3GPP TSG SA WG3 Security **S3-030546**

6th – 10th October, 2003

Povoa de Varzim, Portugal

Agenda Item:	GBA
Source:	Ericsson
Title:	Generic Bootstrapping Architecture (GBA) Technical Specification and Work Item Proposal
Document for:	Discussion/Decision

1. Introduction

Based on discussions about bootstrapping shared secrets at previous SA3 meetings, we think that SA3 should evaluate the need of a new Technical Specification describing the generic bootstrapping architecture (GBA), and also evaluate the need for a new work item to manage the GBA work.

2. Discussion

At SA3 #28, Alcatel submitted a contribution (S3-030253) proposing to move the generic bootstrapping function to a Technical Specification of its own and keep the application specific part in the Support for Subscriber Certificates (SSC) Technical Specification. SA3 #28 agreed to discuss the proposal over e-mail. The e-mail discussion ended with Tao Haukka's (SSC rappourteur) proposal of not splitting the SSC TS.

The SA3 adhoc in September agreed on the Generic Bootstrapping Architecture (GBA) of section 6.2 in contribution S3z030011 by Siemens. The minutes of the SA3 adhoc state the following:

"With regard to the organization of specifications, it was agreed as a working assumption that the GAA (e.g. specification of the AKA bootstrapping architecture and special NAFs for the Authentication Proxy and the PKI portal) should be included in the same TS as the Support for Subscriber Certificates (SSC) feature. This working assumption may have to be revisited at SA3#30."

Based on the agreement on GBA at the SA3 adhoc in September, we think that it could be beneficial to revisit this working assumption, and move out the generic bootstrapping architecture from the SSC TS while keeping the subscriber certificate specific parts in the SSC TS.

We agree with the reasons for the split of the SSC TS stated by Alcatel in the e-mail discussion on the SA3 e-mail list. It's not logical for other services/applications (MBMS, Presence, WLAN, etc) that would use the GBA to refer to an SSC TS. The generic issues could be covered in GBA, and the services/applications TSes would only need to take a stand on the application specific parts.

3 Conclusions

We think that it would be beneficial with a new Technical Specification, describing the generic bootstrapping architecture that would potentially be used in Support for Subscriber Certificates, MBMS, Presence and WLAN. The scope and objective of the GBA need to be clearly captured to progress and manage the GBA work. To initiate discussions on a potential TS and a potential new work item, we provide a draft GBA Technical Specification and a draft GBA Work Item Description as attachments to this contribution.

3GPP TS ab.cde V0.1.0 (2003-09)

Technical Specification

3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Generic Bootstrapping Architecture; System Description (Release 6)

Remove GSM logo from the cover page for pure 3rd Generation documents.

Select keywords from list provided in specs database.

Keywords

<keyword[, keyword]>

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 Technical Specification has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

- x the first digit:
  - 1 presented to TSG for information;
  - 2 presented to TSG for approval;
  - 3 or greater indicates TSG approved document under change control.
- y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the document.

Introduction

This clause is optional. If it exists, it is always the second unnumbered clause.

1 Scope

This clause shall start on a new page.

The present document describes the security features and a mechanism to bootstrap shared secrets for application security from the 3GPP AKA mechanism. Candidate applications to use this bootstrapping mechanism include but are not restricted to subscriber certificate distribution, Presence and MBMS.

2 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.*

[<seq>] <doctype> <#>[([up to and including]{yyyy[-mm]|V<a[.b[.c]]>}[onwards])]: "<Title>".

[1] 3GPP TR 41.001: "GSM Release specifications".

[2] 3GPP TR 21 912 (V3.1.0): "Example 2, using fixed text".

[3] 3GPP TS 33.102: "Security Architecture".

3 Definitions, symbols and abbreviations

Delete from the above heading those words which are not applicable.

Subclause numbering depends on applicability and should be renumbered accordingly.

3.1 Definitions

For the purposes of the present document, the [following] terms and definitions [given in ... and the following] apply.

