S3-040586

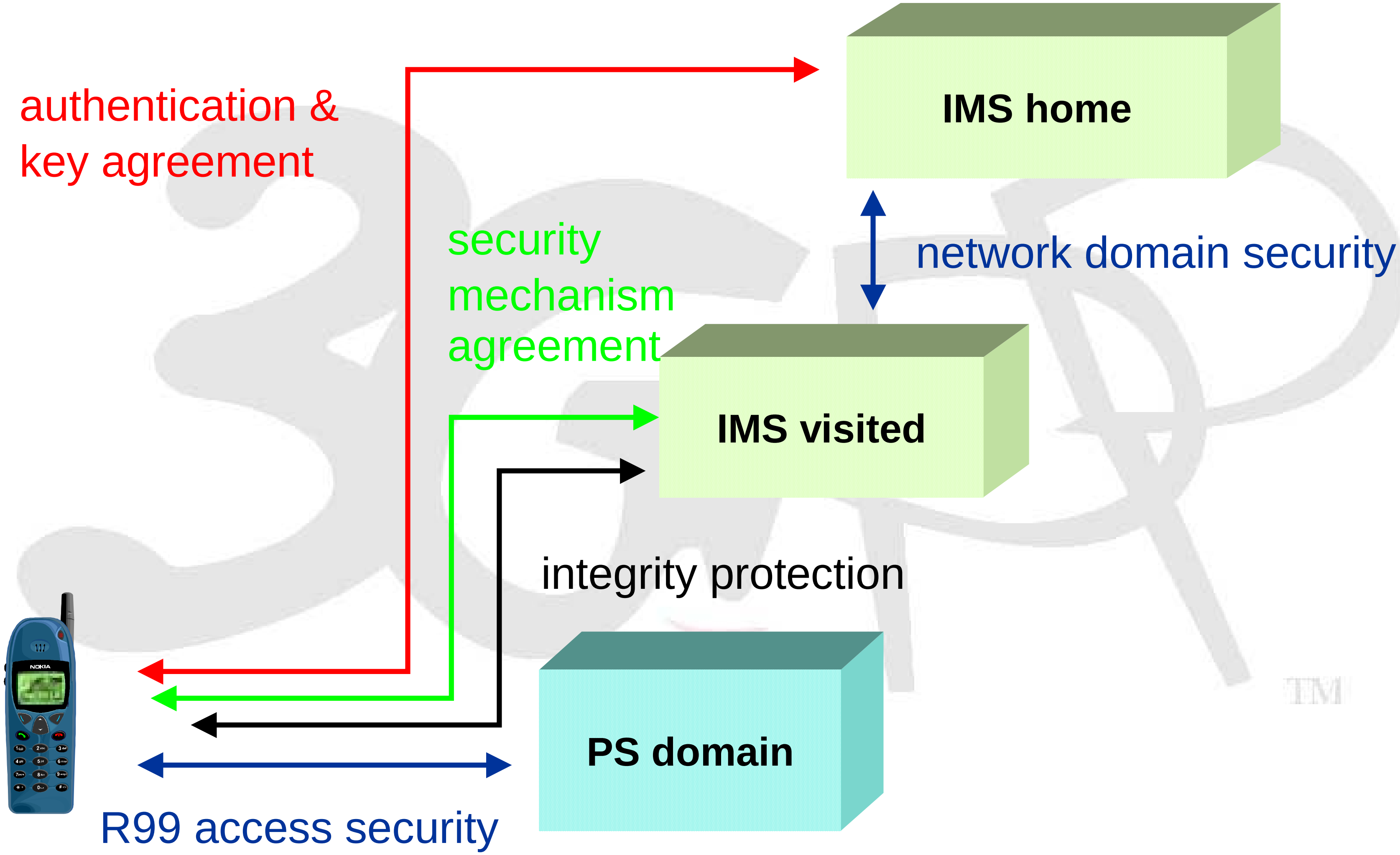
TR-45 AHAG joint session 8th July 2004

Valtteri Niemi

SA3 chairman

- Status of 3GPP AKA itself
- Usage of AKA in different contexts
  - Access security to IMS
  - WLAN interworking
  - Generic Authentication Architecture
  - Presence

