



**Digital cellular telecommunications system (Phase 2+);
Universal Mobile Telecommunications System (UMTS);**

LTE;

**Generic Authentication Architecture (GAA);
Zh and Zn Interfaces based on the Diameter protocol;
Stage 3**

(3GPP TS 29.109 version 9.7.0 Release 9)



ReferenceRTS/TSGC-0429109v970

Keywords

GSM,LTE,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

<http://portal.etsi.org/tb/status/status.asp>

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

<https://portal.etsi.org/People/CommitteeSupportStaff.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.

© European Telecommunications Standards Institute 2015.

All rights reserved.

DECTTM, PLUGTESTSTM, UMTSTM and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members. 3GPPTM and LTETM are Trade Marks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.
GSM[®] and the GSM logo are Trade Marks 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 (<http://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
1 Scope	6
2 References	10
3 Definitions, symbols and abbreviations	12
3.1 Definitions	12
3.2 Symbols.....	12
3.3 Abbreviations	12
4 GBA Bootstrapping Zh interface and Zh' interface.....	14
4.1 Generic bootstrapping network architecture.....	14
4.2 Protocol Zh between BSF and HSS.....	14
4.3 Protocol Zh' between BSF and HLR	18
4.3.1 Public to Private Identity Resolution over Zh between BSF and HLR.....	20
5 GAA Application Zn and Zpn interfaces	22
5.1 Applications" network architecture	22
5.2 Protocol Zn between NAF and BSF based on Diameter	23
5.3 Protocol Zn between NAF and BSF based on Web Services.....	26
5.4 Protocol Zpn between NAF and BSF based on Diameter	29
5.5 Protocol Zpn between NAF and BSF based on Web Services.....	33
6 Diameter application for Zh, Zn and Zpn interfaces.....	36
6.0 Introduction	36
6.1 Command-Code values	36
6.2 Result-Code AVP values.....	36
6.2.1 Success.....	36
6.2.2 Permanent failures	36
6.2.2.1 DIAMETER_ERROR_IDENTITY_UNKNOWN (5401).....	36
6.2.2.2 DIAMETER_ERROR_NOT_AUTHORIZED (5402)	36
6.2.2.3 DIAMETER_ERROR_TRANSACTION_IDENTIFIER_INVALID (5403).....	37
6.2.2.4 Void.....	37
6.2.2.5 Void.....	37
6.2.2.6 Void.....	37
6.2.2.7 Void.....	37
6.3 AVPs	37
6.3.1 Common AVPs	38
6.3.1.1 GBA-UserSecSettings AVP	38
6.3.1.2 Transaction-Identifier AVP	38
6.3.1.3 NAF-Id	38
6.3.1.4 GAA-Service-Identifier AVP	38
6.3.1.5 Key-ExpiryTime AVP	38
6.3.1.6 ME-Key-Material AVP	38
6.3.1.7 UICC-Key-Material AVP	39
6.3.1.8 GBA_U-Awareness-Indicator.....	39
6.3.1.9 BootstrapInfoCreationTime AVP	39
6.3.1.10 GUSS-Timestamp AVP	39
6.3.1.11 GBA-Type.....	39
6.3.1.12 UE-Id.....	39
6.3.1.13 UE-Id-Type	39
6.3.1.14 UICC-App-Label	39
6.3.1.15 UICC-ME.....	40
6.3.1.16 Requested-Key-Lifetime	40
6.3.1.17 Private-Identity-Request	40

