3GPP TSG SA WG3 Security — S3#34

July 6 - 9, 2004, Acapulco, Mexico

S3-040645

AKA usage in 3GPP

TR-45 AHAG joint session 8th July 2004

Peter Howard

SA3 vice-chairman

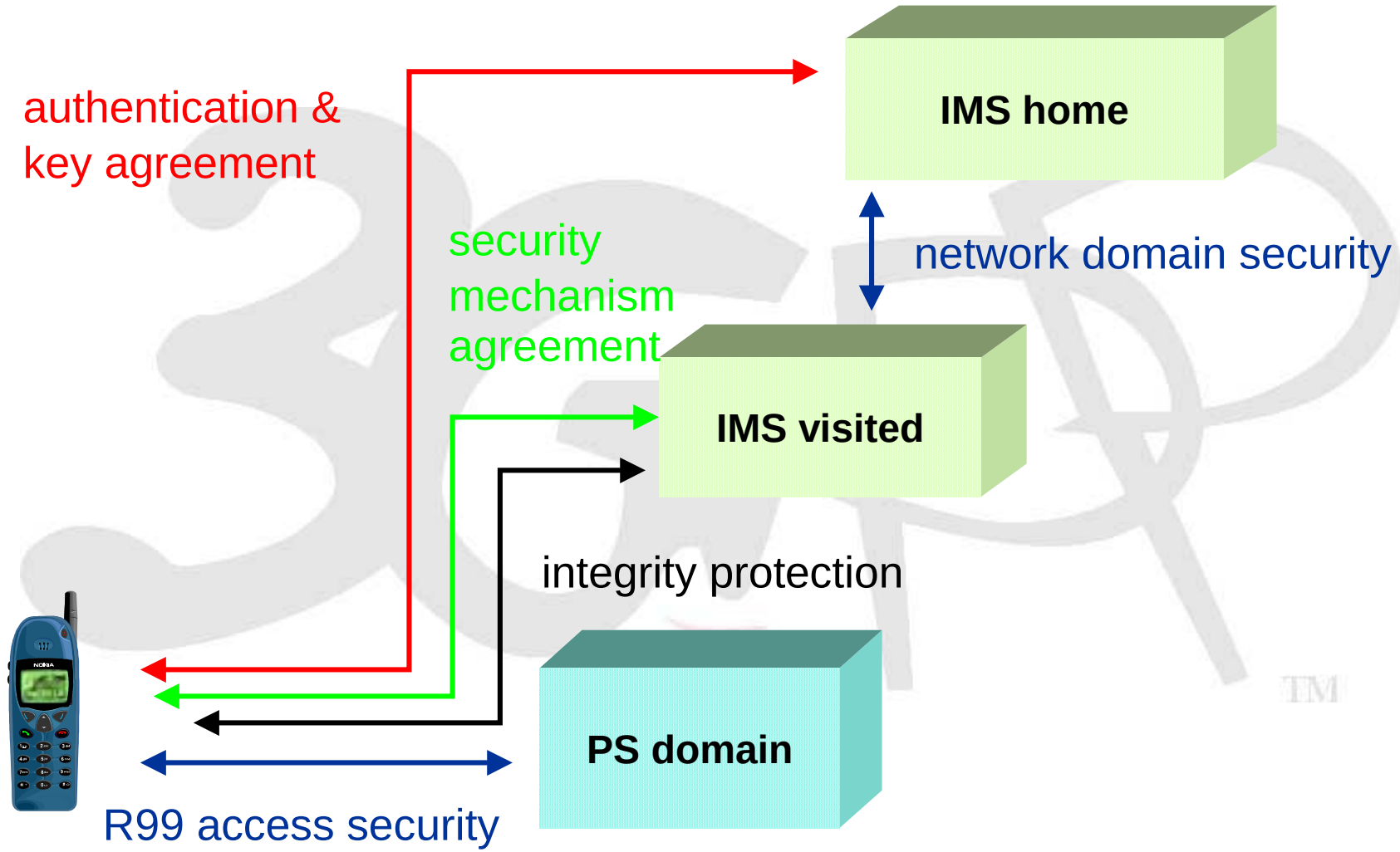
Contents

- Status of 3GPP AKA itself
- Usage of AKA in different contexts
  - Access security to IMS (Release 5)
  - WLAN interworking security (Release 6)
    - Secure WLAN access to Internet connectivity
    - Secure WLAN access to 3GPP services
  - Generic Authentication Architecture (Release 6)
    - Secure list management for presence service
      - including generic solution for securing HTTP based services
    - Key management for Multimedia Broadcast/Multicast Service (MBMS)

