International Telecommunication Union

ITU-T J.366.10

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

(07/2007)

SERIES J: CABLE NETWORKS AND TRANSMISSION OF TELEVISION, SOUND PROGRAMME AND OTHER MULTIMEDIA SIGNALS

IPCablecom

Zh and Zn Interfaces based on the Diameter protocol; Stage 3 specification

Recommendation ITU-T J.366.10

Recommendation ITU-T J.366.10

Zh and Zn Interfaces based on the Diameter protocol; Stage 3 specification

Summary

Recommendation ITU-T J.366.10 defines the Diameter based implementation for bootstrapping Zh interface (BSF-HSS) and Dz interface (BSF-SLF) for HSS resolution for the BSF, and GAA application Zn interface (BSF-NAF) in generic authentication architecture (GAA). It contains procedures, message contents and coding. The procedures for bootstrapping and usage of bootstrapped security association are defined in 3GPP TS 33.220.

The Third Generation Partnership Project (3GPP) has developed the specification in a form optimized for the wireless environment. This Recommendation references the ETSI version of the 3GPP specification and specifies only the modifications necessary to optimize it for the cable environment.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T J.366.10	2007-07-29	9

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T J.366.10

Zh and Zn Interfaces based on the Diameter protocol; Stage 3 specification

1 Scope

The present Recommendation defines the Diameter based implementation for bootstrapping Zh interface (BSF-HSS) and Dz interface (BSF-SLF) for HSS resolution for the BSF, and GAA Application Zn interface (BSF-NAF) in Generic Authentication Architecture (GAA). The definition contains procedures, message contents and coding. The procedures for bootstrapping and usage of bootstrapped security association are defined in [b-3GPP TS 33.220].

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

The Third Generation Partnership Project (3GPP) has developed the specification in a form optimized for the wireless environment. This Recommendation references the ETSI version of the 3GPP specification and specifies only the modifications necessary to optimize it for the cable environment.

It is an important objective of this work that interoperability between IPCablecom 2.0 and 3GPP IMS is provided. IPCablecom 2.0 is based upon 3GPP IMS, but includes additional functionality necessary to meet the requirements of cable operators. Recognizing developing converged solutions for wireless, wireline, and cable, it is expected that further development of IPCablecom 2.0 will continue to monitor and contribute to IMS developments in 3GPP, with the aim of alignment of 3GPP IMS and IPCablecom 2.0.

The modifications to [ETSI TS 129 109 V6.6.0] (2006-03), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Generic Authentication Architecture (GAA); Zh and Zn Interfaces based on the Diameter protocol; Stage 3*, are shown in clause 6.

2 References

[ETSI TS 129 109] ETSI TS 129 109 V6.6.0 (2006), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Generic Authentication Architecture (GAA); Zh and Zn Interfaces based on the Diameter protocol; Stage 3*.

3 Definitions

This Recommendation uses the terms defined in [ETSI TS 129 109].

4 Abbreviations and acronyms

This Recommendation uses the abbreviations provided in [ETSI TS 129 109].

5 Conventions

This Recommendation uses the conventions provided in [ETSI TS 129 109].

6 Modifications to [ETSI TS 129 109]

Modifications introduced by this Recommendation are shown in revision marks. Unchanged text is replaced by ellipsis (…). Some parts of unchanged text (section numbers, etc.) may be kept to indicate the correct insertion points.

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, and GAA Application Zn interface (BSF-NAF) in Generic Authentication Architecture (GAA). 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].

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

The Third Generation Partnership Project (3GPP) has developed the specification in a form optimized for the wireless environment. This Recommendation references the ETSI version of the 3GPP specification and specifies only the modifications necessary to optimize it for the cable environment.

It is an important objective of this work that interoperability between IPCablecom 2.0 and 3GPP IMS is provided. IPCablecom 2.0 is based upon 3GPP IMS, but includes additional functionality necessary to meet the requirements of cable operators. Recognizing developing converged solutions for wireless, wireline, and cable, it is expected that further development of IPCablecom 2.0 will continue to monitor and contribute to IMS developments in 3GPP, with the aim of alignment of 3GPP IMS and IPCablecom 2.0.

