

1 3GPP2 S.R0112-0  
2 Version 1.0  
3 Version Date: 08 December 2005  
4  
5  
6  
7  
8  
9



3RD GENERATION  
PARTNERSHIP  
PROJECT 2  
"3GPP2"

# 10 *Generic Bootstrapping Architecture System* 11 *Requirements*

---

12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24

***COPYRIGHT NOTICE***

*3GPP2 and its Organizational Partners claim copyright in this document and individual Organizational Partners may copyright and issue documents or standards publications in individual Organizational Partner's name based on this document. Requests for reproduction of this document should be directed to the 3GPP2 Secretariat at [secretariat@3gpp2.org](mailto:secretariat@3gpp2.org). Requests to reproduce individual Organizational Partner's documents should be directed to that Organizational Partner. See [www.3gpp2.org](http://www.3gpp2.org) for more information.*

25  
26

1 **EDITOR**  
2 *Adrian Escott*  
3 *5775 Morehouse Drive*  
4 *San Diego*  
5 *CA 92121*  
6 *USA*  
7 [aescott@qualcomm.com](mailto:aescott@qualcomm.com)

8  
9  
10  
11 **REVISION HISTORY**

---

12

<b>REVISION HISTORY</b>		
<b>Revision number</b>	<i>Content changes.</i>	<i>Date</i>
<b>1.0</b>	<i>First publication</i>	<i>12.08.2005</i>

13

## Table of Contents

1		
2		
3	Table of Contents .....	1
4	List of Tables .....	2
5	List of Figures .....	3
6	1 Introduction.....	4
7	2 References .....	4
8	3 Definitions and Abbreviations .....	4
9	3.1 Definitions .....	4
10	3.2 Abbreviations.....	4
11	4 General Description.....	4
12	5 High Level System Requirements.....	5
13	5.1 Network Operator .....	5
14	5.2 Bootstrapping procedure.....	5
15	5.3 Network Application Requirements .....	5
16	5.4 Mobile Station Requirements .....	6
17	5.5 General Requirements .....	6
18		
19		

1  
2  
3

## List of Tables

1

## List of Figures

2

# 1 Introduction

This specification contains the high level requirements for the Generic Bootstrapping Architecture work. The aim of this work is to specify a general method of providing an application and a mobile with some shared keying material. The requirements on how the application and mobile use this shared keying material is out of scope of specification.

## 2 References

## 3 Definitions and Abbreviations

### 3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

**Application:** This is a service that is offered by the Home Operator or a third party. For the purpose of Generic Bootstrapping Architecture, it is assumed that an application runs between a MS and some network or 3<sup>rd</sup> party entity. It is also assumed that some shared keying material is needed to secure the application.

**Bootstrapping Procedure:** This procedure is used for generating shared keying material, which can be used to secure an application. The bootstrapping procedure is run between a MS and some network entity.

**Mobile Station (MS):** This is the device containing the user's subscription. It runs the bootstrapping procedure and uses the resulting shared keying material to secure an application it is performing with some network or 3<sup>rd</sup> party entity.

**Network Application:** This is a network or 3<sup>rd</sup> party entity that runs an application with a MS. Securing that application requires shared keying material that is generated by the bootstrapping procedure.

**Shared key material:** This is the secret that is used by a network application and a MS to secure communication between them. It can be generated for a particular MS and network application pair as the result of a run of the bootstrapping procedure.

**User Identity Module (UIM):** The User Identity Module is a low power processor that contains secure memory. The User Identity Module may be a Removable-UIM (R-UIM) or part of the Mobile Station itself.

### 3.2 Abbreviations

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

GBA	Generic Bootstrapping Architecture
MS	Mobile Station
UIM	User Identity Module

## 4 General Description

Most services that are developed for a mobile environment require some security. A part of this security is specifying where the key material for securing the service comes from. GBA aims to specify a way of providing shared keying material to network applications and MSs such that they can communicate securely. Network operators already have a cryptographic relationship with their subscribers through the UIMs in their MSs. Currently this relationship is used to provide authentication of the MS to the network and keys for protecting network access. GBA will re-use

1 this cryptographic relationship where possible to provide keys for use between a network  
2 application and an MS.

3  
4 Re-using this cryptographic relationship should simplify the development of new services (that  
5 can use GBA), as there will be need to specify where the keys that will be used for the service will  
6 come from. It also avoids the need to provision new keys on an MS and hence may allow new  
7 services to be more easily deployed on to old MSs. Furthermore the applications that can be  
8 developed to use GBA are not restricted to those developed by 3GPP2. Additionally a network  
9 operator may be able to re-use some existing network elements in providing the bootstrapped  
10 keys.

## 11 **5 High Level System Requirements**

12 The following subsections give the requirements on the various elements of GBA including  
13 general requirements.  
14

### 15 **5.1 Network Operator**

16  
17 NOR-1: The network operator shall be able to control whether a particular subscriber can use the  
18 bootstrapping procedure.

19  
20 NOR-2: The network operator shall be able control whether a particular subscriber can use shared  
21 keying material with a particular application.  
22

23 NOR-3: The network operator shall be able to set some security policy (e.g., expiry time of the  
24 shared keying material) for the use of shared keying material between an application and a  
25 particular MS.  
26

27 NOR-4: The network operator shall be able to control which networks elements may perform the  
28 bootstrapping procedure and must trust those elements with cryptographic material.  
29

30 NOR-5: The network operator shall only have to trust the application enough to handle the shared  
31 key material specific to the application.  
32

33 NOR-6: The transfer of shared keying material and authentication material shall be secured.  
34

### 35 **5.2 Bootstrapping procedure**

36  
37 BSR-1: Performing the bootstrapping procedure shall not be dependent on the application.  
38

39 BSR-2: The bootstrapping procedure shall provide different applications with independent shared  
40 keying material (i.e., cryptographic separation of keys), so that if one application is broken then it  
41 will not compromise the security of another application.  
42

43 BSR-3: Running the bootstrapping procedure shall be access independent and shall only require IP  
44 connectively from the MS.  
45

46 BSR-4: Each run of the bootstrapping procedure shall result in fresh shared keying material.  
47

48 BSR-5: One run of the bootstrapping procedure shall be capable of providing shared keying  
49 material for several applications.  
50

### 51 **5.3 Network Application Requirements**

52

1 NAR-1: A network application does not need to be aware of how the bootstrapping is performed.  
2 It only needs to be able to link sufficiently with the Bootstrapping procedure to enable using the  
3 shared key material that is specific to that application.  
4

5 NAR-2: An application shall be able to require a new run of the bootstrapping procedure to  
6 generate the shared keying material to be used with a particular MS.  
7

## 8 **5.4 Mobile Station Requirements**

9  
10 MSR-1: An MS shall have a valid 3GPP2 subscription in order to perform the bootstrapping  
11 procedure.  
12

13 MSR-2: It shall be possible to derive the shared keying material in the UIM.  
14

## 15 **5.5 General Requirements**

16  
17 GR-1: To the extent possible, existing protocols and infrastructure should be re-used (e.g., the  
18 3GPP2 network authentication protocols).  
19

20 GR-2: It shall be possible to use the bootstrapping procedure to generate shared keying material  
21 for applications that are specified outside of 3GPP2.