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

Tdoc ⌘S3-040295

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:	⌘	UE's identities in Presence server access
Source:	⌘	Nokia, Siemens
Work item code:	⌘	Presence security
Date:	⌘	26/04/2004
Category:	⌘	**C**
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:	⌘	The management of UE identity is absent so far in the present specfication.
Summary of change:	⌘	The exact procedure for Presence is specified in section 6.1.
Consequences if not approved:	⌘	The procedure is unclear to the audience.

Clauses affected:	⌘	6.1

Other specs affected: ⌘

Y	N			
X		Other core specifications	⌘	24.109
	X	Test specifications		
	X	O&M Specifications		

Other comments: ⌘

6 Security Mechanisms

The UE and the AP/Presence Server shall support the TLS version as specified in RFC 2246 [6] and WAP-219-TLS [13] or higher. Earlier versions are not allowed.

Editors Note: It is FFS if it is possible to base the Presence Security on TLSv1.1 [14], which is currently in draft status in IETF.

Note 1: The management of Root Certificates is out of scope for this Technical Specification

6.1 Authentication and key agreement

6.1.1 Authentication of the Subscriber

From a TLS point of view the UE shall be considered as un-authenticated, cf. RFC 2246 [6].
The authentication of the UE may take place in either the Authentication Proxy or the Presence s~~S~~erver. However the AP or the ~~Server~~ Presence server may, depending on given the policy of the operator conclude that the AP/Presence Server shall not authenticate the UE using GBA i.e. the UE is considered as authenticated already or the UE is authenticated by other means, cf. initiation of bootstrapping in TS 33.220 [11], section 4.5.1.

Otherwise if the AP/Presence Server concludes that the authentication shall take place in the AP/Presence Server then the UE may be authenticated as specified in TS 33.220 [11] (where the Ua interface is between the UE and the AP/Presence Server).

It shall be possible for the AP/Presence Server~~operator~~ at any time to request a re-authentication of an active UE, cf. TS33.220 [11], section 4.5.3.

~~Editors Note: A clean up what item is used for authentication purposes might be needed i.e. User, Subscriber and UE.~~

6.1.2 Authentication of the AP/Presence Server

The AP/Presence Server is authenticated by the Client as specified in WAP-219-TLS [13], which in turn is based on RFC 2246 [6].

The AP/Presence Server certificate profile shall be based on WAP Certificate and CRL Profile as defined in WAP-211-WAPCert [12].

6.1.3 Management of public user identities

The general concept of Ua interface is specified in TS 33.222 [xx], section 6. This section specifies how TS 33.222 is applied to the case of Presence services. The AP or Presence server shall authenticate the subscriber as specified in TS 33.222, section 5. In particular, the AP or presence server can associate an authenticated HTTP request with a transaction identifier and one or several public user identities (IMPUs). The IMPUs form part of a GAA-specific user profile for presence, which was sent by the BSF to the AP or presence server over the Zn reference point. The UE shall send its preferred public user identity in each HTTP request. The Presence server (or AP) shall then verify that the preferred identity inserted in the HTTP request by the UE is one of the IMPUs, associated with the HTTP request.

If the presence server sits behind an AP and the verification of the preferred identity, which was inserted by the UE in the HTTP request, was successful, then the AP shall verify the value of the preferred identity of the user in the HTTP request before forwarding it to the presence server. How the asserted user identity is carried in each HTTP request is specified in the relevant stage-3 specification.

If there is no preferred-Identity inserted in the HTTP request, the AP shall insert a default IMPU from the user profile in the HTTP request, before forwarding it to the Presence server. If the validation of the UE inserted preferred identity fails in the AP the HTTP request shall be dropped.

NOTE: The IMPI value should not be used as indication of UE's service identity. If it is present in the HTTP request, the HTTP request shall be dropped..

6.1.4 Authentication Failures

If the UE receives a Server Hello Message from the AP/Presence Server that requests a Certificate then the UE shall respond with a Certificate Message containing no Certificate if it does not have a certificate. The AP/Presence Server upon receiving this message may respond with a failure alert, however if the AP/Presence Server shall authenticate the UE as configured by the policy of the operator the AP/Presence Server should continue the dialogue and assume that the UE will be authenticated as specified in TS 33.220 [11].

If there is no response within a given time limit from a network initated re-authentication request an authentication failure has occurred after that the request has been attempted for a limited number of times. This failure can be due to several reasons e.g. that the UE has powered off or due to that the message was lost due to a bad radio channel. The AP/Presence Server shall then still assume that if a TLS session is still valid that it can be re-used by the UE at a later time. Should then the UE re-use an existing session then the AP/Presence Server shall re-authenticate the UE and not give access to the AP/Presence Server unless the authentication was successful.

6.2 Protection mechanisms

The UE shall support the CipherSuite TLS_RSA_ WITH_3DES_EDE_CBC_SHA. All other Cipher Suites as defined in RFC 2246 [6] are optional for implementation for the UE.

The AP/Presence Server shall support the CipherSuite TLS_RSA_ WITH_3DES_EDE_CBC_SHA and the CipherSuite TLS_RSA_WITH_RC4_128_SHA. All other Cipher Suites as defined in RFC 2246 [6] are optional for implementation for the AP/Presence Server.

Editors Note: It is FFS is this specification should mandate any of the AES cipher suites as specified in RFC 3268.

Cipher Suites with NULL encryption may be used. The UE shall always include at least one cipher suite that supports encryption during the handshake phase.

Cipher Suites with NULL integrity protection (or HASH) are not allowed.

Editors Note: It is FFS what parts (if any) of the TLS extensions as specified in RFC 3546 [9] that shall be implemented in this TS

6.3 Key Agreement

The Key exchange method shall not be anonymous. Hence the following cipher suites as defined in RFC 2246 [6] are not allowed for protection of a session for Presence Services:

- CipherSuite TLS_DH_anon_EXPORT_WITH_RC4_40_MD5
- CipherSuite TLS_DH_anon_WITH_RC4_128_MD5
- CipherSuite TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA
- CipherSuite TLS_DH_anon_WITH_DES_CBC_SHA
- CipherSuite TLS_DH_anon_WITH_3DES_EDE_CBC_SHA