3GPP TR 33.920 V7.5.0 (2008-03)

Technical Report

3rd Generation Partnership Project;
Technical Specification Group Services and System Aspects;
SIM card based Generic Bootstrapping Architecture (GBA)
Early implementation feature
(Release 7)

Keywords

UMTS, GSM, security, architecture

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 Report 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

3GPP defined the Generic Bootstrapping Architecture (GBA) in Release 6. The Release 6 GBA is based on 3G USIMs and ISIMs, i.e., 3G GBA TS 33.220 [1]. The security level of 3G Authentication and Key Agreement is higher than the 2G SIM authentication. On the other hand, there are more than one billion people with SIMs in their phones and it will take long time to provision UICCs capable of 3G authentication to such a large population. Meanwhile there should be a way to offer services whose authentication is based on GAA also to 2G subscribers.

Mobile network operators could try first out the success of services without handing out new cards and after successful service usage migrate seamlessly to UICCs. This option leverages the mobile network operators investments into their SIM cards, while still provide easy migration. This could lower the threshold for operators to deploy more sophisticated services that usually would require a UICC from the start. In this way, it might even speed up the process of handing out UICCs to the subscribers. The initial roll-out phases of services and service success testing would not need to rely on passwords. In addition, the introduction of 2G GBA -based authentication provides a security and operational enhancement for users that rely on SIM. Also, the availability of 2G GBA will allow building services where authentication is performed and managed in an analogous way as using USIM. The protocol wherein the SIM card is used, decides the strength of the security of the whole system. Therefore, the solution described for an early implementation feature in this specifications targets to enhance GSM security to address the known GSM vulnerabilities when using 2G GBA.

It should be noted that the work outlined in this feature does not require any change to the existing SIM specifications, in particular GBA_U as in 3G GBA will not be included in 2G GBA.

1 Scope

The present document describes which change requests are to be implemented in addition to the Release 6 specifications TS 33.220 [1], TS 29.109 [2], and TS 24.109 [3] to enable the usage of 2G GBA.

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*.

[1] 3GPP TS 33.220 Release 6: "Generic Authentication Architecture (GAA); Generic bootstrapping architecture".

[2] 3GPP TS 29.109 Release 6: "Generic Authentication Architecture (GAA); Zh and Zn Interfaces based on the Diameter protocol; Stage 3".

[3] 3GPP TS 24.109 Release 6: "Bootstrapping interface (Ub) and network application function interface (Ua); Protocol details".

[4] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in TR 21.905 [4] and the definitions in TS 33.220 [1] apply.

3.2 Abbreviations

The abbreviations of TS 33.220 [1] also apply to this document.

4 Additions to enable 2G GBA

4.1 Additions to TS 33.220

The following changes to TS 33.220 [1] are needed to be implemented to enable 2G GBA:

- CR069 (rev 1) to TS 33.220 [1]: "Normative annex on 2G GBA";

- CR079 to TS 33.220 [1]: "Removal of possible interoperability problems";

- CR078 to TS 33.220 [1]: "IMPI obtained from IMSI in 2G GBA";

- CR076 to TS 33.220 [1]: "Alignment of 2G GBA with recent CRs";

- CR087 to TS 33.220 [1]: "GBA keys handling and UICC presence detection";

- CR089 to TS 33.220 [1]: "Clarify the confusion of the use of NAF-ID and FQDN";

- CR091 to TS 33.220 [1]: "Use of SIM for Ua applications";

- CR0120 (rev 1) to TS 33.220 [1]: "Clarification on NAF_Id coding"

- CR0123 to TS 33.220 [1]: "Details of HLR – BSF reference point"

- CR0124 to TS 33.220 [1]: "Clarifying the terms 2G and 3G for GBA"

- CR0127 (rev 4) to TS 33.220 [1]: "Correction of HLR – BSF reference point".

- CR0131 (rev 1) to TS 33.220 [1]: "2G GBA Certificate Management".

- CR0133 (rev 1) to TS 33.220 [1]: " Usage of OMA References – Update of References".

4.2 Additions to TS 29.109

The following changes to TS 29.109 [2] are needed to be implemented to enable 2G GBA:

- CR0022 to TS 29.109 [2]: "2G GBA implementation to Zh and Zn".

4.3 Additions to TS 24.109

The following changes to TS 24.109 [3] are needed to be implemented to enable 2G GBA:

- CR0023 (rev1) to TS 24.109 [3]: "2G GBA".

- CR0036 to TS 24.109 [3]: "Interoperability problems for request on Ub reference point".

Annex A:
Change history

Change history									
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**Old**	**New**	**WI**
2006-03	SP-31	SP-060063	-	-	-	Approved at SA #31	2.0.0	7.0.0	
2006-06	SP-32	SP-060386	0001	-	D	Reference addition	7.0.0	7.1.0	2G GBA
2007-06	SP-36	SP-070327	0002	-	F	NAF_ID Encoding	7.1.0	7.2.0	2G GBA
2007-09	SP-37	SP-070591	0003	-	F	Update with regard to approved CRs to TS 33.220 Annex I	7.2.0	7.3.0	2G GBA
2007-12	SP-38	SP-070785	0004	1	F	Integration of approved CR to TS 33.220 on HLR integration	7.3.0	7.4.0	SEC7-2GGBA
2008-03	SP-39	SP-080140	0005	-	F	Addition of 2G GBA related CRs	7.4.0	7.5.0	SEC7-2GGBA