The modifications to ETSI TS 23-008 V6.8.0 (2005-12) Internet Protocol (IP) multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3 are listed below.

• • •

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*.

IPCablecom2 defines several Recommendations which are based on 3GPP technical specifications. These IPCablecom2 Recommendations are commonly referred to as IPCablecom2 Delta Recommendations. For references within this Recommendation which have a corresponding IPCablecom2 Delta Recommendation, the IPCablecom2 Delta Recommendation must be used. The list of IPCablecom2 Delta Recommendations is:

ITU-T J.366.1 (TS-23.008)	ITU-T J.366.5 (TS-29.228)
ITU-T J.366.2 (TS-23.218)	ITU-T J.366.6 (TS-29.229)
ITU-T J.366.3 (TS-23.228)	ITU-T J.366.7 (TS-33.203)
ITU-T J.366.4 (TS-24.229)	ITU-T J.366.8 (TS-33.210)
ITU-T J.366.10 (TS-29.109)	ITU-T J.366. 9 (TS-33.220)

References which have corresponding delta specifications are highlighted with an *.

[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 (rel-6)*".

[5] *3GPP TS 33.220, "*Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (rel-6)*".

[6] 3GPP TS 33.221, "*Generic Authentication Architecture (GAA); Support for Subscriber Certificates (rel-6)*".

[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 (rel-6)*".

[9] IETF RFC 3589, "*Diameter Command Codes for Third Generation Partnership Project (3GPP) Release 5*".

[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) (rel-6)*".

[12] *3GPP TS 23.228: "IP Multimedia Subsystem (IMS); Stage 2".

[13] Recommendation ITU-T J.366.3, IP Multimedia Subsystem Stage 2 Specification (TS 23.228).

[14] Recommendation ITU-T J.366.9, Generic Authentication Architecture Specification (TS 33.220).

[15] Recommendation ITU-T J.366.1, Organization of Subscriber Data Specification (TS 23.008).

[16] Recommendation ITU-T J.366.5, Cx and Dx Interfaces Specification (TS 29.288.).

[17] Recommendation ITU-T J.366.6, Cx and Dx Interfaces, Diameter Protocol Specification (TS 29.229).

3 Definitions, symbols and abbreviations

• • •

4.2 Protocol Zh between BSF and HSS

The requirements for Zh interface are defined in 3GPP TS 33.220 [5].

The Bootstrapping Zh interface performs the retrieval of an authentication vector and possibly GBA User Security Settings from the HSS. The overall Bootstrapping procedure is depicted in Figure 4.3. The basic procedure is:

a) A UE starts the bootstrapping procedure by protocol Ub with a BSF giving the IMPI of the user (see 3GPP TS 24.109 [7]).

b) The BSF starts protocol Zh with user's HSS

- The BSF requests user's authentication vector and GBA User Security Settings(GUSS) corresponding to the IMPI.

- The HSS supplies to the BSF the requested authentication vector and GUSS (if any).

  NOTE – If there is more than one HSS deployed within the network, the BSF may have to contact the SLF using the Dz interface prior to sending the request for information to the HSS (see section 6.4).

c) The BSF continues the protocol Ub with the UE (see 3GPP TS 24.109 [7]).