6.3.1.18	GBA-Push-Info	40
6.3.1.19	NAF-SA-Identifier	40
6.3.1.20	Security-Feature-Request	40
6.3.1.21	Security-Feature-Response	40
6.4	User identity to HSS resolution	40
7	Use of namespaces	42
7.1	AVP codes	42
7.2	Experimental-Result-Code AVP values	42
7.3	Command Code values	42
Annex A (normative):	GBA-UserSecSettings XML definition	43
Annex B (normative):	GAA Service Type Codes	48
Annex C (normative):	GAA Authorization flag codes	49
Annex D (normative):	Web Services Definition for Zn interface	50
Annex E (informative):	Liberty authentication context definitions for GBA	52
E.1	Introduction	52
E.2	GBA Authentication context statement data model	52
E.3	GBA authentication context statement schema	53
E.4	GBA authentication context classes	54
E.4.1	GBAOneFactorUnregistered	54
E.4.1.1	Associated 3GPP URI	54
E.4.1.2	Class schema	54
E.4.2	GBATwoFactorUnregistered	55
E.4.2.1	Associated 3GPP URI	55
E.4.2.2	Class schema	55
E.4.3	GBAOneFactorContract	56
E.4.3.1	Associated 3GPP URI	56
E.4.3.2	Class schema	56
E.4.4	GBATwoFactorContract	57
E.4.4.1	Associated 3GPP URI	57
E.4.4.2	Class schema	57
Annex F (informative):	SAML authentication context definitions for GBA	59
F.1	Introduction	59
F.2	GBA authentication context declaration data model	59
F.3	GBA authentication context declaration types	60
F.4	GBA authentication context declaration classes	61
F.4.1	GBAOneFactorUnregistered	61
F.4.1.1	Associated 3GPP URI	61
F.4.1.2	Class schema	61
F.4.2	GBATwoFactorUnregistered	63
F.4.2.1	Associated 3GPP URI	63
F.4.2.2	Class schema	63
F.4.3	GBAOneFactorContract	65
F.4.3.1	Associated 3GPP URI	65
F.4.3.2	Class schema	65
F.4.4	GBATwoFactorContract	67
F.4.4.1	Associated 3GPP URI	68
F.4.4.2	Class schema	68
Annex G (normative):	Web Services Definition for Zpn interface	71
Annex H (informative):	Change history	73
History		75

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.

ITeH STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
<https://standards.iteh.ai/catalog/standards/sist/8c9bdf8-bada-4c54-abf1-7e751eaa6e57/etsi-ts-129-109-v9.7.0-2015-07>

1 Scope

The present stage 3 specification defines the Diameter based implementation for bootstrapping Zh interface (BSF-HSS) and Dz interface (BSF-SLF) for HSS resolution for the BSF, the MAP based implementation for bootstrapping Zh' interface (BSF-HLR) and GAA Application Zn interface (BSF-NAF) in Generic Authentication Architecture (GAA). This specification also defines the Web Services based implementation for GAA Application Zn reference point (BSF-NAF). The definition contains procedures, message contents and coding. The procedures for bootstrapping and usage of bootstrapped security association are defined in 3GPP TS 33.220 [5].

The present document also specifies the Diameter and Web Services based implementation for the GAA Application Push Function Zpn reference point (BSF-NAF). The procedures for bootstrapping are defined in 3GPP TS 33.223 [23].

This specification is a part of the Generic Authentication Architecture (GAA) specification series.

The diameter based implementation for the Zh interface is based on re-usage of Cx interface Multimedia-Auth-Request/Answer messages originally between CSCF and HSS. These messages are defined in 3GPP TS 29.229 [3]. The 3GPP IMS mobility management uses the same definitions between CSCF and HSS. The present document defines how the defined messages are used with the bootstrapping and GAA application procedures (e.g. subscriber certificates) and the application logic that is needed in GAA network elements (BSF, HSS, and NAF).

ITeH STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
<https://standards.iteh.ai/catalog/standards/sist/8c2bdf8-bada-4c54-abf1-7e751eaa6e57/etsi-ts-129-109-v9.7.0-2015-07>

Figure 1.1 depicts the relationships of these specifications to the other specifications for the Diameter based implementations.

