TECHNICAL SPECIFICATION

**Digital cellular telecommunications system (Phase 2+);
Universal Mobile Telecommunications System (UMTS);
LTE;
Key establishment between a UICC hosting device
and a remote device
(3GPP TS 33.259 version 12.0.0 Release 12)**

Reference

RTS/TSGS-0333259vc00

Keywords

GSM,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

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:

http://portal.etsi.org/chaircor/ETSI_support.asp

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://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**", "**may not**", "**need**", "**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

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 [5] 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", PSK TLS as specified in TS 33.310 [19], 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]   Void.

[7]   Void.

[8]   Void.

[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".

[11]   3GPP TS 24.008: "Mobile radio interface Layer 3 specification; Core network protocols; Stage 3".

[12]   NIST, FIPS PUB 180-2: "Secure Hash Standard (SHS)".

[13]   IETF RFC 4634 (2006): US Secure Hash Algorithms (SHA and HMAC-SHA).

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

[15]   TCG Mobile Phone Specifications, https://www.trustedcomputinggroup.org/specs/mobilephone.

[16]   TCG Trusted Network Connect (TNC) Specifications,
             https://www.trustedcomputinggroup.org/specs/TNC.

[17]   IETF RFC 2616 (1999): "Hypertext Transfer Protocol -- HTTP/1.1".

[18]   Void.

[19]   3GPP TS 33.310: " Network Domain Security (NDS); Authentication Framework (AF)".

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 present document. 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 and shall be encoded using BCD coding as defined in section 10.5.1.4 of TS 24.008 [11].

   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 the present document.

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

Appl_ID: It uniquely identifies an application in the UICC Hosting Device and Remote Device. The Appl_ID is an octet string.

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
Ks_local_device_appl	Derived key, which is shared between an application residing in the UICC hosting device and the Remote Device
MAC	Message Authentication Code
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.
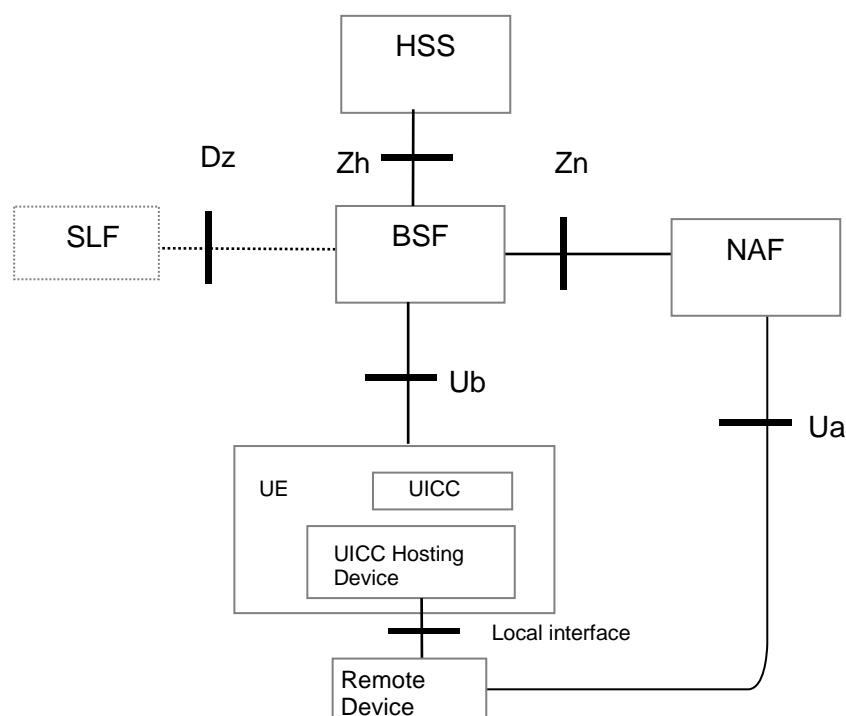
NOTE: The Remote Device might not have a direct connection to the NAF. In this case the Remote Device can connect to the NAF Key Centre via the UICC hosting device.

