ETSI TS 133 259 V7.0.0 (2007-06)

Technical Specification

Digital cellular telecommunications system (Phase 2+);
Universal Mobile Telecommunications System (UMTS);
Key establishment between a UICC hosting device and a remote device
(3GPP TS 33.259 version 7.0.0 Release 7)

Reference

DTS/TSGS-0333259v700

Keywords

GSM, 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

Copyright Notification

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://webapp.etsi.org/IPR/home.asp).

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.

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

The need to establish a secure channel between a UICC Hosting Device and a Remote Device connected via a local interface has been identified by the Personal Network Management work (see TS 22.259 [4]), in order to protect the communication between the UICC Hosting Device and the Remote Device.

This document describes key establishment between a UICC Hosting Device and a Remote Device.

1 Scope

The present document describes the security features and mechanisms to provision a shared key between a UICC Hosting Device and a Remote Device connected via a local interface. The shared secret is then intended to be used to secure the interface between the Remote Device and the UICC hosting device. Candidate applications to use this key establishment mechanism include but are not restricted to Personal Network Management (see TS 22.259 [4]).

The scope of this specification includes an architecture overview and the detailed procedure how to establish the shared key between the UICC Hosting Device and the Remote Device. This is different from the Technical Specification TS 33.110 [6] that describes an architecture overview and the detailed procedure how to establish the shared key between the UICC itself and the terminal hosting the UICC. The use cases utilizing the mechanisms described in this specification are seen to be different to the use cases where "Key establishment between a UICC and a terminal", IETF RFC 4279 [6] is utilized.

The solution described in this document is built on the existing infrastructure defined in "GBA", TS 33.220 [3].

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 TR 21.905: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Vocabulary for 3GPP Specifications".

[2] 3GPP TS 31.101: "3rd Generation Partnership Project; Technical Specification Group Terminals; UICC-terminal interface; Physical and logical characteristics".

[3] 3GPP TS 33.220: "Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture".

[4] 3GPP TS 22.259: "Service Requirements for Personal Network Management; Stage 1".

[5] 3GPP TS 33.110: "Technical Specification Group Services and System Aspects; Key establishment between a UICC and a terminal".

[6] IETF RFC 4279 (2005) "Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)".

[7] IETF RFC 2246 (1999): "The TLS Protocol Version 1".

[8] IETF RFC 3546 (2003): "Transport Layer Security (TLS) Extensions".

[9] 3GPP TS 29.109: "Generic Authentication Architecture (GAA); Zh and Zn Interfaces based on the Diameter protocol; Stage 3".

[10] 3GPP TR 33.905: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Recommendations for trusted open platforms".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in TR 21.905 [1].

NAF Key Centre: Dedicated NAF in charge of performing the key establishment between a UICC Hosting Device and a Remote Device.

UICC Hosting Device: The entity, which is physically connected to the UICC used for key establishment between UICC Hosting Device and Remote Device. The UICC Hosting Device may be the MT or the ME.

Remote Device: A Remote Device is physically separated from the UICC Hosting Device (e.g. PNE as defined in TS 22.259 [4]). The Remote Device may host a UICC by itself but this UICC is not involved in the key establishment between the UICC Hosting Device and the Remote Device. For the purposes of the present document, the term Remote Device denotes a trusted device that can establish a shared key with a UICC Hosting Device.

NOTE 1: The definition of trusted devices is out of the scope of the specification. It is assumed that the home network can decide whether a Remote Device is trusted or not.

Device_ID: It identifies uniquely the Remote Device. The Device_ID of a ME or MT is the IMEI.

NOTE 2: In case that the Remote Device is not a ME or MT the definition of the type of Device_IDs is out of the scope of this specification.

Local interface: The interface between the Remote Device and the UICC Hosting Device is named the local interface.

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in TR 21.905 [1] 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 [1].