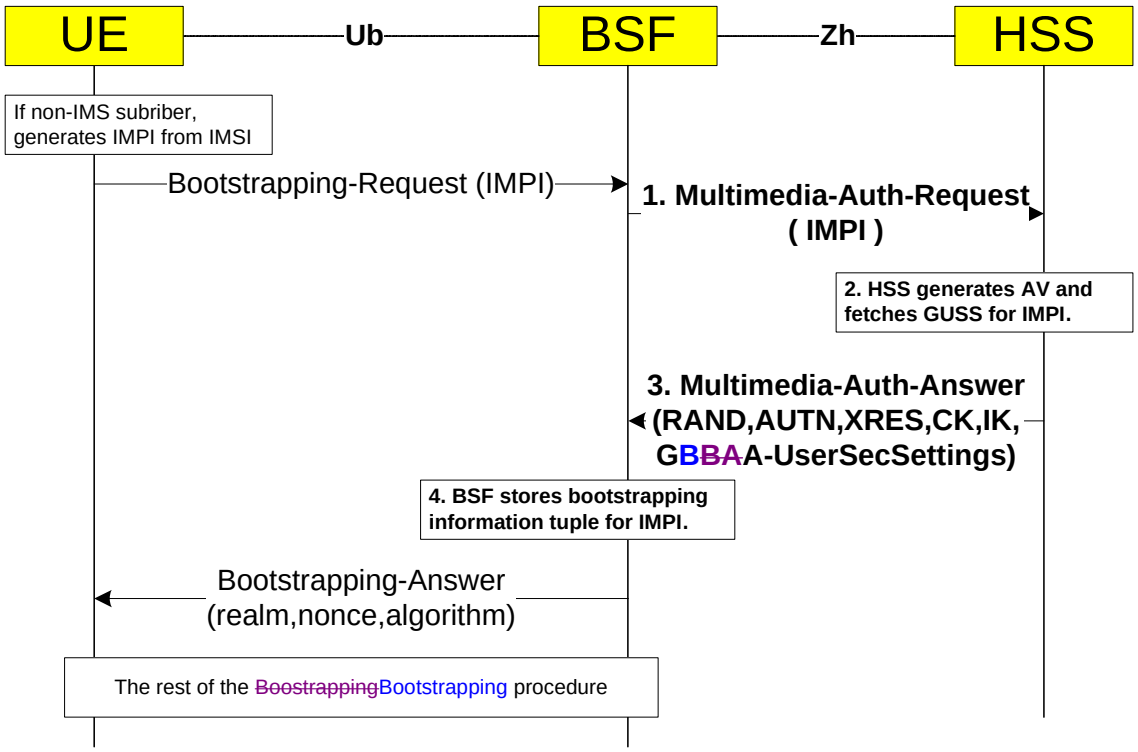

Figure 4.3 – The GBA bootstrapping procedure for IMS-AKA

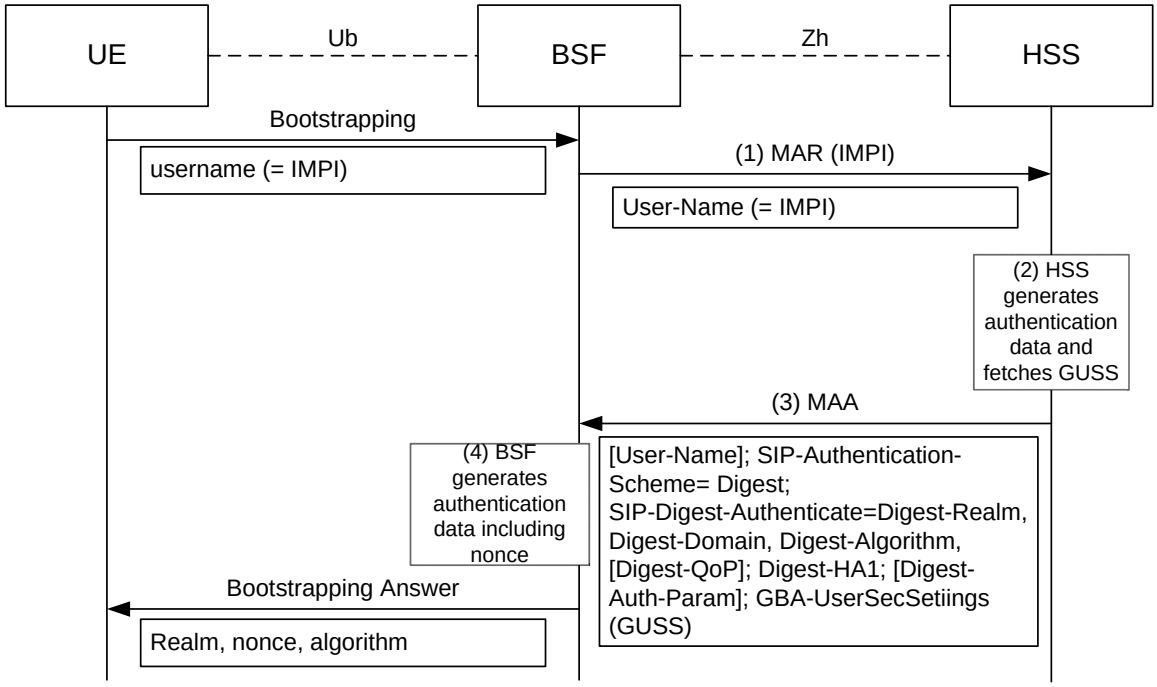

Figure 4.4 – The GBA bootstrapping procedure for SIP-Digest

The steps of the bootstrapping procedure in Figure 4.3 or Figure 4.4 are:

Step 1

The BSF shall send the following Bootstrapping-Request to the HSS in the format of Multimedia-Auth-Request (MAR) message. The content of the message is given below in the same format as in 3GPP TS 29.229 [3]. The curly brackets indicate mandatory AVPs. The square brackets indicate optional AVPs. The "address of" refers to the Fully Qualified Host Name (FQDN).

```
<Multimedia-Auth-Request> ::=<Diameter Header: 303, REQ, PXY, 16777221 >
                  < Session-Id >
                  { Vendor-Specific-Application-Id }
                  { Auth-Session-State }            ; NO_STATE_MAINTAINED
                  { Origin-Host }                   ; Address of BSF
                  { Origin-Realm }                  ; Realm of BSF
                  { Destination-Realm }             ; Realm of HSS
                  [ Destination-Host ]              ; Address of the HSS
                  { User-Name }                     ; IMPI from UE
                  *[ AVP ]
                  *[ Proxy-Info ]
                  *[ Route-Record ]
```

The content of mandatory Vendor-Specific-Application-ID according [1] is:

```
<Vendor-Specific-Application-Id>::=<AVP header: 260>
                  1* [Vendor-Id]                    ; 3GPP is 10415