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 Mobile Phone specifications [15] or 3GPP TR 33.905 'Recommendations for Trusted Open Platforms' [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 TLS with certificate-based mutual authentication and TLS Extensions as defined in TS 33.310 [19], Annex E, 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 using PSK-TLS as defined in TS 33.310 [19], Annex E, 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 document.

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 TLS with certificate-based mutual authentication, TLS Extensions and shared key based mutual authentication using PSK-TLS as defined in TS 33.310 [19], Annex E.

NOTE 1: Configuration of certificates and shared secrets is out of scope of the present document.

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 may be located in the Home Network.

NOTE2: If the NAF Key Centre is not located in the home network, then the mobile network operator can not control directly the handing out of credentials from the NAF Key Centre. Therefore, the network hosting the NAF Key Centre and the home network need to have a strong trust relationship with the NAF Key Centre provider. The operator can use USS for control information for the NAF Key Centre.

If the NAF Key Centre is also offering his services to subscribers that are not subscribed to the same operator that hosts the NAF Key Centre, then the NAF Key Centre shall support USS.

If a network operator intends to support NAF Key Centre in a visited network for his subscribers, then the UE or the Remote Device shall be equipped with a TLS certificate of the NAF Key Centre in the visited network signed by the home operator or cross certification as outlined in TS 33.310 [19] may be used. The NAF Key Centre in a visited network shall be able to validate the TLS certificate presented by the Remote Device.

Editor"s Note: The usage of PSK TLS for the visited network case is for further study and evaluation.

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 (see example in Annex F).

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 the Ks_local_device key or the derived key material from 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 in order to establish a new Ks_local_device key.

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 the Ks_local_device key or the derived key material from 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 Ks_local device 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 Ks_local device 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 the present document.
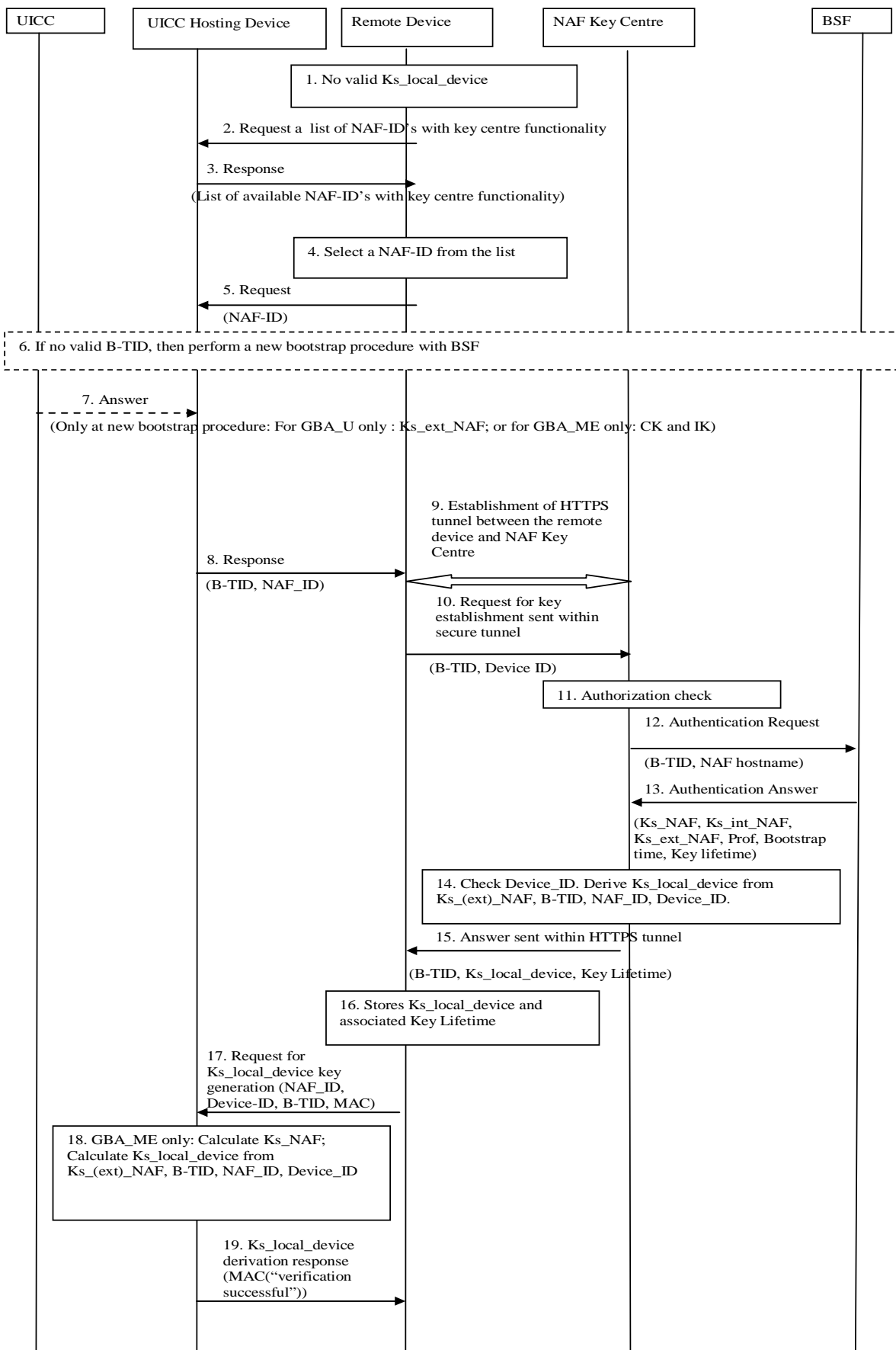
4.5.2 Key establishment procedure