- AKA is specified in TS 33.102
  - No changes in the AKA mechanism itself since long time ago
  - Based on feedback from stage 3 working groups, SA3 has added clarification on authentication re-attempt for release 6 version of 33.102, see S3-040400
- An example algorithm set (MILENAGE) is specified in TS's 35.205 – 208
  - No changes since approval


authentication &
key agreement
IMS home
security
mechanism
agreement
network domain security
IMS visited
integrity protection
PS domain
R99 access security
NOKIA

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**

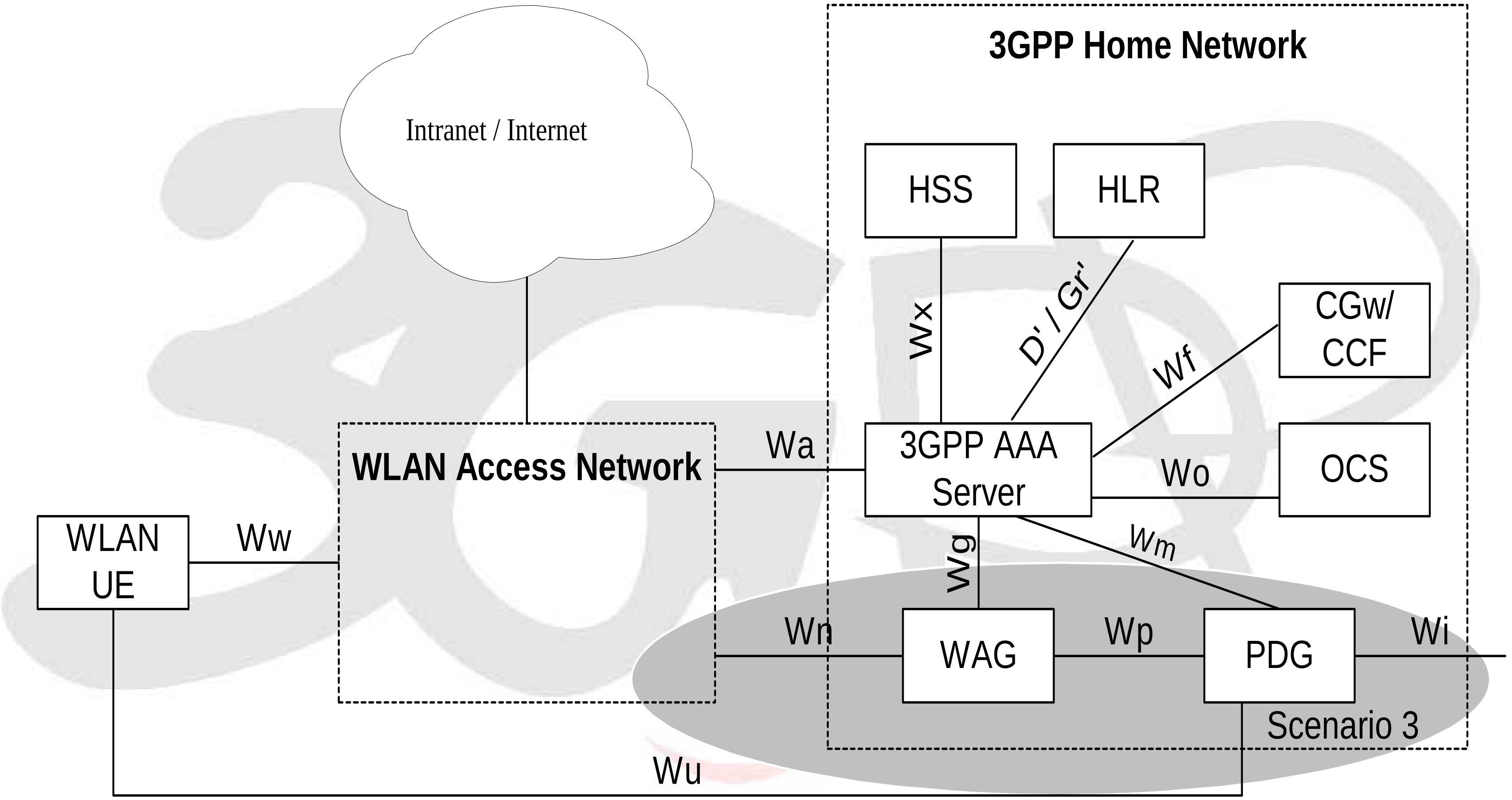
- Strong mutual authentication needed
- Re-use of UMTS AKA protocol
  - Based on secret key cryptography
  - Typically implemented on a tamper-resistant UICC
- UMTS AKA integrated into HTTP Digest
  - According to RFC3310

