tistical purposes.

[0028] The response step can further comprise transmitting by the location entity a part of the predefined policy. This has the advantage that the location entity can instruct the requesting entity to act in certain ways regarding the identity-related information, e.g., not to transfer it further, or to delete it after a while, or not to delete it for a certain period.

[0029] The location entity may use the connection established from the client application to the location entity in the redirecting step for the interaction with a person during the transfer step. The benefit of interacting with the person is that the person can be authenticated and can make additions to the predefined policy, and the benefit of reusing the said connection (in contrast to releasing that connection before the acquiring step) is that the interaction is possible without delay.

[0030] A release of identity-related information to the requesting entity can comprise the following steps: presenting information about the requesting entity; presenting a pre-authorized attribute values known to the location entity, where pre-authorized means that the predefined policy allows the release to the requesting entity, and/or presenting a not pre-authorized attribute values known to the location entity, and/or presenting names of attributes with values unknown to the location entity assigned to empty fields for entering respective attribute values; requesting for editing the attribute values; and sending the edited attribute values to the requesting entity. By doing so, the user is requested only to fill in unknown attribute values and to make yes/no decisions about not pre-authorized values. This simplifies the procedure and allows the user to have full control over his personal information requested by the requesting entity.

[0031] The different attribute values may be presented differently, preferably in different colors. This allows a clear presentation of the information to the user, who then can decide which information to enter, delete, amend, or send unchanged.

[0032] The acquiring step can further comprise the steps of generating a random value k by the location entity, sending the random value k to the requesting entity on the same connection as the identity-related information, sending the random value k to the client application to enable the client application to prove its authenticity with respect to the identity-related information to the requesting entity. This has the advantage that the client application running at the user can be given additional privileges by the requesting entity after the transfer of the identity-related information.

[0033] In accordance with a second aspect of the present invention, there is presented a system according to claim 14.

[0034] The system facilitates the identification of the relevant authority, i.e. the location entity, for a user without the need to contact any third party, thus avoiding a privacy and performance problem present in some prior art solutions.

[0035] The system works with standard, SSL-capable HTTP browsers, i.e. secure socket layer capable hyper text transfer protocol browser, and does not require any functionality that requires users to accept that some additional information, e.g. cookies, or software like active content: Javascript, Java, ActiveX, etc. is installed on their machine. At the same time, it allows for efficiency improvements in cases where additional information can be stored.

[0036] The system provides more security against certain attacks, e.g. man-in-the-middle attack, than in known solutions.

[0037] In another example, the client application interacts with several location entities. This means the user may have multiple location entities on different places or on the same place, and the client application, together with the person or user, chooses an appropriate one in answer to the request for the location information. Thereby the location entities can be local or remote. The advantage of such an arrangement is that it avoids a single point of failure for the person, and enables privacy among the different location entities.

[0038] The identity-related information can be provided by a further location entity. Then the identity-related information is obtainable by the requesting entity via the location entity. The location information of the further location entity is stored on the location entity. The advantage of such an arrangement is that it avoids that the client application or person has to choose among the location entities, while still allowing different types of identity-related information to be stored in different location entities.

DESCRIPTION OF THE DRAWINGS

[0039] Preferred embodiments of the invention are described in detail below, by way of example only, with reference to the following schematic drawings.

FIG. 1 shows a schematic illustration of a system according to the present invention.

FIG. 2 shows a schematic illustration of the message flow of a first embodiment according to the present invention.

FIG. 3 shows a schematic illustration of the message flow of a second embodiment.

FIG. 4 shows a schematic illustration of the message flow of a third embodiment.

FIG. 5 shows an illustration of a form to be presented to a potential user with a location query as sent in step II in FIG. 4.

FIG. 6 shows a schematic illustration of an extension of the third embodiment as shown in **FIG. 4.**