B-TID	Bootstrapping Transaction Identifier
BSF	Bootstrapping Server Function
GBA	Generic Bootstrapping Architecture
GBA_ME	ME-based GBA
GBA_U	GBA with UICC-based enhancements
HSS	Home Subscriber System
KDF	Key Derivation Function
Ks_ext_NAF	Derived key in GBA_U
Ks_NAF	Derived key in GBA_ME
Ks_(ext)_NAF	Combined abbreviation denoting Ks_NAF in case of GBA_ME and Ks_ext_NAF in case of GBA_U
Ks_local_device	Derived key, which is shared between a UICC hosting device and a Remote Device
NAF	Network Application Function
PNE	Personal Network Element
SLF	Subscriber Locator Function
USS	User Security Setting

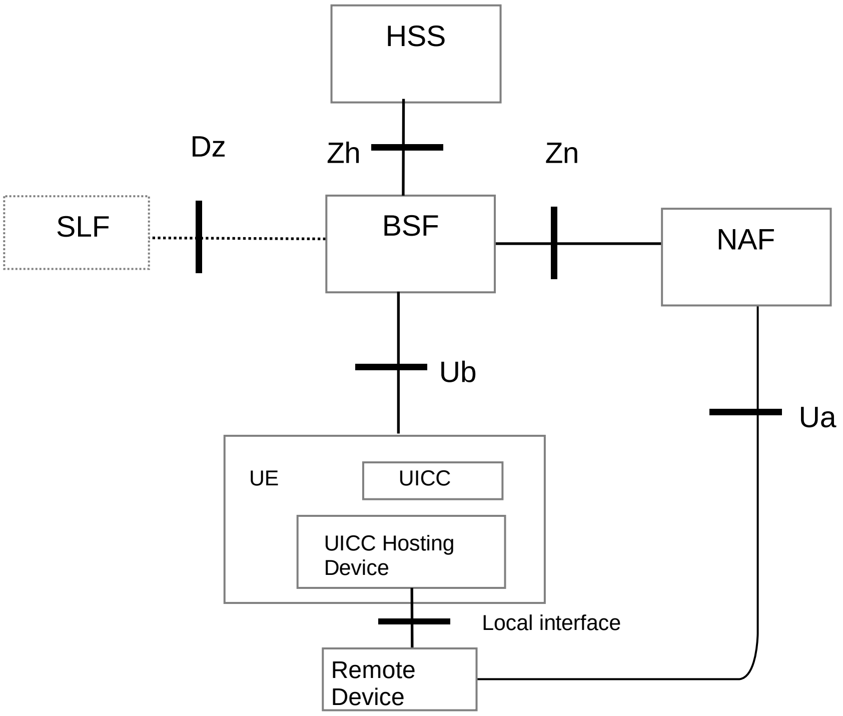
4 Key Establishment between a UICC Hosting Device and a Remote Device

4.1 Reference model

A Remote Device, which for example could be a PNE as defined in TS 22.259 [4] or any other Remote Device containing a Ua application according to this specification, is connected to a UICC Hosting Device, via a local interface. The communication over the local interface could take place via for example Bluetooth, USB, IR or a serial cable.

GBA_ME or GBA_U is used to provision a shared key (i.e. Ks_local_device) between the UICC Hosting Device and the Remote Device. The shared key (i.e. Ks_local_device) is derived by the UICC Hosting Device and the NAF Key Centre from the Ks_ext_NAF or Ks_NAF residing in the UICC Hosting Device and NAF Key Centre after a complete GBA run according to TS 33.220 [3].The NAF Key Centre securely delivers Ks_local_device to the Remote Device through a TLS tunnel, which is established between the NAF Key Centre and the Remote Device. The Ks_local_device can then be used to secure the local interface between the UICC Hosting Device and the Remote Device.

Figure 4.1 shows a network model of the entities that utilize the bootstrapped secrets, and the reference points used between them.



