Claims

1. A computer—implemented for managing identities in a network, the method comprising the steps of

generating, by a first device, a first cryptographic key pair comprising a first public key;

submitting, by a user of the first device, the first public key to an identity service;

registering, by the identity service, the first public key under a main user identifier;

generating, by a second device of the user, a second cryptographic key pair comprising a second public key;

submitting, by the user of the first and the second device, the main user identifier and the second public key to the identity service;

providing, by the identity service, to the user of the first and the second device, an authentication request/form to authenticate with respect to the first public key;

generating, by the first device, authentication information that is valid with respect to the first public key;

receiving, by the identity service, an authentication response comprising the authentication information of the first device being valid with respect to the first public key; and

registering, upon successful authentication, the second public key under the main user identifier.

2. A computer—implemented method according to claim 1, wherein the main user identifier is a user name.

3. A computer—implemented method according to claim 1, wherein the main user identifier is a natural number.

4. A computer—implemented method according to any of the preceding claims, wherein the first device and/or the second device is a secure hardware device.

5. A computer—implemented method according to any of the preceding claims, wherein

the step of providing the authentication request comprises

providing a link, a barcode or other authentication means, the link, the barcode or the other authentications means comprising an authentication form to authenticate with respect to the first public key.

6. A computer—implemented method according to any of the preceding claims, further comprising authenticating with respect to the first public key and/or the second public key by means of a face scan, a fingerprint and/or a password.

7. A computer-implemented method according to claim 4, wherein the first device and/or the second device is a security chip.

8. A distributed network which is configured to perform one or more steps of the method according to any of the preceding claims.

9. A node for a distributed network which is configured to perform one or more steps of the method according to any of the preceding claims.

10. A computer program product for operating a network according to claim 8 or a node according to claim 9, the computer program product comprising a computer

readable storage medium having program instructions embodied therewith, the program instructions executable by one or more of the plurality of nodes to cause the one or more of the plurality of nodes to perform one or more steps of a method according to any one of the claims 1—7.