Status of AKA itself

- **AKA is specified in TS 33.102**
  - **No changes to the AKA mechanism itself for several years now**
  - **Based on feedback from stage 3 working groups, SA3 has made a clarification to the authentication re-attempt parameter in the Release 6 version of 33.102, see S3-040400**
- **An example algorithm set (MILENAGE) is specified in TSs 35.205 – 208**
  - **No changes since approval**

IMS security architecture



ISIM

ISIM **is a term that indicates the collection of IMS security data and functions on a UICC. The following implementation options are permitted:**

- **Use of a distinct ISIM application on a UICC which does not share security functions with the USIM**
- **Use of a distinct ISIM application on a UICC which does share security functions with the USIM**
- **Use of a R99/Rel-4 USIM application on a UICC**

IMS authentication and key agreement

- **Re-use of UMTS AKA protocol**
  - **Implemented on a UICC in the UA**
- **UMTS AKA protocol integrated into IMS SIP signalling according to HTTP Digest AKA (RFC3310)**

Access security architecture

- Initial authentication based on long-term SA
  - Protocol is run between UA and SIP proxy server (the S-CSCF) in home network
  - UA uses SA credentials and functions stored in ISIM
  - SIP proxy server (S-CSCF) interacts with authentication server (the HSS) in home network using Diameter Cx application
- Subsequent signalling messages between UA and first hop SIP proxy (the P-CSCF) are protected using short-term SA created during initial authentication
  - Session keys for integrity at SIP proxy server (S-CSCF) are passed to an authorised first hop SIP proxy (P-CSCF) further downstream
  - ISIM at user side securely delegates keys to UA
- Message protection is applied directly after initial authentication

Authentication at registration

- Authentication can only occur during registration
- Initial registration is always authenticated
- IMS private id (NAI) is used as the basis for authentication
- Subsequent registrations may be authenticated
- 3GPP mandates that UA registers before initiating services
  - One reason for this is that UA can be authenticated before session set-up to reduce session set-up time
- IMS public ids (SIP URIs) are not authenticated directly but the network checks that the public user identity is associated to the private id during registration