- 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
- 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 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 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 access zone can be connected to cellular core network
- Shared subscriber database & charging & authentication (scenario 2)
- Shared services (scenario 3)



Source: 3GPP TS 33.234

- Authentication methods
  - between WLAN-UE and 3GPP AAA server
  - based on EAP
  - SIM: based on GSM AKA and network authentication (eap-sim)
  - USIM: based on UMTS AKA (eap-aka)

- 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

- 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

- Goal of scenario 3 is to provide access to 3GPP system PS based services available to the user through the WLAN
  - IMS and corporate network
- Security requirements of scenario 2 are applied for scenario 3:
  - level of security of the 3GPP system shall not be compromised by deployment of the 3GPP-WLAN IW system
  - access control for users accessing WLAN shall have the same level of security as 3GPP system authentication procedure

- GAA consists of three parts:
- (GBA) offers generic authentication capability for various applications based on shared secret. Subscriber authentication in GBA is based on HTTP Digest AKA [RFC 3310].
- PKI Portal issues subscriber certificates for UEs and delivers an operator CA certificates. The issuing procedure is secured by using shared keys from bootstrapping.
- will also be based on GBA.

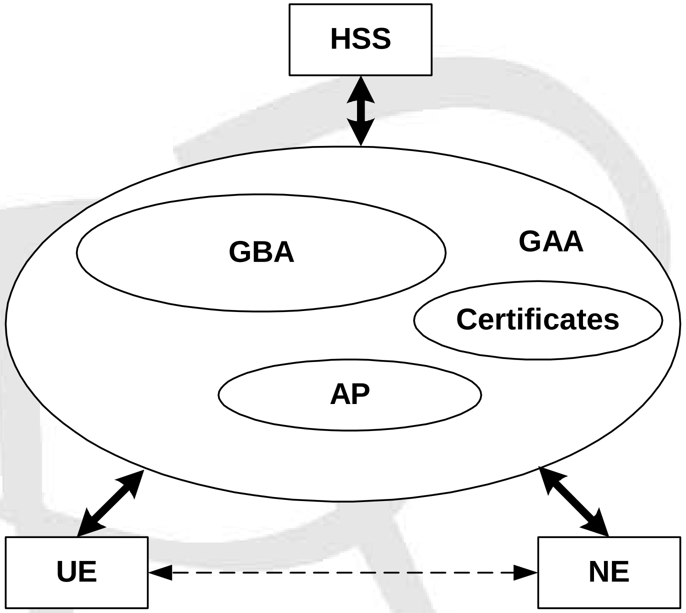
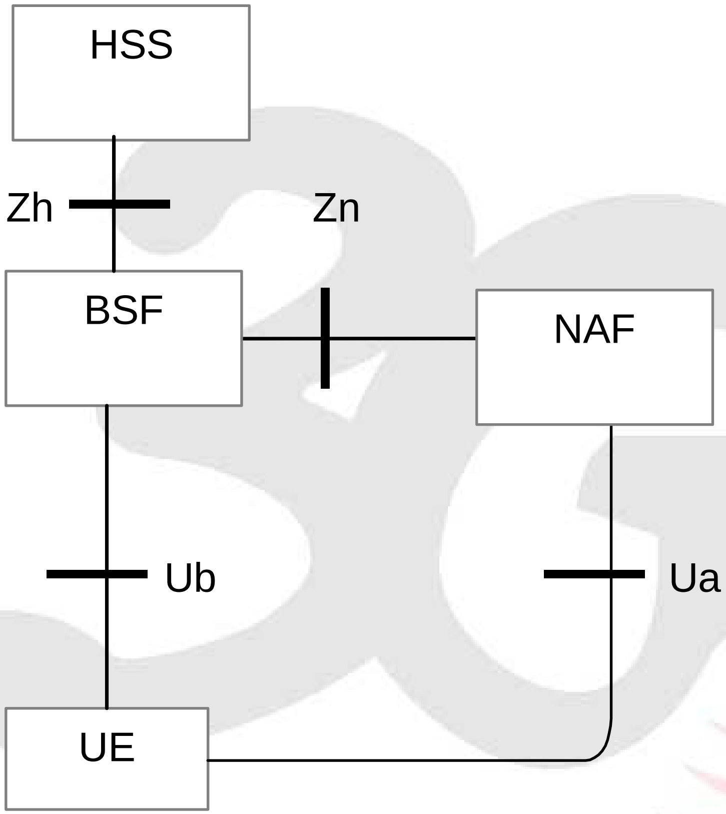
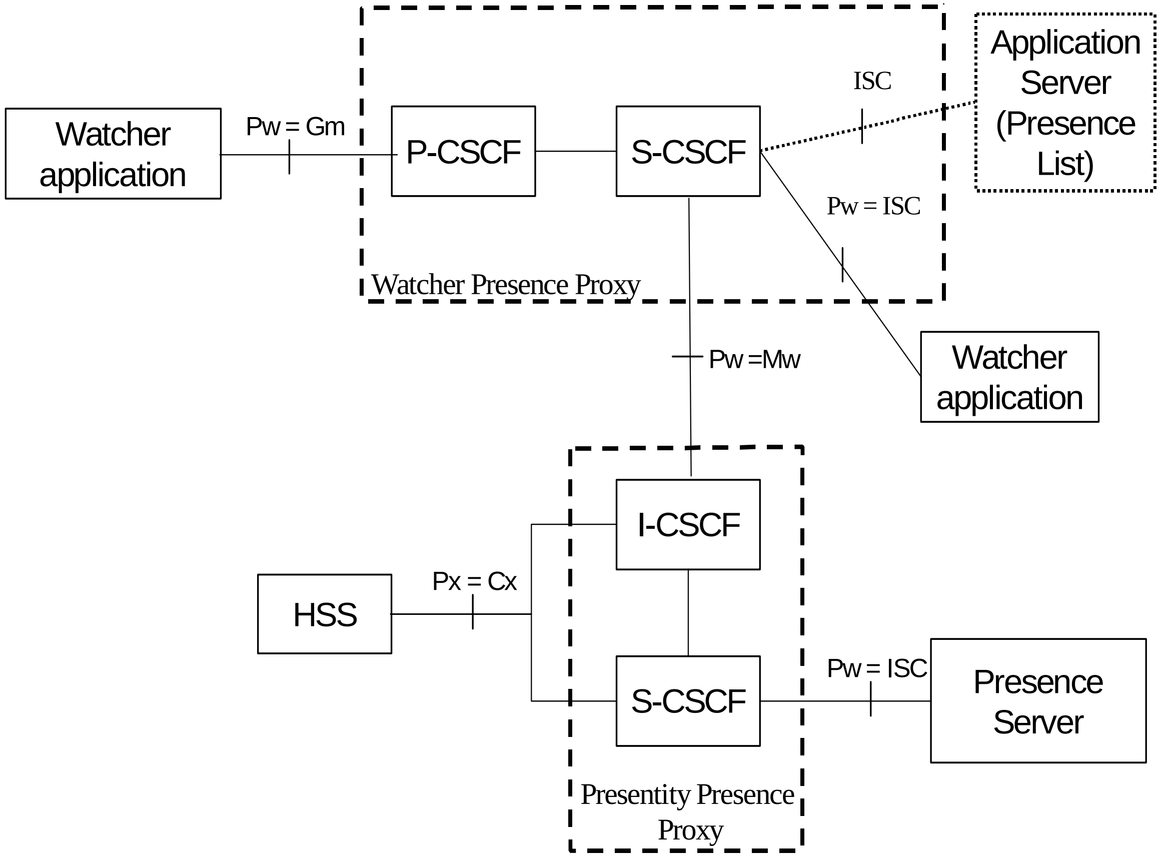