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 in order for the UICC Hosting Device to be able to calculate a new Ks_(ext)_NAF.

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 sends a response including the B-TID and NAF_ID to the Remote Device.

9. 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 (TLS according to TS 33.310 [19], Annex E) or based on a shared key based mutual authentication between the Remote Device and the NAF Key Centre (PSK TLS according to TS 33.310 [19], Annex E).

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) Mobile Phone Specifications [15]. In PC-based TCG technology [16], 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 may in the future 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 the present document.

10. 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.

11. 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 document.

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

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

14. 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.

15. 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.

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

17. The Remote Device sends a response to the UICC Hosting Device to indicate that the key establishment procedure with NAF Key Centre is now completed. The Remote Device sends the NAF_ID corresponding to the NAF Key Centre, Device-ID, B-TID and the Key lifetime to the UICC Hosting Device. The Remote Device also includes a MAC which is computed as MAC = HMAC-SHA-256(Ks_local_device, NAF-ID || Device-ID || B-TID) truncated to 16 octets, where HMAC-SHA-256 with truncation is defined in [12], [13], [14].

18. The UICC Hosting Device retrieves the Ks_(ext)_NAF associated with the received NAF_ID and B-TID. If the requested association is authorised, then the UICC Hosting Device derives Ks_local_device key. 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 (see Annex A).

   The UICC Hosting Device verifies the MAC value received from the Remote Device by computing MAC' = HMAC-SHA-256(Ks_local_device, NAF_ID || Device_ID || B-TID) truncated to 16 octets. If the MAC' does not equal MAC, then the UICC Hosting Device terminates the key agreement procedure and returns a MAC verification failure message in response to the Ks_local_device derivation request.

19. If MAC'=MAC then the UICC Hosting Device stores Ks_local_device and associated parameters as Device_ID. The UICC Hosting Device then sends to the Remote Device a Ks_local_device derivation response containing a MAC of the ASCII-encoded string "verification successful" using the key Ks_local_device and the MAC algorithm HMAC-SHA-256 [13] truncated to 16 octets [14].

