According to a first aspect of the present invention, there is provided a network system comprising: a lookup unit; a clearing unit having a storage device, the lookup unit and the clearing unit being different from each other; and a client unit being adapted for providing user-related data to the lookup unit, the user-related data being based on user-specific data, the user-specific data being associated with a user, the user-related data allowing for unambiguous identification of the user-specific data, and the user-related data being a first fingerprint of the user-specific data; the lookup unit being further adapted for providing a second fingerprint of the user-specific data to the clearing unit, the second fingerprint being based on the first fingerprint of the user-specific data, the second fingerprint allowing for unambiguous identification of the user-specific data; the lookup unit being adapted for retrieving identification data from the clearing unit by using the second fingerprint, the identification data being associated with the user-specific data; the clearing unit being adapted for retrieving from the storage device the identification data associated with the user-specific data; the clearing unit being adapted for selecting from the storage device the identification data associated with the user-specific data by using the second fingerprint of the user-specific data; the clearing unit being adapted for providing the identification data to the lookup unit; the lookup unit being adapted for retrieving configuration related data for a service provided to the user by using the identification data; and the lookup unit further being adapted for providing the configuration related data to the client unit.

According to a second aspect of the present invention, there is provided a lookup unit of a network system, the lookup unit being adapted for receiving user-related data from a client unit, wherein the user-related data is based on user-specific data, the user-specific data is associated with a user, the user-related data allows for unambiguous identification of the user-specific data, and the user-related data being a first fingerprint of the user-specific

data; the lookup unit being further adapted for providing a second fingerprint of the user-specific data to the clearing unit, the second fingerprint being based on the first fingerprint of the user-specific data, the second fingerprint allowing for unambiguous identification of the user-specific data and the clearing unit and the lookup unit being different from each other; the lookup unit being adapted for retrieving identification data from a clearing unit by using the second fingerprint, the identification data being associated with the user-specific data; the lookup unit being adapted for retrieving configuration related data for a service provided to the user by using the identification data; and the lookup unit further being adapted for providing the configuration related data to the client unit.

According to a third aspect of the present invention, there is provided a method of operating a network system comprising a lookup unit, a clearing unit and a client unit, wherein the clearing unit and the lookup unit are different from each other, the method comprising: providing user-related data from the client unit to the lookup unit, the user-related data being based on user-specific data, the user-specific data being associated with a user, the user-related data allowing for unambiguous identification of the user-specific data, and the user-related data being a first fingerprint of the user-specific data; operating the lookup unit so as to provide a second fingerprint of the user-specific data to the clearing unit, the second fingerprint being based on the first fingerprint of the user-specific data, the second fingerprint allowing for unambiguous identification of the user-specific data; operating the lookup unit so as to retrieve identification data from the clearing unit by using the second fingerprint, the identification data being associated with the user-specific data; operating the clearing unit so as to retrieve identification data associated with the user-specific data; operating the clearing unit so as to select from the storage device the identification data associated with the user-specific data by using the second fingerprint of the user-specific data; providing the identification data from

the clearing unit to the lookup unit; operating the lookup unit so as to retrieve configuration related data for a service provided to the user by using the identification data; and operating the lookup unit so as to provide the configuration related data to the client unit.

According to a fourth aspect of the present invention, there is provided a method of operating a lookup unit of a network system, the method comprising: receiving user-related data from a client unit, wherein the user-related data is based on user-specific data, the user-specific data is associated with a user, the user-related data allows for unambiguous identification of the user-specific data, and the user-related data being a first fingerprint of the user-specific data; providing a second fingerprint of the user-specific data to a clearing unit, the clearing unit and the lookup unit being different from each other, the second fingerprint being based on the first fingerprint of the user-specific data, the second fingerprint allowing for unambiguous identification of the user-specific data; retrieving identification data from a clearing unit by using the second fingerprint, the identification data being associated with the user-specific data; retrieving configuration related data for a service provided to the user by using the identification data; and providing the configuration related data to the client unit.

According to a fifth aspect of the present invention, there is provided a computer program which is adapted for, when executed by a processor device, controlling the method according to any one of the third and fourth aspect.

According to an example of the herein disclosed subject-matter, a network system is provided, the network system comprising: a lookup unit (e.g. a provider lookup server, herein also referred to as PLS); a clearing unit having a storage device; and a client unit being adapted for providing user-

related data to the lookup unit, the user-related data being based on user-specific data (e.g. a first fingerprint of the user-specific data), the user-specific data (e.g. e-mail address, phone number, etc) being associated with a user, and the user-related data (e.g. the first fingerprint of the user-specific data) allowing for unambiguous identification of the user-specific data; the lookup unit (e.g. the PLS) being adapted for retrieving identification data (e.g. a provider ID) from the clearing unit by using the user-related data (e.g. first fingerprint of the user-specific data), the identification data (e.g. provider ID) being associated with the user-specific data (e.g. e-mail address of the user); the clearing unit being adapted for retrieving from the storage device the identification data (e.g. provider ID) associated with the user-specific data; the clearing unit being adapted for providing the identification data (e.g. provider ID) to the lookup unit (e.g. PLS); and the lookup unit (e.g. PLS) being adapted for retrieving configuration related data (provider URL, login name, etc.) for a service provided to a user; the lookup unit being adapted for retrieving the configuration related data (e.g. provider URL) by using the identification data (e.g. provider ID).

This example of the herein disclosed subject-matter is based on the idea that by separating the retrieval of configuration related data for a user-specific service and the identification of the corresponding user a network system may be provided which provides a high level of security and user comfort. The separation of the retrieval of configuration related data and the identification of the user may be provided by a lookup unit and a clearing unit according to examples of the herein disclosed subject matter.

According to an example, the user-specific data identify the user unambiguously. For example, the user-specific data may be an email address of the user or a phone number of the user (or fingerprints of such data). However, other user-specific data may also be used in conjunction with examples of the herein disclosed subject-matter.

A service provided to a user may be a user-specific service (provided to only a single user) or a provider-specific service (provided to a plurality of users).

