

3GPP TR 33.919 V0.1.0 (2003-10)

Technical Report

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



The present document has been developed within the 3rd Generation Partnership Project (3GPP™) and may be further elaborated for the purposes of 3GPP.

The present document has not been subject to any approval process by the 3GPP Organizational Partners and shall not be implemented. This Specification is provided for future development work within 3GPP only. The Organizational Partners accept no liability for any use of this Specification. Specifications and reports for implementation of the 3GPP™ system should be obtained via the 3GPP Organizational Partners' Publications Offices.

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>

Copyright Notification

No part may be reproduced except as authorized by written permission.
The copyright and the foregoing restriction extend to reproduction in all media.

© 2003, 3GPP Organizational Partners (ARIB, CWTS, ETSI, T1, TTA, TTC).
All rights reserved.

Contents

Contents	3
Foreword.....	3
Introduction.....	4
1 Scope.....	4
2 References	4
3 Definitions, symbols and abbreviations	5
3.1 Definitions.....	5
3.2 Symbols	5
3.3 Abbreviations	5
4 Generic Authentication Architecture	6
4.1 GAA overview	6
4.2 Authentication using shared secret	6
4.3 Authentication based on (public, private) key pair and certificates	6
5 Issuing authentication credentials.....	6
5.1 Schematic overview.....	6
5.2 GBA: Mechanism to issue shared secret	6
5.3 SSC: Mechanism to issue subscriber certificates.....	7
6 GAA building blocks	7
6.1 Overview.....	Error! Bookmark not defined.
6.2 GAA	8
6.3 GBA.....	8
6.4 SSC.....	8
6.5 HTTPS	8
6.5.1 HTTPS with AP	8
6.5.2 HTTPS without AP	8
7 Application guidelines to use GAA.....	8
7.1 Use of shared secrets and GBA	8
7.2 Use of certificatesAnnex <X> (informative): Change history.....	8
7.2 Annex <X> (informative): Change history	9

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

Context of GAA and clarification of how we end up writing this TR (with some reference to 3 TS documents).

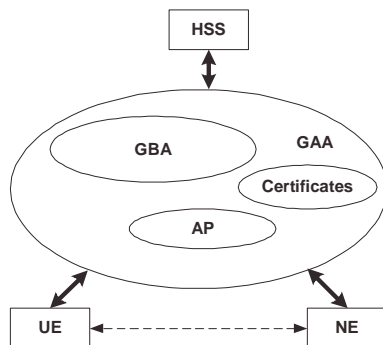


Figure 1. Schematic illustration of GAA

1 Scope

Put different specifications under the work item Support for Subscriber Certificates into perspective. Clarifying the logic for having three technical specifications, sketching their content and explaining the inter-relation among these three TSs and the relation with this TR.

Give an overview of the different mechanisms that applications can rely upon for authentication between server and user (person and/or device). Give guidelines for applications related to the use of GAA and the choice of authentication mechanism.

2 References

The following documents contain provisions that, 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 TS 33.102: "Security Architecture".

[2] 3GPP TS 33.220: "Generic Authentication Architecture; Generic Bootstrapping Architecture"

[3] 3GPP TS 33.221: "Generic Authentication Architecture; Support for Subscriber certificates"

- [3] 3GPP TS ab.cde: “Generic Authentication Architecture; Access to Network Application Function using HTTPS”

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.

Subscriber certificate: a certificate issued to a subscriber. It contains subscriber's own public key and possibly other information such as subscriber's identity in some form.

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:

AKA	Authentication and Key Agreement
AP	Authentication Proxy
GAA	Generic Authentication Architecture
GBA	Generic Bootstrapping Architecture
HSS	Home Subscriber System
NE	Network Element
SSC	Support for Subscriber Certificates
UE	User Equipment

