3GPP TR 33.918 V7.0.0 (2005-12)

3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Generic Authentication Architecture (GAA); Early implementation of Hypertext Transfer Protocol over Transport Layer Security (HTTPS) connection between a Universal Integrated Circuit Card (UICC) and a Network Application Function (NAF) (Release 7)

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.
Contents

Foreword ............................................................................................................................................................. 5
Introduction ........................................................................................................................................................ 5

1 Scope ........................................................................................................................................................... 6

2 References ................................................................................................................................................... 6

3 Definitions, symbols and abbreviations .................................................................................................. 6

3.1 Definitions ............................................................................................................................................... 6

3.2 Abbreviations ......................................................................................................................................... 6

4 Requirements ........................................................................................................................................... 7

5 Security architecture ................................................................................................................................. 7

6 Authentication schemes ............................................................................................................................. 7

6.1 Reference model .................................................................................................................................... 7

6.2 GBA functions split in the UE ............................................................................................................... 7

6.3 General requirements and principles .................................................................................................. 7

6.3.1 Requirements on the UE .................................................................................................................. 8

6.3.1.1 Requirements on the ME ............................................................................................................. 8

6.3.1.2 Requirements on the UICC ........................................................................................................ 8

6.3.2 Requirements on the NAF ............................................................................................................... 8

6.4 Shared key-based UICC authentication with certificate-based NAF authentication ....................... 8

6.5 Shared key-based mutual authentication between UICC and NAF ..................................................... 8

6.6 Certificate based mutual authentication between UICC and Application Server ............................. 9

Annex A: Bearer Independent Protocol overview .................................................................................. 10

A.1 Architecture ........................................................................................................................................ 10

A.2 BIP usage ............................................................................................................................................. 10

Annex B: Change history ............................................................................................................................ 12
Foreword

This Technical Report 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

TS 33.222 [3] describes how the access over HTTP can be secured using TLS in the Generic Authentication Architecture. An application residing on a UICC may advantageously use such a mechanism to secure its communication with a Network Application Function (NAF). Due to time constraint, this scenario was not fully covered in release 6.

The "HTTPS connection between a UICC and a NAF" functionality is a candidate for early implementation since all required mechanisms are available in release 7 specifications.
1 Scope

The present document gives guidance on how to perform an early implementation of HTTPS connections between a UICC-based application and a Network Application Function in the Generic Authentication Architecture (GAA).

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.


3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in TS 33.222 [3] and TR 21.905 [1] apply.

3.2 Abbreviations

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

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BIP</td>
<td>Bearer Independent Protocol</td>
</tr>
<tr>
<td>HTTP</td>
<td>Hypertext Transfer Protocol</td>
</tr>
<tr>
<td>HTTPS</td>
<td>HTTP over TLS</td>
</tr>
<tr>
<td>ME</td>
<td>Mobile Equipment</td>
</tr>
<tr>
<td>NAF</td>
<td>Operator-controlled Network Application Function functionality</td>
</tr>
<tr>
<td>TLS</td>
<td>Transport Layer Security</td>
</tr>
</tbody>
</table>
4 Requirements

The new requirements and procedures that enable the termination of HTTPS connections in the UICC have been defined in the following Change Requests:

- CR022 to TS 33.222 [3]: "Usage of Ks_int_NAF for HTTPS connection between a UICC and a NAF"
- CR062 to TS 33.220 [6]: "Introduction of key selection mechanism"
- CR020 (rev 1) to TS 24.109 [4]: "Ks_int_NAF usage"
- CR019 (rev 1) to TS 29.109 [5]: "Key indication in USS"

These new requirements and procedures have been introduced in the corresponding release 7 specifications.

The early implementation should fulfill all the requirements and procedures specified for "Access to network application function using HTTPS" in the aforementioned Change Requests and in TS 33.222 [3], TS 24.109 [4] and TS 29.109 [5].

The early implementation of HTTPS connection between a UICC and a NAF should provide the same security level as the solution defined in TS 33.222 [7] for UICC-based application.

5 Security architecture

The overall security architecture conforms to the architecture defined in TS 33.220 [6].

6 Authentication schemes

6.1 Reference model

The reference model conforms to the model specified in TS 33.222 [3].

6.2 GBA functions split in the UE

The GBA security association between a UICC-based application and a NAF can be established as follows:

- The ME executes the bootstrapping procedure with the BSF (i.e. supporting the Ub reference point). This ME function can be initiated by the UICC as described in section 6.3.1.1.
- The UICC, which hosts the HTTPS client, runs the bootstrapping usage procedure with a NAF (i.e. supporting the Ua reference point).