AK	Anonymity Key
AKA	Authentication and Key Agreement
BSF	Bootstrapping server functionality BSF is hosted in a network element under the control of an MNO.
BSP	BootStrapping Procedure
HSS	Home Subscriber System
IK	Integrity Key
MNO	Mobile network operator
NAF	Operator-controlled network application function functionality. NAF is hosted in a network element under the control of an MNO.
UE	User Equipment

3.2 Symbols

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

Symbol format

<symbol> <Explanation>

3.3 Abbreviations

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

Abbreviation format

<ACRONYM> <Explanation>

4 Generic Authentication Architecture

The 3GPP authentication infrastructure, including the 3GPP Authentication Centre (AuC), the USIM and the 3GPP AKA protocol run between them, is a very valuable asset of 3GPP operators. It has been recognised that this infrastructure could be leveraged to enable application functions in the network and on the user side to communicate in situations where they would not be able to do so without the support of the 3GPP authentication infrastructure. Therefore, 3GPP can provide the “bootstrapping of application security” to authenticate the subscriber by defining a generic bootstrapping function based on AKA protocol.

4.1 Requirements for GBA

GBA should fulfill the following requirements :

1. A Generic Authentication Architecture (GAA) shall provide shared secrets to entities for use with 3G security features for Release 6 and future releases. Features already specified for Release 5 and earlier releases shall not be affected by the GAA.

2. This provision of shared secrets shall be based on the 3G AKA infrastructure (bootstrapping from AKA).

3. The GAA should be applicable as widely as possible to 3G security features for Release 6 and future releases, whether they are http-based or not.

4. The co-existence of several bootstrapping procedures in the 3G architecture should be avoided. In particular, the co-existence of a procedure for bootstrapping of HTTP-based services (as in S3-030367 and S3-030371) and a procedure for generic bootstrapping, as described in the context of support for subscriber certificates (S3-030317), should be avoided.

5. Dependencies on external bodies should be minimised. This would still allow to re-use completed external specifications if seen beneficial.

6. The GAA should respect the HSS/HLR-related security architecture guidelines, as documented in S3-030460. If further guidelines and other criteria regarding service provision or the impact on other entities are agreed by SA3 in the future these should be taken into account in the design as well.

7. Traffic bottlenecks should be avoided. (In particular, it should be investigated whether an HTTP authentication proxy could be such a bottleneck.)

8. The GAA should be able to support applications requiring end-to-end security.

9. The usefulness of the cryptographic separation of keys among applications should be further investigated under the aspect of future-proofing the GAA. If found that such a separation may be useful the GAA should be able to support it.

10. The GAA should support scenarios which require mutual authentication between UE and application server, based on the bootstrapped shared secret. This should not preclude the use of the GAA in scenarios where mutual authentication is provided also using other means (e.g. network certificates).

11. The Generic Architecture should be able to allow the application servers and the terminal to acquire (re-)fresh keys for use.

12. It would be desirable for the GAA to be applicable to non-3GPP security features.

13. For Release 6, the GAA should concentrate on home-provided services, i.e.the authentication is always performed by a server in the home network. But the GAA should not prevent future extension to a scenario where the authentication is performed by a server in a visited networks.

14. The GAA should not mandate intervention by the human user.

Editor's note: The description of AKA bootstrapping shall be added here.

- The bootstrapping function shall not depend on the particular network application function
- The server implementing the bootstrapping function needs to be trusted by the home operator to handle authentication vectors.
- The server implementing the network application function needs only to be trusted by the home operator to handle derived key material.
- It shall be possible to support network application functions in the operator's home network
- The architecture shall not preclude the support of network application function in the visited network, or possibly even in a third network.
- To the extent possible, existing protocols and infrastructure should be reused.
- In order to ensure wide applicability, all involved protocols are preferred to run over IP.

4.1.2 Authentication methods

Authentication method that is used to authenticate the bootstrapping function must be dependent on cellular subscription. In other words, authentication to bootstrapping function shall not be possible without valid cellular subscription. Authentication shall be based on AKA protocol.

4.2 Bootstrapping architecture

4.2.1 Reference model

Figure 1 shows a simple network model of the entities involved in the bootstrapping approach, and the protocols used among them.

Editor's note: The names for the reference points, A, B, C, and D need to be decided.

