CLAIMS

1. A distributed system for managing identity, ID, data of registered users, wherein the ID data contains biometric characteristics of a registered user, the ID management system comprising:

a client application running on an electronic device associated with the registered user, the client application comprising a graphic user interface, GUI, for interacting with the corresponding registered user;

a network of ID processing touchpoints, wherein an ID processing touchpoint is configured to process ID data for the authentication of users, wherein the ID processing touchpoint is configured to issue a status notification associated with the processing and/or use of the ID data by the ID processing touchpoint;

an ID server configured to receive and distribute the status notification issued by the ID processing touchpoint to the corresponding client application;

wherein each client application is configured, in response to receiving the status notification from the ID server, to issue user alerts on the GUI to notify the registered user on the status of the corresponding ID data at the ID processing touchpoint; wherein the client application is configured to display on the GUI a set of user-selectable options for initiating one or more actions in response to the notification received from the ID server and/or an ID processing touchpoint, wherein the selectable options comprise issuing a breach notification indicating an unauthorised ID transaction at an ID processing touchpoint;

wherein upon receiving a selection for issuing a breach notification, the client application is configured to issue a corresponding breach notification, which is communicated to a security server, where it is stored in a registry, the security server being part of the ID management system;

wherein the security server, upon receiving the breach notification is configured to initiate a set of breach control actions for assessing and managing the identified ID breach, the breach control actions comprising at least one of investigating the cause of the breach, notifying other ID processing touchpoints of the breach, and deleting the breached ID data from the ID management system and/or other ID processing touchpoints.

2. The ID management system of claim 1, wherein the client application is configured, upon receiving a user response through the GUI, to issue counter-notification to the ID server and/or ID processing touchpoints.

3. The ID management system according to claim 1 or 2, wherein the selectable options further comprise providing consent for the sharing of the corresponding ID data to ID processing touchpoints.

4. The ID management system according to claim 3, wherein the client application is configured, in response to the user selecting to provide consent for the sharing of the corresponding ID data, to communicate a consent notification comprising the requested ID data of the user to the ID server, the ID server being configured to distribute the ID data at a selected set of ID processing touchpoints.

5. The ID management system according to any one of the preceding claims, wherein the security server is further configured upon receiving the breach notification to collect information from the one or more ID processing touchpoints associated with the unauthorised transaction and accordingly communicate a report to the client application of the registered user, the report comprising information associated with the breach.

6. The ID management system according to any one of the preceding claims, wherein the client application is configured to display on the GUI a graphical representation of the status of the corresponding ID data at different ID processing touchpoints.

7. The ID management system according to claim 6, wherein the graphic representation is in the form of a route displaying the transfer of the ID data between different ID processing touchpoints.

8. The ID management system according to claim 7, wherein, based on the status notification, the client application is configured to display on the route the current status of the ID data at the different ID processing touchpoints.

9. The ID management system according to any one of claims 7 or 8, wherein the route is generated based on information obtained from a travel itinerary of the registered user.

10. The ID management system according to any one of the preceding claims, wherein the ID processing touchpoints are connected to the ID server on the basis of membership.

11. The ID management system according to claim 10, wherein the ID server is configured to include or exclude ID processing touchpoints from membership based on metrics indicative their ID security performance.

12. A method for managing identity, ID, data of registered users, wherein the ID data contains biometric characteristics of a registered user, the method comprising:

receiving, at an ID server, a status notification issued by an ID processing touchpoint of a network of ID processing touchpoints associated with the processing and/or use of ID data of the registered user;

distributing, from the ID server, the status notification to a corresponding client application, wherein the client application is running on an electronic device associated with the registered user and comprising a graphic user interface, GUI for interacting with the corresponding registered user;

notifying, by the client application, the registered user on the status of the corresponding ID data by

issuing user alerts on the GUI in response to receiving status notifications from the ID server and/or an ID processing touchpoint;

displaying, on the GUI (111) of the client application (110), a set of user-selectable options for initiating one or more actions in response to the notification received from the ID server (120) and/or an ID processing touchpoint (150), wherein the selectable options comprise issuing a breach notification indicating an unauthorised ID transaction at the ID processing touchpoint (150);

issuing, by the client application (110) upon receiving a selection for issuing a breach notification, a corresponding breach notification, which is communicated to a security server (130), where it is stored in a registry; and

initiating, at the security server (130) upon receiving the breach notification, control actions for assessing and managing the identified ID breach, the breach control actions comprising at least one of investigating the cause of the breach, notifying other ID processing touchpoints (150) of the breach, and deleting the breached ID data (140) from the ID server (120) and/or other ID processing touchpoints (150).

13. The ID management method according to claim 12 further comprising issuing, by the client application (110), upon receiving a user response through the GUI (111), counter-notification to the ID server (120) and/or ID processing touchpoints (150).

14. The ID management method according to claim 12 or 13, wherein the selectable options further comprise providing consent for the sharing of the corresponding ID data (140) to ID processing touchpoints (150), and wherein the method further comprises communicating, by the client application (110) in response to the user selecting to provide consent for the sharing of the corresponding ID data (140), a consent notification comprising the requested ID data (140) of the user to the ID server (120), the ID server (120) being configured to distribute the ID data (140) at a selected set of ID processing touchpoints (150).

15. The ID management method according to any one of claims 12 to 14 further comprising collecting, by the security server (130) upon receiving the breach notification, information from the one or more ID processing touchpoints (150) associated with the unauthorised transaction and accordingly communicating a report to the client application (110) of the registered user, the report comprising information associated with the breach.