According to an example, retrieving the configuration related data by using the identification data is retrieving the configuration related data which are associated with the identification data. The fact that the retrieved configuration related data are associated with the identification data does not necessarily imply that the configuration related data are unambiguously identified by the identification data. Rather, the configuration related data may be unambiguously identified by the identification data and some further data, e.g. the user-related data (e.g. a fingerprint of the user's e-mail address) and/or further user-related data (e.g. a fingerprint of the user's password).

According to an example, the lookup unit is adapted for retrieving the configuration related data locally, i.e. within the lookup unit. According to a further example, the lookup unit is adapted for retrieving the configuration related data from a remote unit.

According to an example, the user-related data is anonymous data, i.e. data which do not allow to reconstruct the user-specific data from the user-related data, at least not with reasonable computation power. For example,

the user-related data is a fingerprint of the user-specific data. This fingerprint of the user-specific data may be referred to as a first fingerprint of the user-specific data. Hence, in accordance with the above specification of the user-related data, the first fingerprint of the user-specific data is based on the user-specific data and the first fingerprint allows for unambiguous identification of the user-specific data. The characteristics of the network system and the security may be increased by using a fingerprint of user-specific data for retrieving configuration related data for a user-specific service. According to another example, user-related data may be an encrypted version of the user-specific data. Other types of user-related data are also possible. However, the use of fingerprints may provide a higher security of the network system.

According to an example, a fingerprint of "input data" is data derived from the input data in an unambiguous way. According to an example, the term "fingerprint" implies the determination of the fingerprint by a mathematical function which reproducibly provides the fingerprint from the input data. In this way the fingerprint allows for unambiguous identification of the fingerprint. According to an example, the fingerprint does not allow to calculate the input data from the fingerprint, at least not with reasonable computation power. For this reason, such a function for determining a fingerprint may be referred to as a one-way function. Typical functions for determination of a fingerprint are so-called hash functions, for example MD5, SHA1, SHA2, etc. It should be understood that the function used to calculate the fingerprint must be available to the units which assess (e.g. verify) the input data based on the fingerprint of the input data. To this end, the function used to calculate the fingerprint may be predetermined (e.g. fixedly defined or stored) in the respective units. According to another example, the function used to calculate the fingerprint may be provided with the same transmission which transmits the fingerprint to a receiving unit or with a separate configuration transmission.

According to an example, a fingerprint may be a salted fingerprint which is calculated by combining the input data with a cryptographic salt and calculating the fingerprint of the combination of the salt and the input data (i.e. fingerprint of (salt + input data). According to an example, the user-specific data is input data in the above-mentioned sense. Generally herein, it should be understood that if a salted fingerprint of an input data is used, while the salted fingerprint allows for unambiguous identification of the input data, further the cryptographic salt is necessary in order to actually identify the user-specific data.

According to an example the fingerprint is an iterated fingerprint. For example, an iterated fingerprint may be generated by hashing the input data two or more times. An example of an iterated fingerprint is obtained by combining a salt with the input data and hashing the result repeatedly. For example, a fingerprint of further user-specific data may be a fingerprint of a salted fingerprint of a user's password (= Hash(salt|Hash (password)).

Retrieving identification data from the clearing unit by using the user-related data may be performed in any suitable way, e.g. by providing the user-related data to the clearing unit or by providing data, which is derived from the user-related data, to the clearing unit.

According to an example, the lookup unit is further adapted for providing a fingerprint of the user-specific data to the clearing unit. This fingerprint of the user-specific data which is provided to the clearing unit may be referred to as second fingerprint of the user-specific data. According to an example, the second fingerprint of the user-specific data is based on the first fingerprint of the user-specific data. According to a further example, the second fingerprint allows for unambiguous identification of the user-specific data. It is noted that the term „first fingerprint" is used for

the fingerprint sent from the client unit to the lookup unit and the term "second fingerprint" is used for fingerprint sent from lookup unit to the clearing unit. However the use of "first" and "second" in this regard shall not be considered as limiting.

Generally herein the term "is based on" is intended to include the meaning "is different but is derived from" and the meaning "is identical to". In other words, the term "is based on" is to be interpreted as including "is derived from" and "is".

Hence, in an example, the second fingerprint of the user-specific data is the first fingerprint of the user-specific data. In other words, according to an example, the lookup unit may be adapted for receiving the first fingerprint of user-specific data from the client unit and forwarding the first fingerprint of the user-specific data to the clearing unit. According to a further example, the second fingerprint of the user-specific data may be derived from the first fingerprint of the user-specific data.

According to an example, the clearing unit is adapted for selecting from the storage device the identification data associated with the user-specific data by using the second fingerprint of the user-specific data. For example, the clearing unit may have stored in the storage device a plurality of fingerprints of user-specific data (e.g. of a plurality of users) and associated identification data. Hence, in such an example, the identification data may be retrieved by the clearing unit by searching in the storage device for a fingerprint which matches the second fingerprint of the user-specific data and selecting the identification data associated with this matching fingerprint. According to an example, the clearing unit includes a database system which stores in the storage device the first fingerprint of the user-specific data and the associated identification data for a plurality of users. By storing the first fingerprint of the user-specific data, the clearing

unit does not need to know the user-specific data as such. This may improve the security of the network system.

Configuration related data may be data necessary for configuring the access of the client unit to a remote unit, e.g. a provider unit. For example, the configuration related data may be information on the domain (e.g. a URL) of a provider unit.

According to an example, the network system comprises a provider unit. According to an example, the provider unit is accessible by the client unit. For example, according to an example, the provider is the provider of the user-specific service the configuration related data is for. According to an example, the lookup unit is adapted for providing the configuration related data to at least one entity that needs to be configured for enabling the client unit to access the provider unit or doing provider specific customization, labeling or displaying. According to a further example, the lookup unit is adapted for providing the configuration related data to the client unit. According to other examples, the configuration related data may be provided to a different entity for use by the client unit. According to an example, the configuration related data (e.g. the provider URL) is part of a response transmission provided by the lookup unit, wherein the response transmission further includes a status indicator indicating the status of the user-specific data corresponding to user-related data. For example, the status indicator indicates whether or not the user-specific data corresponding to the user-related data (e.g. corresponding to the first fingerprint) have been considered as being valid.