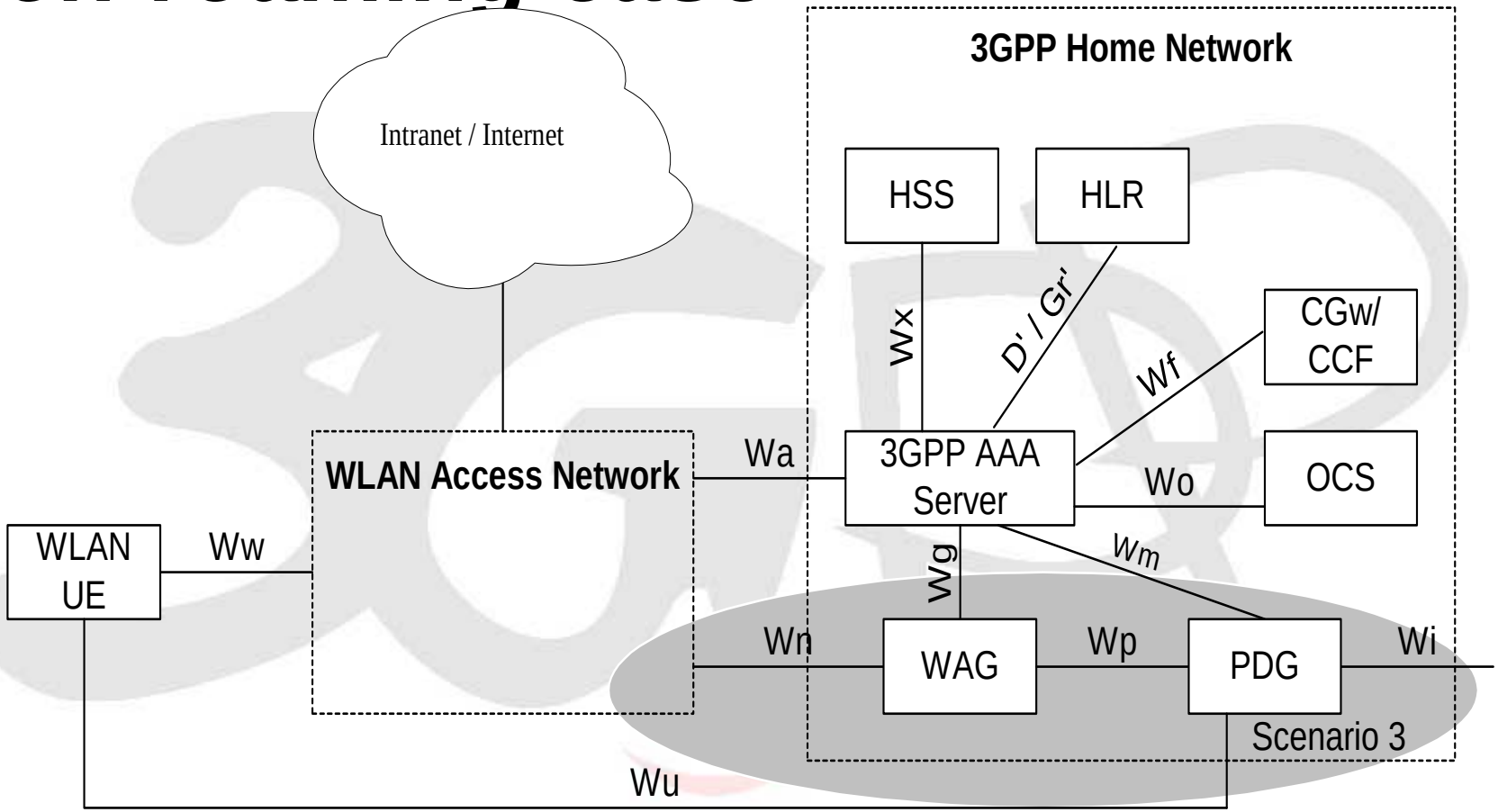
Re-authentication

- **Re-authentication policy**
  - **User should not be able to incur high amount of charges between two authentications**
  - **Avoid unnecessary authentications of users that have remained largely inactive**
- **Network may ask UA to re-register in order to force a re-authentication**
  - **The triggers may include charging thresholds, number of events, session duration, etc.**

WLAN interworking in 3GPP

- **WLAN access zone can be connected to cellular core network**
- **Security for**
  - **WLAN access to Internet connectivity (scenario 2)**
  - **WLAN access to 3GPP PS domain services (scenario 3)**

WLAN interworking – non-roaming case



Source: 3GPP TS 33.234

Scenario 2 security

- **Authentication methods**
  - **between WLAN-UE and 3GPP AAA server**
  - **based on EAP**
  - **AAA fetches authentication vectors from HSS using DIAMETER (Wx interface)**
  - **SIM: based on GSM AKA and network authentication (eap-sim)**
  - **USIM: based on UMTS AKA (eap-aka)**

EAP

- Extensible Authentication Protocol (EAP) is a general protocol framework that supports
  - multiple authentication mechanisms
  - allows a back-end server to implement the actual mechanism
    - authenticator simply passes authentication signaling through
- EAP was initially designed for use with PPP network access
  - But has been adapted by for many types of access authentication
    - WLAN (IEEE 802.1X), Bluetooth, …
- EAP consists of several Request/Response pairs; Requests are sent by network

WLAN-3GPP interworking with EAP-SIM/EAP-AKA

- **EAP-SIM**
  - **Internet draft**
  - **Describes how GSM authentication and key agreement protocol can be done in EAP**
  - **Additionally enhances GSM AKA with mutual entity authentication based on derived key Kc**
  - **Utilizes a bundle (at least two) of GSM triplets (RAND,SRES,Kc) in one run of the entity authentication → network authentication is based on (at least) 128-bit secret**
- **EAP-AKA**
  - **Internet draft**
  - **Describes how UMTS AKA can be done in EAP**