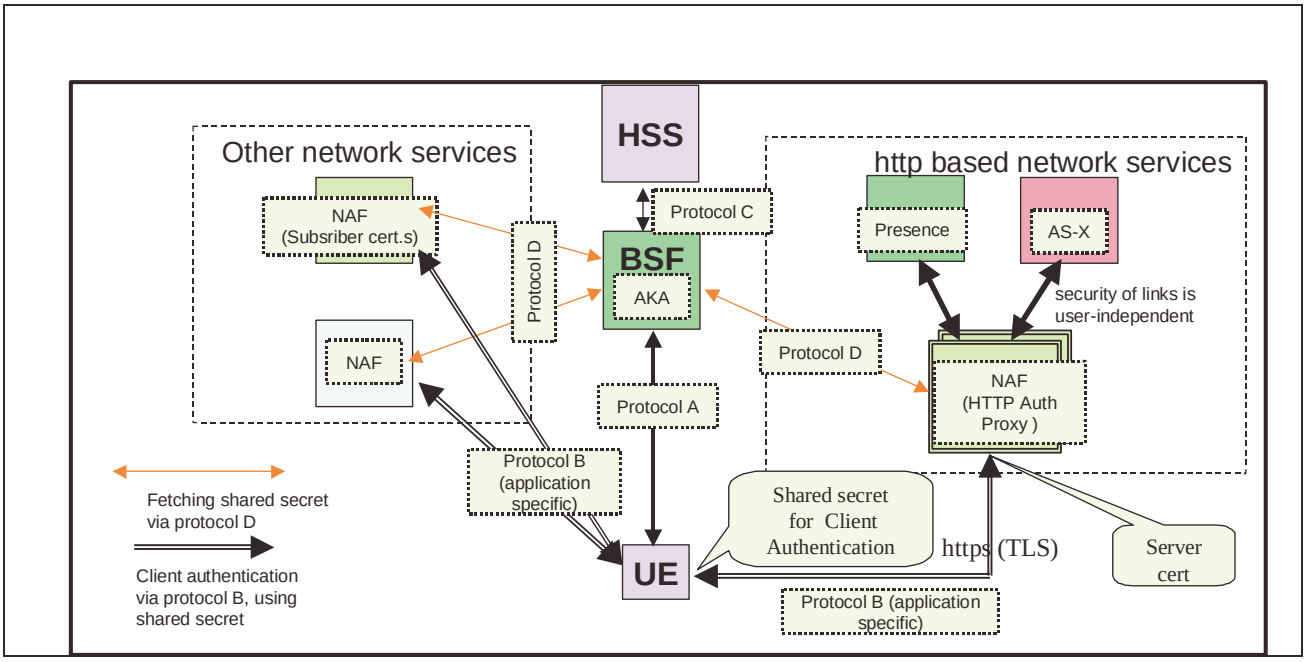

Figure 1: Simple network model for bootstrapping

Figure 2 illustrates a protocol stacks structure in network elements that are involved in bootstrapping of application security from 3G AKA and support for subscriber certificates.

Editor's note: The current protocol stack figure is placed here as a holder. The actual protocols will be defined later.

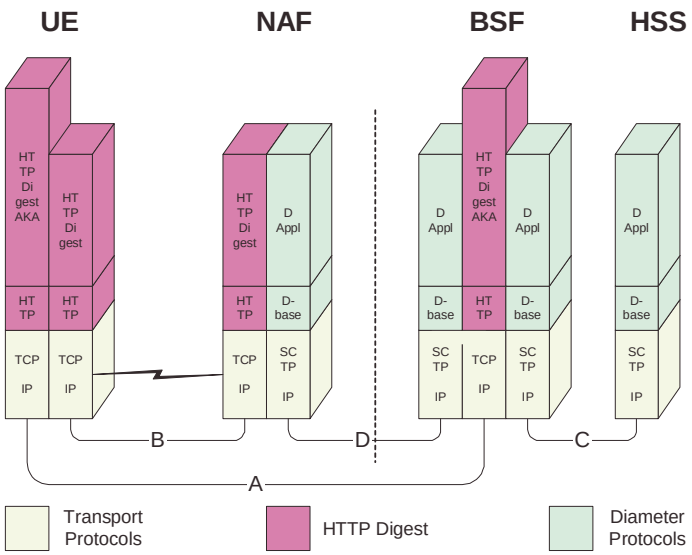

Figure 2: Protocol stack architecture

4.2.2 Network elements

4.2.2.1 Bootstrapping server function (BSF)

A generic bootstrapping server function (BSF) and the UE shall mutually authenticate using the AKA protocol, and agree on session keys that are afterwards applied between UE and an operator-controlled network application function (NAF). The key material must be generated specifically for each NAF independently.

