3GPP TSG-SA WG3 Meeting #37 S3-050147
Sophia Antipolis, France, February 21-25, 2005

Use-case of Ks_int_NAF for HTTPS

Comments to S3-050069

Gemplus, Axalto

Introduction

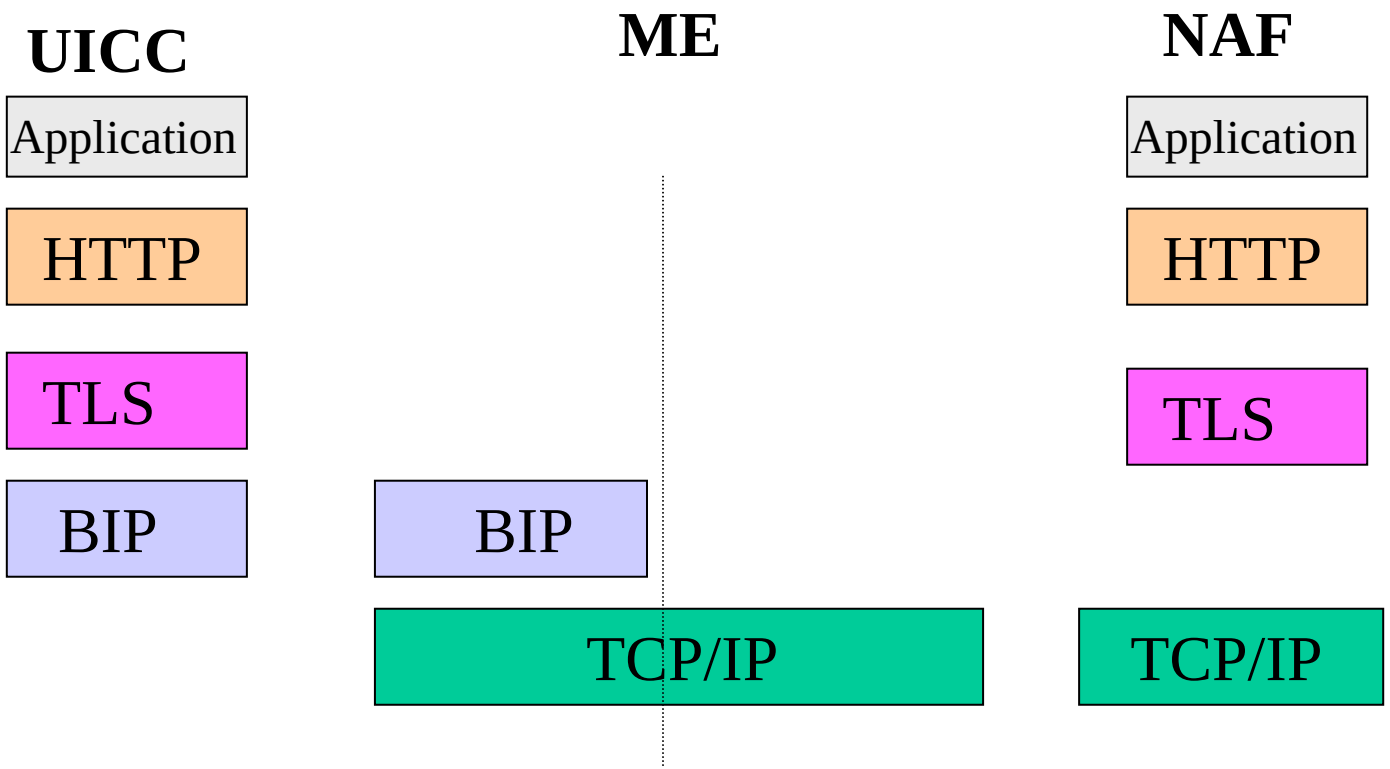
- S3-050069 CR states in “reason for change” that the use of the Ks_int_NAF for the TS 33.222 has never been intended since there is no use-case.

- At the moment, Rel-6 mechanisms are available to allow the use of the Ks_int_NAF for TS 33.222 authentication mechanisms.

