Title:	LS on Definition of Public Service Identities.
Release:	6
Work Item:	IMS

Source:	**SA2**
To:	CT, CT4
Cc:	-

Contact Person:
   Name: Gavin Wong
   E-mail Address: gavin.wong@vodafone.com

Attachments: S2-050988

1. Overall Description:

SA2 has discussed and approved the attached CR (S2-050988) to move the format definition of the Public Service Identity (PSI) from TS 23.228 to the TS 23.003. However, it was noted that from the related and agreed CR to TS 23.003 (CR# 100), the TS makes use of a reference to an IETF RFC 2806 for TEL URIs that has been made obsolete by RFC 3966. The IETF RFC used previously in TS 23.228 is RFC 3966 as can be seen in the attached CR.

Therefore the intended definition of tel uris within public service identities will be incorrect and as such will need to be updated to reference IETF RFC 3966.

2. Actions:

To CT and CT4 group.

ACTION: SA2 kindly asks CT and CT4 groups to consider the attached CR in approval of CR to TS 23.003 CR#100 and update TS 23.003 accordingly.

3. Date of Next TSG-SA2 Meetings:

SA2 #47	27 June – 1 July 2005	Montreal, Canada
SA2 #48	5 – 9 September 2005	Sophia Antipolis, France.

CR-Form-v7.1

CHANGE REQUEST

| ⌘ | **23.228** CR **0491** | ⌘**rev** | **-** | ⌘ | Current version: | **6.9.0** | ⌘ |

*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:	⌘	Corrections to wildcarded PSIs

Source:	⌘	Vodafone, Nokia, HP

Work item code:⌘	IMS2		**Date:** ⌘	29/04/2005

Category:	⌘	**F**		**Release:** ⌘	Rel-6

Use <u>one</u> 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 <u>one</u> of the following releases:
Ph2 (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)
Rel-7 (Release 7)

Reason for change:	⌘	The CT WG4 group have now updated 3GPP TS 23.003 (Numbering, Naming and Addressing spec) to describe Public Service Identities. Therefore, there is now overlap with PSI format definition in 23.228.

Summary of change:⌘	Remove overlap with 3GPP TS 23.003. Also, a few grammatical improvements to the text have been made, as well as implementation of correct 3GPP terminology.

Consequences if not approved:	⌘	PSIs will be defined twice in the 3GPP specification set. This is bad as it will inevitably at some point in the future diverge and 3GPP will have conflicting definitions which lead to non-interoperability of equipment.

Clauses affected:	⌘	4.3.6, 5.4.12

		Y	**N**			
Other specs affected:	⌘	**X**		Other core specifications	⌘	CR 23.003-100
			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.

**** First Modified Section ****

4.3.6   Public Service Identities

With the introduction of standardized presence, messaging, conferencing, and group service capabilities in IM CN subsystem, there is a need for Public Service Identities (PSIs). These identities are different from the Public User Identities in the respect that they identify services, which are hosted by Application Servers. In particular, Public Service Identities are used to identify groups, see clause 4.10. For example a chat-type service may use a Public Service Identity (e.g. sip:chatlist_X@example.com) to which the users establish a session to be able to send and receive messages from other session participants. As another example, local service may be identified by a globally routable Public Service Identity.

Public Service Identities shall take the form ~~of SIP URI as defined in RFC 3261 [12] and RFC 2396 [13] or the "tel:" URI format as defined in RFC 3966 [15]~~as defined in 3GPP TS 23.003 [24].

The IM CN subsystem shall provide the capability for users to create, manage, and use Public Service Identities under control of AS. It shall be possible to create statically and dynamically a Public Service Identity.

Each Public Service Identity is hosted by an Application Server, which executes the service specific logic as identified by the Public Service Identity.

The IM CN Subsystem shall provide capability of routing IMS messages using Public Service Identity.

**** Next Modified Section ****

5.4.12   Configuration and Routing principles for Public Service Identities

5.4.12.0   General

Depending on the service nature, different mechanisms may be used for configuration and routing of PSIs according to operator preference.

When PSIs are created, the uniqueness of a PSI shall be ensured. Note that only the username part of a PSI is definable within a predefined hostname(s).

Whenever possible, routing to/from a Public Service Identity (PSI) should be provided using basic principles used for IMS routing.

5.4.12.1   PSIs on the originating side

The Application Server hosting the PSI may be invoked as an originating Application Server. This can be achieved by modifying the filter information within the subscription information of the users intending to use the service identified by the PSI. The PSI is then made available to these users.

The SIP requests are directed to the corresponding Application Server hosting the service according to the originating filtering rules in the S-CSCF of the user who is using the service.

Such statically pre-configured PSIs are only accessible internally from within the IMS of the operator's domain where the PSI is configured.

5.4.12.2   PSIs on the terminating side

The Application Server hosting the PSI may be invoked as a terminating Application Server via information stored in the HSS. Such PSIs are globally routable and can be made available to users within and outside the operator domain, and can take the following form:

- Distinct PSIs are defined in 3GPP TS 23.003 [24]~~(e.g. sip:my_service@example.com)~~. Distinct PSIs can be created, modified and deleted in the HSS by the operator via O&M mechanisms. Distinct PSIs can also be

created and deleted by users using the Ut interface using the means described in sub-clause 5.4.12.3 for subdomain-based PSIs. The distinct PSI may then be created in the HSS by the AS using the Sh interface.