Annex A (normative):
Key Derivation Function definition

A.1 Platform specific key (Ks_local_device): 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 10 octets),

- 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.

Annex B (normative):
HTTP based key request procedure

B.1 Introduction

Clause 4.5 specifies the HTTP based Key request procedure between the NAF Key Centre and the Remote Device. It specifies how the Remote Device retrieves the Ks_local_device key from the NAF Key Centre together with some associated parameters.

B.2 Key request procedure

This clause contains the following HTTP based procedures:

- Key request;

B.2.1 Key request

The Remote Device shall generate a request for Key Request according to clause 4.5.2. The Remote Device shall send the Key Request to the NAF Key Centre in the HTTP payload in a HTTP POST request. The Request-URI shall indicate the type of the message, i.e. Key Request. Upon successful request, NAF Key Centre shall return indication of success together with the Ks_local_device key.

The Remote Device populates the HTTP POST request as follows:

- the HTTP version shall be 1.1 which is specified in RFC 2616 [17];

- the base of the Request-URI shall contain the full NAF Key Centre key establishmentURI (e.g. http://nafkeycentre.home1.net:1234);

- the Request-URI shall contain an URI parameter "requesttype" that shall be set to "key-request-devicekey", i.e. Request-URI takes the form of "/keyestablishment?requesttype=key-request-devicekey";

- the Remote Device may add additional URI parameters to the Request-URI;

- the HTTP header Content-Type shall be the MIME type of the payload, i.e. "application/keyest-devicekeyrequest+xml". The XML schema of the payload is specified in Annex D.1 in this specification;

- the Remote Device may add additional HTTP headers to the HTTP POST request.

The Remote Device sends the HTTP POST to the NAF Key Centre. The NAF Key Centre checks that the HTTP POST is valid, and extracts the Key request for further processing. The NAF Key Centre shall verify that the Remote Device is authorized to use this service according to clause 4.5.2.

Upon successful authorization verification, the NAF Key Centre shall return the HTTP 200 OK to the Remote Device.

The NAF Key Centre shall populate HTTP response as follows:

- the HTTP status code in the HTTP status line shall be 200;

- the HTTP header Content-Type shall be the MIME type of the payload, i.e. "application/keyest-keyresponse+xml". The XML schema of the payload is specified in Annex D.2 in this specification;

The NAF Key Centre shall send the HTTP response to the Remote Device. The Remote Device shall check that the HTTP response is valid.

B.2.2 Error situations

The key request procedure may not be successful for multiple reasons. The error cases are indicated by using 4xx and 5xx HTTP Status Codes as defined in RFC 2616 [17]. The 4xx status code indicates that the Remote Device seems to have erred, and the 5xx status code indicates that the NAF Key Centre is aware that it has erred. Possible error situations during key establishment and their mappings to HTTP Status Codes are described in table B.2.2.1.

NOTE: In table B.2.2.1, the "Description" column describes the error situation in NAF Key Centre. The "NAF Key Centre error" column describes the typical reason for the error.

The NAF Key Centre shall send the HTTP response to the Remote Device. The Remote Device shall check that the HTTP response is valid.