According to an example, the lookup unit is adapted for providing a fingerprint of the user-specific data to the provider unit, e.g. for verification of the correctness of the user-specific data by the provider unit and/or for

retrieving the configuration related data from the provider unit. This fingerprint of the user-specific data which is provided from the lookup unit to the provider unit is herein also referred to as third fingerprint. According to an example, the third fingerprint is based on (e.g. derived from or identical to) the first fingerprint of user-specific data. For example, the third fingerprint may be a fingerprint of the first fingerprint. According to another example, the third fingerprint is identical to the first fingerprint. In other words, in such an example the lookup unit is adapted for forwarding the first fingerprint received from the client unit to the provider unit.

According to an example, the provider unit is adapted for providing some status information regarding the validity of the user-specific data to the lookup unit in response to the third fingerprint received from the lookup unit. For example, the provider unit is adapted for providing status information, which indicates that the third fingerprint corresponds to valid user-specific data, to the lookup unit if the third fingerprint corresponds to valid user-specific data. Verifying the correctness of the user-specific data may increase the security of the network system.

According to an example, the provider unit is adapted for providing the configuration related data or at least part of the configuration related data in response to receiving the third fingerprint from the lookup unit.

According to a further example, the lookup unit is adapted for retrieving the configuration related data by using the identification data. For example, the lookup unit may use the identification data to identify the provider unit and to transmit to the identified provider unit the third fingerprint of user-specific data. Identifying a provider includes, in an example, retrieval of a network address of the provider unit associated with the provider unit. According to an example, the lookup unit is adapted for retrieving the configuration related data from the provider unit by using the third

fingerprint, e.g. by providing the third fingerprint to the provider unit. According to an example, the provider unit includes a storage device or a data base, the storage device or the data base having stored therein identification data and associated network addresses for a plurality of providers.

According to an example, the client unit is adapted for providing further user-related data (e.g. a salted fingerprint of a user password or a fingerprint of a user password) to the lookup unit, the further user-related data being based on further user-specific data (e.g. a user password), the further user-specific data being associated with the user, and the further user-related data allowing for unambiguous identification of the further user-specific data. According to an example, the further user-specific data is a user password of the user. For example, the password may be the password of the user necessary for the user to log in at the provider unit, at a sub-provider unit associated with the provider unit or at a further entity. According to other examples, other secrets may be used as further user-specific data.

According to a further example, the further user-related data is a fingerprint of the further user-specific data. This fingerprint of the further user related data provided from the client unit to the lookup unit is also referred to as first fingerprint of the further user-related data in the following. In accordance with examples, the first fingerprint of the further user-related data may be a salted fingerprint and/or may be a fingerprint of the user-related data.

By providing the further user-related data to the lookup unit, the security of the network system and its operation may be increased.

According to an example, the lookup unit is adapted for providing data, which is based on the further user-related data, to the provider unit and receiving in response hereto a status information regarding the validity of at least one of the further user-specific data, the further user related data, and the data which is based on the further user-related data). According to an example, the data which is based on the further user-related data is a fingerprint of the further user-specific data. This fingerprint of the further user-related data which is provided from the lookup unit to the provider unit is also referred to as second fingerprint of the further user-related data in the following. According to an example, the second fingerprint of the further user-specific data is based on (e.g. identical to or derived from) the first fingerprint of user-specific data. For example, this second fingerprint may be a fingerprint of the first fingerprint of the further user-specific data. According to another example, the second fingerprint is the first fingerprint. In other words, in such an example the lookup unit is adapted for forwarding the first fingerprint of the further user-specific data received from the client unit to the provider unit. According to an example, the data which is based on the further user-related data as well as the fingerprint of the user-specific data is provided to the provider unit and optionally the provider unit is adapted for providing the configuration related data or at least part of the configuration related data in response to receiving from the lookup unit the data which is based on the further user-related data (e.g. the salted hash of the user's password hash) and the fingerprint of the user-specific data (e.g. the user's e-mail address).

According to an example, the provider unit may be adapted for verification of the validity of the user-specific data and/or further user-specific data. This may be performed in any suitable way. For example, according to an example, the provider unit may have stored the further user-specific data and/or the user-specific data and may be adapted for generating the a respective fingerprint of the user-specific data and/or a

respective fingerprint of the further user-specific data. In order to verify validity of the user-specific data, the provider unit may be adapted for comparing the fingerprint of the user-specific data received from the lookup unit with the respective fingerprint of the user-specific data generated by the provider unit. In order to verify validity of the further user-specific data, the provider unit may be adapted for comparing the fingerprint of the further user-specific data received from the lookup unit with the respective fingerprint of the further user-specific data generated by the provider unit. Upon match of the compared fingerprints, the provider unit may provide a status information and/or the configuration related data (the configuration related data may e.g. be associated with the user, the user-specific data and/or the further user-specific data) to the lookup unit. However, it should be understood that any suitable method for verification might be used for verifying that the fingerprint of the further user-specific data provided by the lookup unit corresponds to the further user-specific data stored in the storage device of the provider unit.

While according to an example the provider unit may provide the configuration related data, according to other examples, the configuration related data may be stored at a different entity, e.g. at the lookup unit and may be selected upon confirmation of successful verification of the further user-specific data at the provider unit. According to another example, the verification at the provider unit is omitted and the lookup unit may in such a case be adapted to provide the configuration related data upon reception of the provider ID from the clearing unit.

According to an example, retrieving the configuration related data from the provider unit includes providing the fingerprint of the user-specific data and optionally the fingerprint of the further user-specific data to the provider unit and receiving from the provider unit the configuration related data. According to an example, the lookup unit is adapted for not

providing the fingerprint of the further user-specific data to the clearing unit. For example, according to an example, the further user-specific data or data derived therefrom are only provided to the provider unit which already has stored therein the further user-specific data or data derived therefrom (e.g. a fingerprint of the user-specific data). In particular in case the further user-specific data is secret data (e.g. a password), the security of the network system is improved by not providing the fingerprint of the further user-specific data to the clearing unit.

