

ETSI TS 133 220 V14.1.0 (2017-07)



**Digital cellular telecommunications system (Phase 2+) (GSM);
Universal Mobile Telecommunications System (UMTS);
LTE;
Generic Authentication Architecture (GAA);
Generic Bootstrapping Architecture (GBA)
(3GPP TS 33.220 version 14.1.0 Release 14)**



Reference

RTS/TSGS-0333220ve10

Keywords

GSM,LTE,SECURITY,UMTS

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

The present document can be downloaded from:

<http://www.etsi.org/standards-search>

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status.

Information on the current status of this and other ETSI documents is available at

<https://portal.etsi.org/TB/ETSI/DeliverableStatus.aspx>

If you find errors in the present document, please send your comment to one of the following services:

<https://portal.etsi.org/People/CommiteeSupportStaff.aspx>

Copyright Notification

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.

The content of the PDF version shall not be modified without the written authorization of ETSI.

The copyright and the foregoing restriction extend to reproduction in all media.

© ETSI 2017.

All rights reserved.

DECT™, PLUGTESTS™, UMTS™ and the ETSI logo are trademarks of ETSI registered for the benefit of its Members.

3GPP™ and LTE™ are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.

oneM2M logo is protected for the benefit of its Members.

GSM® and the GSM logo are trademarks registered and owned by the GSM Association.

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (<https://ipr.etsi.org/>).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Specification (TS) has been produced by ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities, UMTS identities or GSM identities. These should be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between GSM, UMTS, 3GPP and ETSI identities can be found under <http://webapp.etsi.org/key/queryform.asp>.

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the [ETSI Drafting Rules](#) (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Contents

Intellectual Property Rights	2
Foreword.....	2
Modal verbs terminology.....	2
Foreword.....	7
1 Scope	8
2 References	8
3 Definitions, abbreviations symbols and conventions	10
3.1 Definitions	10
3.2 Abbreviations	11
3.3 Symbols.....	11
3.4 Conventions.....	12
4 Generic Bootstrapping Architecture.....	12
4.1 Reference model.....	12
4.2 Network elements.....	14
4.2.1 Bootstrapping server function (BSF).....	14
4.2.2 Network application function (NAF).....	14
4.2.2a Zn-Proxy.....	15
4.2.3 HSS.....	15
4.2.4 UE.....	16
4.2.5 SLF	16
4.2.6 HLR	17
4.3 Bootstrapping architecture and reference points	17
4.3.1 Reference point Ub	17
4.3.2 Reference point Ua	17
4.3.3 Reference point Zh.....	17
4.3.4 Reference point Zn.....	17
4.3.5 Reference point Dz	17
4.3.6 Reference point Zh'.....	17
4.4 Requirements and principles for bootstrapping.....	17
4.4.1 Access Independence.....	18
4.4.2 Authentication methods	18
4.4.3 Roaming.....	18
4.4.4 Requirements on reference point Ub	18
4.4.5 Requirements on reference point Zh.....	19
4.4.6 Requirements on reference point Zn.....	19
4.4.7 Requirements on Bootstrapping Transaction Identifier	20
4.4.8 Requirements on selection of UICC application and related keys.....	21
4.4.8.1 UICC application activation procedure in GBA	22
4.4.9 Requirements on reference point Ua.....	23
4.4.10 Requirements on reference point Dz.....	23
4.4.11 Requirements on GBA keys and parameters handling.....	23
4.4.12 Requirements on reference point Zh'	24
4.4.13 Requirements on TMPI handling.....	25
4.5 Procedures	25
4.5.1 Initiation of bootstrapping	25
4.5.2 Bootstrapping procedures	26
4.5.3 Procedures using bootstrapped Security Association	28
4.5.4 Procedure related to service discovery.....	30
5 UICC-based enhancements to Generic Bootstrapping Architecture (GBA_U)	31
5.1 Architecture and reference points for bootstrapping with UICC-based enhancements	31
5.2 Requirements and principles for bootstrapping with UICC-based enhancements.....	31
5.2.1 Requirements on UE	31
5.2.2 Requirements on BSF	31