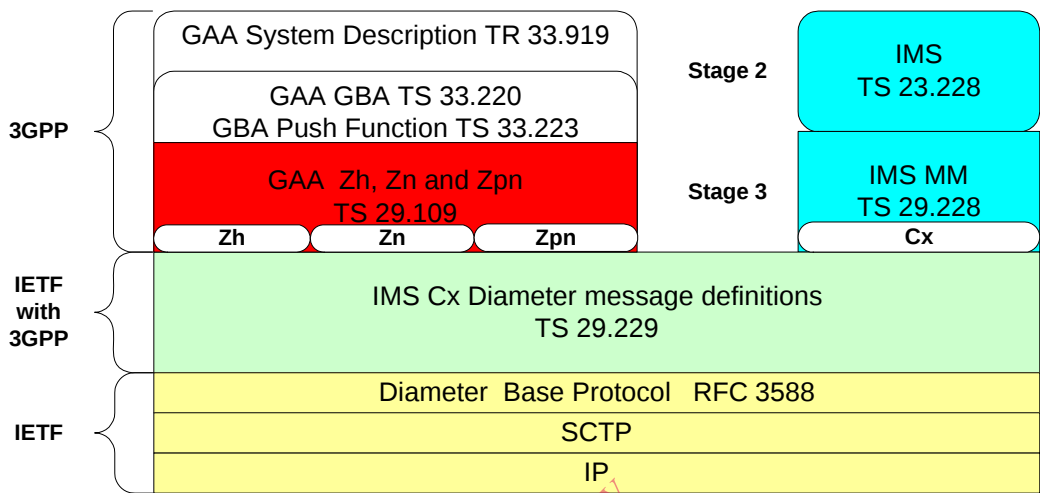


Figure 1.1: Relationships to other specifications

Figure 1.2 provides an informal overall quick introduction to the whole signalling procedures in GAA system. The important identifiers are marked bold and optional data items are italicised. The Ub and Ua interfaces, not defined in this TS, are simplified.

NOTE: The Zh' interface (BSF-HLR) is not represented in this figure.