Editor's note: key generation for NAF is ffs. Potential solutions may include:

- *· Separate run of protocol A for each request of key material from a NAF*
- *Derivation of NAF-specific keys in BSF*

4.2.2.2 Network application function (NAF)

After the bootstrapping has been completed, the UE and an operator-controlled network application function (NAF) can run some application specific protocol where the authentication of messages will be based on those session keys generated during the mutual authentication between UE and BSF.

General assumptions for the functionality of an operator-controlled network application function (NAF):

- There is no previous security association between the UE and the NAF.
- NAF shall able to locate and communicate securely with subscriber's BSF.
- NAF shall be able to acquire a shared key material established between UE and the bootstrapping server function (BSF) during running application-specific protocol.

4.2.2.3 HSS

HSS shall store new parameters in subscriber profile related to the usage of bootstrapping function. Possibly also parameters related to the usage of some network application function are stored in HSS.

Editor's note: Needed new parameters are FFS.

4.2.2.4 UE

The required new functionalities from UE are:

- The support of HTTP Digest AKA protocol,
- The capability to derive new key material to be used with protocol B from CK and IK, and
- Support of NAF specific application protocol (see annex A).

4.2.3 Reference points

4.2.3.1 A

The reference point A is between the UE and the BSF. The functionality is radio access independent and can be run in both CS and PS domains.

Editor's notes: The solution for CS domain is ffs.

4.2.3.1.1 Functionality

Reference point A provides mutual authentication between the UE and the BSF entities. It allows the UE to bootstrap the session keys based on the 3G infrastructure. The session key as result of key agreement functionality, is used to support further applications e.g. certificate issuer.

4.2.3.1.2 Protocol

Protocol A is in format of HTTP Digest AKA, which is specified in [RFC3310]. It is based on the 3GPP AKA [4] protocol that requires information from USIM and/or ISIM. The interface to the USIM is as specified for 3G [3].

4.2.3.2 B

Protocol B is the application protocol which is secured using the keys material agreed between UE and BSF as a result of the run of protocol A. For instance, in the case of support for subscriber certificates, it is a protocol, which allows the user to request certificates from the NAF. In this case NAF would be the PKI portal.

4.2.3.3 C

Protocol C is used between the BSF and the HSS to allow the BSF to fetch the required authentication information and subscriber profile information from the HSS. The interface to the 3G Authentication Centre is HSS-internal, and it need not be standardised as part of this architecture.

4.2.3.4 D

Protocol D is used by the NAF to fetch the key material agreed in protocol A from the BSF. It may also be used to fetch subscriber profile information from BSF.

4.3 Procedures

This chapter 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 latter the key material generation procedure.

4.3.1 Bootstrapping procedures

When a UE wants to interact with an NAF, it shall first perform a bootstrapping authentication (see Figure 3):Editor's notes: Protocol C related procedure will be added here in future development. It may re-use Cx interface that is specified in TS 29.228.