- Wildcarded PSIs are defined in 3GPP TS 23.003 [24](sip:chatlist_*@example.com):. A range of PSIs with the same domain part in the SIP URI is defined using a wildcard indication in the userpart of the SIP URI. Wildcarded PSI ranges can be created, modified and deleted in the HSS by the operator via O&M mechanisms. Specific PSIs within a wildcarded range can be created and deleted by users using the Ut interface to the AS hosting the wildcarded range, or by the operator via O&M mechanisms.

For both the distinct PSIs and wildcarded PSIs, there are two ways to route towards the AS hosting the PSI:

a) The HSS maintains the assigned S-CSCF information and ISC Filter Criteria information for the "PSI user" to route to the AS hosting the PSI according to IMS routing principles. In this case, the I-CSCF receives SIP requests at the terminating side, queries the HSS and directs the request to the S-CSCF assigned to the "PSI user". The S-CSCF forwards the session to the Application Server hosting the PSI according to the terminating ISC Filter Criteria.

b) The HSS maintains the address information of the AS hosting the PSI for the "PSI user". In this case, the AS address information for the PSI is returned to the I-CSCF in the location query response, in which case the I-CSCF will forward the request directly to the AS hosting the PSI.

The AS hosting the PSI in combination with its entry in the HSS is referred to as "PSI user".

Figure 5. 19d depicts a routing example for incoming session where the session request is routed directly to the AS hosting the PSI.

Figure 5.19e depicts an example routing scenario where the basic IMS routing via S-CSCF is used to route the session.

5.4.12.3   Subdomain based PSIs

Subdomains defined for PSIs allow both operators and users to define specific PSIs within subdomains for specific applications. For this purpose, subdomains can be defined by the operator in the DNS infrastructure. Specific PSIs within a subdomain can be created and deleted by users using the Ut interface to the AS hosting the subdomain, or by the operator via O&M mechanisms.

Subdomain based PSIs are globally routable and can be made available to users within and outside the operator domain.

In this case, there are two ways to route towards the AS hosting the PSI:

a) When the subdomain name is defined in the global DNS, then the originating S-CSCF receives the IP address of the AS hosting the PSI, when it queries DNS. The principles defined in RFC 3263 [44] may be used. For example, a NAPTR query and then a SRV query may be used to get the IP address of the AS.

b) The PSI is resolved by the global DNS to an I-CSCF address in the domain where the AS hosting the PSI is located. The I-CSCF recognises the subdomain (and thus does not query the HSS). It resolves the same PSI to the address of the actual destination AS hosting the PSI using an internal DNS mechanism, and forwards the requests directly to the AS.

Figure 5.19f shows an example of DNS based routing of an incoming session from an external network. The routing from the external network leads to the entry point of the IMS subsystem hosting the subdomain of the PSI.

5.4.12.4   PSI configuration in the HSS

In order to support configuration of an AS hosting a PSI, the distinct PSIs and/or wildcarded PSI ranges hosted in the AS need to be configured in the HSS. The configuration shall include procedures to allow:

- • Distinct PSIs and wildcarded PSI ranges to be configured in the HSS via operation and maintenance procedures,

- • Authorization and verification of access as "PSI user" with the Public Service Identity hosted by the AS, e.g. for AS-originating requests,

- • Access to "PSI user" information (e.g. the S-CSCF assigned) over the Cx reference point from the CSCF nodes,

- • Defining the "PSI user" similar to the principle of IMS user, without requiring any subscription/access information (e.g. CS/PS domain data) that are required for IMS user.

Further functional requirements such as how S-CSCF is provisioned with the PSI data need to be studied.

Note that the PSI configuration in the HSS does not affect the filter criteria based access to an AS as defined in the user profiles.

5.4.12.5 Requests originated by the AS hosting the PSI

The AS hosting the PSI may originate requests with the PSI as the originating party. For such originating requests, the home IMS network shall be capable to perform the following functions:

- If~~n case~~ network configuration hiding is to be applied, the request shall be routed as per the principles described in sub-clause 4.6.2.1. This means that the last hop within the originating IMS is an I-CSCF (THIG), which processes the request further on and routes it towards the destination network.

- Network Domain Security, TS 33.210 [20], shall be used where applicable.

- Charging requirements such as providing appropriate accounting and charging functions via the charging entities shall be supported according to TS 32.200 [25].

- If~~n case~~ the target identity is a tel: URL, ENUM translation needs to be performed, and the request shall be routed based on the translation result.

Routing from the Originating AS hosting the PSI can be performed as follows:

a) The AS may forward the originating request to the destination network without involving a~~n~~ S-CSCF. If this option is applied where the target identity is a ~~t~~Tel~~:~~ URI~~L~~, the AS shall perform~~s~~ an ENUM query and route~~s~~ the request based on the translation result. ENUM support for an AS is optional~~.~~ therefore ~~I~~if an AS does not support ENUM and the target identity is a Tel URI, it shall be configured to use b)~~ at least in case of tel: URLs~~.

b) If~~n case~~ the PSI has a~~n~~ S-CSCF assigned, the AS forwards the originating request to this S-CSCF, which then processes the request as per regular originating S-CSCF procedures.

To prevent fraudulent or unsecure IMS traffic possibly caused by AS originated requests, security and authentication procedures may be performed towards the AS.