Table B.2.2-1: HTTP Status Codes used for key request errors

HTTP Status Code	HTTP Error	Remote Device should repeat the request	Description	NAF Key Centre error
400	Bad Request	No	Request could not be understood	Request was missing, or malformed
401	Unauthorized	Yes	Not used by NAF Key Centre	-
402	Payment Required	No	Not used by NAF Key Centre	-
403	Forbidden	No	NAF Key Centre understood the request, but is refusing to fulfil it	The request was valid, but Remote Device is not allowed to use this service
404	Not Found	No	NAF Key Centre has not found anything matching the Request-URI	The Request-URI was malformed and NAF Key Centre cannot fulfil the request
405	Method not allowed	No	The method specified in the Request-Line is not allowed for the resource identified by the Request-URI.	
406 to 417	*	No	Not used by NAF Key Centre	-
500	Internal Server Error	No	Not used by NAF Key Centre	-
501	Not Implemented	No	NAF Key Centre does not support the requested functionality	The server does not contain particular NAF Key Centre service requested
502	Bad Gateway	No	Not used by NAF Key Centre	-
503	Service Unavailable	Yes	NAF Key Centre service is currently unavailable	NAF Key Centre is temporarily unavailable, Remote Device may repeat the request after delay indicated by "Retry-After" header
504	Gateway Timeout	No	The server, while acting as a gateway or proxy, did not receive a timely response from the upstream server	The NAF Key Centre did not get response over Zn interface.
505	HTTP Version Not Supported	No	NAF Key Centre does not support the HTTP protocol version that was used in the request line	Remote Device should use HTTP/1.1 version with NAF Key Centre

Annex C (informative):
Signalling flows for key request procedure

C.1 Introduction

This annex gives examples of signalling flows for using HTTP. It is assumed that TLS with certificate based mutual-authentication or PSK-TLS has been established before the HTTP signalling flow described in this section takes place.

The Remote Device requests a Ks_local_device key from the NAF Key Centre and an example of the signalling flow of the key request procedure between the Remote Device and the NAF Key Centre is given in clause C.2.

C.2 Signalling flow demonstrating a successful key request procedure

The signalling flow in figure C.2-1 describes the generic message exchange between a Remote Device and an NAF Key Centre using HTTP. The HTTP client application resides in the Remote Device.
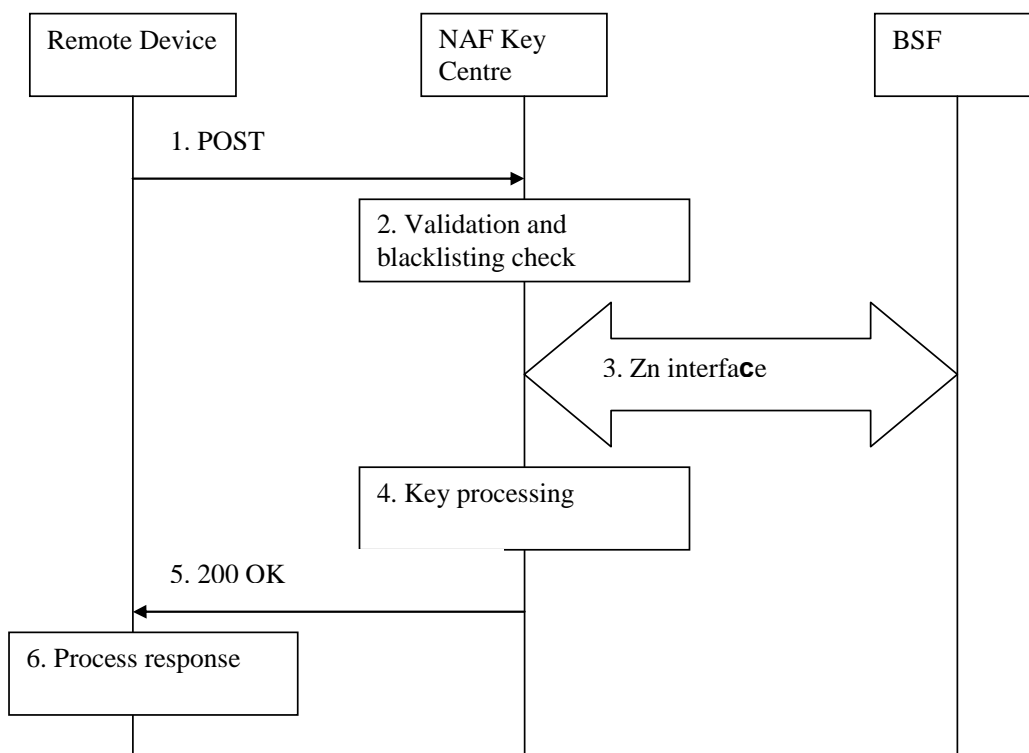

Figure C.2-1: Successful key request procedure between Remote Device and NAF Key Centre

1. Key request (Remote Device to NAF Key Centre) - see example in table C.2-1

The Remote Device sends an HTTP request to the NAF Key Centre containing a Key request.