According to an example, the provider unit is adapted for retrieving the login name of the user on the basis of the fingerprint of the user-specific data (e.g. from a database of the provider unit). Further, in an example where the further user-specific data is the password of the user at the provider unit, the provider unit may be adapted for verifying the password fingerprint for the selected login. According to an example, the provider unit is adapted for providing the login name associated with the user-specific data and/or the further user-specific data to the lookup unit in response to receiving the data which is based on the user-related data and/or the data which is based on the further user-related data from the lookup-unit.

While in the above there have been described communications between the client unit, the lookup unit, the clearing unit in order to provide the configuration related data for the client unit, in the following the registration of a provider unit to the lookup unit and the clearing unit is described.

According to an example which is related to the registration of the provider unit at the lookup unit and the clearing unit, the provider unit is adapted for providing a registration request to the lookup unit, the registration request including at least part of the identification data (e.g. a provider ID) and verification-related data (e.g. a fingerprint of a

clearing password), wherein the verification-related data are based on verification data (e.g. a clearing password) and wherein the verification-related data allow for unambiguous identification of the verification data; the lookup unit being further adapted for receiving the registration request; and the lookup unit being further adapted for providing the at least part of the provider identification data (e.g. the provider ID) and data which are based on the verification-related data (e.g. a fingerprint of the verification-related data, e.g. a fingerprint of the clearing password) to the clearing unit, e.g. in response to the received registration request.

According to an example, the verification-related data is a fingerprint (e.g. a salted fingerprint) of the verification data. The verification data may e.g. be a clearing secret which is known to the clearing unit and the provider unit that wants to register at the clearing unit. According to an example, the verification data (e.g. clearing secret) is exchanged between the clearing unit and the provider unit by encrypted e-mail or, in another example, manually by phone. According to an example, the verification data is generated by the clearing unit and provided to the provider unit.

According to an example, the data which are based on the verification-related data are a fingerprint of the verification-related data and verification-related data allow for unambiguous identification of the verification data. According to another example, the data which are based on the verification-related data are identical with the verification-related data. In other words, according to an example, the lookup unit is adapted for forwarding the verification-related data to the clearing unit.

According to an example, the registration request includes a provider address under which the provider unit can be contacted. The provider address may be e.g. a unified resource locator (URL) of the provider unit.

According to an example, the lookup unit is adapted for storing the at least part of the identification data and the associated provider address.

According to an example, the lookup unit is further adapted for receiving the registration request. Further, according to an example, the lookup unit is configured for storing the at least part of the provider identification data and the associated provider address in a storage device of the lookup unit. In such a case, the lookup unit may provide to the client unit the provider address as configuration related data. Communication with the provider unit for retrieval of configuration related data is not necessary in this case, can however be performed, for example in order to verify the user-specific data and the further user-specific data. Instead of or in addition to provider address, other configuration related data may be included in the registration request and may be stored by the lookup unit or provided to the clearing unit.

According to an example, the lookup unit may be adapted for providing a password to the clearing unit, the password being necessary for the clearing unit to accept the at least part of the provider identification data and the fingerprint of the verification data provided by the lookup unit.

According to an example, the verification data is agreed between the provider unit and the clearing unit before registration of the provider unit at the lookup unit. In this way, the clearing unit may, in an example, calculate a fingerprint of the verification data and compare the result to the fingerprint of the verification data received from the lookup unit. If for example a salted fingerprint is provided by the lookup unit, also the cryptographic salt is provided by the lookup unit so that the clearing unit can calculate the fingerprint of the combined cryptographic salt plus verification data in order to verify the verification data.

According to an example, the clearing unit is adapted for verifying the verification data and providing a status information element to the lookup unit, the status information element indicating whether or not the verification of the verification data was successful.

If the at least part of the provider identification data is complete, i.e. if the provider identification data allows for unambiguous identification of the provider unit, the clearing unit may be adapted in such a case to provide a status information element to the lookup unit, the status information element indicating whether or not the verification of the verification data was successful.

According to an example, only part of the provider identification data is provided by the provider unit to the lookup unit and hence only this part of the provider identification data is provided by the lookup unit to the clearing unit. In this way, the lookup unit need not to know the whole provider identification data for registering the provider unit at the clearing unit. This can improve the security of the whole network system. In an implementation of the herein disclosed subject-matter where only part of the provider identification data is provided to the clearing unit by the lookup unit, the clearing unit may be adapted for completing the provider identification data and for providing the completed provider identification data or the missing part of the provider identification data to the lookup unit if the verification of the verification data is successful.

According to an example, the clearing unit is adapted for providing an error information element to the lookup unit in case an error occurs during looking up the provider identification data and/or verifying the verification data. Furthermore, according to an example, the clearing unit is adapted for providing an information element to the lookup unit in case the verification of the verification data failed, wherein the information element

indicates to the lookup unit that the fingerprint of the verification data was invalid.

According to an example, the lookup unit is adapted for storing the identification data (e.g. the provider identification data) and the associated configuration related data (e.g. an associated provider URL) in the storage device of the lookup unit.

According to an example, a client unit of a network system is provided, the client unit being adapted for initiating a configuration of a provided to a user by providing user-related data to a lookup unit, wherein user-related data is associated with the user, the user-related data is based on user-specific data, and the user-related data allows for unambiguous identification of the user-specific data.

According to various examples, the client unit is adapted for providing the functionality of one or more of the aforementioned examples and/or for providing the functionality as required by one or more of the aforementioned examples. Moreover, according to an example, the client unit is adapted as described with regard to one or more of the aforementioned examples.

According to an example, a lookup unit of a network system is provided, the lookup unit being adapted for receiving user-related data from a client unit, wherein the user-related data is based on user-specific data, the user-specific data is associated with a user, and the user-related data allows for unambiguous identification of the user-specific data; the lookup unit being adapted for retrieving identification data (e.g. a provider ID) from a clearing unit by using the user-related data (e.g. a

fingerprint of an e-mail address of the user), the identification data being associated with the user-specific data; the lookup unit being adapted for retrieving configuration related data for a service provided to the user; the lookup unit being adapted for retrieving the configuration related data by using the identification data.

