3GPP TSG-SA WG3 Meeting S3#33
Beijing, China, May 10-14, 2004

Tdoc ⌘S3-040339

CR-Form-v7

CHANGE REQUEST

⌘ **33.141** **CR** **CRNum** ⌘ **rev** **-** ⌘ Current version: **1.1.1** ⌘

*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 ☐

Title:	⌘	ISIM Support
Source:	⌘	Nokia, Motorola, Gemplus, Alcatel
Work item code:	⌘	Presence security
Date:	⌘	26/04/2004
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 should be possible to access the Presence server with an ISIM, since the presence account based on an ISIM may be different than that in a USIM, which are received from a BSF, e.g., IMPI value, and IMPUs added to enable new services. Note the two applications ISIM and USIM can be independent to each other.
Summary of change:	⌘	Support for an ISIM to access the Presence server is added.
Consequences if not approved:	⌘	It may cause confusion because the user's information retrieved from a BSF based on a USIM account, could be different than that from an HSS based on an ISIM account.

Clauses affected:	⌘	5.1.1

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

Other comments: ⌘

5 Security features

5.1 Secure Access to the Presence Server

5.1.1 Authentication of the subscriber and the network

A subscriber shall be authenticated before accessing user data in a server. The subscriber shall only be able to manipulate data that is associated with that particular subscriber.

Editors note: Relationship between Transaction Identifier and subscriber identity is ffs. In the case of Presence Ut interface, there are several potential identities that are related to the Transaction Identifier, i.e. IMPI and IMPUs. The subscriber may have several Presence accounts related to same IMPI. Transaction Identifier does not carry enough information on which IMPU the end-user is trying to use.

Authentication between the subscriber and the network shall be performed as specified in clause 6.1. Subscriber authentication can be made by the operator using proprietary or non-3G standardized methods. In case 3GPP authentication mechanisms are used (specified in TS33.220 [11]), the authentication of the subscriber shall be based on the USIM/ISIM. The authentication of the subscriber and the network shall be based on Generic Authentication Architecture as defined in 3GPP TR 33.919 [15]. Generic Authentication Architecture enables the use of different authentication methods to be used for the authentication of the subcriber by using:

- subscriber certificates (e.g., TLS, cf. [6,8,9]), or
- shared secrets (e.g., TLS with HTTP Digest, cf. [17]).

The server certificate to be used for application server authentication shall be based on WAPCert [12].

NOTE: The interleaving attack shall not be possible.

Editors Note: It is agreed that the shared key TLS draft need to be more mature in IETF before being considered for Presence. It is FFS and a decision is expected at SA3#32, cf. also S3-030721 and S3-030732.

~~Editors Note: If 3GPP decides that ISIM-only UICCs are allowed then it needs to be studied further if also the ISIM may be used in the Generic Authentication Architecture~~

A UE may contact the Presence Server/Presence Server for further instructions on authentication procedures. The consumption of Authentication Vectors should be minimized. The architecture shall ensure that SQN synchronization failures is minimized.