Table C.2-1: Key request (Remote Device to NAF Key Centre)

```
POST /keyestablishment?requesttype=key-request-devicekey  HTTP/1.1

Host: nafkeycentre.home1.net:1234

Content-Type: application/keyest-devicekeyrequest+xml

Content-Length: (...)

User-Agent: KeyestAgent; Release-7

Date: Thu, 27 June 2007 10:50:35 GMT

Accept: */*

Referrer: http://nafkeycentre.home1.net:1234/service


<Key request BLOB>
```

Request-URI: The Request-URI (the URI that follows the method name, "POST", in the first line) indicates the resource of this POST request. The Request-URI contains the parameter "requesttype" which is set to "key-request-devicekey" to indicate to the NAFKey Centre the desired request type, i.e. Remote Device requests for a Ks_local_device key.

Host: Specifies the Internet host and port number of the NAF Key Centre, obtained from the original URI given by referring resource.

Content-Type: Contains the media type "application/keyest-devicekeyrequest+xml", i.e.Key request.

Content-Length: Indicates the size of the entity-body, in decimal number of OCTETs, sent to the recipient.

User-Agent: Contains information about the user agent originating the request and the release of it.

Date: Represents the date and time at which the message was originated.

Accept: Media types which are acceptable for the response.

Referrer: Allows the user agent to specify the address (URI) of the resource from which the URI for the NAF Key Centre was obtained.

2. **Validation and blacklisting check**

   The NAF Key Centre will also verify that the DNS name in the realm attribute matches the NAF Key Centre hostname. If the conversation is taking place inside a server-authenticated TLS tunnel, the NAF Key Centre will also verify that this DNS name is the same as that of the TLS server.

   The NAF Key Centre verifies that the Remote Device is authorized to use this service as described in clause 4.5.2. If the authorization succeeds, the incoming client-payload request is taken in for further processing.

   If the NAF Key Centre does not have the NAF specific key material (Ks_NAF or Ks_ext_NAF), then the NAF Key Centre retrieves that and one or more user security setting (USS) from the BSF. For detailed signalling flows see 3GPP TS 29.109 [9].

3. **Zn: NAF Key Centre specific key procedure**

   NAF Key Centre retrieves the NAF specific key material and IMPI of the user.

For detailed signalling flows see TS 29.109 [9].

4. Key **processing in the NAF Key Centre**

> NAF Key Centre further derives the key establishment specific key material Ks_local_device as specified in Annex A.

5. **Response indicating success (NAF Key Centre to Remote Device)** - see example in table C.2-2

> The NAF Key Centre sends 200 OK response to the Remote Device to indicate the success of the Key request.

Table C.2-2: Key response (NAF Key Centre to Remote Device)

```
POST /keyestablishment?requesttype=key-response-devicekey  HTTP/1.1

Host: nafkeycentre.home1.net:1234

Content-Type: application/keyest-devicekeyresponse+xml

Content-Length: (...)

Date: Thu, 27 June 2007 10:50:35 GMT

Accept: */*

Referrer: http://nafkeycentre.home1.net:1234/service



<Key request BLOB>
```

Request-URI: The Request-URI (the URI that follows the method name, "POST", in the first line) indicates the resource of this POST request. The Request-URI contains the parameter "requesttype" which is set to "key-response-devicekey" to indicate to the Remote Device the desired response type, i.e. UICC Hosting Device responses with a Ks_local_device key.