According to various examples, the lookup unit is adapted for providing the functionality of one or more of the aforementioned examples and/or for providing the functionality as required by one or more of the aforementioned examples. Moreover, according to an example, the lookup unit is adapted as described with regard to one or more of the aforementioned examples. For example, the lookup unit is adapted for receiving a fingerprint of user-specific data, wherein the user-specific data are associated with a user and the fingerprint of the user-specific data allows for unambiguous identification of the user-specific data; wherein the lookup unit is further adapted for retrieving the configuration related data by using the fingerprint of the user-specific data. For example, the lookup unit is adapted for retrieving the configuration related data from a provider unit by using the fingerprint of the user-specific data.

According to an example of the herein disclosed subject-matter, a clearing unit of a network system is provided, the clearing unit comprising a storage device and the clearing unit being adapted for receiving user-related data from a lookup unit of the network system, wherein the user-related data is based on user-specific data, the user-specific data is associated with a user, and the user-related data allows for unambiguous identification of the user-specific data; the clearing unit being adapted for retrieving from the storage device the identification data

associated with the user-specific data; and the clearing unit being further adapted for providing the identification data to the lookup unit.

According to various examples, the clearing unit is adapted for providing the functionality of one or more of the aforementioned examples and/or for providing the functionality as required by one or more of the aforementioned examples. Moreover, according to an example, the clearing unit is adapted as described with regard to one or more of the aforementioned examples.

For example, according to an examplea clearing unit of a network system is provided, the clearing unit being adapted for receiving a fingerprint of user-specific data from a lookup unit, wherein the user-specific data are associated with the user and the fingerprint of the user-specific data allows for unambiguous identification of the user-specific data; wherein the clearing unit is further adapted for retrieving provider identification data associated with the received fingerprint of the user-specific data, wherein the provider identification data identify a provider unit. According to an example, the provider unit is adapted for providing a user-specific service to the user.

According to an example of the herein disclosed subject-matter, a provider unit of a network system is provided, the provider unit being adapted for receiving user-related data from a lookup unit of the network system, wherein the user-related data is based on user-specific data, the user-specific data is associated with a user, and the user-related data allows for unambiguous identification of the user-specific data; the provider unit being adapted for verifying validity of the user-specific data by using the received user-related data; the provider unit being adapted for verifying

validity of the user-specific data by using the received user-related data and/or retrieving configuration related data for a service provided to the user.

According to an example, the provider unit is adapted for providing a status information to the lookup unit, the status information being indicative of a validity of the user-specific data corresponding to the fingerprint.

According to a further example, the provider unit is adapted for providing the configuration related data to the lookup unit.

According to various examples, the provider unit is adapted for providing the functionality of one or more of the aforementioned examples and/or for providing the functionality as required by one or more of the aforementioned examples. Moreover, according to an example, the provider unit is adapted as described with regard to one or more of the aforementioned examples.

For example, according to an example, the provider unit is adapted for receiving a fingerprint of user-specific data, wherein the user-specific data are associated with the user and the fingerprint of the user-specific data allows for unambiguous identification of the user-specific data; the provider unit being further adapted for retrieving the configuration related data by using the fingerprint of user-specific data, the configuration related data being associated with the user-specific data.

According to an example of the herein disclosed subject-matter, a method of operating a client unit of a network system is provided, the method comprising: initiating a configuration of a service provided to a user

by providing user-related data to a lookup unit, wherein user-related data is associated with the user, the user-related data is based on user-specific data, and the user-related data allows for unambiguous identification of the user-specific data.

According to various examples, the method is adapted for providing the functionality of one or more of the aforementioned examplesand/or for providing the functionality as required by one or more of the aforementioned examples.

For example, according to various examples the method comprises providing a fingerprint of user-specific data to a lookup unit, wherein the user-specific data are associated with a user and the fingerprint of the user-specific data allows for unambiguous identification of the user-specific data; and receiving configuration related data for a service provided to the user from the lookup unit.

According to an example of the herein disclosed subject-matter a method of operating a lookup unit of a network system is provided, the method comprising: receiving user-related data from a client unit, wherein the user-related data is based on user-specific data, the user-specific data is associated with a user, and the user-related data allows for unambiguous identification of the user-specific data; retrieving identification data (provider ID) from a clearing unit by using the user-related data (fingerprint of e-mail address), the identification data being associated with the user-specific data; retrieving configuration related data for a service provided to the user; the retrieving of the configuration related data being performed by using the identification data.

According to various examples, the method is adapted for providing the functionality of one or more of the aforementioned examples and/or for providing the functionality as required by one or more of the aforementioned examples.

For example, according to various examples the method comprises: receiving a fingerprint of user-specific data from the client unit, wherein the user-specific data are associated with a user and the fingerprint of the user-specific data allows for unambiguous identification of the user-specific data; retrieving provider identification data from the clearing unit by using the fingerprint of the user-specific data, the identification data being associated with the user-specific data; retrieving the configuration related data for a service provided to the user; wherein the retrieving of the configuration related data is performed by using the provider identification data.

According to an example of the herein disclosed subject-matter, a method of operating a clearing unit of a network system is provided, the method comprising receiving user-related data from a lookup unit of the network system, wherein the user-related data is based on user-specific data, the user-specific data is associated with a user, and the user-related data allows for unambiguous identification of the user-specific data; retrieving identification data associated with the user-specific data; providing the identification data to the lookup unit.

According to various examples, the method is adapted for providing the functionality of one or more of the aforementioned examples and/or for providing the functionality as required by one or more of the aforementioned examples.

For example, according to various examples the method comprises receiving a fingerprint of user-specific data from a lookup unit, wherein the user-specific data are associated with a user and the fingerprint of the user-specific data allows for unambiguous identification of the user-specific data; retrieving provider identification data associated with the fingerprint of the user-specific data, wherein the provider identification data identify a provider unit; and providing the provider identification data to the lookup unit.