4 Generic Authentication Architecture

4.1 GAA overview

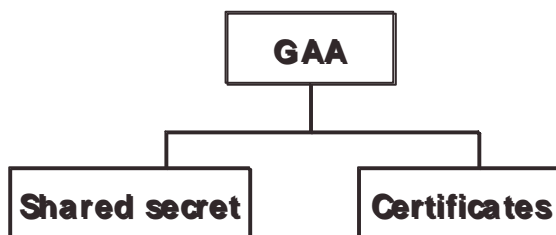


Figure 2: GAA schematic overview

4.2 Authentication using shared secret

4.3 Authentication based on (public, private) key pair and certificates

5 Issuing authentication credentials

5.1 Schematic overview

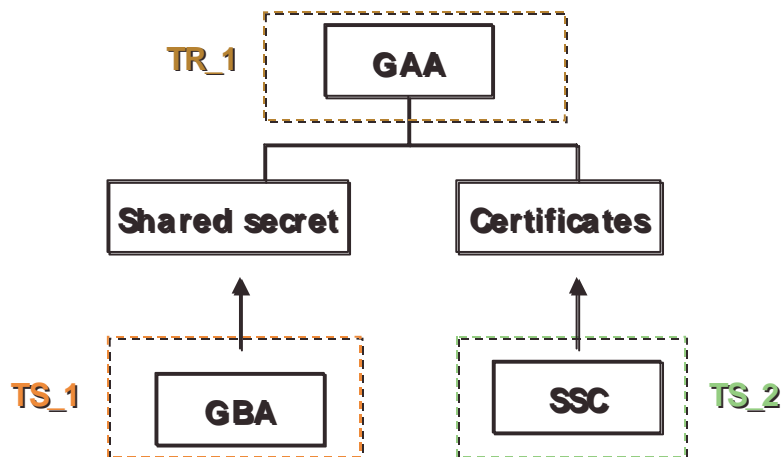


Figure 3 Illustration of mechanisms to issue authentication credentials

Note: other mechanisms for issuing authentication credentials may exist but are out of scope for this TR and the TSs under the referenced WI and will not be discussed here.

5.2 GBA: Mechanism to issue shared secret

Editor's note: To be completed with a very short explanation and reference to GBA TS.

5.3 SSC: Mechanism to issue subscriber certificates

Editor's note: To be completed with a very short explanation and reference to SSC TS.

6 GAA building blocks

6.1 GAA structural overview

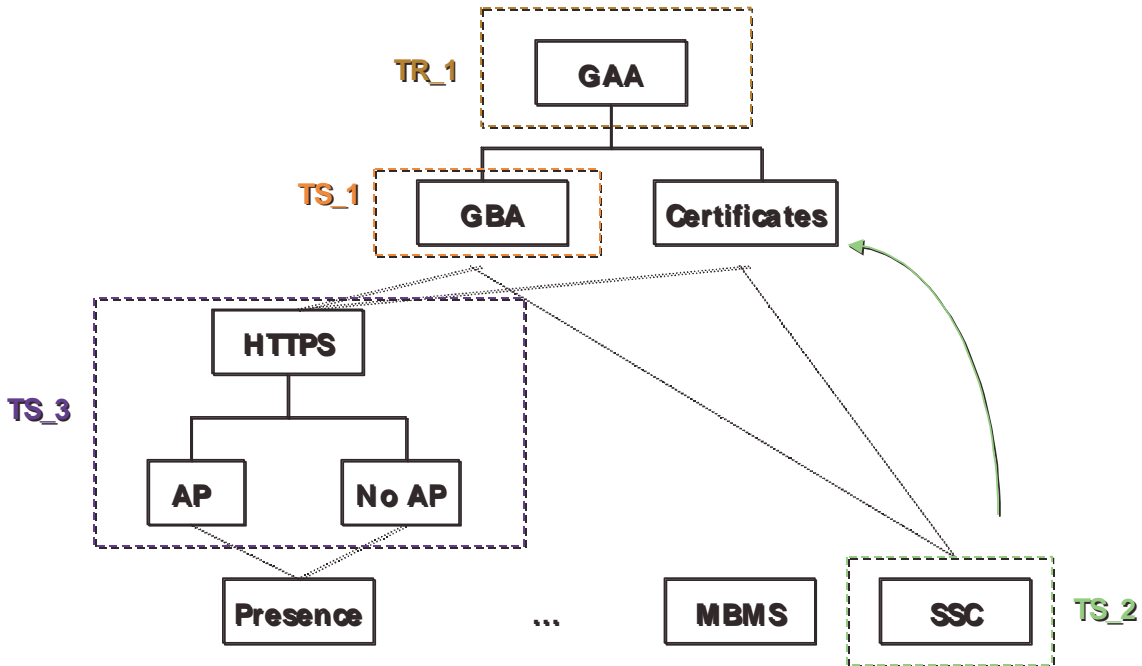


Figure 4 Detailed overview of inter-relationship of GAA building blocks

6.2 GAA

6.3 GBA

6.4 SSC

6.5 HTTPS

6.5.1 HTTPS with AP

6.5.2 HTTPS without AP

7 Application guidelines to use GAA

7.1 Use of shared secrets and GBA

7.2 Use of certificates

Annex <X> (informative):
Change history

Change history							
Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Old	New
2003-10	SA3#30				New Draft TR: Generic Authentication Architecture (GAA).		0.1.0