NOTE: The Remote Device might not have a direct connection to the NAF. In this case the Remote Device can connect to the NAF Key Centre via the UICC hosting device.

Figure 4.1: High level reference model

4.2 Network elements

4.2.1 General

This document is based on the architecture specified in TS 33.220 [3]. The Network elements that are not explained in this section can be found in TS 33.220 [3].

4.2.2 NAF Key Centre

The NAF Key Centre is the NAF in charge of performing the Key Establishment between a UICC Hosting Device and a Remote Device.

4.3 Key establishment architecture and reference points

4.3.1 General

This document is based on the architecture specified in TS 33.220 [3]. The Reference Points that are not explained in this section can be found in TS 33.220 [3] and TS 29.109 [9] (including GAA Service Type Code for this specification).

4.3.2 Reference point Ub

The reference point Ub is implemented between the UICC Hosting Device and the BSF as described in TS 33.220 [3]. The UICC Hosting Device runs the HTTP Digest AKA protocol. This allows the UICC/UICC Hosting Device and the BSF to generate the bootstrapping key Ks.

4.3.3 Reference point Ua

The reference point Ua is used to deliver Ks_local_device and the associated parameters to the Remote Device.

4.3.4 Reference point Local interface

The reference point Local interface is used to initiate the Key establishment procedure between the UICC Hosting Device and the Remote Device. The UICC Hosting Device sends a B-TID together with associated parameters on this interface to allow the Remote Device to receive a Ks_local_device key from the NAF Key Centre.

4.4 Requirements and principles for key establishment between a UICC Hosting Device and a Remote Device

4.4.1 General requirements

The following requirements and principles are applicable to the procedure for key establishment between a UICC Hosting Device and a Remote Device:

- The UICC Hosting Device and the Remote Device shall be able to establish a shared key (i.e. Ks_local_device);
- The UICC Hosting Device shall be trusted;

NOTE 1: The definition of trusted UICC Hosting Device is out of scope of the specification. The UICC Hosting Device could be compliant to requirements defined in TCG specifications or TR 33.905 [10].

- The Remote Device shall be trusted;

NOTE 2: The definition of trusted Remote Device is out of scope of the specification. The Remote Device could be compliant to requirements defined in TCG specifications or TR 33.905 [10].

- The shared key to establish between the UICC Hosting Device and the Remote Device (i.e. Ks_local_device) shall not be exchanged on the interface between the UICC Hosting Device and the Remote Device;
- The Remote Device and the network shall be able to authenticate each other;
- The server implementing the key establishment function (i.e. the NAF Key Centre) needs to be trusted by the home operator to handle the authentication parameters and the shared key;
- The home network shall be able to control whether this Remote Device is authorized to establish a shared key with the UICC Hosting Device;

- The procedure for the key establishment between a UICC Hosting Device and a Remote Device shall be access independent;
- To the extent possible, existing protocols and infrastructure should be reused.

4.4.2 Requirements on the Remote Device

The Remote Device shall support certificate-based mutual authentication as defined in RFC 2246 [7] and RFC 3546 [8] in which case the Remote Device shall be equipped with a valid Client Certificate or the Remote Device shall support shared key based mutual authentication as defined in RFC 4279 [6] in which case the Remote Device shall be equipped with a valid pre-shared key.

NOTE: Configuration of certificates and shared secrets is out of scope of the present specification.

It may be possible to configure the NAF_ID of the NAF Key Centre in the Remote Device.

4.4.3 Requirements on the UICC Hosting Device

The UICC Hosting Device shall implement GBA_ME and GBA_U as defined in TS 33.220 [3].

The UICC Hosting Device shall be capable of deriving the Ks_local_device key from the Ks_(ext)_NAF key.

It shall be possible to configure the NAF_ID of the NAF Key Centre in the UICC Hosting Device.

NOTE: The home operator could configure the NAF_ID of the NAF Key Centre by utilising e.g. OMA Device Management.

