.X.1	M				M	M	P
GAA Service Identifier	3.X.2	M				M	M	P
GAA Service Subscription	3.X.3	M				M	M	P
User Public Identity	3.X.4	M				M	M	P
GAA Authorization flag	3.X.5	M				M	M	P
Bootstrapping Transaction Identifier	3.X.6					M	M	T
Key Lifetime	3.X.7					M	M	T