ETSI TS 133 224 V15.0.0 (2018-11)

Universal Mobile Telecommunications System (UMTS);
LTE;
Generic Authentication Architecture (GAA);
Generic Bootstrapping Architecture (GBA) push layer
(3GPP TS 33.224 version 15.0.0 Release 15)

Reference

RTS/TSGS-0333224vf00

Keywords

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/ETSIDeliverableStatus.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

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables 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.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

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

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

3GPP defined the Generic Authentication Architecture (GAA). The adoption of GAA by other standardization bodies showed that some services can not make the assumption that the User Equipment (UE) has always the possibility to connect to the Bootstrapping Server Function (BSF). This specification introduces a generic push layer that makes use of the GBA Push Function as specified in TS 33.223 [2].

1 Scope

The present document specifies a generic push layer that makes use of the GBA Push Function as specified in TS 33.223 [3]. The GPL specification includes a message format, cipher suites and processing model. GPL assumes that keys and other SA parameters have been preinstalled in the Push-NAF and UE in the form of a NAF SA. GPL is a protection protocol that can be applied in a unidirectional fashion.

The rationale for GPL is that having each application specify its own security mechanisms would for obvious reasons lead to duplication of work, specifications and implementations. Using a generic secure push layer avoids these problems. A generic secure push layer may also relieve the applications using the service of having to be aware of inner working of the security layer. As an analogy, TS 33.222 [4] can be mentioned, which provides a generic security layer for HTTP based applications.

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 33.220: "Generic Authentication Architecture (GAA); Generic bootstrapping architecture".

[2] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[3] 3GPP TS 33.223: "Generic Authentication Architecture (GAA); Generic bootstrapping architecture: Push Function"

[4] 3GPP TS 33.222: "Generic Authentication Architecture (GAA); Access to network application functions using Hypertext Transfer Protocol over Transport Layer Security (HTTPS)".

[5] FIPS PUB 180-2 (2002): "Secure Hash Standard".

[6] IETF RFC 2104 (1997): "HMAC: Keyed-Hashing for Message Authentication".

[7] ISO/IEC 10118-3:2004: "Information Technology – Security techniques – Hash-functions – Part 3: Dedicated hash-functions".

[8] NIST Special Publication 800-38 A (2001): "Recommendation for Block Cipher Modes of Operation - Methods and Techniques "

[9] FIPS PUB 197 (2001): "Advanced Encryption Standard"

[10] OMA-WAP-TS-WSP-V1_0-20020920-C: "Wireless Session Protocol 1.0"

[11] 3GPP TS 31.111: "Universal Subscriber Identity Module (USIM) Application Toolkit (USAT)"

[12] ETSI TS 102 600: "UICC-Terminal interface; Characteristics of the USB interface

[13] ETSI TS 102 483: "UICC-Terminal interface; Internet Protocol connectivity between UICC and terminal"

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in TR 21.905 [2], TS 33.220 [1] and the following apply.

SN_h The highest sequence number received in a GPL message with validated MAC. SN_h is used for replay protection.
SN_s A counter used to generate sequence numbers for outgoing messages.

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in TR 21.905 [2] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in TR 21.905 [2].

GBA Generic Bootstrapping Architecture
GPI GBA Push Information
GPL Generic Push Layer
GPL_ME GPL hosted in the ME
GPL_U GPL hosted in the UICC
HSP High Speed Protocol
NAF Network Application Function
KDF Key Derivation Function
MAC Message Authentication Code
SA Security Association
SAID Security Association Identifier
SN Sequence Number

4 GPL requirements

4.1 Session concept

It is reasonable to expect that there will exist Push-NAF based services that rely on some form of per device session concept, and which would benefit from pushing more than one message based on the same security association. An example could be a virus signature update server. It is possible that the virus signatures are delivered in multiple pushed messages (for size limitation reasons of the underlying push transport mechanism), and it would then be inefficient to establish a new security association for each message.

This requires that GPL provides replay protection in addition to integrity protection (and possibly confidentiality protection). Figure 4.1-1 depicts the usage scenario, where three push messages are delivered from the Push-NAF to the UE using a single security association. Note that steps 1 and 2 in Figure 4.1-1 are out of scope for this specification. One way to achieve steps 1 and 2 is to use TS 33.223 [3].

