Source:	**Nokia**
Title:	**Naming in Generic Authentication Architecture (GAA)**
Document for:	**Discussion and Decision**
Agenda Item:	**7.9 GAA and Support for subscriber certificates**

1. INTRODUCTION

Discussion and decision paper “Interface Naming in Bootstrapping System” [S3-030348] suggested new interface names for interfaces in SA3 draft TS “Bootstrapping of application security using AKA and Support for Subscriber Certificates” [S3-030488]. The current interface names (A, B, C and D) for Bootstrapping Function (BSF) and Network Application Function (NAF), i.e. applications that utilize the security associations created by bootstrapping, are only placeholders. The suggested interface names were Ub, Ua, Bb, and Ba, respectively.

SA3#29 decided to ask SA2 to comment on the suitability of the suggested interface names on LS [S3-030471]. SA2 commented in their reply [S3-030484] that new reference point identifiers have not been used before, but asked SA3 to reconsider the usage of the “B series” since it has been exclusively used for interfaces related to billing (as defined in TS 32.200 by SA5). Instead of using the “B series” SA2 suggested the usage of the “Z series” as it is currently used in SA3 specifications only.

In the last SA3 meeting a new term “generic authentication architecture” (GAA) was introduced. In the last SA3 ad hoc meeting the relations within GAA were discussed in detail, and the meeting defined a new term “generic bootstrapping architecture” (GBA). GBA is the system supporting provisioning of shared secrets. The interrelation of general concepts of GAA and GBA are outlined in Figure 1.

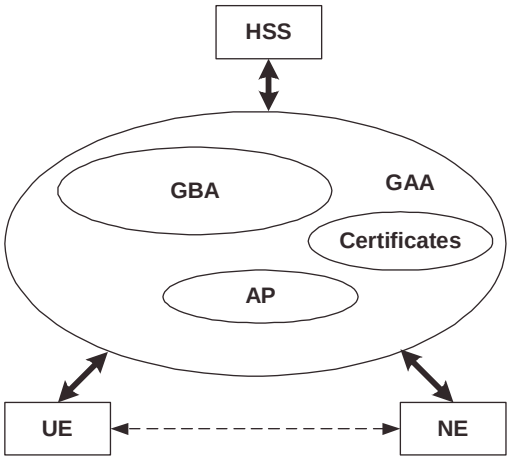

Figure 1. The interrelations of GBA and GAA.

It has been agreed as a working assumption that the current TS SSC [S3-030488] should contain the description of the GAA. Therefore, the current TS (and still non-existing stage 3 specification TSs for protocols C and D) should be named with more logical name(s). Also, a description of the terms GAA and GBA should be included into TS SSC.

2. DISCUSSION

2.1 Interface study: Z series

The “Z series” is used by SA3 specifications TS 33.200 and TS 33.210. The specifications have reserved the following interface names:

Za	Interface between SEGs belonging to different networks/security domains [TS 33.210]
Zb	Interface between SEGs and Nes and interface between Nes within the same network/security domain [TS 33.210]
Zf	The MAP application layer security interface between MAP-Nes engaged in security protected signalling [TS 33.200]

Also the interfaces in Zc, Zd, and Ze have previously been reserved but are available now.

2.2 Specification names

In order to reflect the decisions made by SA3 in S3#29 and S3#29b ad hoc meeting by the introduction of GAA. The names of the current specification set should be renames. Currently three specifications are or going to be under work in 3GPP:

- The current TS SSC specification in SA3,
- New TS for describing protocol C and D in stage 3 detail in CN4, and
- New TS for describing protocol A in stage 3 detail in CN1.

Current name of the TS SSC [S3-030488] is:

> Bootstrapping of application security using AKA and
> Support for Subscriber Certificates;

We propose a new name for the TS SSC:

> Generic Authentication Architecture (GAA)
> System Description;
> Stage 2

For CN1 and CN4 specification there are no current names since the specifications do not exist as of yet. But we propose to name those specifications the following way. For CN1 specification:

> Generic Authentication Architecture (GAA)
> Ub Interface;
> Protocol details

And for CN4 specification:

> Generic Authentication Architecture (GAA)
> Zh and Zn Interfaces based on the Diameter Protocol;
> Protocol details

The new names add more logic to the naming of the specifications.