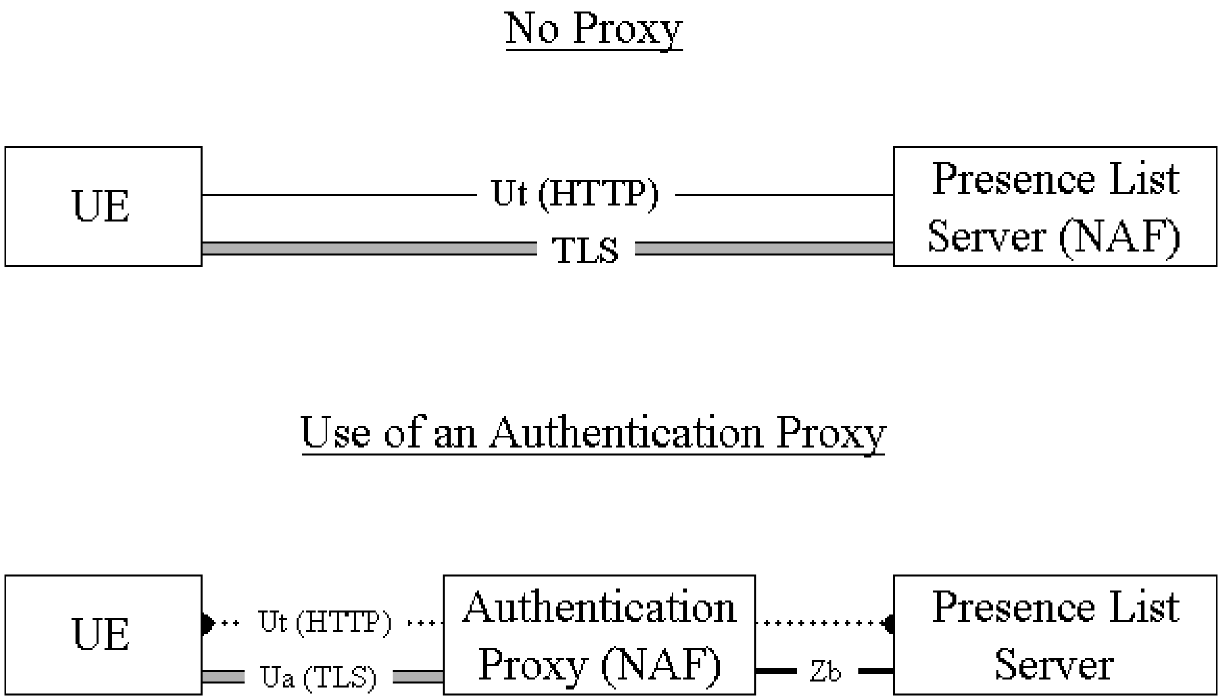
Figure from 3GPP TR 33.919



- 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 of messages will be based on those session keys generated during the mutual authentication between UE and BSF.



Source: 3GPP TS 23.141



No Proxy

UE

Ut (HTTP)

TLS

Presence List Server (NAF)

Use of an Authentication Proxy

UE

Ut (HTTP)

Ua (TLS)

Authentication Proxy (NAF)

Zb

Presence List Server

Source: 3GPP TS 33.141

- Security mechanisms for Presence should be applicable also to other http-based services (e.g. Conferencing)
- Basic ”tools” are TLS and 3GPP AKA: still partly open how these are used and combined together
  - AKA is used via GBA (and GAA)
  - Work in progress: IETF draft about shared key TLS