                  0*1 {Auth-Application-Id}         ; 16777221
                  0*1 {Acct-Application-Id}         ; Omitted
```

When determining the value of Destination-Host AVP the BSF can use redirector function (SLF) to resolve the address of the HSS if needed (see 3GPP TS 29.229 [3]). The BSF shall set the Auth-Session-State AVP to NO_STATE_MAINTAINED to inform that the HSS does not need to maintain any status information for this session according 3GPP TS 29.229 [3]. The User-name is the IMS Private User Identity (IMPI) as required in 3GPP TS 29.228 [2].

Step 2

When the HSS receives the MAR message, the HSS shall derive ~~the user Authentication Vector (AV) information~~ the required authentication data (depending on the authentication scheme) according to the IMPI and populates it into SIP-Auth-Data AVP as defined in PKT-SP-29.229-D01-060530 ~~3GPP TS 29.229~~ [~~3~~17]. If GUSS exists for the IMPI, the HSS shall also fetch the GUSS into the GBA-UserSecSettings AVP.

The MAR/MAA sequence in the Zh interface must not change possible status information of the possible simultaneously ongoing IMS MM application sessions in the HSS.

If the User-Name (IMPI) from the BSF is totally unknown to the HSS, the error situation 5401 is raised.

Step 3

• • •

Step 4

When the BSF receives the MAA message, the BSF shall check the value of the SIP-Authentication-Scheme AVP. If the BSF does not support the authentication-scheme the BSF shall stop processing the message and should indicate an error via the O&M subsystem.