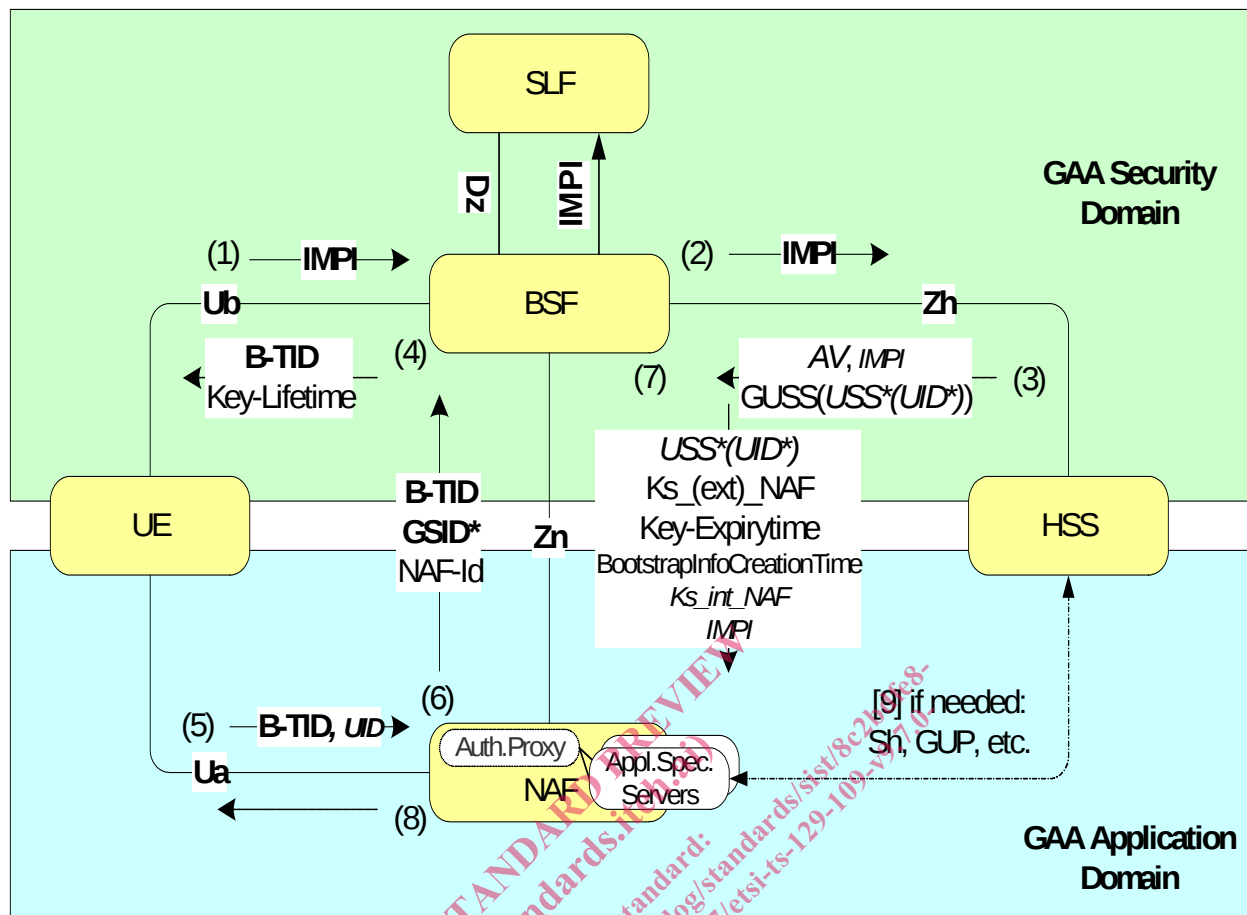


Figure 1.2: The whole signalling procedure in GAA system

Figure 1.3 provides an informal overall quick introduction to the whole signalling procedures in GAA Push Function. The important identifiers are marked bold and optional data items are italicised. The **Ua** and **Upa** interfaces, not defined in this TS, are simplified.