5.3	Procedures for bootstrapping with UICC-based enhancements	31
5.3.1	Initiation of bootstrapping	31
5.3.2	Bootstrapping procedure.....	31
5.3.3	Procedures using bootstrapped Security Association	34
5.3.4	Procedure related to service discovery.....	36
Annex A (informative):	(Void)	37
Annex B (normative):	Specification of the key derivation function KDF.....	38
B.1	Introduction	38
B.2	Generic key derivation function	38
B.2.0	General	38
B.2.1	Input parameter encoding	38
B.2.1.1	General.....	38
B.2.1.2	Character string encoding.....	39
B.2.1.3	Non-negative integer encoding	39
B.2.2	FC value allocations	39
B.3	NAF specific key derivation in GBA and GBA_U	40
B.4	Derivation of TMPI.....	40
B.5	Derivation of passwd and Ks.....	41
B.6	NAF specific key derivation in GBA_Digest.....	42
Annex C (informative):	(Void)	43
Annex D (informative):	Dialog example for user selection of UICC application used in GBA.....	44
Annex E (normative):	TLS profile for securing Zn/Zn' reference points.....	45
Annex F (informative):	Handling of TLS certificates.....	46
Annex G (normative):	GBA_U UICC-ME interface.....	47
G.1	GBA_U Bootstrapping procedure	47
G.2	GBA_U NAF Derivation procedure.....	47
Annex H (normative):	Ua security protocol identifier	49
H.1	Definition	49
H.2	Organization Octet	49
H.3	Ua security protocol identifiers for 3GPP specified protocols	49
Annex I (normative):	2G GBA.....	51
I.0	Introduction	51
I.1	Reference model.....	51
I.2	Network elements.....	51
I.2.1	Bootstrapping server function (BSF).....	51
I.2.2	Network application function (NAF)	52
I.2.2a	Zn-Proxy.....	52
I.2.3	HSS	52
I.2.4	UE	53
I.2.5	SLF.....	53
I.2.6	HLR.....	54
I.3	Bootstrapping architecture and reference points	54
I.3.1	Reference point Ub.....	54
I.3.2	Reference point Ua.....	54

I.3.3	Reference point Zh	54
I.3.4	Reference point Zn	54
I.3.5	Reference point Dz	54
I.3.6	Reference point Zh'	54
I.4	Requirements and principles for bootstrapping	54
I.4.0	General requirements	54
I.4.1	Access Independence	55
I.4.2	Authentication methods	55
I.4.3	Roaming	55
I.4.4	Requirements on reference point Ub	55
I.4.5	Requirements on reference point Zh	56
I.4.6	Requirements on reference point Zn	56
I.4.7	Requirements on Bootstrapping Transaction Identifier	57
I.4.8	Requirements on selection of UICC application and SIM card	58
I.4.9	Requirements on reference point Ua	58
I.4.10	Requirements on reference point Dz	58
I.4.11	Requirements on reference point Zh'	58
I.5	Procedures	58
I.5.1	Initiation of bootstrapping	58
I.5.2	Bootstrapping procedures	58
I.5.3	Procedures using bootstrapped Security Association	61
I.5.4	Procedure related to service discovery	63
I.6	TLS Profile	63
I.6.1	void	64
I.6.2	Authentication of the BSF	64
I.6.3	Authentication of the UE	64
I.6.4	Set-up of Security parameters	64
Annex J (informative):	Usage of USS with local policy enforcement in BSF	65
J.1	General	65
J.2	Usage scenarios	65
J.2.1	Scenario 1: NAF does not use USSs, BSF does not have local policy for NAF	66
J.2.2	Scenario 2: NAF does not use USSs, BSF does have local policy for NAF	66
J.2.3	Scenario 3: NAF does use USSs, BSF does not have local policy for NAF	66
J.2.4	Scenario 4: NAF does use USSs, BSF does have local policy for NAF	67
Annex K (informative):	Interoperator GBA-usage examples	68
K.1	Example on interoperator GBA setup	68
K.2	Example on interoperator GBA operation	70
Annex L (informative):	Information on how security threats related to known GSM vulnerabilities are addressed by the 2G GBA solution	73
L.1	Impersonation of the UE to the BSF during the run of the Ub protocol	73
L.2	Impersonation of the BSF to the UE during the run of the Ub protocol	73
L.3	Finding the GBA key Ks during or after the Ub protocol run	74
L.4	Bidding down attack	74
Annex M (normative):	GBA_Digest	75
M.1	General	75
M.2	Reference model	75
M.3	Network elements	75
M.3.1	Bootstrapping server function (BSF)	75
M.3.2	Network application function (NAF)	76

