

[0177] As discussed above, in this disclosure it is proposed to use the SIP as transport protocol for carrying that data format either in XML or in another concrete format.

[0178] For that purpose the use of a new Content-Type attribute is shown for indicating that the SIP contains that information on the payload such as:

[0179] Content-Type: Presence-Info/TID

[0180] What follows is an example using a Presence Service. Described is a specific situation where the user registers her information to be available for another user or making use of Location based services. The examples show how the whole registration and the security mechanism provided by SIP is performed for supporting user privacy.

[0181] Description of the Figure:

[0182] Referring now to **FIG. 8** a user registration with location data is shown: The user (Quex) registers her information in the Presence Server through the SIP CSCF. Thus, the Presence Server has complete knowledge of that user. It knows that she is logged in and her spatial information is available if it is needed for Location based Services.

[0183] The SIP UA utilizes the location data format named TID (or any other XML based format) and the Content-Type will indicate the type of format that is carried in the Payload.

[0184] The user indicates in the TID structure the level of publicity she wants to give to that information. In this case she didn't allow to other user to access that information. Thus, that data is kept hidden based on the user specifications. In case of emergency services that data is retrieved without any obstacle with the previous authorization. An example of data format for location information is presented in the Appendix 3.

[0185] After this process, the SIP will receive that information and will register the user location. At this point the SIP Registrar will need to interact with the HSS (see **FIG. 9**) or storing this data and make it globally available to other networks. In the next section the different entities for storing the location information in UMTS is shown.

[0186] Now, the user is registered and the system knows where she is located. If there is another user trying to find out where she is, the Presence Server or the SIP CSCF responsible will retry that information. That request is authenticated using the SIP security mechanism. The user location will be retrieved if the user gave rights to this new user to do that. It was specified during the registration using the message attributes described in Appendix 4.

[0187] User Location Information in UMTS

[0188] **FIG. 9** shows a GPP Network architectural model. The main entities to be considered relate particularly to mobility transactions as follows:

[0189] Mobility Manager. It undertakes Handoff Management across networks. It interacts with the Location Server and the Home Subscriber Register.

[0190] Session Manager. The SM establishes and manages Sessions, State and handoffs through and across the various networks, brings into call/session required resources such as announcements, bridging, transfers, etc. It collects Session States and end of State information and passes it to the Service Agent. It also communicates with the Resource

Manager for gateway control functionality into the various media-dependent gateways. Additionally, the following functions are included: call routing, session and state management, query address translation, signaling protocol translation between legacy call control and the IP network call control protocol (e.g., ISUP) and all IP control protocol (e.g., SIP, H.323).

[0191] Roaming Signaling Gateway. The Roaming Signaling Gateway undertakes the transformation of packet signaling (SIP, MGCP, etc) into and from ISUP and TCAP signaling in the Circuit switched network. It interworks with the Session Manager. The SIG GW provides an interface between the all IP network and the legacy signaling SS7 network.

[0192] Location Server. The Location Server provides a register of Location information, Mobile Positioning Center (MPC)(GPS, Triangulization and cell/sector information). It also includes a PDE (Position Determination Equipment) interface to collect the GPS information (e.g. WAG, Foreign Agent, IP address, etc.). The LS also contains a Registration Marker to indicate if the subscriber or device is registered in one or more specifically defined Network. The Location Server updates the Location Database in the HSS.

[0193] Equipment Register. The Equipment Register is a database of equipment information, including but not limited to a record of stolen equipment. The Equipment Register is part of the Home Subscriber Server.

[0194] Home Location Register. The Home Location Register contains the subscriber profile data (usable resources/rights of interdomain services, IP priority services, SLA, etc.) which is capable of being referenced in real time, or downloaded into a cache.

[0195] From these definitions the most relevant element is the Home Subscriber Server (HSS) where user data is stored. The LS receive and retrieve information directly from the HSS. The LS is also tightly connected with the Mobility Manager, which is part of the Call State Control Function (CSCF). Thus, the CSCF will receive the registration and will retrieve it to the HSS through the LS. At the LS it can be performed some kind of translation in case of different location formats. If backward interoperability is required, it is necessary to extract the information from the TID structure and create the normal structures used at the HSS. That kind of adaptation has to be analyzed according to the different implementations.

[0196] Various Implementation Alternatives (PS)

[0197] SIP is used as the signalling for call control between CSCF for Presence and Messaging services. The SIP payload is the most suitable part of the message for transporting that information. The SIP facilitates data privacy in the sense that the whole payload can be encrypted.

[0198] The basic idea of this approach to allow backward interoperability with all the systems SIP enhanced networks. Thus, to avoid huge changes in existing implementations it is decided to define this new feature using already existing mechanisms. The SIP itself provides this feature utilizing the headers for specific purposes. That gives it a lot of flexibility. The User Agent will define his information that is inserted in the initial registration within the SIP body. In this way the packet is completely encrypted end-to-end and there is no