The BSF generates the needed key material (Ks) ~~from confidential key (CK) and integrity key (IK)~~ as described in ~~3GPP TS 33.220 [5]~~ PKT-SP- 33.220-I01-060406 [14] and stores temporarily the tuple <IMPI,Ks,GBA-UserSecSettings> for further use in GAA applications. The rest of the bootstrapping procedure in Ub interface will later add also the Bootstrapping Transaction Identifier (B-TID) to that tuple as key and the key lifetime (expiry time).

…

5.2 Protocol Zn between NAF and BSF

The requirements for Zn interface are defined in 3GPP TS 33.220 [5].

…

The common GAA application procedure is presented in Figure 5.3.

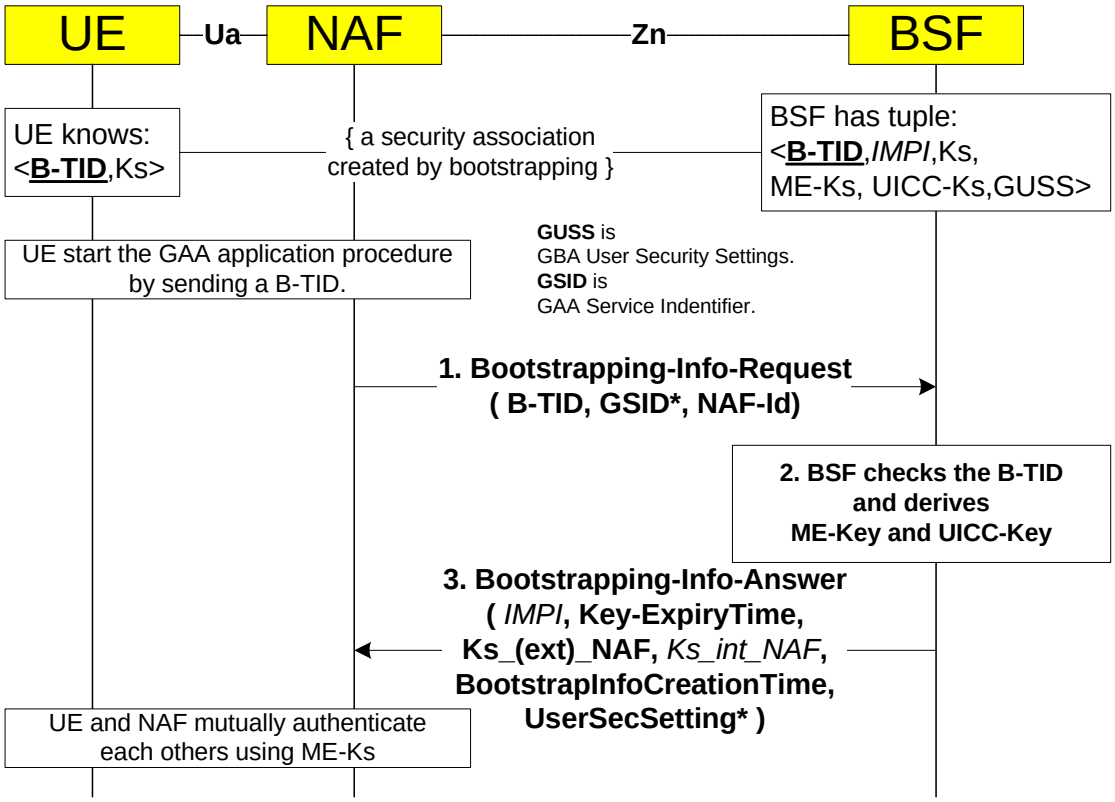

Figure 5.3 – The GAA application procedure

The steps of the GAA application procedure in Figure 5.3 are:

Step 1

…

Step 2

In the successful case the BSF has a tuple <B-TID,IMPI,Ks, Key lifetime, Bootstrapinfo creation time, GBA-UserSecSettings> identified by Bootstrapping Transaction Identifier (B-TID). When the BSF receives the request it checks the existence and validity of the tuple for given B-TID. If checking fails the BSF sends an Answer message with Experimental-Result set to indicate the error type 5403. If the tuple for B-TID exists, but is expired, error type 5403 is also send to indicate needs for renewal of the ~~boostrapping~~bootstrapping procedure. In successful case the Result-Code is set to 2xxx as defined in [1].

