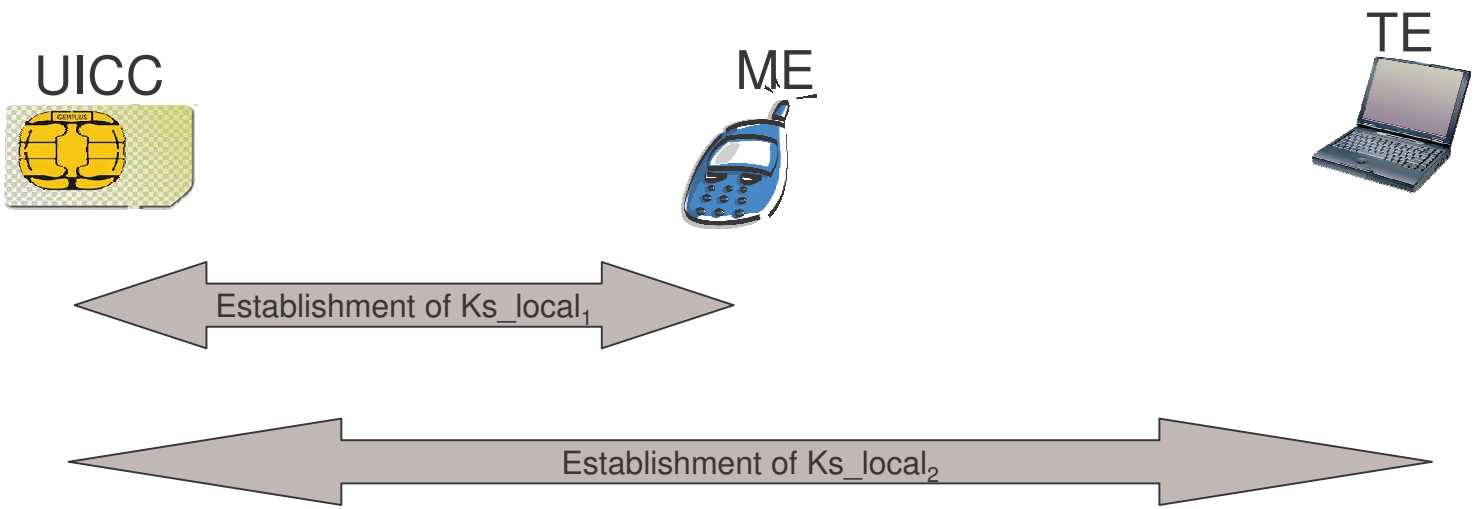
Key establishment between a UICC and a terminal, terminal aspects

Gemalto (Axalto), Gemalto (Gemplus)

3GPP TSG-SA WG3 Meeting #44
Tallinn, Estonia, 11-14 July, 2006
S3-0600465

Current definition

- TS 33.110 currently defines “terminal” as follows:
  - “For the purposes of the present document, the term terminal denotes a trusted device that can establish a shared key with a UICC. The terminal may host the UICC (e.g. ME) or be connected to a device hosting the UICC via a local interface (e.g. PNE as defined in TS 22.259 [4]).”