M.3.3	Zn-Proxy.....	76
M.3.4	HSS	76
M.3.5	UE	77
M.3.6	SLF.....	77
M.4	Bootstrapping architecture and reference points	78
M.4.1	Reference point Ub.....	78
M.4.2	Reference point Ua.....	78
M.4.3	Reference point Zh	78
M.4.4	Reference point Zn	78
M.4.5	Reference point Dz	78
M.5	Requirements and principles for bootstrapping.....	78
M.5.1	General Requirements	78
M.5.2	Access independence.....	79
M.5.3	Authentication methods.....	79
M.5.4	Roaming	79
M.5.5	Requirements on reference point Ub	79
M.5.6	Requirements on reference point Zh	79
M.5.7	Requirements on reference point Zn	80
M.5.8	Requirements on Bootstrapping Transaction Identifier.....	81
M.5.9	Requirements on reference point Ua	82
M.5.10	Requirements on reference point Dz	82
M.5.11	Requirements on GBA keys and parameters handling	82
M.6	Procedures	82
M.6.1	General	82
M.6.2	Initiation of bootstrapping	82
M.6.3	Bootstrapping procedures.....	83
M.6.4	Procedures using bootstrapped Security Association	85
M.6.5	Procedure related to service discovery	88
M.7	TLS Profile	88
M.7.1	General	88
M.7.2	Authentication of the BSF	89
M.7.3	Authentication of the UE.....	89
M.7.4	Set-up of Security parameters	89
Annex N (informative):	Change history	90
History		94

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.

1 Scope

The present document describes the security features and mechanisms to bootstrap authentication and key agreement for application security. Candidate applications to use this bootstrapping mechanism include but are not restricted to subscriber certificate distribution TS 33.221 [5]. Subscriber certificates support services whose provision mobile operator assists, as well as services that mobile operator provides.

The scope of this specification includes generic bootstrapping functions, an architecture overview and the detailed procedure how to bootstrap the credential.

Clause 4 of this specification describes a mechanism, called GBA_ME, to bootstrap authentication and key agreement, which does not require any changes to the UICC. Clause 5 of this specification describes a mechanism, called GBA_U, to bootstrap authentication and key agreement, which does require changes to the UICC, but provides enhanced security by storing certain derived keys on the UICC. Annex I of this specification describes a mechanism, called 2G GBA, to bootstrap authentication and key agreement using 2G AKA protocol. Annex M of this specification describes a mechanism, called GBA_Digest, to bootstrap authentication and key agreement using HTTP Digest protocol with SIP Digest credentials.

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 31.102: "Characteristics of the USIM application". |
| [2] | 3GPP TS 33.102: "3G Security; Security architecture". |
| [3] | IETF RFC 2617: "HTTP Authentication: Basic and Digest Access Authentication". |
| [4] | IETF RFC 3310: "Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA)". |
| [5] | 3GPP TS 33.221: "Generic Authentication Architecture (GAA); Support for Subscriber Certificates". |
| [6] | Void |
| [7] | Void |
| [8] | 3GPP TS 23.228: "IP Multimedia Subsystem (IMS); Stage 2 (Release 6)". |
| [9] | Void. |
| [10] | 3GPP TS 31.103: "Characteristics of the IP Multimedia Services Identity Module (ISIM) application". |
| [11] | 3GPP TS 23.003: "Numbering, addressing and identification". |
| [12] | IETF RFC 3548: "The Base16, Base32, and Base64 Data Encodings". |
| [13] | 3GPP TS 33.210: "3G Security; Network domain security; IP network layer security". |
| [14] | Void. |