According to an example of the herein disclosed subject-matter, a method of operating a provider unit of a network system is provided, the method comprising: receiving user-related data from a lookup unit of the network system, wherein the user-related data is based on user-specific data, the user-specific data is associated with a user, and the user-related data allows for unambiguous identification of the user-specific data; verifying validity of the user-specific data by using the received user-related data and/or retrieving configuration related data for a service provided to the user; and optionally providing a status information and/or the configuration related data to the lookup unit, the status information being indicative of a validity of the user-specific data corresponding to the fingerprint.

According to various examples, the method is adapted for providing the functionality of one or more of the aforementioned examples and/or for providing the functionality as required by one or more of the aforementioned examples.

For example, according to various examples, the method comprises receiving a fingerprint of the user-specific data from the lookup

unit, wherein the user-specific data are associated with a user and the received fingerprint of the user-specific data allows for unambiguous identification of the user-specific data; verifying validity of the received fingerprint of the user-specific data; and providing a status information to the lookup unit if the information element corresponds to a valid user-specific data, the status information indicating that the information element corresponds to valid user-specific data.

According to an example of the herein disclosed subject-matter, a method of operating a network system is provided, the network system comprising a lookup unit, a clearing unit and a client unit, and the method comprising: providing user-related data from the client unit to the lookup unit, the user-related data being based on user-specific data, the user-specific data being associated with a user, and the user-related data allowing for unambiguous identification of the user-specific data; operating the lookup unit so as to retrieve identification data (e.g. a provider ID) from the clearing unit by using the user-related data (e.g. a fingerprint of an e-mail address of the user), the identification data being associated with the user-specific data; operating the clearing unit so as to retrieve identification data associated with the user-specific data; providing the identification data from the clearing unit to the lookup unit; operating the lookup unit so as to retrieve configuration related data for a service provided to the user; operating the lookup unit so as to retrieve the configuration related data by using the identification data.

According to various examples, the method is adapted for providing the functionality of one or more of the aforementioned examples and/or for providing the functionality as required by one or more of the aforementioned examples.

For example, according to various examples, the method comprises providing a fingerprint of the user-specific data from the client unit to the lookup unit, wherein the user-specific data are associated with a user and the fingerprint of the user-specific data allows for unambiguous identification of the user-specific data; operating the clearing unit so as to retrieve provider identification data associated with the fingerprint of the user-specific data; and operating the lookup unit so as to retrieve configuration related data associated with the provider identification data by using the fingerprint of the user-specific data.

According to an example of the herein disclosed subject-matter, a computer program is provided, the computer program being adapted for controlling (e.g. carrying out) the method according to one or more aforementioned examples. In particular, for each method disclosed herein, a respective computer program may be provided which is adapted for, when executed by a processor device, controlling the respective method.

As used herein, reference to a computer program is intended to be equivalent to a reference to a program element and/or a computer readable medium containing instructions for controlling a computer system to effect and/or coordinate the performance of the above described method.

The computer program may be implemented as computer readable instruction code by use of any suitable programming language, such as, for example, JAVA, C++, and may be stored on a computer-readable medium (removable disk, volatile or non-volatile memory, embedded memory/processor, etc.). The instruction code is operable to program a computer or any other programmable device to carry out the intended

functions. The computer program may be available from a network, such as the World Wide Web, from which it may be downloaded.

The herein disclosed subject matter may be realized by means of a computer program respectively software. However, the herein disclosed subject matter may also be realized by means of one or more specific electronic circuits respectively hardware. Furthermore, the herein disclosed subject matter may also be realized in a hybrid form, i.e. in a combination of software modules and hardware modules.

For example, each unit disclosed herein may be implemented in software and/or hardware, e.g. by a respective device or by a service running on a computer. A device may be a computer, e.g. a server having software running thereon which provides the described functionality of the unit. Generally, a device may be e.g. a processor device having a at least one processor for carrying out instructions in order to provide functions as described with regard to examples of the respective entity.

According to an example, the functionality of the units disclosed herein, for example of the client unit, the lookup unit, the clearing unit and the provider unit, may be implemented by means of a respective software component, e.g. a PHP component.

In the above there have been described and in the following there will be described examples of the subject matter disclosed herein with reference to a network system, the individual units thereof and respective methods of operation. It has to be pointed out that of course any combination of features relating to different aspects of the herein disclosed subject matter is also possible. In particular, some features have been or will be described with reference to apparatus type examples whereas other features have been or will be described with reference to method type

examples. However, a person skilled in the art will gather from the above and the following description that, unless other notified, in addition to any combination of features belonging to one aspect also any combination of features relating to different aspects or examples, for example even a combinations of features of apparatus type examples and features of the method type examples is considered to be disclosed with this application.

According to respective examples, the user specific data is the e-mail address of the user; the further user specific data is a fingerprint of a salted fingerprint of a user password, wherein the salted fingerprint of the user password is the user password combined with a cryptographic salt and the client unit is adapted for providing the cryptographic salt to the lookup unit; the configuration related data includes a unified resource locator (URL) of the provider unit and a login name of the user at the provider unit; the user-related data provided from the client unit to the lookup unit is transmitted to lookup unit in a lookup request, wherein the optionally this user-related data is fingerprint of the user-specific data and the lookup request optionally further includes a salted fingerprint of a fingerprint of a user password required for the user to login to a service of the provider unit, and the cryptographic salt used to generate the salted fingerprint; the user-related data provided from the lookup unit to the clearing unit is transmitted to clearing unit in a request transmission, wherein the optionally this user-related data is fingerprint of the user-specific data and the request transmission optionally further includes a password for login to the clearing unit; the user-related data provided to the provider unit is transmitted to the provider unit in a provider request, wherein optionally this user-related data optionally includes the fingerprint of the user-specific data and the provider request optionally includes the salted fingerprint of a fingerprint of a user password required for the user to

login to a service of the provider unit, and the cryptographic salt used to generate the salted fingerprint.

Responses to the requests (lookup request, request transmission, provider request) may be provided by the responding unit in a respective response transmission.