6.3 General requirements and principles

The general requirements and principles are provided in TS 33.222 [3] and CR022 to TS 33.222 [3]. This section identifies the UE functionalities that have to be supported in order to enable the implementation of an HTTPS client in a UICC.
6.3.1 Requirements on the UE

6.3.1.1 Requirements on the ME

In order to enable HTTPS connections between a UICC and a NAF, the ME shall support BIP commands (only class "e") and the "Toolkit-initiated GBA" command as specified in TS 31.111 [2].

A ME that is compliant with TS 33.222 [3] doesn't require any upgrade to enable the termination of HTTPS connections in the UICC, if the aforementioned functionalities are implemented.

When the "Toolkit-initiated GBA" command is supported by the ME, the UICC can request the ME to perform a GBA bootstrapping procedure (as defined in TS 31.111 [2]). As a result, the UE and the BSF will share a new bootstrapping key Ks.

The BIP commands allow the UICC to establish a data channel through the ME with a NAF. Then the UICC can run a bootstrapping usage procedure, which is required for the establishment of an HTTPS tunnel.

6.3.1.2 Requirements on the UICC

In order to enable HTTPS connections between a UICC and a NAF, the network access application on the UICC shall be the USIM to enable the usage of the BIP commands and the "Toolkit-initiated GBA" command as specified in TS 31.111 [2].

The UICC-based application shall implement a HTTPS client, as defined in TS 33.222 [3] and CR022 to TS 33.222 [3]. The UICC-based mechanisms in charge of the HTTPS connection shall be located on a USIM Toolkit Application on the UICC.

6.3.2 Requirements on the NAF

In order to enable HTTPS connections between a UICC and a NAF, the NAF shall support:

- GBA_U and
- the requirements, the procedures and the key decision mechanism defined in TS 33.222 [3], TS 24.109 [4], TS 29.109 [5], CR022 to TS 33.222 [3], CR062 to TS 33.220 [6], CR020 (rev 1) to TS 24.109 [4] and CR019 (rev 1) to TS 29.109 [5].

6.4 Shared key-based UICC authentication with certificate-based NAF authentication

The authentication and tunnel establishment mechanisms are described in TS 33.222 [3], TS 24.109 [4], TS 29.109 [5], CR022 to TS 33.222 [3], CR062 to TS 33.220 [6], CR020 (rev 1) to TS 24.109 [4] and CR019 (rev 1) to TS 29.109 [5]. Compared to release 6, the only additional procedures that should be supported are described in the aforementioned Change Requests.

6.5 Shared key-based mutual authentication between UICC and NAF

The authentication and tunnel establishment mechanisms are described in TS 33.222 [3], TS 24.109 [4], TS 29.109 [5], CR022 to TS 33.222 [3], CR062 to TS 33.220 [6], CR020 (rev 1) to TS 24.109 [4] and CR019 (rev 1) to TS 29.109 [5]. Compared to release 6, the only additional procedures that should be supported are described in the aforementioned Change Requests.
6.6 Certificate based mutual authentication between UICC and Application Server

The authentication and tunnel establishment mechanisms are described in TS 33.222 [3], TS 24.109 [4] and TS 29.109 [5].
Annex A: Bearer Independent Protocol overview

This annex provides an overview of the Bearer Independent Protocol (BIP) usage to establish the HTTPS connection between a UICC and a NAF.

A.1 Architecture

A.2 BIP usage
When the UICC opens a BIP channel with the NAF as described in TS 31.111 [2] then an active TCP/IP connection is established between the UICC and the NAF. This channel is further used to exchange HTTPS and HTTP packets.
## Annex B: Change history

<table>
<thead>
<tr>
<th>Date</th>
<th>TSG #</th>
<th>TSG Doc.</th>
<th>CR</th>
<th>Rev</th>
<th>Cat</th>
<th>Subject/Comment</th>
<th>Old</th>
<th>New</th>
<th>WI</th>
</tr>
</thead>
<tbody>
<tr>
<td>05/09/2005</td>
<td></td>
<td></td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>Created at SA3 #40</td>
<td>0.0.0</td>
<td>0.1.0</td>
<td>UICNAFSec</td>
</tr>
<tr>
<td>21/09/2005</td>
<td>SP-29</td>
<td>SP-050574</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>Presented for information at SA #29</td>
<td>0.1.0</td>
<td>1.0.0</td>
<td>UICNAFSec</td>
</tr>
<tr>
<td>19/11/2005</td>
<td>SP-30</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Raised to version 2.0.0 for presentation to SA #30 for approval</td>
<td>1.0.0</td>
<td>2.0.0</td>
<td>UICNAFSec</td>
</tr>
<tr>
<td>2005-12</td>
<td>SP-30</td>
<td>SP-050770</td>
<td></td>
<td></td>
<td></td>
<td>Approved at SA #30</td>
<td>2.0.0</td>
<td>7.0.0</td>
<td>UICNAFSec</td>
</tr>
</tbody>
</table>