The BSF derives the key material for the ME (i.e., Ks_NAF in the case of GBA_ME, and Ks_ext_NAF in the case of GBA_U) and possibly the key material for the UICC (i.e., Ks_int_NAF

in the case of GBA_U) according to the B-TID and packs them into ME-Key-Material AVP and possible UICC-Key-Material AVP. The ME-Key-Material contains Ks_(ext)_NAF and the UICC-key-Material contains the Ks_int_NAF key. The BSF select correct user's Security Settings according the request's GAA-Service-Identifier AVP to GBA-UserSecSettings AVP. If NAF grouping is used by the operator and there are one or more USSs corresponding to the requested GSID, then also the nafGroup attribute of USS is checked. If the NAF has sent a GAA-Service-Identifier that does not have corresponding user's security settings, and the BSF is locally configured to reject those requests from the NAF, then the error 5402 is raised. If the NAF has sent a GAA-Service-~~Identifierthat~~Identifier that have corresponding user's security settings, but the BSF is locally configured to reject those from that NAF, then the error 5402 is raised too.

The NAF may be addressed from the UE with different FQDNs. The BSF shall check if this NAF-Id is allowed to be used for the NAF. If the NAF identified by its Origin-Host AVP is configured in the BSF not to be authorized to use the given NAF-Id, the BSF may raise the error situation 5402. The BSF may also be configured so that a certain NAF is not authorized to use a certain GAA-Service-Identifier. This situation may be also indicated by error code 5402.

Step 3

After that the BSF shall send a Bootstrapping-Info-Answer message (BIA) back to the NAF.

```
< ~~Boostrapping~~Bootstrapping-Info-Answer> ::= < Diameter Header: 310, PXY, 16777220 >
                  < Session-Id >
                  { Vendor-Specific-Application-Id }
                  [ Result-Code ]
                  [ Experimental-Result]
                  { Origin-Host }                    ; Address of BSF
                  { Origin-Realm }                   ; Realm of BSF
                  [ User-Name ]                      ; IMPI
                  [ ME-Key-Material ]                ; Required
                  [ UICC-Key-Material ]              ; Conditional
                  [ Key-ExpiryTime ]                 ; Time of expiry
                  [ BootstrapInfoCreationTime ]      ; Bootstrapinfo creation time
                  [ GBA-UserSecSettings ]            ; Selected USSs
                  [ GBA-Type ]                       ; GBA type used in bootstrapping
                  *[ AVP ]
                  *[ Proxy-Info ]
                  *[ Route-Record ]
```

The BSF may or may not send the User-name AVP (IMPI) according its configuration.

The mandatory common key material with the ME (Ks_NAF or Ks_ext_NAF) is sent in the ME-Key-Material AVP. The common key material with the UICC (Ks_int_NAF) is optionally sent in the UICC-Key-Material AVP only if the "uiccType" tag in bsfInfo from the HSS is set to "GBA_U".

The Key-ExpiryTime AVP contains the expiry time of the Bootstrapping information in the BSF according its configuration. The expiry time is represented according the Diameter Time data format in seconds that have passed since 0h on January 1, 1900 UTC . If a special key lifetime value is given in the "lifeTime" tag inside the bsfInfo from the HSS in ~~bootstraping~~bootstrapping procedure, it is used instead of the BSF default configuration value when the expiry time is calculated.

• • •

Bibliography

[b-3GPP TS 33.220] 3GPP Technical Specification TS 33.220, *Technical Specification Group Services and System Aspects; Generic Authentication Architecture (GAA); Generic bootstrapping architecture.*

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	**Cable networks and transmission of television, sound programme and other multimedia signals**
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Terminals and subjective and objective assessment methods
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	Global information infrastructure, Internet protocol aspects and next-generation networks
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2011