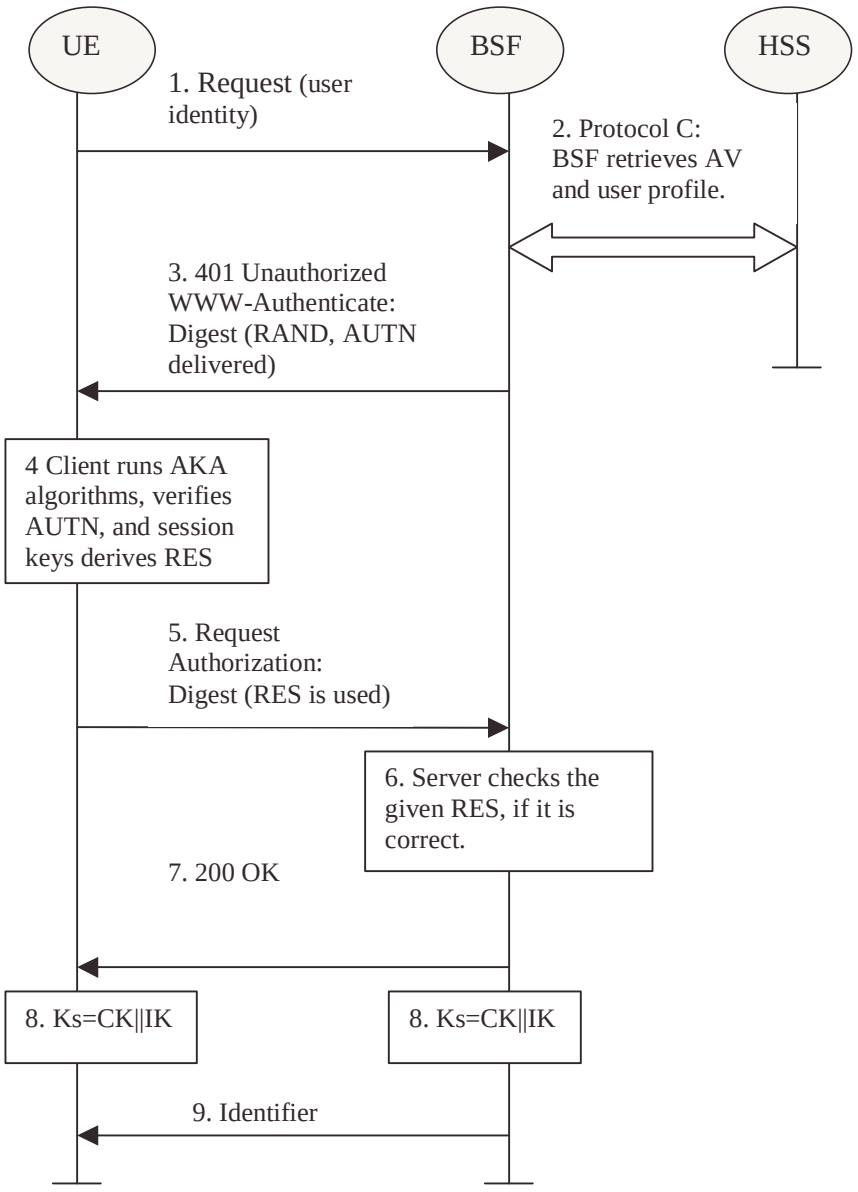

Figure 3: The bootsrapping procedure

1: The UE sends an HTTP request towards the BSF.

2. BSF retrieves the user profile and a challenge, i.e. the Authentication Vector (AV, AV = RAND||AUTN||XRES||CK||IK) by protocol C from the HSS.

3. Then BSF forwards the RAND and AUTN to the UE in the 401 message (without the CK, IK and XRES). This is to demand the UE to authenticate itself.

4: The UE calculates the message authentication code (MAC) so as to verify the challenge from authenticated network; the UE also calculates CK, IK and RES. This will result in session keys IK and CK in both BSF and UE.

5. The UE sends request again, with the Digest AKA RES as the response to the BSF.

6: If the RES equals to the XRES that is in the AV, the UE is authenticated.

7. The BSF shall send 200 OK message to the UE to indicate the success of the authentication.

8. The key material Ks is generated in both BSF and UE by concatenating CK and IK. The Ks is used for securing the protocol B.

Editor's note: The key material Ks is 256 bits long. It is up each NAF to make the usage of the key material specifically.

9. BSF may supply a transaction identifier to UE in the cause of protocol A.

4.3.2 Procedures using bootstrapped Security Association

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 Figure4:

UE starts protocol B with the NAF

- In general, UE and NAF will not yet share the key(s) required to protect protocol B. If they already do, there is no need for NAF to invoke protocol D.
- It is assumed that UE supplies sufficient information to NAF, e.g. a transaction identifier, to allow the NAF to retrieve specific key material from BSF.
- The UE derives the keys required to protect protocol B from the key material.

NAF starts protocol D with BSF

- The NAF requests key material corresponding to the information supplied by the UE to the NAF (e.g. a transaction identifier) in the start of protocol B.
- The BSF supplies to NAF the requested key material.
- The NAF derives the keys required to protect protocol B from the key material in the same way as the UE did.