According to an example, the units, which communicate with each other according to examples of the herein disclosed subject matter, are communicatively coupled via any suitable connection/protocol, e.g. via a secured connection over which the element is transmitted in encrypted form, such as a virtual private network connection (VPN connection) or a secure socket layer connection (SSL connection). It should be understood that – as usual – providing of an element (e.g. a fingerprint of user-specific data) over a secured connection from a sending unit to a receiving unit implicitly discloses encrypting the element, transmitting the encrypted element from the sending unit to the receiving unit and decrypting the encrypted element at the receiving unit to make the element available at the receiving unit. Herein, the sending unit and the receiving unit may be any suitable unit as disclosed herein. It is noted that any communication between units as disclosed herein may be a communication over a secured connection between the units.

It should be understood that a disclosure of a communication between different units implicitly discloses the transmittance, reception and retrieval of respective transmissions by the involved units and vice versa. For example, the disclosure of receiving some input data and providing in response hereto some return data implicitly discloses the retrieval of the return data by providing the input data, the sending of the input data, the receiving of the return data, etc. Further each transmission from a first unit to another, second unit may include an operation identifier which specifies

an operation to be carried out by the second unit. Further, the disclosure of providing response data, e.g. a status information, an identity, configuration related data, etc., from a first unit to a second unit is considered to disclose, according to an example, that the second unit which receives the response data is adapted to provide a respective request to the first unit and that the first unit is adapted to receive the request and provide in response hereto the response data.

According to an example, providing the response data implies providing the response data with a predetermined delay. In this way, brute force and timing attacks to the respective unit which transmits the response data may be prevented and thus the security of the network system be increased.

Generally herein "providing data" includes providing the data in unencrypted form or providing the data in encrypted form. Anyway, "providing data" refers generally to provide the data in a representation that allows to reconstruct the data in its original form from the representation.

Further, if a first entity (e.g. the identification data) is specified herein as being associated with a second entity (e.g. the user-specific data), according to an example the term "associated with" also includes an association of the first entity and the second entity in the sense that from the first entity related data (e.g. a fingerprint) can be derived which are assigned to the second entity, e.g. by means of a database.

Whenever an action or method performed by a unit is disclosed herein, it should be understood that according to an example the unit is adapted for performing the action or the method.

The clearing unit and the lookup unit are different from each other. However, despite being different units, according to an example the

clearing unit and the lookup unit are provided in a single device. For the clearing unit and the lookup unit may be two different software components running on a single processor device. Further, in another example, one of the clearing unit and the lookup unit may be a software component running in a virtual machine, the virtual machine running on the processor device. The other of the clearing unit and the lookup unit may be a software component running directly on the processor device or in a further, different virtual machine. According to a further example, the clearing unit and the lookup unit may be spatially remote from each other.

An exemplary implementation of the herein disclosed subject matter may include the following features (e.g. in the form of the exemplary processes (A), (B)):

(A) PLS process (done each time configuration related data is required by the client unit)

1. The client unit generates the first fingerprint of the user-specific data and the first fingerprint of the further user-specific data and sends this to the PLS.
2. The PLS uses the first fingerprint of the user-specific data to get the numeric provider ID of the user’s provider from the clearing.
3. The PLS uses its own database to determine the URL of the assigned provider.
4. The PLS contacts the provider (by using the URL) and sends the first fingerprint of the user-specific data and the first fingerprint of the further user-specific data and used salt.
5. The provider verifies the data (user with such e-mail address fingerprint exists and with the given salt the users password fingerprint matches the given one). Result is “OK” with URL to contact the provider or “INVALID”. This might be different because of

subproviders. The provider determines the correct URL (e.g. https://portal.regify.com) out of his user database.

6. The PLS returns to the client unit the URL to use.
7. The client unit contacts the provider at the given URL to get the desired information (e.g. the client's configuration).

Finally, the PLS still does not know the users password or the e-mail address. The clearing does not know the users e-mail address.

(B) PLS registration process (done at least once for each new provider):

The PLS learns the association between provider ID and the correct URL by registering. For this process:

1. The provider unit calls the PLS together with his URL, ID, a fingerprint of his clearing password (clearingPassword) and the used salt. fingerprint = Hash(salt|clearingPassword)
2. The PLS verifies this information with the clearing unit by sending the provider ID and the fingerprint to the clearing.
3. If this was successful the PLS updates his database. Now he knows the provider ID and its associated URL (needed for above step 3 and 4).

Finally, the PLS does not know the providers clearing password but now has an association of provider ID and URL which is proven by the clearing.

The aspects and examples defined above and further aspects and examples of the herein disclosed subject matter are apparent from the examples to be described hereinafter and are explained with reference to the drawings, but to which the invention is not limited.

Claims

1. A network system (100) comprising:

a lookup unit (104);

a clearing unit (110) having a storage device (111), the lookup unit (104) and the clearing unit (110) being different from each other; and

a client unit (102) being adapted for providing user-related data (106) to the lookup unit (104), the user-related data (106) being based on user-specific data, the user-specific data being associated with a user, the user-related data (106) allowing for unambiguous identification of the user-specific data, and the user-related data (106) being a first fingerprint of the user-specific data;

the lookup unit (104) being further adapted for providing a second fingerprint of the user-specific data to the clearing unit (110), the second fingerprint being based on the first fingerprint of the user-specific data, the second fingerprint allowing for unambiguous identification of the user-specific data;

the lookup unit (104) being adapted for retrieving identification data (114) from the clearing unit (110) by using the second fingerprint, the identification data (114) being associated with the user-specific data;

the clearing unit (110) being adapted for retrieving from the storage device (111) the identification data (114) associated with the user-specific data;

the clearing unit (110) being adapted for selecting from the storage device the identification data (114) associated with the user-specific data by using the second fingerprint of the user-specific data;

the clearing unit (110) being adapted for providing the identification data (114) to the lookup unit (104);

the lookup unit (104) being adapted for retrieving configuration related data (115) for a service provided to the user by using the identification data (114); and

the lookup unit (104) further being adapted for providing the configuration related data (115) to the client unit (102).