Scenario 3 security

- **IPsec tunnel established between UE and PDG**
- **Current status**
  - **IKEv2 used to establish IPsec SAs**
  - **EAP methods integrated into IKEv2 for client authentication**
    - **SIM: based on GSM AKA and network authentication (eap-sim)**
    - **USIM: based on UMTS AKA (eap-aka)**
  - **Server authentication based on PDG certificates**

Generic Authentication Architecture (GAA)

- GAA consists of three parts:
- *TS 33.220 Generic Bootstrapping Architecture* (GBA) offers generic authentication capability for various applications based on shared secret. Subscriber authentication in GBA is based on HTTP Digest AKA [RFC 3310].
- *TS 33.221 Support of subscriber certificates:* PKI Portal issues subscriber certificates for UEs and delivers an operator CA certificates. The issuing procedure is secured by using shared keys from GBA.
- *TS 33.222 Access to Network Application Function using HTTPS* will also be based on GBA.

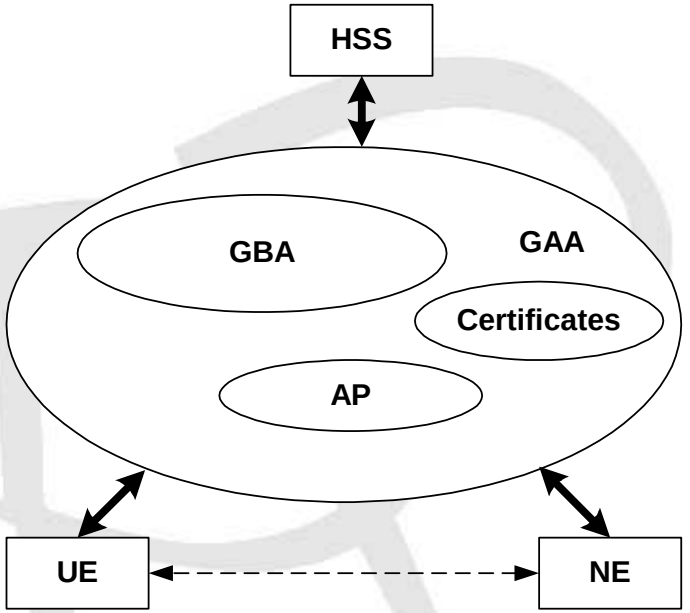
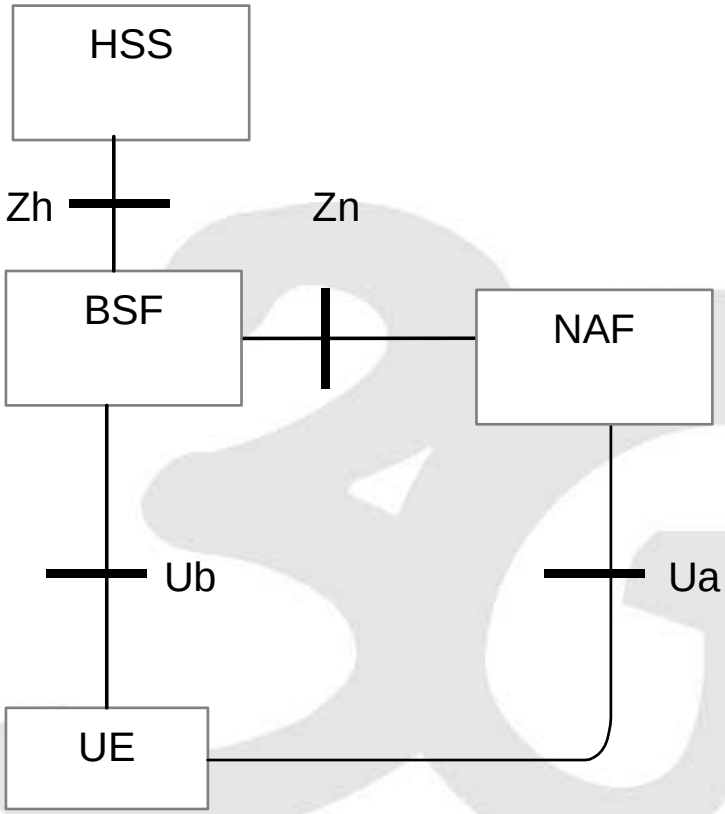