NAF continues protocol B with UE

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

Editor's note: Message sequence diagram presentation and its details will be finalized later.

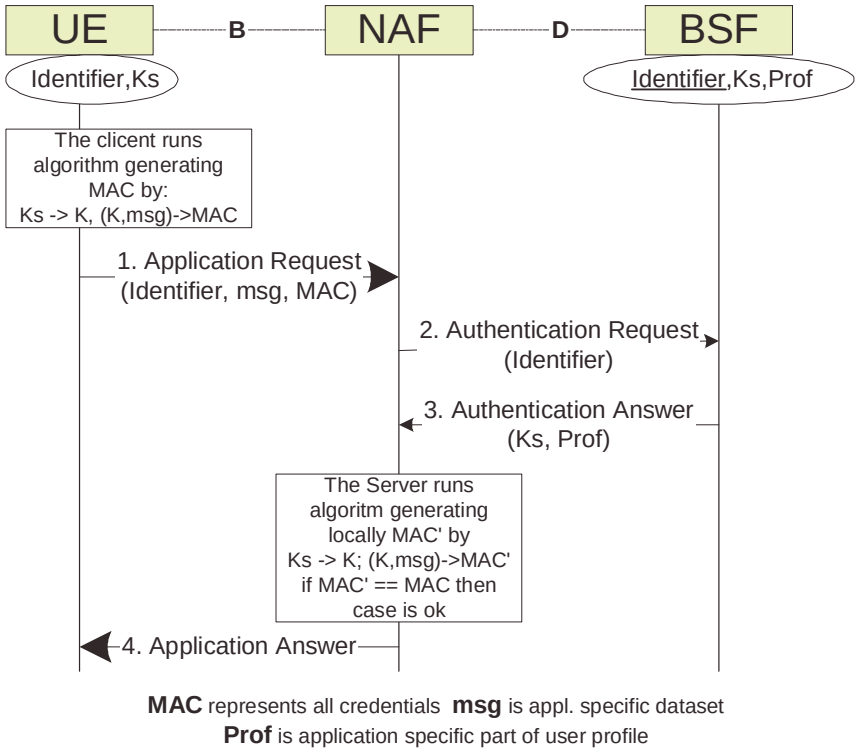

Figure 4: The bootstrapping usage procedure

"TSG <Name>" on the front page

*The following text are used for the Technical Specification Group "<**Name**>" on the front Page:*

TSG	Full Name
TSG CN	Core Network
TSG RAN	Radio Access Network
TSG SA	Services and System Aspects
TSG T	Terminals
TSG GERAN	GSM/EDGE Radio Access Network

Annex <X> (informative): Change history

It is usual to include an annex (usually the final annex of the document) for specifications under TSG change control which details the change history of the specification using a table as follows:

Change history							
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**
2001-07					*Copyright date changed to 2001; space character added before TTC in coyright notification; space character before first reference deleted.*	*1.3.2*	*1.3.3*
2002-01					*Copyright date changed to 2002.*	*1.3.3*	*1.3.4*
2002-07					*Extra Releases added to title area.*	*1.3.4*	*1.3.5*
2002-12					*“TM” added to 3GPP logo*	*1.3.5*	*1.3.6*
2003-02					*Copyright year changed to 2003.*	*1.3.6*	*1.3.7*

Work Item Description

Title

Generic Bootstrapping Architecture

1 3GPP Work Area

	Radio Access
X	Core Network
	Services

2 Linked work items

Support for subscriber certificates (SSC) (ab.cde)
Presence (33.cde)
MBMS (33.246)
WLAN (33.234)

3 Justification

At the S3 adhoc held in Antwerp September 2003, SA3 agreed as a working assumption that a generic bootstrapping architecture (GBA) is needed for bootstrapping of shared secrets. The basis for the for the GBA is presented in Figure 1 in section 6.1 of S3z030011. The architecture incorporates the bootstrapping architecture from the draft SSC TS, amended with special NAFs for authentication proxy and PKI portal.

