

[0126] Location Server (LS) stores and distributes location information related to a specific terminal. It is typically implemented in the terminal or in a server at an arbitrary place, not necessarily owned by a Network Provider. The Location Server will interact directly with the User Interface. Thus, the LS will receive the location information and presumably will use well-formed and reliable protocols for provide that information to the Client in case the Target had specified this requirement when his location information is stored on the LS. In the same manner the location information will be provided directly to the Client from the LS.

[0127] Positioning Function (PF) determines the location of a given terminal. It is typically an integral terminal function, e.g. based on GPS, Location Information Service (LIS) (M. korkea-aho "Some Scenarios for an ISL Architecture" Mar. 10, 2000, IETF draft-korkea-aho-isl-scenarios-00.txt) or Local Positioning System (LPS) (J. M. Polk et al. "Spatial Location Protocol Location Server Authentication" Mar. 10, 2000, IETF draft-polk-slp-loc-auth-server-00.txt) provided by a Network Provider, e.g. based on radio cell information or a triangulation mechanism. It can be located at the Target (SIP UA) or at the LS if the Target does not have this capabilities.

[0128] Information User (IU) is typically a value-added service, a lifesaving service that can access to the user location information previous authentication. It behaves like a client when is accessing the LA to know the user location information that has been required by any external elements such a routing, signaling protocol, lifesaving service, etc. And the IU will also perform as a server entity when it acts such an interface for accessing Directory services or local facilities (taxi, restaurants, etc). In this case the IU will know the user location through the LA and will take care of requesting the services needed by the user.

[0129] Messages Structure

[0130] The format of the messages has to be defined according to the location needs. The important part of the message corresponds to the location information, which can be defined in different ways depending on the device. It was mentioned in the Requirements section that this information would be negotiated according to the user device capabilities. The message format based in a header and a body. Thus, the header will contain the default data for security and other properties. The body of the message will carry the location information or any other data. If the device has no capabilities for calculating the location, then the body can be empty and the message is just a recipient of the user demands about his information. The main fields inserted in the header could contain the data shown in FIG. 5.

[0131] Apart from these fields it is necessary consider also others to perform the initial contracting, update the changes and the rest of protocol behavior.

[0132] FIG. 6 depicts the proposed syntax based on the message coding presented in the above section describing the Spatial Location Architecture. It contains the header and the Body parts, where the former contains the Target identifier and the essential data of the structure and the latter includes the location data and attributes identified in this section.

[0133] Spatial Location Architecture Using SIP

[0134] Based on the illustrated Architecture Requirements and elements an architecture based on the SIP signalling protocol is disclosed. The SIP is chosen as transport protocol since it can work either with TCP or UDP. Consequently, this approach will incorporate security and reliability mechanisms. In this disclosure the SLO data format will be part of the protocol payload and it will be indicated in one of the protocol headers that it is carrying SL data.

[0135] Spatial Location Representation

[0136] Accordingly, the SLO information will be part of the SIP message body. This body will contain the Location message with the structure and attributes defined above. The SIP is used as a simple transport mechanism that will be well extended since it has been adopted as Call Control protocol for IP Telephony Signalling. The content of the body in the SIP message is indicated in the "Content-Type" header. The IANA allows the registration of new types of contents and it would be indicated in a manner similar to "Content-Type: application/SLO". The SIP permits encryption of the entire payload in case a high security rate is required.

[0137] FIG. 7A illustrates an example of a SIP registration where it is using the SLO as payload. After the registration the SLO data is stored in a database that can be the SIP Location server and from there can be retrieved if it is necessary to run any supplementary service.

[0138] Security Mechanism

[0139] The SIP protocol has defined various security approaches based in end-to-end and hop by hop. The SIP servers may require user authentication previous to any access. The SLO architecture will rely on the transport protocol for this issue, the user just indicates the rate of security designated and the SIP will take care of it. The SIP enabled servers will authenticate and encrypt the data according to the restrictions defined by the user. If the user tries to register and it is not allowed the Registrar will return a "401 Unauthorized" response. It indicates that the registration requires a previous authorization using any of the mechanisms defined in SIP. The user has to re-issue again the request including the "Authorization" header where the credential containing the authentication information is added.

[0140] The SIP security is implemented basically using two approaches, using HTTP basic and digest schemes. J. Franks et al "HTTP authentication: Basic and digest access authentication," RFC 2617, IETF, June 1999 as well as using PGP J. Callas et al "Open PGP message format" RFC 2440, IETF, November 1998.

[0141] The former approach uses the headers "Proxy-Authorization", "WWW-Authenticate" and "Authorization" in the various messages based on the RFC 2617. The Registrar will send back a 401 response indicating that it needs to be authenticated. Then the user will send back the registration including the "Authorization" header with the relevant information.

[0142] The latter approach uses the syntax based on the PGP authentication mechanism. It is based on the model that the client authenticates itself with a request signed with the client's private key. The server can then ensure the origin of the request if it has access to the public key that should be signed by a trusted third party. The algorithms of this scheme