Figure from 3GPP TR 33.919

GBA: Generic Bootstrapping



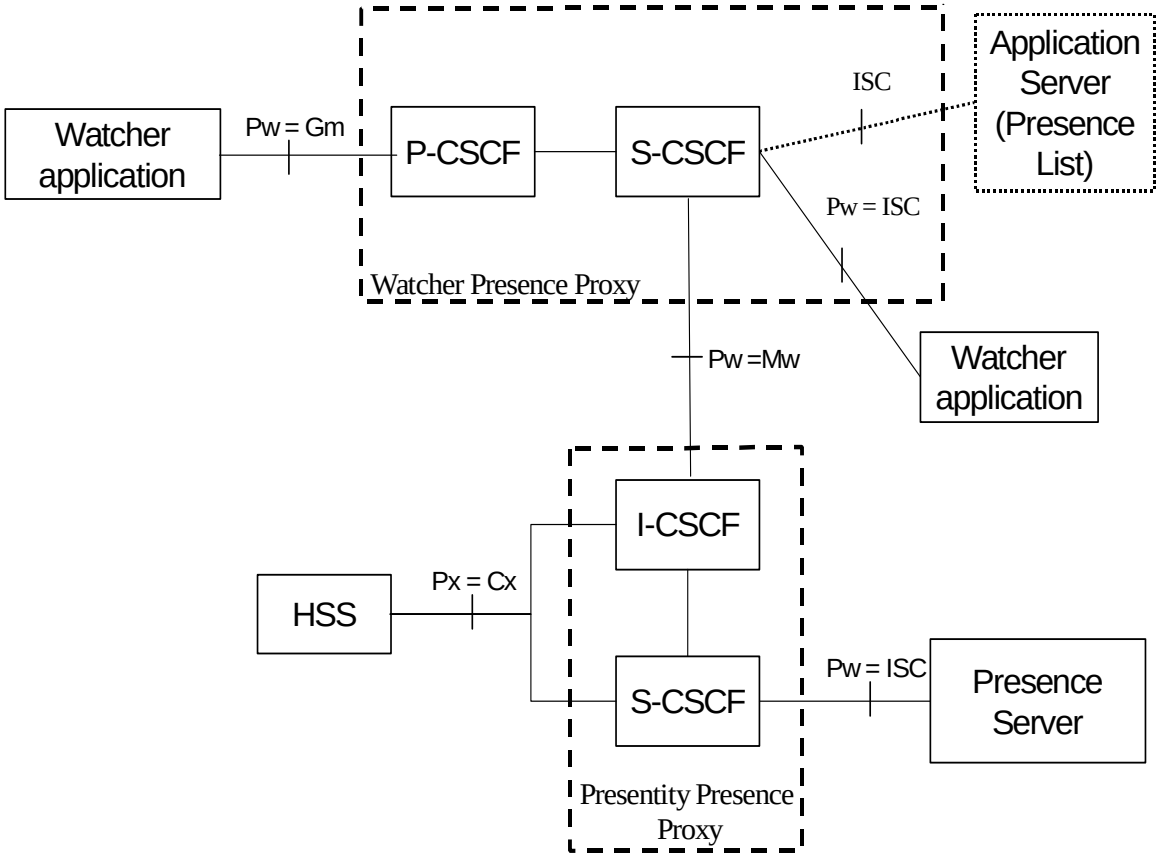
- Bootstrapping Server Function (BSF) and the UE shall mutually authenticate using the AKA protocol, and agree on session keys that are afterwards applied between UE and an operator-controlled Network Application Function (NAF).
- After the bootstrapping, the UE and NAF can run some application-specific protocol where the authentication / encryption of messages will be based on those session keys generated during the mutual authentication between UE and BSF.