4.4.4 Requirements on the UICC

The UICC may implement GBA_U as defined in TS 33.220 [3].

It shall be possible to configure the NAF_ID of the NAF Key Centre on the UICC.

NOTE: The home operator could configure the NAF_ID of the NAF Key Centre by utilising e.g. OTA commands.

4.4.5 Requirements on the NAF Key Centre

The NAF Key Centre shall support certificate-based mutual authentication as defined in RFC 2246 [7] and RFC 3546 [8] and shared key based mutual authentication as defined in RFC 4279 [6].

NOTE: Configuration of certificates and shared secrets is out of scope of the present specification.

The NAF Key Centre shall be capable of determining whether a Remote Device is trusted or not.

The NAF Key Centre shall be capable of determining whether the Remote Device is authorized to establish a shared key.

The NAF Key Centre shall implement GBA_ME and GBA_U as defined in TS 33.220 [3].

The NAF Key Centre dedicated to the Key Establishment Mechanism shall be located in the Home Network.

The NAF Key Centre shall be capable of deriving the Ks_local_device key from the Ks_(ext)_NAF key.

4.4.6 Requirements on Ks_local_device key and associated parameters handling in Remote Device

One key (i.e. Ks_local_device) shall be established per UICC Hosting Device and Remote Device pair. One established Ks_local_device key shall only be shared between one specific UICC Hosting Device and one specific Remote Device.

NOTE: Further key derivations from the Ks_local_device are allowed to be used at e.g. application layer, to be able to differentiate the keys to be used by different applications. However, this is out of the scope in this specification.

The Remote Device receives the Ks_local_device key and the lifetime of the Ks_local_device key from the NAF Key Centre on a secured interface.

The Remote Device shall delete the Ks_local_device key and the corresponding key lifetime when at least one of the conditions below is met:

1 the key lifetime of the Ks_local_device key expires;

2 the Remote Device discovers that the UICC Hosting Device does not share the same Ks_local_device key any more due to e.g. deletion.

4.4.7 Requirements on Ks_local_device key and associated parameters handling in UICC Hosting Device

One key (i.e. Ks_local_device) shall be established per UICC Hosting Device and Remote Device pair. One established Ks_local_device key shall only be shared between one specific UICC Hosting Device and one specific Remote Device.

NOTE: Further key derivations from the Ks_local_device are allowed to be used at e.g. application layer, to be able to differentiate the keys to be used by different applications. However, this is out of the scope in this specification.

The lifetime of Ks_local_device key in the UICC Hosting Device shall not exceed the lifetime of the Ks_(ext)_NAF key.

The UICC Hosting Device shall delete the Ks_local_device key and the corresponding parameters when the key lifetime of the Ks_local_device expires.

The UICC Hosting Device shall handle the Ks key and the NAF specific keys (i.e. Ks_NAF, Ks_ext_NAF and Ks_local_device) and related parameters as described in clause 4.4.11 of TS 33.220 [3]. This means that the Ks_local_device key shall be handled in the same way as the Ks_(ext)_NAF key is handled in clause 4.4.11 of TS 33.220 [3], i.e. as a NAF specific key.

4.5 Procedures

4.5.1 Initiation of key establishment between a UICC Hosting Device and a Remote Device

If the Remote Device has a Ks_local_device key stored for a particular UICC Hosting Device, then the Remote Device should attempt to use it with the UICC Hosting Device. If this fails due to the UICC Hosting Device not sharing the same Ks_local_device key, then the Remote Device shall initiate a new request to the UICC Hosting Device to initiate a new key establishment procedure as described in clause 4.5.2.

If the UICC Hosting Device has a Ks_local_device stored for a particular Remote Device then the UICC Hosting Device should attempt to use it with the Remote Device. The UICC Hosting Device does not know whether the Remote Device has deleted the Ks_local_device key or not. If the UICC Hosting Device receives an error due to the Remote Device not sharing the same key, then the UICC Hosting Device should trigger the Remote Device to send a new request to the UICC Hosting Device to establish a new key.

