gemalto

C6-070252

Overview of 3GPP TS 33.110

Key establishment between a UICC and a Terminal

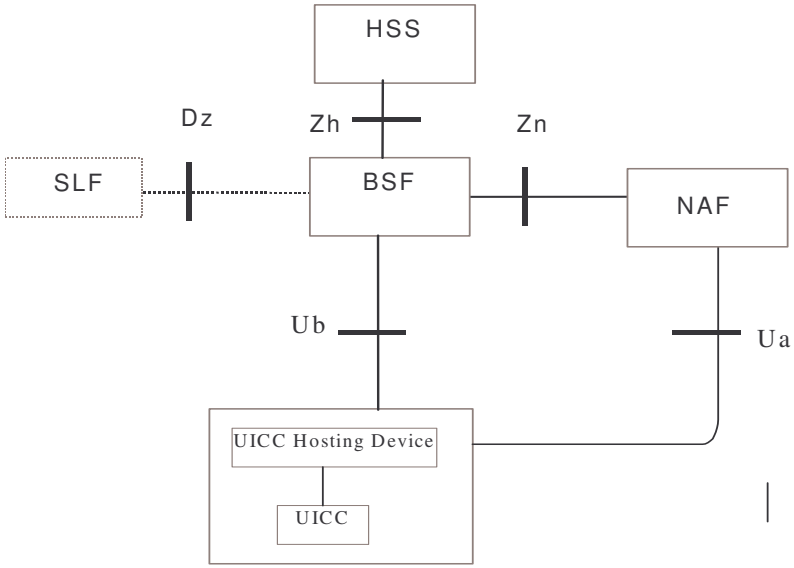
3GPP TSG–CT6 Meeting #43
Osaka, Japan, 8 – 11 May 2007

Key Establishment between a UICC and a Terminal

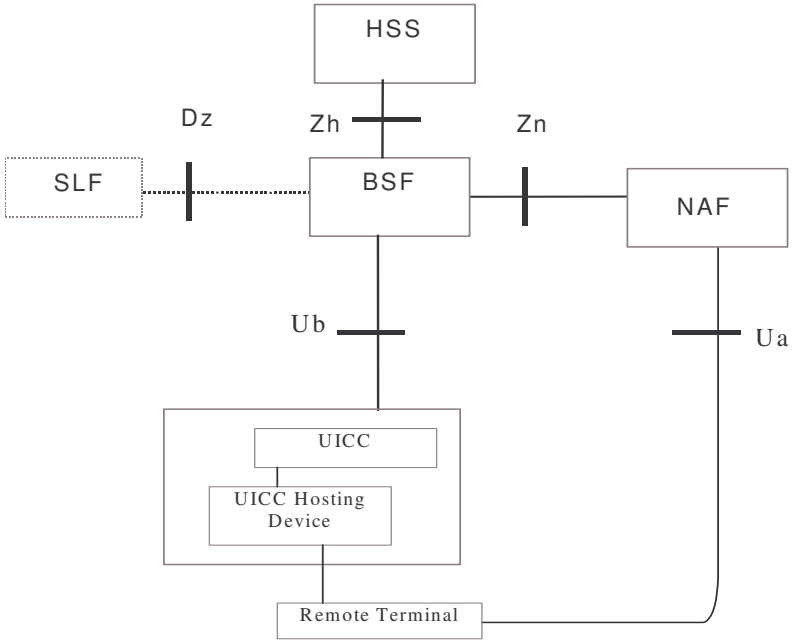
- SA3 specified the key establishment between a UICC and a terminal in 3GPP TS 33.110.
  - Current version is TS 33.110 v7.1.0
- TS 33.110
  - describes the security features and mechanisms to provision a shared key between a UICC and a terminal that may host the UICC or be connected to the device hosting the UICC via a local interface.
- TS 33.110 Key establishment solution relies on
  - GBA_U
    - UICC-based Generic Bootstrapping Authentication specified in 3GPP TS 33.220
  - Certificate-based HTTPS between the Terminal and the NAF Key Center
- The shared key, Ks_local,
  - may be established “per application” or “per platform”

Reference model

- "Terminal"
  - Terminal denotes a trusted device that can establish a shared key with a UICC. The Terminal is a generic term aiming to address either the scenario where it is part of the UICC Hosting Device or the scenario where it is a physically separated component (e.g. PNE as defined in TS 22.259)