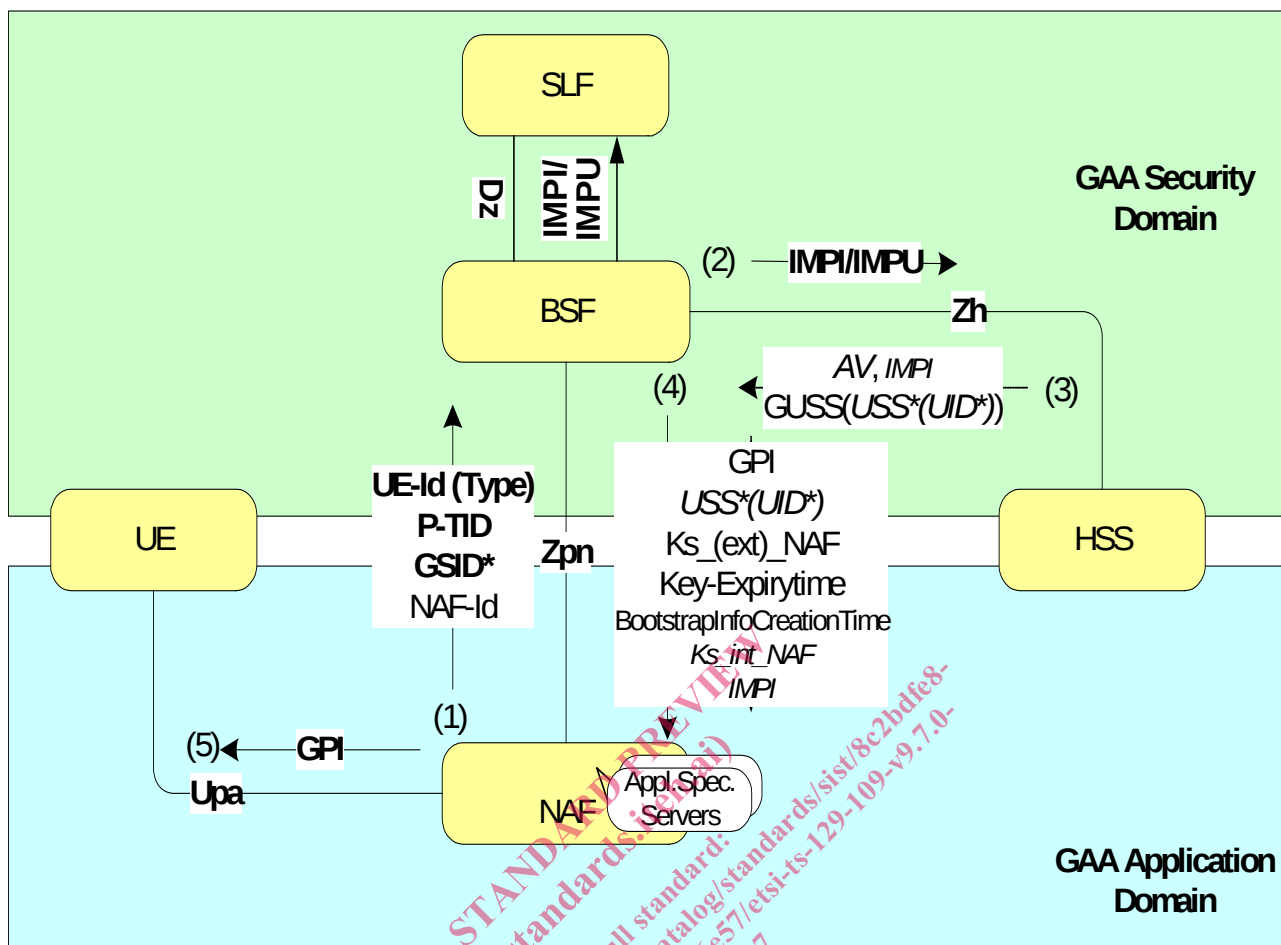


Figure 1.3: Signalling procedure in GAA Bootstrapping Push Function

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*.

- [1] IETF RFC 3588, "Diameter Base Protocol".
- [2] 3GPP TS 29.228: "IP Multimedia (IM) Subsystem Cx and Dx Interfaces; Signalling flows and message contents".
- [3] 3GPP TS 29.229: "Cx and Dx interfaces based on the Diameter protocol".
- [4] 3GPP TR 33.919 "Generic Authentication Architecture (GAA); System Description".
- [5] 3GPP TS 33.220 "Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture".
- [6] 3GPP TS 33.221 "Generic Authentication Architecture (GAA); Support for Subscriber Certificates".
- [7] 3GPP TS 24.109: "Bootstrapping interface (Ub) and Network application function interface (Ua);Protocol details".
- [8] 3GPP TS 29.230: "Diameter applications; 3GPP specific codes and identifiers"
- [9] IETF RFC 3589: "Diameter Command Codes for Third Generation Partnership Project (3GPP)".
- [10] 3GPP TS 23.008: "Organisation of subscriber data"
- [11] 3GPP TS 33.222: "Generic Authentication Architecture (GAA); Access to network application functions using secure hypertext transfer protocol (HTTPS)".
- [12] 3GPP TS 23.228: "IP Multimedia Subsystem (IMS); Stage 2"
- [13] W3C: "Web Services Activity", <http://www.w3.org/2002/ws/>.
- [14] W3C: "Web Services Description Language (WSDL) Version 2.0 Part 0: Primer",
<http://www.w3.org/TR/2005/WD-wsdl20-primer-20050803/>.
- [15] 3GPP TR 33.980: "Liberty Alliance and 3GPP Security Interworking; Interworking of Liberty Alliance ID-FF, ID-WSF and Generic Authentication Architecture".
- [16] Liberty Alliance Project: "Liberty ID-FF Authentication Context Specification".
- [17] 3GPP TS 33.110: "Key establishment between a Universal Integrated Circuit Card (UICC) and a terminal"
- [18] 3GPP TS 33.259: "Key establishment between a UICC Hosting Device and a Remote Device"
- [19] 3GPP TS 29.002: "Mobile Application Part (MAP) Specification"
- [20] 3GPP TS 33.102: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security architecture".
- [21] 3GPP TS 23.003: "Numbering, addressing and identification".
- [22] OASIS Standard: "Authentication Context for the OASIS Security Assertion Markup Language (SAML) V2.0 OASIS Standard, 15 March 2005, saml-authn-context-2.0-os".