- Zh and Zn are based on DIAMETER
- Ub uses HTTP Digest AKA
- Ua is application-specific

GBA_U

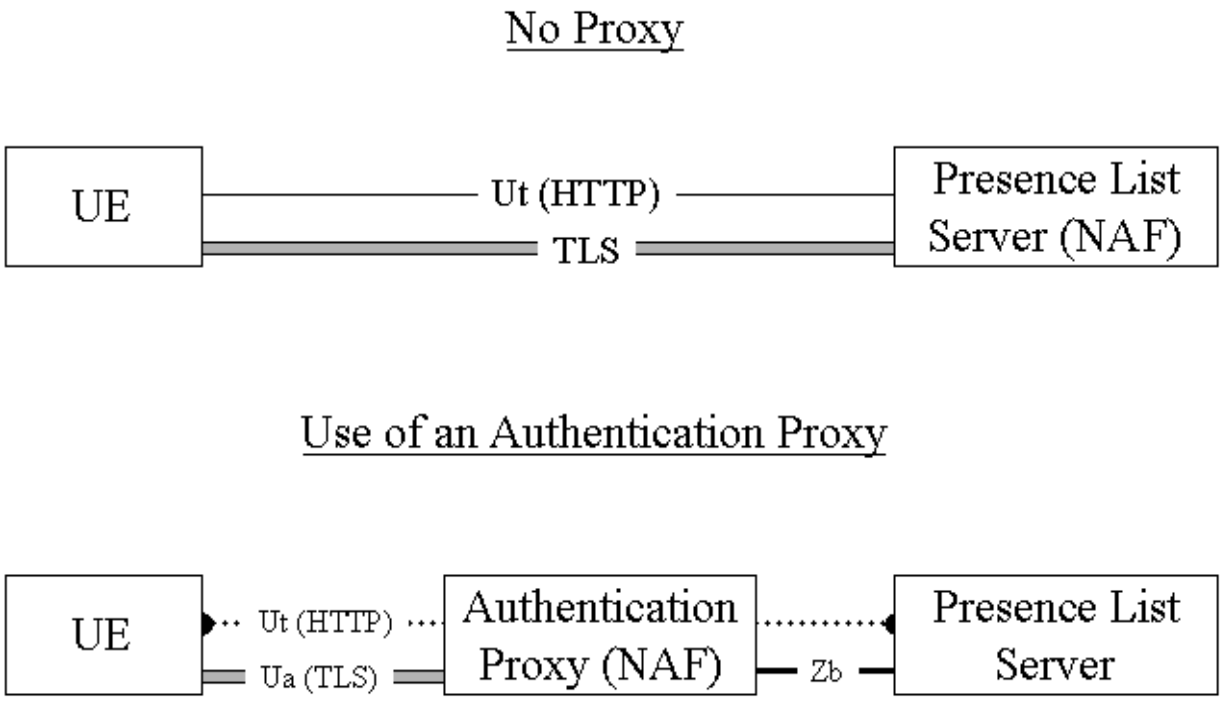
- GBA establishes session keys between the ME and the NAF
- An enhanced version called GBA_U allows session keys to be established between UICC and NAF
  - The session keys are not revealed outside the UICC
  - The application-specific NAF protocol is implemented on the UICC
  - This enhancement offers a higher level of security which is needed for certain applications like MBMS

Application of GBA: Presence service



Source: 3GPP TS 23.141

Application of GBA: Presence service



Source: 3GPP TS 33.141

Use of GBA for presence list management

- **TLS used to secure communications between the UE and the list management server**
- **GBA provides session keys between UE and list management server (acting as a NAF)**
- **TLS may actually be terminated in an authentication proxy**
  - **in this case the authentication proxy acts as the NAF**
- **Exact way to use session keys to establish the TLS tunnel is still open**
  - **e.g. shared key TLS**

HTTP-based services

- **Security mechanisms for Presence list management should also be applicable to other HTTP-based services**
  - **General purpose architecture for securing HTTP-based services provided in TS 33.222**
  - **Presence security specification (TS 33.141) aligned with TS 33.222**

Use of GBA / GBA_U for MBMS key management

- **GBA provides session keys between UE and Broadcast/Multicast Service Centre (BM-SC) (acting as an NAF)**
- **Session keys are used to provide authentication between UE and BM-SC**
- **Session keys also used to encrypt the MBMS group keys in transit between the BM-SC and the UEs**
- **GBA_U provides session keys between UICC and BM-SC so that MBMS group keys can be provisioned directly to the UICC for enhanced security**