2. The network system according to claim 1, further comprising

a provider unit (118), the provider unit (118) being accessible by the client unit (102);

the lookup unit (104) being further adapted for providing a third fingerprint of the user-specific data to the provider unit (118) for verifying, by the provider unit (118), validity of the user-specific data by using the third fingerprint; and

the provider unit (118) being optionally adapted for providing a status information regarding the validity of the user-specific data to the lookup unit (104);

wherein optionally the third fingerprint is identical to the first fingerprint.

3. The network system according to any one of claims 1 to 2, further comprising

a provider unit (118), the provider unit (118) being accessible by the client unit (102);

the client unit (102) being further adapted for providing further user-related data (108) to the lookup unit (104), the further user-related data (108) being based on further user-specific data, the further user-specific data being associated with the user, and the further user-related data (108) allowing for unambiguous identification of the further user-specific data;

the lookup unit (104) being further adapted for providing data, which is based on the further user-related data (108), to the provider unit (118) and receiving in response hereto a status information regarding the validity of the further user-specific data.

4. The network system according to claim 1, further comprising

a provider unit (118);

the provider unit (118) being adapted for providing a registration request (220) to the lookup unit (104), the registration request (220) including at least part of the identification data (114) and a verification-related data, the verification-related data being based on verification data and wherein the verification-related data allows for unambiguous identification of the verification data;

the lookup unit (104) being further adapted for receiving the registration request (220);

the lookup unit (104) being further adapted for providing to the clearing unit (110) the at least part of the provider identification data (114) and data which is based on the verification-related data and allows for unambiguous identification of the verification data.

5. The client unit (102) of the network system according to any one of claims 1 to 4,

the client unit (102) being adapted for initiating a configuration of a service provided to a user by providing user-related data (106) to a lookup unit (104).

6. A lookup unit (104) of a network system,

the lookup unit (104) being adapted for receiving user-related data (106) from a client unit (102), wherein the user-related data (106) is based on user-specific data, the user-specific data is associated with a user, the user-related data (106) allows for unambiguous identification of the user-specific data, and the user-related data (106) being a first fingerprint of the user-specific data;

the lookup unit (104) being further adapted for providing a second fingerprint of the user-specific data to the clearing unit (110), the second fingerprint being based on the first fingerprint of the user-specific data, the second fingerprint allowing for unambiguous identification of the user-specific data and the clearing unit (110) and the lookup unit (104) being different from each other;

the lookup unit (104) being adapted for retrieving identification data (114) from a clearing unit (110) by using the second fingerprint, the identification data (114) being associated with the user-specific data;

the lookup unit (104) being adapted for retrieving configuration related data (115) for a service provided to the user by using the identification data (114); and

the lookup unit (104) further being adapted for providing the configuration related data (115) to the client unit (102).

7. The clearing unit (110) of the network system according to any one of claims 1 to 4,

the clearing unit (110) being adapted for receiving the second fingerprint from a lookup unit (104) of the network system.

8. The provider unit (118) of the network system according to any one of claims 2 to 4,

the provider unit (118) being further adapted for receiving the user-related data (106) from the lookup unit (104) of the network system;

the provider unit (118) being adapted for

verifying validity of the user-specific data by using the received user-related data (106) and/or

retrieving configuration related data (115) associated with the user-specific data.

9. A method of operating a network system comprising a lookup unit (104), a clearing unit (110) and a client unit (102), wherein the clearing unit and the lookup unit are different from each other, the method comprising:

providing user-related data (106) from the client unit (102) to the lookup unit (104), the user-related data (106) being based on user-specific data, the user-specific data being associated with a user, the user-related data (106) allowing for unambiguous identification of the user-specific data, and the user-related data (106) being a first fingerprint of the user-specific data;

operating the lookup unit (104) so as to provide a second fingerprint of the user-specific data to the clearing unit (110), the second fingerprint being based on the first fingerprint of the user-specific data, the second fingerprint allowing for unambiguous identification of the user-specific data;

operating the lookup unit (104) so as to retrieve identification data (114) from the clearing unit (110) by using the second fingerprint, the identification data (114) being associated with the user-specific data;

operating the clearing unit (110) so as to retrieve identification data (114) associated with the user-specific data;

operating the clearing unit (110) so as to select from the storage device the identification data (114) associated with the user-specific data by using the second fingerprint of the user-specific data;

providing the identification data (114) from the clearing unit (110) to the lookup unit (104);

operating the lookup unit (104) so as to retrieve configuration related data (115) for a service provided to the user by using the identification data (114); and

operating the lookup unit (104) so as to provide the configuration related data (115) to the client unit (102).

10. The method according to claim 9, the method further comprising operating the client unit (102) by:

initiating a configuration of a service provided to a user by providing the user-related data (106) to a lookup unit (104).

11. The method according to claim 9, the method further comprising operating the clearing unit (110) by:

receiving the second fingerprint from the lookup unit (104);

providing the identification data (114) to the lookup unit (104).

12. The method according to claim 9, the method further comprising operating a provider unit (118) of the network system by:

receiving the user-related data (106) from the lookup unit (104);

verifying validity of the user-specific data by using the received user-related data (106) and/or retrieving configuration related data (115) associated with the user-specific data; and

optionally providing a status information and/or the configuration related data (115) to the lookup unit (104), the status information being indicative of a validity of the user-specific data corresponding to the user-related data (106).

13. A Method of operating a lookup unit (104) of a network system, the method comprising:

receiving user-related data (106) from a client unit (102), wherein the user-related data (106) is based on user-specific data, the user-specific data is associated with a user, the user-related data (106) allows for unambiguous

identification of the user-specific data, and the user-related data (106) being a first fingerprint of the user-specific data;

providing a second fingerprint of the user-specific data to a clearing unit (110), the clearing unit and the lookup unit being different from each other, the second fingerprint being based on the first fingerprint of the user-specific data, the second fingerprint allowing for unambiguous identification of the user-specific data;

retrieving identification data (114) from a clearing unit (110) by using the second fingerprint, the identification data (114) being associated with the user-specific data;

retrieving configuration related data (115) for a service provided to the user by using the identification data (114); and

providing the configuration related data (115) to the client unit (102).

14. Computer program which is adapted for, when executed by a processor device, controlling the method according to any one of claims 9 to 13.