Host: Specifies the Internet host and port number of the NAF Key Centre, obtained from the original URI given by referring resource.

Content-Type: Contains the media type "application/keyest-devicekeyresponse+xml", i.e.Key response.

Content-Length: Indicates the size of the entity-body, in decimal number of OCTETs, sent to the recipient.

Date: Represents the date and time at which the message was originated.

Accept: Media types which are acceptable for the response.

Referrer: Allows the user agent to specify the address (URI) of the resource from which the URI for the NAF Key Centre was obtained.

6. **Process response at Remote Device**

> The Remote Device receives the response and accepts the server-payload for further processing. The Remote Device stores the Ks_local_device key, the Key Lifetime and B-TID locally.

Annex D (normative):
XML schema for Key Request and Key Response

D.1   Introduction

This annex contains the XML schema which defines a format for the key request sent from the Remote Device to the NAF Key Centre requesting a Ks_local_device key and for the key response sent from the NAF Key Centre to the Remote Device containing the Ks_local_device key, according to the procedures in section 4.5.2.

D.2   Key Request Format

D.2.1   Data Format

The below XML schema defines a format used to request a Ks_local_device key from the NAF Key Centre.

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema
    xmlns:xs="http://www.w3.org/2001/XMLSchema"
    xmlns="urn:3GPP:metadata:2005:Keyest:DeviceKeyRequest"
    targetNamespace="urn:3GPP:metadata:2005:Keyest:DeviceKeyRequest"
    elementFormDefault="qualified"
    attributeFormDefault="unqualified">

    <xs:element name="keyestDeviceKeyRequest">
        <xs:annotation>
            <xs:documentation>
                Keyest Key Request as defined by 3GPP TS 33.259
            </xs:documentation>
        </xs:annotation>
        <xs:complexType>
            <xs:sequence>
                <xs:element name="BTID" type="xs:string" minOccurs="1" maxOccurs="1"/>
                <xs:element name="DEVICEID" type="xs:string" minOccurs="1" maxOccurs="1"/>
            </xs:sequence>
            <xs:anyAttribute processContents="skip"/>
        </xs:complexType>
    </xs:element>
</xs:schema>
```

D.2.2   Example

The below example is used to request a new Ks_local_device key derived from a GBA key with identity BTID "jhg876jhg"and a DEVICE ID "64783934857".

```
<?xml version="1.0" encoding="UTF-8"?>
<keyestDeviceKeyRequest
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns="urn:3GPP:metadata:2005:Keyest:DeviceKeyRequest">
    <BTID>jhg876jhg</BTID>
    <DEVICEID>64783934857</DEVICEID>
</keyestDeviceKeyRequest>
```

D.3   Key Response Format

D.3.1   Data Format

The below XML schema defines a format used in the response to a Key request from the Remote Device according to the procedure in section 4.5.2.

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema
    xmlns:xs="http://www.w3.org/2001/XMLSchema"
    xmlns="urn:3GPP:metadata:2005:Keyest:DeviceKeyResponse"
    targetNamespace="urn:3GPP:metadata:2005:Keyest:DeviceKeyResponse"
    elementFormDefault="qualified"
    attributeFormDefault="unqualified">

    <xs:element name="keyestDeviceKeyResponse">
        <xs:annotation>
            <xs:documentation>
                Keyest Key Response as defined by 3GPP TS 33.259
            </xs:documentation>
        </xs:annotation>
        <xs:complexType>
            <xs:sequence>
                <xs:element name="BTID" type="xs:string" minOccurs="1" maxOccurs="1"/>
                <xs:element name="KSLOCALDEVICE" type="xs:string" minOccurs="1" maxOccurs="1"/>
                <xs:element name="KEYLIFETIME" type="xs:string" minOccurs="1" maxOccurs="1"/>
            </xs:sequence>
            <xs:anyAttribute processContents="skip"/>
        </xs:complexType>
    </xs:element>

</xs:schema>
```