NOTE: The UICC Hosting Device needs a unique way to distinguish or map different Ks_local_device keys to different Remote Devices and vice versa. This is out of the scope of this specification.

4.5.2 Key establishment procedure

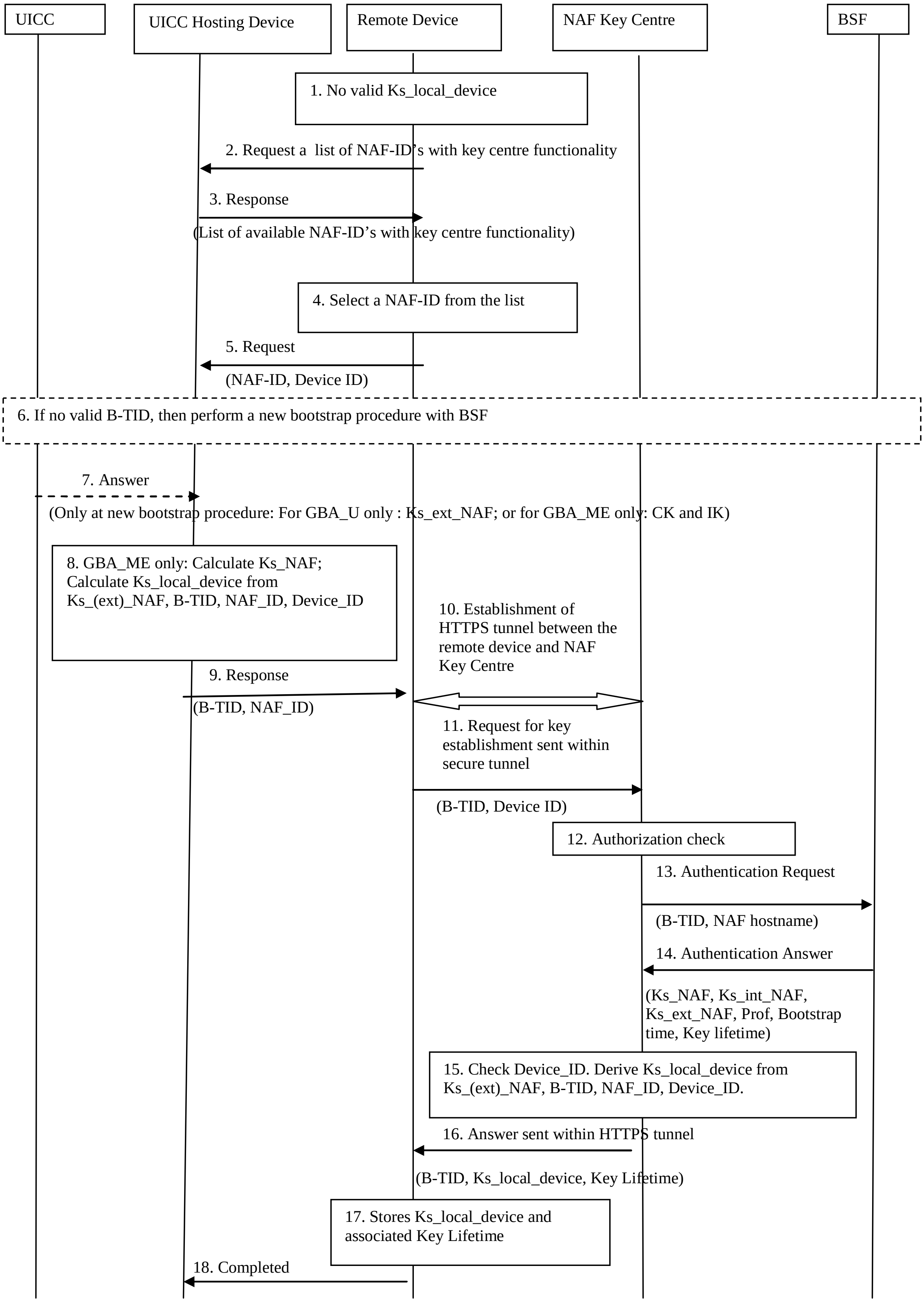

UICC
UICC Hosting Device
Remote Device
NAF Key Centre
BSF
1. No valid Ks_local_device
2. Request a list of NAF-ID's with key centre functionality
3. Response
(List of available NAF-ID's with key centre functionality)
4. Select a NAF-ID from the list
5. Request
(NAF-ID, Device ID)
6. If no valid B-TID, then perform a new bootstrap procedure with BSF
7. Answer
(Only at new bootstrap procedure: For GBA_U only : Ks_ext_NAF; or for GBA_ME only: CK and IK)
8. GBA_ME only: Calculate Ks_NAF; Calculate Ks_local_device from Ks_(ext)_NAF, B-TID, NAF_ID, Device_ID
10. Establishment of HTTPS tunnel between the remote device and NAF Key Centre
9. Response
(B-TID, NAF_ID)
11. Request for key establishment sent within secure tunnel
(B-TID, Device ID)
12. Authorization check
13. Authentication Request
(B-TID, NAF hostname)
14. Authentication Answer
(Ks_NAF, Ks_int_NAF, Ks_ext_NAF, Prof, Bootstrap time, Key lifetime)
15. Check Device_ID. Derive Ks_local_device from Ks_(ext)_NAF, B-TID, NAF_ID, Device_ID.
16. Answer sent within HTTPS tunnel
(B-TID, Ks_local_device, Key Lifetime)
17. Stores Ks_local_device and associated Key Lifetime
18. Completed

Figure 4-2: Key establishment procedure

1. The Remote Device has no valid Ks_local_device key stored.

2. If the Remote Device has no list of NAF_ID's with NAF Key Centre functionality, then the Remote Device sends a request to the UICC Hosting Device to send a list of available NAF_ID's with NAF Key Centre functionality stored in the UICC Hosting Device. If the Remote Device has such a list and knows which NAF-ID to take, it immediately proceeds with step 5.

