3GPP TSG-CN Meeting #25 **Tdoc NP-040427**
Palm Springs, USA. 8th to 10th September 2004.

revision of Tdoc N1-041566 in NP-040380

3GPP TSG-CN1 Meeting #35 **Tdoc N1-04xxxx**
Sophia Antipolis, France, 16-20 August 2004

CR-Form-v7

CHANGE REQUEST

⌘ **24.141 CR 006** ⌘ **rev 2** ⌘ 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 ☒

Title:	⌘	GAA impacts
Source:	⌘	Siemens
Work item code:	⌘	PRESNC
Date:	⌘	08/09/2004
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:	⌘	The UE authenticats the NAF and not the authentication proxy. Ambiguous condition when an AS has to implement the role of a NAF. Correct condition is that no authentication proxy in the network and the AS implements the role of a DMS. Missing statement that AS has to implement TLS.
Summary of change:	⌘	See reason for change
Consequences if not approved:	⌘	Incorrect specification

Clauses affected:	⌘	2, 6.2.1, 6.2.2, 6.2.3

Other specs affected: ⌘

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

Other comments: ⌘

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document in the same Release as the present document.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 22.141: "Presence Service; Stage 1".

[3] 3GPP TS 23.002: "Network architecture".

[4] 3GPP TS 23.141: "Presence service; Architecture and functional description; Stage 2".

[5] 3GPP TS 23.218: "IP Multimedia (IM) session handling; IM call model; Stage 2".

[6] 3GPP TS 23.228: "IP Multimedia Subsystem (IMS); Stage 2".

[7] 3GPP TS 24.109: "Bootstrapping interface (Ub) and Network application function interface (Ua); Protocol details".

[8] 3GPP TS 24.228: "Signalling flows for the IP multimedia call control based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3".

[9] 3GPP TS 24.229: "Internet Protocol (IP) multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3".

[10] 3GPP TS 29.228: "IP Multimedia (IM) Subsystem Cx and Dx Interfaces; Signalling flows and message contents".

[11] 3GPP TS 33.141: "Presence service; Security".

[12] IETF RFC 2664 (1999): "FYI on Questions and Answers - Answers to Commonly asked New Internet User Questions".

[13] IETF RFC 2246 (1999): "The TLS Protocol Version 1.0".

[14] IETF RFC 2387 (August 1998): "The MIME Multipart/Related Content-type".

[15] IETF RFC 2616 (June 1999): "Hypertext Transfer Protocol -- HTTP/1.1".

[15A] IETF RFC 2617 (June 1999): " HTTP Authentication: Basic and Digest Access Authentication".

[16] IETF RFC 2778 (2000): "A Model for Presence and Instant Messaging".

[17] IETF RFC 3261 (June 2002): "SIP: Session Initiation Protocol".

[18] IETF RFC 3263 (June 2002): "Session Initiation Protocol (SIP): Locating SIP Servers".

[19] IETF RFC 3265 (March 2002): "Session Initiation Protocol (SIP)-Specific Event Notification".

[20] IETF RFC 3310 (2002): "Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA)".

[21] draft-ietf-impp-cpim-pidf-08 (May 2003): "Presence Information Data Format (PIDF)".

[22] draft-ietf-simple-event-list-04 (June 2003): "A Session Initiation Protocol (SIP) Event Notification Extension for Resource Lists".

[23] draft-ietf-sip-publish-03 (February 2004): "An Event State Publication Extension to the Session Initiation Protocol (SIP)".

[24] draft-ietf-simple-partial-notify-01 (January 2004): "Partial Notification of Presence Information".

[25] draft-ietf-simple-prescaps-ext-00 (February 2004): "Device capability PIDF status extension".

[26] draft-ietf-simple-rpid-03 (March 2004): "RPID: Rich Presence: Extensions to the Presence Information Data Format (PIDF)".

[27] draft-ietf-simple-presence-10 (January 2003): "A Presence Event Package for the Session Initiation Protocol (SIP)".

[28] draft-ietf-simple-winfo-package-05 (January 2003): "A Session Initiation Protocol (SIP) Event Template-Package for Watcher Information".

[29] draft-ietf-simple-winfo-format-04 (January 2003): "An Extensible Markup Language (XML) Based Format for Watcher Information".