D.3.2   Example

The below example is used in the key response from the NAF Key Centre with identity BTID "jhg876jhg", KSLOCALDEVICE "64783934857" and a KEYLIFETIME "5675".

```
<?xml version="1.0" encoding="UTF-8"?>
<keyestDeviceKeyResponse
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns="urn:3GPP:metadata:2005:Keyest:DeviceKeyResponse">
    <BTID>jhg876jhg</BTID>
    <KSLOCALDEVICE>64783934857</KSLOCALDEVICE>
    <KEYLIFETIME>5675</KEYLIFETIME>
</keyestDeviceKeyResponse>
```

Annex E (normative):
TLS profiles

The Remote Device and NAF Key Centre shall use the TLS profile defined in TS 33.310 [19] for TLS with certificate based mutual authentication and PSK-TLS.

Annex F (informative):
Application specific key (Ks_local_device_appl)

This Annex gives an example on how the applications in the UICC Hosting Device and Remote Device could derive further key material (Ks_local_device_appl) from the Ks_local_device key.

F.1 Example of Ks_local_device_appl key derivation in key establishment

The applications in the UICC Hosting Device and Remote Device could use the Ks_local_device key to derive further key material, which is application specific, to ensure that different applications in the UICC Hosting Device and Remote Device use different keys.

Application specific key material could be computed in the UICC Hosting Device and the Remote Device as: Ks_local_device_appl = KDF (Ks_local_device, B-TID, Appli_ID), where KDF is the key derivation function as specified in Annex G, and the key derivation parameters consist of the Appli_ID and the B-TID.

NOTE: The definition of the Appli_ID is out of the scope of this specification. The Appli_ID could be defined in an application specification utilising the key establishment procedure. The Appli_ID could also be exchanged on the Local Interface between the applications to initiate the key derivation of the application specific key material.

Annex G (informative):
Application specific key (Ks_local_device_appl): Key Derivation Function definition

G.1 Ks_local_device_appl 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 annex is implemented as defined in TS 33.220 [3].

G.2 Input parameters for Ks_local_device_appl key derivation

When the application specific key (i.e. Ks_local_device_appl) is computed, the input parameters for the key derivation function could be the following:

-   FC = 0x01,

-   P0 = Appl_ID,

-   L0 = length of Appl_ID is variable (not greater than 65535),

-   P1 = B-TID,

-   L1 = length of B-TID 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_local_device key.

Annex H (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
2007-09	SP-37	SP-070598	001	1	Stage 3 details - Ua interface and adding TLS Profiling	7.0.0	7.1.0
2007-09	SP-37	SP-070598	002	1	Introduction of key confirmation and some various other changes	7.0.0	7.1.0
2007-09	SP-37	SP-070598	003	1	Clarifications regarding the use of Ks_local_device key	7.0.0	7.1.0
2007-12	SP-38	SP-070889	005	1	Correction of XML schema	7.1.0	7.2.0
2007-12	SP-38	SP-070889	004	1	Visited NAF Key Centre Requirements	7.1.0	8.0.0
2008-03	SP-39	SP-080146	006	-	Correction of typos in references	8.0.0	8.1.0
2008-12	SP-42	SP-080745	007	-	Input parameter encoding shall rely on TS 33.220 KDF	8.1.0	8.2.0
2008-12	SP-42	SP-080745	008	-	Removing editor's note on IANA registration	8.1.0	8.2.0
2009-12	-	-	-	-	Update to Rel-9 version (MCC)	8.2.0	9.0.0
2011-03	-	-	-	-	Update to Rel-10 version (MCC)	9.0.0	10.0.0
2012-09	SP-57	SP-120605	009	-	Correction for TLS references to point to TS 33.310	10.0.0	11.0.0
2014-09	-	-	-	-	Update to Rel-12 version (MCC)	11.0.0	**12.0.0**

History

Document history		
V12.0.0	October 2014	Publication