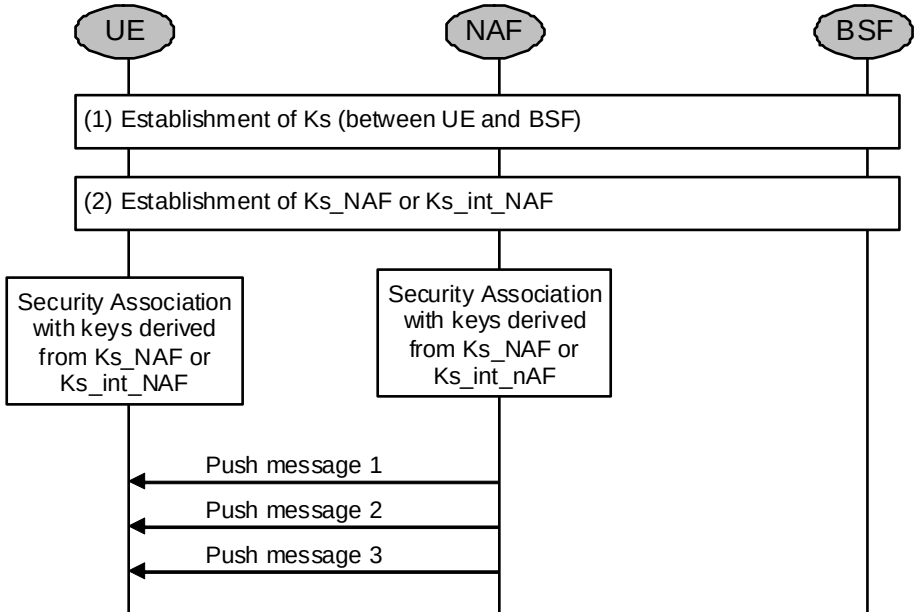

Figure 4.1-1: Example of a secure session

If GPL was to provide a complete session concept including reliability of delivered messages using timeouts/acknowledgments and re-transmissions, re-establishments of sessions, re-ordering of messages etc., GPL would be unnecessarily complex and the size of the GPL messages would be too large for many applications (e.g., when the underlying transport is SMS). Therefore GPL shall only provide sufficient session state to ensure that the security of multiple GPL messages is not compromised. GPL shall hence provide the security services confidentiality, integrity protection and replay protection for a GPL session.

If a more complex session concept is required by the application, where the session concept includes services other than security services, then, e.g., WSP [10] could be applied on top of GPL, but this is out of scope for this specification.

Even though it sometimes is sufficient with a secure downlink channel from the Push-NAF to the UE (for broadcast only UEs) a uplink channel may be present. An example of this is OMA's location based services, where a server requests location information from a terminal, which responds with its location information. This request/response exchange may be repeated every ten minutes. It is prudent to require that it shall be possible to secure also such an uplink channel. The security of the uplink channel can conveniently be based on the same NAF SA as the downlink channel.

To send a GPL message to the UICC, the Push-NAF selects a delivery channel that targets a UICC and that is supported by the GPL-capable ME (e.g. SMS class 2). The protocols that the GPL-capable ME shall support to receive the GPL_U messages depend on the type of interface between the ME and the UICC (ISO or HSP).

GBA Push as specified by TS 33.223 [3] is capable of establishing a Ks_int_NAF and a Ks_ext_NAF using one GPI. However, GPL is not designed to make full use of this. It is not possible to establish GPL SAs for both GPL_U and GPL_ME from a single GPI.

4.2 Requirements

The following requirements shall be posed for the generic secure push layer:

R1: It shall perform encapsulation of generic application layer messages from the Push-NAF to the UE.

R2: It shall allow sending multiple messages based on the same security association.

R3: Integrity protection and confidentiality protection shall be possible to provide for the messages. Integrity protection is mandatory to apply, while confidentiality protection is optional to apply.

R4: Detection of replayed messages within the same session shall be possible.

R5: If uplink messages are present in the application protocol, it shall be possible to apply the same level of protection to these messages, based on keys derived from the Ks_NAF or Ks_int_NAF.

R6: The Push-NAF shall select the target of the GPL message, UICC or ME, by choosing the type of delivery channel. To send a GPL message to the UICC, the Push-NAF shall select a delivery channel that targets a UICC and that is supported by the GPL-capable ME (e.g. SMS class 2).

R7: The protocols that the GPL-capable ME shall support to receive the GPL_U message depend on the type of interface between the ME and the UICC:

- In case of ISO interface between the ME and the UICC, the ME shall support "ENVELOPE SMS-PP data download" and "Bearer Independent Protocol in client mode" (class e in client mode) as specified in 3GPP TS 31.111 [11]
- In case of HSP interface between the ME and the UICC as specified in TS 102 600 [12], the ME shall support "ENVELOPE SMS-PP data download" over HSP and ETSI TS 102 483 [13]

NOTE: There is no need to specify new interface between the ME and the UICC.

To utilise GPL as described in this document the ME and/or UICC shall be equipped with a GPL protocol entity implementing the processing of the protocol. In addition, to be able to use GPL it is necessary to implement the GPI processing described in TS 33.223 [3].

The GPL protocol entity resides in the ME (called GPL_ME) or in the UICC (called GPL_U). When the GPL protocol entity to be used is in the ME, Ks_NAF shall be used as the shared master key between the ME and the Push-NAF. When the GPL protocol entity to be used resides in the UICC, Ks_int_NAF shall be used as the shared master key between the UICC and the Push-NAF.