[30] draft-ietf-simple-filter-format-00 (February 2004): "An Extensible Markup Language (XML) Based Format for Event Notification Filtering".

[31] draft-ietf-simple-event-filter-funct-00 (February 2003): "Functional Description of Event Notification Filtering".

[32] draft-ietf-simple-cipid-01 (March 2004): "CIPID: Contact Information in Presence Information Data Format".

[33] draft-ietf-simple-xcap-02 (February 2004): "The Extensible Markup Language (XML) Configuration Access Protocol (XCAP)".

[34] draft-isomaki-simple-xcap-pidf-manipulation-usage-00 (February 2004): "An Extensible Markup Language (XML) Configuration Access Protocol (XCAP) Usage for Manipulating Presence Document Contents".

[35] draft-ietf-simple-xcap-presence-rules-00 (May 2004): "Extensible Markup Language (XML) Configuration Access Protocol (XCAP) Usages for Setting Presence Authorization".

[36] draft-ietf-simple-xcap-list-usage-02 (February 2004): "An Extensible Markup Language (XML) Format for Representing Resource Lists".

[37] draft-ietf-geopriv-pidf-lo-01 (February 2004): "A Presence-based GEOPRIV Location Object Format".

[38] draft-ietf-simple-partial-pidf-format-00 (January 2004): "Presence Information Data Format (PIDF) Extension for Partial Presence".

[39] draft-ietf-simple-xcap-package-01 (February 2004): "A Session Initiation Protocol (SIP) Event Package for Modification Events for the Extensible Markup Language (XML) Configuration Access Protocol (XCAP) Managed Documents".

[40] draft-ietf-sip-content-indirect-mech-03 (June 2003): "A Mechanism for Content Indirection in Session Initiation Protocol (SIP) Messages".

6 Protocol for data manipulation at the Ut reference point

6.1 Introduction

Hypertext Transfer Protocol (HTTP) and XML Configuration Access Protocol (XCAP) are used to store, alter and delete data related to the presence service. The general information that can be manipulated is user groups, subscription authorization policy, resource lists, hard state presence publication, MIME objects referenced from the hard state presence information, etc. Soft state presence information manipulated with a PUBLISH request is not manipulated by the mechanism provided over the Ut reference point.

6.2 Functional entities

6.2.1 User Equipment (UE)

The UE implements the Data Manipulator (DM) role as described in subclause 6.3.1.

The UE shall implement HTTP digest AKA (see RFC 3310 [20]) and it shall initiate a bootstrapping procedure with the bootstrapping server function located in the home network, as described in 3GPP TS 24.109 [7].

The UE shall acquire the subscriber's certificate from PKI portal by using a bootstrapping procedure, as described in 3GPP TS 24.109 [7].

The UE shall implement HTTP digest authentication (see RFC 2617 [15A]).

The UE ~~and the authentication proxy~~ shall ~~both~~ implement TLS (see RFC 2246 [13]). The UE shall be able to authenticate the ~~authentication proxy~~ network application function based on the received certificate during TLS handshaking phase.

6.2.2 Application Server (AS)

If an AS implements the role of a PS (see subclause 5.3.3) or of a RLS (see subclause 5.3.4), then the AS shall also implement the role of a Data Manipulation Server (DMS) (see subclause 6.3.2).

If there is no authentication proxy in the network, then the AS shall~~ ~~:~~also~~

1) implement the role of a network application function, as described in 3GPP TS 24.109 [7]; ~~and it shall~~

2) implement TLS (see RFC 2246 [13]);

3) ~~support~~ implement HTTP digest authentication (see RFC 2617 [15A]); and

4) support certificate authentication.

Editor's note: It needs to be clarified what physical entities can contain the Authentication Proxy and its relationship with the IMS architecture.

6.2.3 Authentication proxy

The authentication proxy shall implement the role of a network application function, as described in 3GPP TS 24.109 [7] and it shall support HTTP Digest Authentication (see RFC 2617 [15A]) and certificate authentication.

The Authentication Proxy shall authenticate the UE and integrity protect the messages sent towards the UE.

Editor's note: It is FFS how the Authentication Proxy passes the user's identity to the Application Server (AS).