3. The UICC Hosting Device sends its list of available NAF-ID's with NAF Key Centre functionality to the Remote Device.

4. The Remote Device selects a NAF-ID with NAF Key Centre functionality from the list provided by the UICC Hosting Device or proposes a NAF-ID stored in it's own memory.

5. The Remote Device sends a request to the UICC Hosting Device for a B-TID. The Remote Device includes parameters NAF_ID and Device_ID in order for the UICC Hosting Device to be able to calculate a new Ks_(ext)_NAF and Ks_local_device key.

6. If the UICC Hosting Device does not have a valid B-TID, then the UICC Hosting Device performs a new bootstrapping procedure. The UICC Hosting Device asks for a complete GBA run: a GBA bootstrapping procedure and a GBA_ME – or a GBA_U - NAF Derivation procedure.

7. When the GBA run has been completed then the UICC provides a Ks_ext_NAF key to the UICC Hosting Device if GBA_U has been used; or the CK and IK to the UICC Hosting Device if GBA_ME has been used. If GBA_ME has been used, then the UICC Hosting Device further derives Ks and Ks_NAF.

8. The UICC Hosting Device calculates the Ks_local_device key from the Ks_(ext)_NAF, B-TID, NAF_ID and Device_ID and stores it locally.

9. The UICC Hosting Device sends a response including the B-TID and NAF_ID to the Remote Device.

10. The Remote Device and the NAF Key Centre establish a secure tunnel. The secure tunnel may be a HTTPS tunnel with certificate based mutual authentication (cf. RFC 2246 [7] and RFC 3546 [8]) or based on a shared key based mutual authentication between the Remote Device and the NAF Key Centre (cf. RFC 4279 [6]).