As GBA may be used by several applications (support for subscriber certificates, Presence, MBMS), it would be logical to create a new GBA TS, describing the generic, application independent parts of the architecture. The applications, e.g. SSC, Presence and MBMS that use the GBA would reference the GBA TS and applications specific parts would be specified in the application specific technical specifications.

4 Objective

The objective of this work item is to specify a Generic Bootstrapping Architecture (GBA) that can be used for installing shared secrets between a UE and a network element (typically a UE and an application server).

GBA should fulfill the following requirements :

1. A Generic Bootstrapping Architecture (GBA) shall provide shared secrets to entities for use with 3G security features for Release 6 and future releases. Features already specified for Release 5 and earlier releases shall not be affected by the GBA.
2. This provision of shared secrets shall be based on the 3G AKA infrastructure (bootstrapping from AKA).
3. The GBA should be applicable as widely as possible to 3G security features for Release 6 and future releases, whether they are http-based or not.

4. The co-existence of several bootstrapping procedures in the 3G architecture should be avoided. In particular, the co-existence of a procedure for bootstrapping of HTTP-based services (as in S3-030367 and S3-030371) and a procedure for generic bootstrapping, as described in the context of support for subscriber certificates (S3-030317), should be avoided.
5. Dependencies on external bodies should be minimised. This would still allow to re-use completed external specifications if seen beneficial.
6. The GBA should respect the HSS/HLR-related security architecture guidelines, as documented in S3-030460. If further guidelines and other criteria regarding service provision or the impact on other entities are agreed by SA3 in the future these should be taken into account in the design as well.
7. Traffic bottlenecks should be avoided. (In particular, it should be investigated whether an HTTP authentication proxy could be such a bottleneck.)
8. The GBA should be able to support applications requiring end-to-end security.
9. The usefulness of the cryptographic separation of keys among applications should be further investigated under the aspect of future-proofing the GBA. If found that such a separation may be useful the GBA should be able to support it.
10. The GBA should support scenarios which require mutual authentication between UE and application server, based on the bootstrapped shared secret. This should not preclude the use of the GBA in scenarios where mutual authentication is provided also using other means (e.g. network certificates).
11. The Generic Architecture should be able to allow the application servers and the terminal to acquire (re-)fresh keys.
12. It would be desirable for the GBA to be applicable to non-3GPP security features.
13. For Release 6, the GBA should concentrate on home-provided services, i.e.the authentication is always performed by a server in the home network. But the GBA should not prevent future extension to a scenario where the authentication is performed by a server in a visited networks.
14. The GBA should not mandate intervention by the human user.

5 Service Aspects

The GBA provides for means to bootstrap shared secrets. It is up to each service to specify how the shared secrets are used for that specific service.

6 MMI-Aspects

None identified

7 Charging Aspects

None identified

8 Security Aspects

This is a security work item.

9 Impacts

Affects:	UICC apps	ME	AN	CN	Others
Yes		X		X	
No			X		
Don't know	X				X

10 Expected Output and Time scale (to be updated at each plenary)

Meeting	Date	Activity
S3#30	October 7-10, 2003	Approval of this WID. Progress the TS
S3#31	November 17-21, 2003	Definition and agreement on security architecture. Progress the TS.
S3#32	February, 2004	The required CRs approved.

New specifications						
Spec No.	Title	Prime rsp. WG	2ndary rsp. WG(s)	Presented for information at plenary#	Approved at plenary#	Comments

Affected existing specifications				
Spec No.	CR	Subject	Approved at plenary#	Comments
ab.cde		Moving the generic bootstrapping parts from the SSCTS to GBA TS		
		Including application specific parts to application specific TSes		The SSC TS, the presence TS and the MBMS TS are affected

11 Work item raporteurs

Bengt Sahlin, Ericsson

12 Work item leadership

TSG SA WG3

13 Supporting Companies

Ericsson, …

14 Classification of the WI (if known)

	Feature (go to 14a)
	Building Block (go to 14b)
	Work Task (go to 14c)

14a The WI is a Feature: List of building blocks under this feature

(list of Work Items identified as building blocks)

14b The WI is a Building Block: parent Feature

(one Work Item identified as a feature)

14c The WI is a Work Task: parent Building Block

(one Work Item identified as a building block)

form change history:
2002-07-04: "USIM" box changed to "UICC apps"