3GPP TSG-SA WG3 Meeting #34
Acapulco, Mexico, 6-9 July 2004

Tdoc ⌘S3-040661

CR-Form-v7

CHANGE REQUEST

⌘ **33.141** **CR** **CRNum** ⌘ **rev** **-** ⌘ Current version: **6.0.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ ☐ ME ☐ Radio Access Network ☐ Core Network **X**

Title:	⌘	Clarification on Ut interface
Source:	⌘	Vodafone, Ericsson
Work item code:	⌘	Presence Security
Date:	⌘	28/06/2004
Category:	⌘	**F**
Release:	⌘	Rel-6

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	It is not clear which entities implement the Ut interface. The abbreviation AP is missing from the abbreviations list.
Summary of change:	⌘	The term AS in section 4 is replaced to make it clear that the Ut interface applies to both the presence server and the presence list server. A minor editorial change is also made. The abbreviation AP is added to the abbreviations list.
Consequences if not approved:	⌘	Lack of clarity and consistency in the specification.

Clauses affected:	⌘	3.2, 4

Other specs affected:	⌘	Y	N		⌘
			N	Other core specifications	
			N	Test specifications	
			N	O&M Specifications	

Other comments:	⌘	

***** Begin of Change ****

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply, TR 21.905 [1] contains additional applicable abbreviations:

AKA	Authentication and key agreement
AP	Authentication Proxy
CSCF	Call Session Control Function
HSS	Home Subscriber Server
IM	IP Multimedia
IMPI	IM Private Identity
IMPU	IM Public Identity
IMS	IP Multimedia Core Network Subsystem
ISIM	IM Services Identity Module
MAC	Message Authentication Code
ME	Mobile Equipment
SA	Security Association
SEG	Security Gateway
SDP	Session Description Protocol
SIP	Session Initiation Protocol
UA	User Agent

***** End of Change ****

***** Begin of Change ****

4 Overview of the security architecture

An IMS operator using the CSCFs as Watcher Presence proxies and Presentity Presence proxies may offer the Presence services on top of the IMS network, see TS 22.141 [2]. The access security for IMS is specified in TS 33.203 [4] ensuring that SIP signalling is integrity protected and that IMS subscribers are authenticated through the use of IMS AKA. The security termination point from the UE towards the network is in the P-CSCF utilising IPsec ESP.

A watcher can be sending a SIP SUBSCRIBE over IMS towards the network to subscribe or to fetch presence information, i.e. the Presence Service supports SIP-based communications for publishing presence information. The presence information is provided by the Presence Server to the Watcher Application using SIP NOTIFY along the dialogue setup by SUBSCRIBE. This traffic is protected in a hop-by-hop fashion using a combination of SEGs as specified in TS 33.210 [10] with the access security provided in TS 33.203 [4].

The Presence Server is responsible for managing presence information on behalf of the presence entity and it resides in the presentity's home network. Furthermore the Presence Server provides with a subscription authorization policy that is used to determine which watchers are allowed to subscribe to certain presence information. Also the Presence Server shall before subscription is accepted try to verify the identity of the watcher before the watcher subscribes to presence information. Optionally, depending on the implementation, the Presence Server may authenticate an anonymous watcher depending on the Subscription Authorization Policy.

A Presence List Server is responsible of storing grouped lists of watched presentities and enable a Watcher Application to subscribe to the presence of multiple presentities using a single SIP SUBSCRIBE transaction. The Presence List Server also stores and enables management of filters in the presence list, see figure 1.

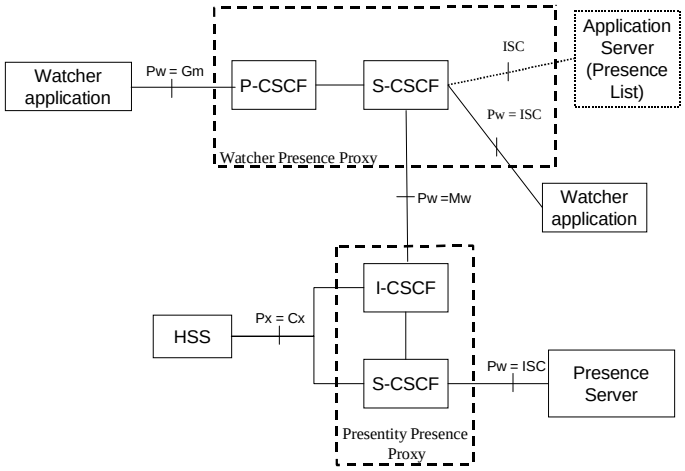

Figure 1: The Location of the Presence Server and the Presence List Server from an IMS point of view

A Presence User Agent shall be able to manage the data on the ~~AS~~ Presence Server and the Presence List Server over the Ut interface, see TS 23.002 [7], which is based on HTTP. This interface is not covered in TS 33.203 [4] and it is mainly this interface for Presence use, which is covered in this specification. Before manipulation is allowed the user needs to be authenticated.

NOTE: In the text below the term Presence Server refers to both the Presence Server and the Presence List Server as depicted in figure 1 above. For definitions of the Presence Server and the Presence List Server ~~Application Servers for Presence services~~ see TS 23.141 [3].

The Ut interface needs the following security features:

1) it shall be possible to provide ~~with~~ mutual authentication between the Presence Server and the Watcher/Presentity;

2) a secure link and security association shall be established between the Presence Server and the Watcher/Presentity. Data origin authentication shall be provided as well as confidentiality protection.

Editor's Note: The exact details of the security architecture is FFS and dependant on decisions related with the ongoing work on GBA (Generic Bootstrapping Architecture).

An overview of the security architecture for Presence Ut Interface is depicted in figure 2:

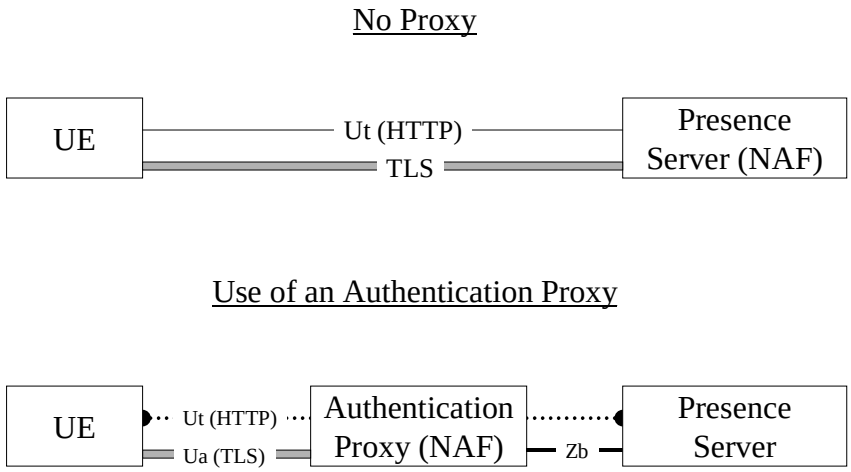

Figure 2: An overview of the Security architecture for the Ut interface including the support of an Authentication Proxy

Editor's Note: The Authentication Proxy and the Presence Server shall utilize the security protection specified in TS 33.210 [10] to protect the data carried between them. This is compliant with the mechanism specified in TS 33.222 [19].

***** End of Change ****