- [23] 3GPP TS 33.223 "Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA) Push Function".
- [24] 3GPP TS 33.402: "3GPP System Architecture Evolution (SAE); Security aspects of non-3GPP accesses".
- [25] Void
- [26] 3GPP TS 26.237: "IP Multimedia Subsystem (IMS) based Packet Switched Streaming (PSS) Multimedia Broadcast/Multicast Services (MBMS); User Service; Protocols".
- [27] Void
- [28] Void
- [29] 3GPP TR 33.924: "Identity Management and 3GPP Security Interworking; Identity Management and Generic Authentication Architecture (GAA) Interworking".
- [30] 3GPP TS 33.224: "Generic Authentication Architecture (GAA); Generic Push Layer".
- [31] 3GPP TS 33.203: "Access security for IP-based services".
- [32] 3GPP TS 29.329: " Sh Interface based on the Diameter protocol; Protocol details".

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
<https://standards.iteh.ai/catalog/standards/sist/8c2bdf8-bada-4c54-abf1-7e751eaa6e57/etsi-ts-129-109-v9.7.0-2015-07>

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in 3GPP TS 23.008 [10], 3GPP TR 33.919 [4], 3GPP TS 33.220 [5] apply with following additions.

Bootstrapping information (Bootstrapped data) in a BSF consists of a bootstrapping transaction identifier (B-TID), a key material (Ks), the key lifetime (expiry time), the bootstrapinfo creation time, the IMPI and the GUSS (if received from HSS) with BSF control information. Each bootstrapping procedure creates a bootstrapped data entity with B-TID as retrieval key..

GAA application is an application that uses the security association created by GBA Bootstrapping procedure.

GAA service is an operator specific end user service that uses the security association created by GAA Bootstrapping procedure. GAA services are identified by **GAA Service Identifiers**. A GAA service is implemented using some standardised or proprietary GAA application defined by GAA application type.

NAF specific Bootstrapping information transferred from a BSF to a NAF contains NAF and its service specific parts from bootstrapped data and needed key information derived from the bootstrapped data.

Service/Application. The term service is used here in its common meaning. A service is something that a MNO offers to subscribers. GAA Services are identified by GAA Service Identifier (GSID). In stage 2 documents ([4], [5], [6] and [11]) the term application is used in the same meaning i.e. MNOs offer applications to subscribers. There is a reason to avoid the usage of the term application here. The application is an already reserved term in Diameter. In Diameter applications are identified by Application Identifiers.

3.2 Symbols

For the purposes of the present document, the terms and definitions given in 3GPP TS 23.008 [10].

3.3 Abbreviations

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

AK	Anonymity Key
AKA	Authentication and Key Agreement
AUTN	Authentication token
AV	Authentication Vector. 3GPP AV=[RAND,AUTN,XRES,CK,IK].
AVP	Attribute-Value-Pair in Diameter messages.
BIA	BootstrappingInfo-Answer message
BIR	BootstrappingInfo-Request message
BS	BootStrapping Procedure
BSF	Bootstrapping server functionality
	BSF is hosted in a network element under the control of an MNO.
B-TID	Bootstrapping Transaction Identifier
CA	Certificate Authority
CK	Confidential Key
FQDN	Full Qualified Domain Name in URI (e.g. http://FQDN:80)
GAA	Generic Authentication Architecture
GBA	Generic Bootstrapping Architecture
GPI	GBA Push Information
GSID	GAA Service Identifier
GUSS	GBA User Security Settings
HSS	Home Subscriber System
IK	Integrity Key
IMPI	IP Multimedia Private Identity
IMPU	IP Multimedia Public Identity
Ks	Key Material
Ks_ext_NAF	MEbased key for a specific NAF