

WHAT IS CLAIMED IS:

1 1. A server apparatus comprising:
2 one or more processors; and
3 a memory including instructions that, when executed by the one or more
4 processors, cause the server apparatus to:
5 receive a request from a computing device to conduct an action
6 with respect to a user;
7 identify an electronic identifier associated with a user, the electronic
8 identifier having been generated from sensitive information specific to the user;
9 identify, within a verification network, an electronic record
10 comprising a number of interaction records associated with the electronic
11 identifier, each of the interaction records signed by an originating entity;
12 verify the authenticity of at least one interaction record of the
13 plurality of interaction records using a public key associated with the originating
14 entity; and
15 determine, based at least in part on the verified interaction record,
16 whether to execute the action.

1 2. The server apparatus of claim 1, wherein determining whether to
2 execute the action comprises determining a risk assessment for the action.

1 3. The server apparatus of claim 2, wherein the risk assessment for the
2 action takes into consideration a trust value determined for each originating entity
3 associated with the number of interaction records in the electronic record.

1 4. The server apparatus of claim 1, wherein the instructions further cause
2 the server apparatus to:
3 upon executing the action with respect to the user, generate a new
4 interaction record to include an indication of the action; and
5 provide the new interaction record to the verification network to be added
6 to the electronic record.

1 5. The server apparatus of claim 4, wherein the instructions further cause
2 the server apparatus to sign the new interaction record using a private key maintained
3 by the server apparatus prior to providing the new interaction record to the verification
4 network.

1 6. The server apparatus of claim 1, wherein the instructions further cause
2 the server apparatus to request additional information associated with the user from at
3 least one originating entity associated with an interaction record of the number of
4 interaction records.

1 7. The server apparatus of claim 6, wherein the instructions further cause
2 the server apparatus to:
3 receive the requested additional information associated with the user from
4 the at least one originating entity; and
5 store the requested additional information associated with the user in
6 relation to an account associated with the user.

1 8. The server apparatus of claim 1, wherein the information specific to the
2 user comprises specific user information in a predetermined format.

1 9. The server apparatus of claim 1, wherein the electronic identifier has
2 been generated by applying a hash function to the information specific to the user.

1 10. The server apparatus of claim 1, wherein at least a first interaction
2 record associated with the electronic identifier includes a location of user-specific
3 information associated with the user, wherein the instructions further cause the server
4 apparatus to request the user-specific information associated with the user from the
5 location at a first originating entity.

1 11. The server apparatus of claim 10, wherein determining whether to
2 execute the action comprises accessing the user-specific information associated with
3 the user at the location;

4 determining a risk assessment based on the accessed user-specific
5 information associated with the user; and
6 determining whether the risk assessment is within an acceptable range.

1 12. A method comprising:

2 receiving a request from a computing device to conduct an action with
3 respect to a user;

4 identifying an electronic identifier associated with a user, the electronic
5 identifier having been generated from sensitive information specific to the user;

6 identifying, within a verification network, an electronic record comprising a
7 number of interaction records associated with the electronic identifier, each of the
8 interaction records signed by an originating entity;

9 verifying the authenticity of at least one interaction record of the plurality of
10 interaction records using a public key associated with the originating entity; and

11 determining, based at least in part on the verified interaction record,
12 whether to execute the action.

1 13. The method of claim 12 wherein determining whether to execute the
2 action comprises determining a risk assessment for the user.

1 14. The method of claim 13 wherein determining the risk assessment
2 includes determining a level of trust to be associated with each originating entity
3 associated with an interaction record for the electronic identifier, wherein different levels
4 of trust may be determined for each originating entity.

1 15. The method of claim 12, further comprising:

2 requesting, from an originating entity associated with at least one
3 interaction record of the number of interaction records, user-specific information stored
4 by that originating entity; and

5 obtaining, in response to the request, the user-specific information that
6 includes sensitive information associated with the user.

1 16. The method of claim 15, wherein the request includes a document
2 address included in an interaction record and the user-specific information is obtained
3 from a document located at the document address.

1 17. The method of claim 15, wherein determining whether to execute the
2 action is based at least in part on the user-specific information.