3. PROPOSAL

3.1 Interface names

In Figure 2 we show the mapping between current and proposed names:

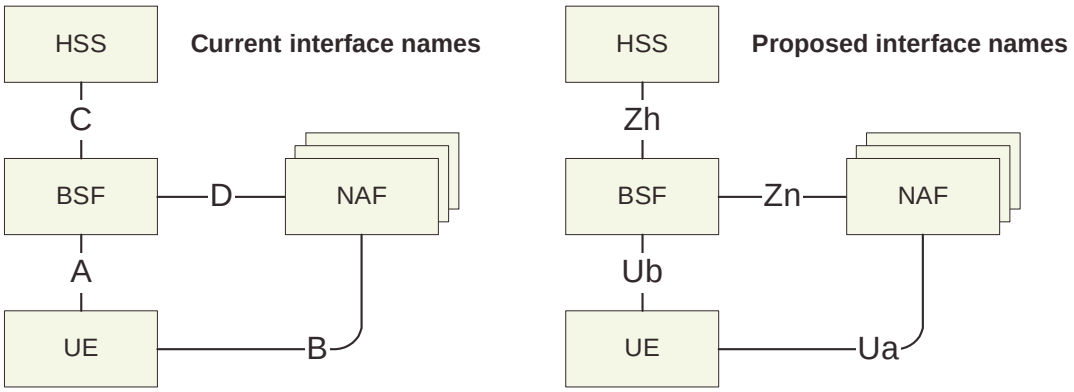

Figure 2: The current and proposed interface names

We propose that the interface names in draft TS [S3-030488] are changed as outlined in this contribution.

Ub **B**ootstrapping air interface (from UE to BSF)

Ua **A**pplication air interface (from UE to NAF)

Zh **H**SS interface from BSF

Zn **N**AF interface from BSF

3.2 Introduction and specification names

We propose to add the definitions of GAA and GBA terms to the Scope section of the SA3 TS SSC [S3-030488], which are in the attached pseudo CR. We also propose to rename the SA3 TS SSC and name the non-existing CN1 and CN4 specifications according to section 2.2.

4. REFERENCES

[S3-030484] LS from SA2: “LS Response on new interface names”, response to S3-030471, SA WG2.

[S3-030488] Draft 3GPP TS 33.109 v0.3.0 “Bootstrapping of application security using AKA and Support for Subscriber Certificates; System Description (Release 6)”.

[S3-030471] LS to SA2, “LS on new interface names”, SA WG3.

[TS 33.200] 3GPP TS 33.200 “3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Network Domain Security; MAP application layer security”.

[TS 33.210] 3GPP TS 33.210 “3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Network Domain Security; IP network layer security”.

CR-Form-v7

CHANGE REQUEST

⌘ SpecNumber CR CRNum ⌘rev - ⌘ Current version: 0.3.0 ⌘

*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:	⌘	Introduction of GBA and GAA terms
Source:	⌘	Nokia
Work item code:	⌘	SEC1-SC
Date:	⌘	2003-09-25
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:

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)*

Reason for change:	⌘	SA3 has taken into use the Generic Bootstrapping Architecture (GBA) and Generic Authentication Architecture (GAA) terms, they need to be introduced in the specification.
Summary of change:	⌘	Introduction of GBA and GAA terms
Consequences if not approved:	⌘	

Clauses affected:	⌘	Title and 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.

title change

3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Generic Authentication Architecture (GAA) System Description; Stage 2 ~~Bootstrapping of application security using AKA and Support for Subscriber Certificates; System Description~~ (Release 6)

********* next modified section**********

1 Scope

The present document describes the security features and a mechanism to bootstrap authentication and key agreement for application security from the 3GPP AKA mechanism. The system supporting provisioning of shared secrets is called Generic Bootstrapping Architecture (GBA). Candidate applications to use this ~~bootstrapping mechanism~~GBA include but are not restricted to subscriber certificate distribution, etc.

GBA and security features based on GBA (e.g. support for subscriber certificates) form together Generic Authentication Architecture (GAA). The security features offered by GAA (e.g. shared secrets or subscriber certificates) should be used as widely as possible to fulfil the security needs of various 3G features.~~Subscriber certificates support services whose provision mobile operator assists, as well as services that mobile operator provides.~~

The scope of this specification includes two parts. The first part presents GBA: a generic AKA bootstrapping function, an architecture overview and the detailed procedure how to bootstrap the credential. The second part is the requirement for applications utilizing the ~~bootstrapping function~~GBA, as well as the procedure of the utilization. Specifically the present document presents signalling procedures for support of issuing certificates to subscribers and the standard format of certificates and digital signatures. It is not intended to duplicate existing standards being developed by other groups on these topics, and will reference these where appropriate.

Editor's note: The specification objects are scheduled currently in phases. For the first phase of standardisation, only the case is considered where bootstrapping server functionality and network application function are located in the same network as the HSS. In later phases, other configurations may be considered.