The Push-NAF must have knowledge of ME's capabilities to support GPL_ME and/or the USIM/ISIMs capabilities to support GPL_U (depending on which GPL protocol entity is targeted). Otherwise the Push-NAF cannot know if it can send GPL messages to the UE or which type of GPL messages the UE understands. Therefore the GPL capabilities of the ME shall be indicated to the Push-NAF during GBA-Push UE registration procedure which is specified in Annex B in TS 33.223 [3]. The GPL_U capabilities of the USIM/ISIM shall be stored in the GUSS in the HSS.

5 GPL Processing

5.1 Processing model

In case of GPL_ME, the GPL protocol entity is conceptually located either between the transport mechanism (which could e.g. be SMS, IP, IP/UDP) and the application, or included in the application.

In case of GPL_U, the GPL_U protocol entity is located within the targeted USIM or ISIM.

When receiving a GPL protected message, the recipient transfers the message to the GPL protocol entity How the recipient knows that the message is a GPL message is up to each transport mechanism to define. It could be through, e.g., a special application ID that is tagged onto the message, in which case a GPL application ID needs to be defined.

In GPL_ME, the message is delivered to the transport mechanism again after GPL processing is complete. This time around the GPL application ID and GPL related data has been removed, and what remains is a regular application data message (which is routed to the intended application using the transport layers normal dispatching mechanism). The processing model for GPL_ME is depicted in Figure 5.1-1.

In case of GPL_U, the GPL protected message is delivered to the targeted USIM or ISIM that will process the GPL message. The application data remain in the USIM or ISIM for use by the application defined therin.

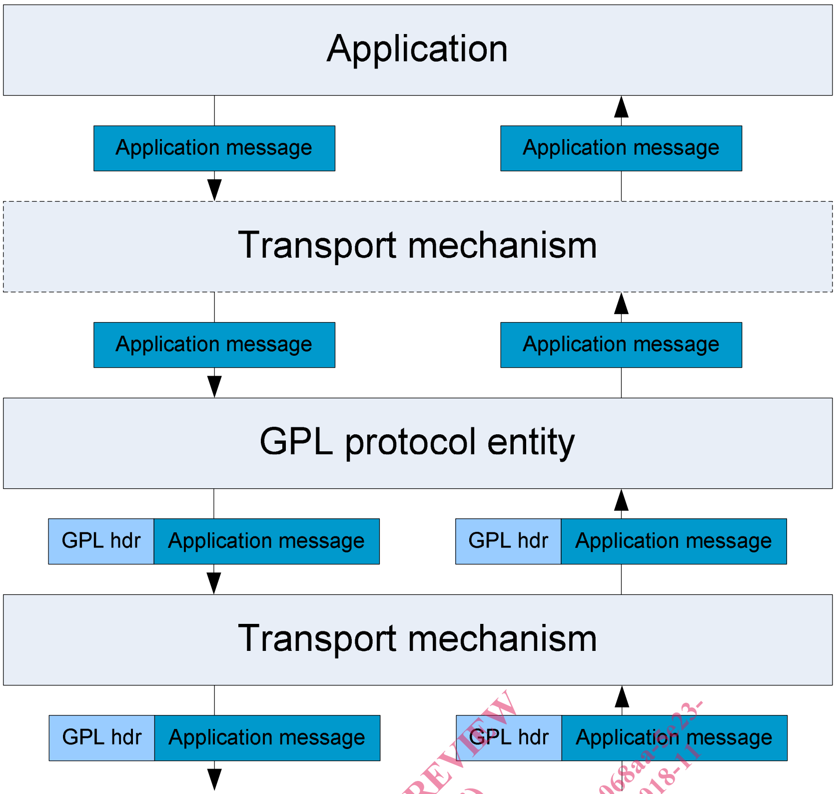

Figure 5.1-1: The processing model for GPL_ME agnostic applications. Inbound processing to the right and outbound processing to the left.

The case when the GPL_ME protocol entity is logically located between the transport mechanism and the application is illustrated in Figure 5.1-1. In this case the application does not need to be aware of GPL, and any legacy application can use GPL without modifications. The other case is that the application is aware of GPL. The reason for this may be that the application needs to inform the GPL protocol entity about which security association to use (i.e., the application calls the GPL protocol entity directly, and the GPL protocol entity may either pass the GPL encapsulated message to the transport mechanism, or return it to the application).

5.2 Session start

A GPL session is considered started in a GPL protocol entity when the corresponding GPL Security Association (GPL-SA) is initialised, see clause 5.9 For the Push-NAF, this means that the session shall be considered initiated as soon as it has received the GPI from the BSF and configured the NAF SA (see [3]) and corresponding GPL-SA. For the UE, the session shall be considered started when it has received the GPI and configured the GPL-SA.

In addition to the GPI, the GPL protocol entity needs to get GPL policy information for the session, e.g., which encryption and integrity algorithms to use etc. The policy information may be decided by the application itself or by some other management entity.

The Push-NAF shall choose the policy to use for the downlink messages and it shall be included in the GPL message. The Push-NAF shall choose a cipher suite for downlink GPL messages, and the UE shall (in case an uplink is present) choose the cipher suite for the uplink. It is recommended that the UE chooses the same cipher suite for the uplink as the Push-NAF chose for the downlink.