NOTE 1: One potential way to reach a trusted state is if the Remote Device is compliant with the requirements defined in TCG (Trusted Computing Group) MPWG (Mobile Phone Working Group) specifications. HTTPS tunnel establishment can be bound to the trust status of the Remote Device, through the attestations of relevant trusted engine of the Remote Device. Thus, HTTPS tunnel establishment will be possible only if the Remote Device is in a trusted state.

The psk_identity_hint shall be used by the server to indicate to the PSK TLS client which PSK to use. The pre-shared key is pre-administrated to the Remote Device and NAF Key Centre.

NOTE 2: If other PSKs are allowed, then the psk_identity_hint needs to be specified in the relevant key specifications.

If several PSKs are allowed, then the different hints are separated by semi-colon The usage of the psk_identity_hint in PSK TLS handshake is out of scope of this specification.

11. The Remote Device sends a "service request" message to the NAF Key Centre node in the mobile operator network. The message is sent within the secure tunnel.

    The request contains the following payload: the identity (B_TID) and the Remote Device identifier (Device_ID) requiring the establishment of key Ks_local_device.

12. If the Device_ID is IMEI, then the NAF Key Centre shall check if the Device_ID is blocked (blacklisted) and if so, it shall not proceed with the key establishment procedure but responds with an appropriate error code and terminates the secure connection with the remote device. If the Device_ID is not IMEI, then the NAF Key Centre should, if applicable, check if the Device_ID is blocked (blacklisted) and if so, it shall not proceed with the key establishment procedure but responds with an appropriate error code and terminates the secure connection with the remote device.

NOTE 3: Details of how blacklisting is implemented are out of scope of the present specification.

13. The NAF Key Centre contacts the BSF and sends the identity B_TID in a credential request.

14. The BSF returns the shared secret Ks_(ext)_NAF to the NAF Key Centre.

15. The NAF Key Centre shall behave as follows:

    a) If the NAF Key Centre has requested a USS, and if the USS indicates to the NAF Key Centre that the key establishment procedure is not allowed for the targeted user, then the NAF Key Centre shall respond with appropriate error code and terminate the secure connection with the Remote Device.

    b) The NAF Key Centre calculates the Ks_local_device key from the Ks_(ext)_NAF, B-TID, NAF_ID and Device_ID and stores it locally. The NAF Key Centre associates a key lifetime to the derived key Ks_local_device.

16. The NAF Key Centre sends within HTTPS tunnel a request response message to the Remote Device with the following payload: B-TID, Ks_local_device, Key Lifetime.

17. The Remote Device stores Ks_local_device and associated Key Lifetime.

18. The Remote Device sends a response to the UICC Hosting Device to indicate that the key establishment procedure is now completed.

Annex A (normative): Key Derivation Function definition

A.1 Ks_local_device key derivation in key establishment

The description of this key derivation function KDF and input parameter encoding can be found in TS 33.220 [3]. The key derivation function KDF in this document shall be implemented as defined in TS 33.220 [3].

A.2 Input parameters for Ks_local_device key derivation

In the key establishment between a UICC Hosting Device and a Remote Device, the input parameters for the key derivation function shall be the following:

- FC = 0x01,
- P0 = Device_ID,
- L0 = length of Device ID is variable (not greater than 65535),
- P1 = B-TID,
- L1 = length of B-TID is variable (not greater than 65535),
- P2 = NAF_ID,
- L2 = length of NAF_ID is variable (not greater than 65535).

The input parameter Key to the key derivation function defined in TS 33.220 [3] shall be the Ks_ext_NAF or the Ks_NAF key.

A character string shall be encoded to an octet string according to UTF-8 encoding rules as specified in IETF RFC 3629 [24].

Annex B (informative): Change history

Change history							
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**
2007-06	-	-	-	-	Approved at SP-36 and updated to version 7.0.0	2.0.0	7.0.0

History

Document history		
V7.0.0	June 2007	Publication