Mapping with 3GPP terminology

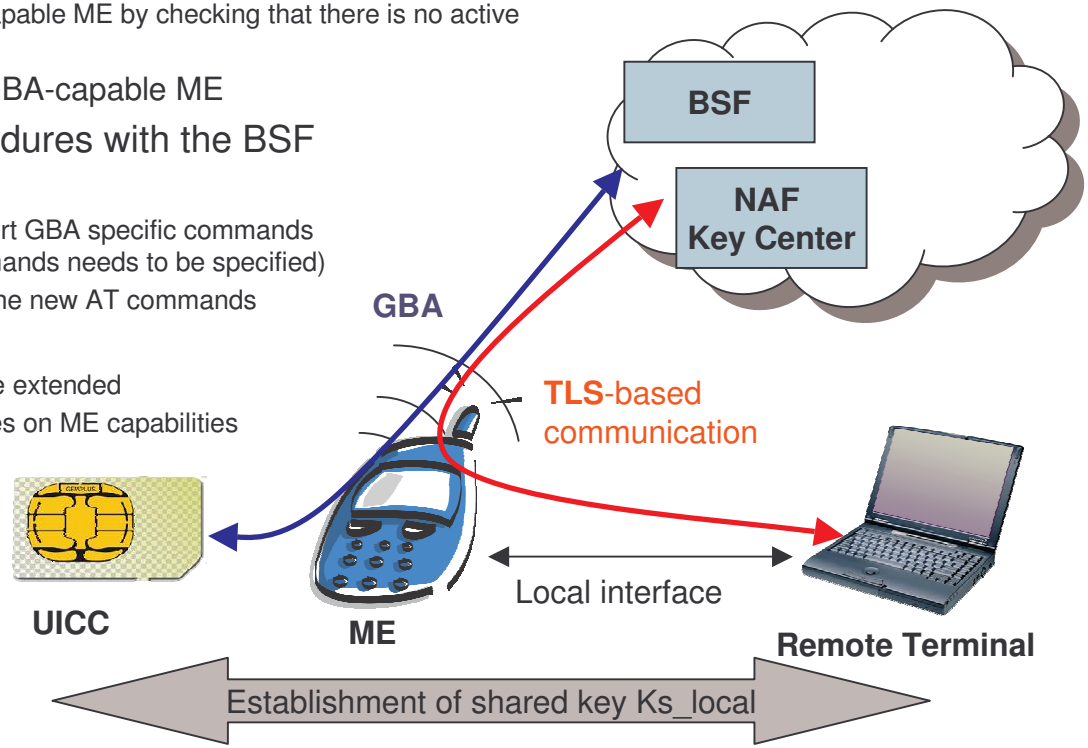
- “terminal” may be the MT, ME or TE part of the UE.
  - TS 21.905 defines the UE as the combination of the ME and the UICC. The ME may also be subdivided into a MT and a TE.
- “terminal” may be any part of the WLAN-UE (except the UICC).
  - TS 33.234 defines the WLAN-UE.
- “terminal” may be a PNE as defined in TS 22.259
- The current definition reflects the new assumption that the device needs to be trusted

Extension of the current definition

- During the last SA3 meeting (SA3#43), it was noted that it might be necessary to extend the current terminal definition to cover two types of “terminals”.
  - First case: the “terminal” is the device hosting the UICC. In this case, the terminal contacts the BSF to establish Ks (the “terminal” shall support the Ub interface).
  - Second case: the “terminal” is not the device hosting the UICC (called hereafter “remote terminal”). Both the device hosting the UICC or the “remote terminal” can contact the BSF to establish Ks (the “remote terminal” may support the Ub interface).
- Consequently, the requirements on “remote terminals” could be different from the requirements on “terminals”.

Remote Terminals (RT) specific requirements

- The ME provides the RT with an IP connection
- Two implementation options:
  - 1- RT runs bootstrapping procedure with the BSF
    - Prerequisites:
      - ✓ The RT shall be capable of establishing a a communication channel with the UICC (generic UICC AT commands or Bluetooth SAP can be used)
      - ✓ The RT shall support the Ub interface
      - ✓ It should be ensured that the ME and RT will not try to bootstrap simultaneously (this could be done by a GBA-capable ME by checking that there is no active connection with the BSF)
    - Major advantage: no need for a GBA-capable ME
  - 2- ME runs the bootstrapping procedures with the BSF
    - Prerequisite:
      - ✓ The ME-RT interface shall support GBA specific commands (e.g. new GBA specific AT commands needs to be specified)
      - ✓ The ME shall support GBA and the new AT commands
    - Major drawbacks:
      - ✓ Existing ME-RT interface shall be extended
      - ✓ Introduce additional dependencies on ME capabilities



Recommendations

- Put the same requirements on all ‘terminals” (in particular, all “terminals” that support the Key Establishment Mechanism shall support the Ub interface). This is to enable the implementation of the Key Establishment Mechanism on Remote Terminals that are compliant with the release 7 specifications (no GBA specific AT commands are defined in release 7).
- Enhance the current “terminal” definition in TS 33.110
- S3-060466 implements the above recommendations