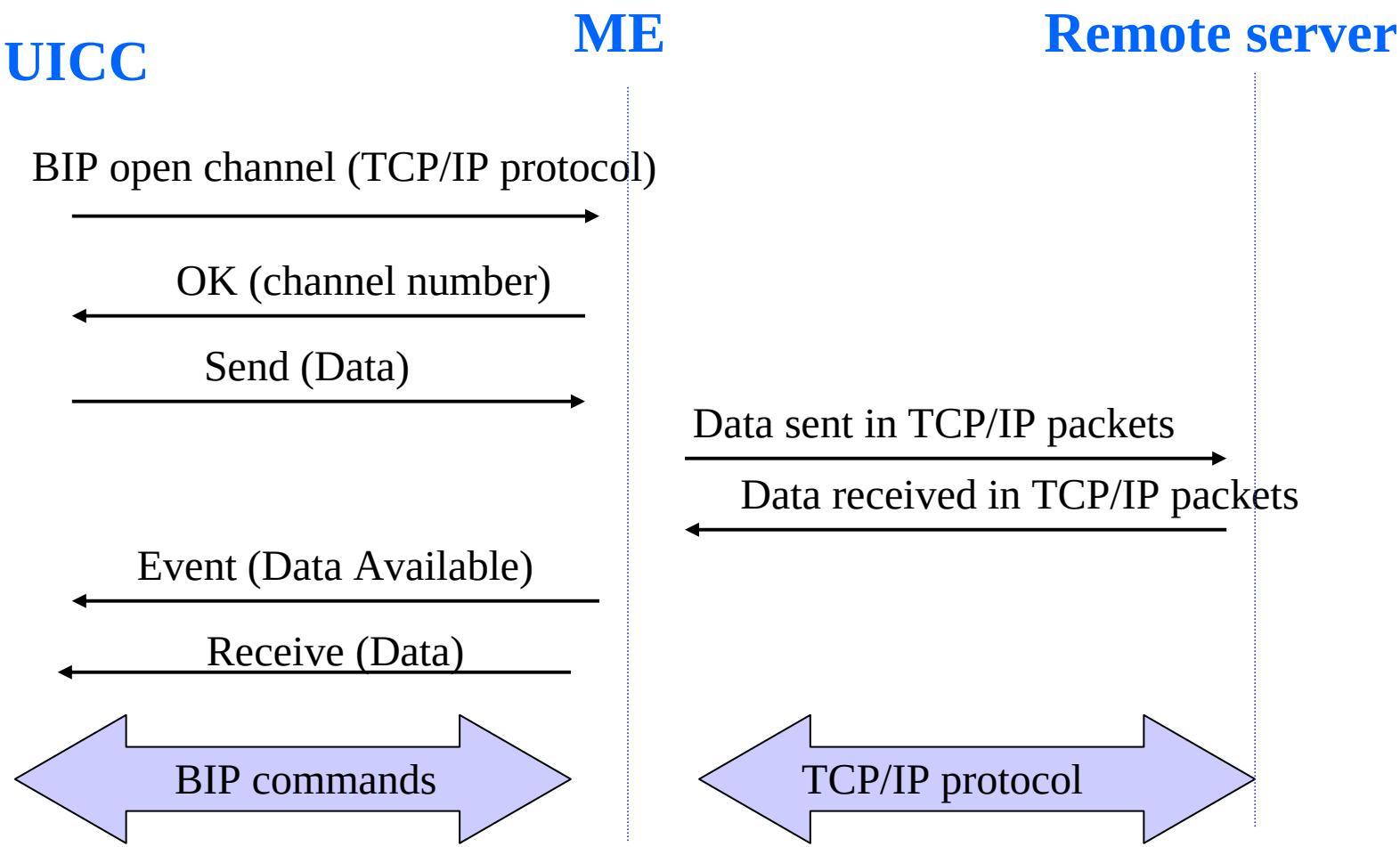
- This document description a way to use the Ks_int_NAF for HTTPS

- PS: Other comments on S3-050069 are provided in S3-050098

Architecture



BIP usage


UICC
ME
Remote server
BIP open channel (TCP/IP protocol)
OK (channel number)
Send (Data)
Data sent in TCP/IP packets
Data received in TCP/IP packets
Event (Data Available)
Receive (Data)
BIP commands
TCP/IP protocol

Procedures

- The UICC requests the ME to perform a bootstrapping operation as described in section 6.4.7.2 of TS 31.111
  - The UICC and BSF share Ks key
- The UICC opens a BIP channel with the NAF as described in TS 31.111
  - An active TCP/IP connection is established between the NAF and the UICC. This channel will be further used to exchange HTTP & HTTPS packets
- The UICC derives NAF-specific keys and sends the B-TID to the NAF in order to enable the NAF to retrieve NAF keys from the BSF (see TS 33.220)
  - UICC and NAF share Ks_int_NAF and Ks_ext_NAF keys
- The Ks_int_NAF can be used for TS 33.222 authentication mechanisms. The UICC and NAF can establish HTTPS sessions as described in TS 33.222 by means of BIP protocol.

Conclusion

- Ks_int_NAF could be used for HTTPS release 6
- All GBA_U NAF-specific keys should not be excluded to access services by means of HTTPS in TS 33.222

References

- **3GPP TS 33.222:** Generic Authentication Architecture (GAA); Access to network application functions using Hypertext; Transfer Protocol over Transport Layer Security (HTTPS)
- **3GPP TS 33.220:** Technical Specification Group Services and System Aspects; Generic Authentication Architecture (GAA); Generic bootstrapping architecture
- **3GPP TS 31.111:** Technical Specification Group Terminals; USIM Application Toolkit (USAT)
- **S3-050069:** Clarify the GBA requirements for https supporting applications at Ua reference point
- **S3-050098:** Comments to S3-050069 “Clarify the GBA requirements for https applications at Ua reference point”.