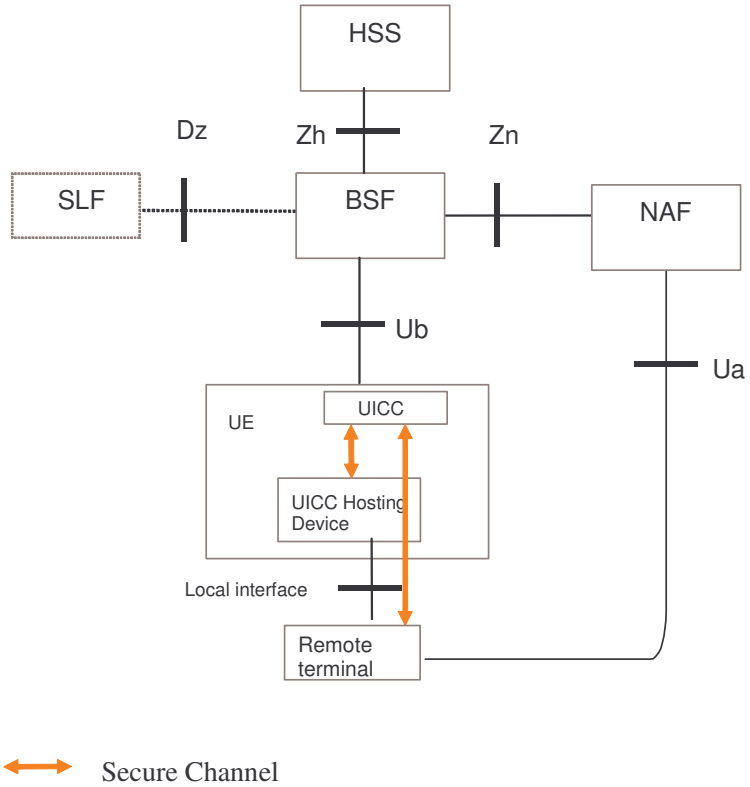


The Terminal is part of the UICC Hosting Device



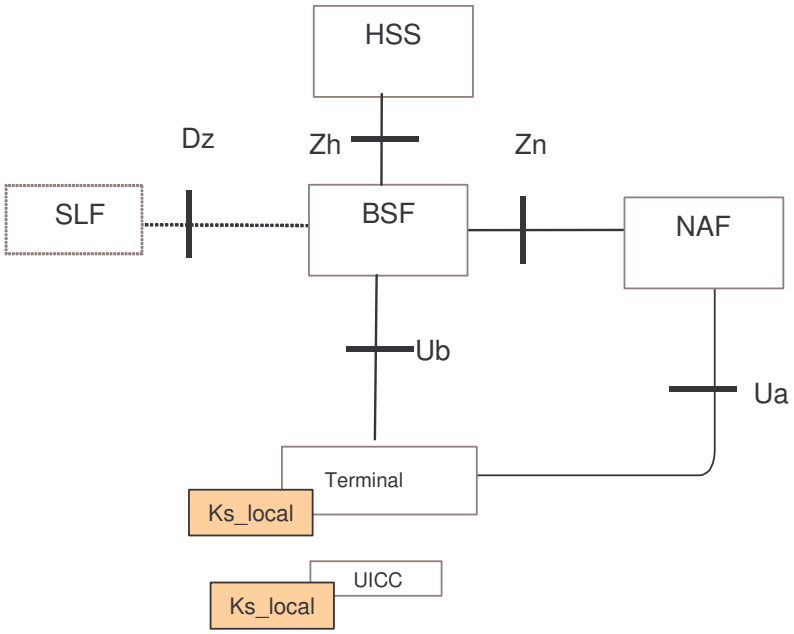
The Remote Terminal is connected to the UICC Hosting Device

Scope



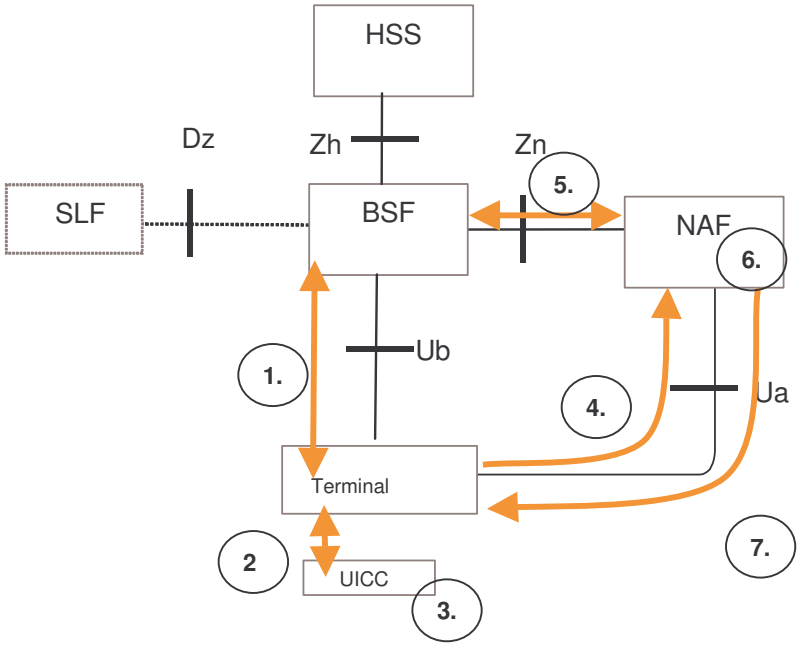
- To provision a shared key, Ks_local, between a UICC and a Terminal that may host the UICC or be connected to the device hosting the UICC via a local interface.
- Candidate applications to use this key establishment mechanism include but are not restricted to secure channel between a UICC and an end point terminal as defined by ETSI SCP 102 484.
- Secure Channel use-cases are
  - Personal Area Network
  - DRM and distributed applications
  - UICC as control point for Device Management
  - User Interface

Key Establishment features



- NAF Key Center
  - Dedicated NAF located in the Home Network and in charge of performing the key establishment between a UICC and a Terminal
  - It shall be possible to configure the NAF Key Center to restrict the key establishment based on the targeted UICC and Terminal applications
- The shared key Ks_local is derived “per application” or “per platform”
- A key lifetime is associated to each Ks_local
- Ks_local derivation is performed within USIM or ISIM application

Key Establishment of Ks_local



1. The Terminal runs GBA_U bootstrapping procedure to get Ks_int_NAF associated to the NAF Key Center
2. Exchange of NAF Key Center ID and B-TID and request for Ks_local derivation
3. UICC derives Ks_local
4. Terminal requests Ks_local key over certificate-based HTTPS
5. NAF Key Center fetches NAF specific keys
6. NAF Key Center calculates Ks_local key
7. NAF sends Ks_local to the Terminal via the protected HTTPS channel