

Claims

1. Server (100;200;300) for providing one or more data sets via a digital communication network (90), wherein the server (100;200;300) is configured for :
 - 5 associating an unique identifier (115;215;315) with an identified data set (110;210;310), the unique identifier (115;215;315) representing a network address for accessing the identified data set (110;210;310) via the digital communication network (90), wherein the unique identifier (115;215;315) is specific to the identified data set (110;210;310),
 - 10 validating an authentication information (172;272;372) provided by an authenticator (170;270;370) of a client (160;260;360) requesting access to the server (100;200;300) via the unique identifier (115;215;315), and
 - selectively providing the client (160;260;360) with an access right for one or more data sets, if the authentication information (172;272;372) identifies the authenticator (170;270;370) as being associated with a registered user.
- 15 2. Server (100;200;300) according to claim 1,
 - wherein the server (100;200;300) is configured for validating the authentication information (172;272;372) provided by the authenticator (170;270;370) of the client (160;260;360) requesting access to the identified data set (110;210;310) via the unique identifier (115;215;315);
 - 20 wherein the server (100;200;300) is configured for selectively providing the client (160;260;360) with an access right for the identified data set (110;210;310), and
 - wherein the access right for the identified data set (110;210;310) is specific to the registered user associated with the authenticator (170;270;370).
- 25 3. Server (100;200;300) for providing a data set (110;210;310) via a digital communication network (90), wherein the server (100;200;300) is configured for :
 - associating an unique identifier (115;215;315) with the data set (110;210;310), the unique identifier (115;215;315) representing a network address for accessing the data set (110;210;310) via the digital communi-

cation network (90), wherein the unique identifier (115;215;315) is specific to the data set (110;210;310),

validating an authentication information (172;272;372) provided by an authenticator (170;270;370) of a client (160;260;360) requesting access to the data set (110;210;310) via the unique identifier (115;215;315), and

selectively providing the client (160;260;360) with an access right for the data set (110;210;310), the access right being specific to a registered user that is associated with the authenticator (170;270;370).

4. Server (100;200;300) according to any of the preceding claims,

wherein the server (100;200;300) is configured for registering the authenticator (170;270;370) by associating the authenticator (170;270;370) with an identity information identifying the registered user.

5. Server (100;200;300) according to any of the preceding claims,

wherein the server (100;200;300) comprises an access information, the access information associating the registered user with the access right for the identified data set (110;210;310).

6. Server (100;200;300) according to any of the preceding claims,

wherein the server (100;200;300) is configured for directing the client (160;260;360) requesting access to the server (100;200;300) to the identified data set (110;210;310).

7. Server (100;200;300) according to any of the preceding claims,

wherein the server (100;200;300) is configured for using a cryptographic system for validating the authentication information (172;272;372),

wherein the server (100;200;300) is configured for associating the authenticator (170;270;370) with a cryptographic key that is specific to the authenticator (170;270;370).

8. Device (150;250;350) for obtaining a data set (110;210;310) via a digital communication network (90),

- 5 wherein the device is configured for obtaining an unique identifier (115;215;315) of the data set (110;210;310), the unique identifier (115;215;315) representing a network address for accessing the data set (110;210;310) via the digital communication network (90), wherein the unique identifier (115;215;315) is specific to the data set (110;210;310),
- wherein the device comprises a client (160;260;360) configured for using the unique identifier (115;215;315) for sending a request for accessing the data set (110;210;310) to a server (100;200;300) providing the data set (110;210;310),
- 10 wherein the client (160;260;360) is configured for providing the server (100;200;300) with an authentication information (172;272;372) of an authenticator (170;270;370) for authenticating the client (160;260;360) against the server (100;200;300), wherein the authenticator (170;270;370) is associated with a registered user.
- 15 9. Device (150;250;350) according to claim 8, wherein the device comprises the authenticator (170;270;370).
10. Device (150;250;350) according to claim 8, wherein the device is configured for having access to the authenticator (170;270;370) via a digital interface.
11. Device (150;250;350) according to any of the claims 8-10,
- 20 wherein the device comprises an input interface (380) for receiving an user input (382), and
- wherein the device is configured for selectively providing the authentication information (172;272;372) to the server (100;200;300) in dependence on the user input (382).
- 25 12. Device (150;250;350) according to any of the claims 8-11,
- wherein the device is configured for obtaining a biometric information about a user, and
- wherein the device is configured for selectively providing the authentication information (172;272;372) to the server (100;200;300), if the biometric in-

formation identifies the user as being associated with the authenticator (170;270;370).

13. Device (150;250;350) according to any of the claims 8-12, wherein the device is configured for retrieving the unique identifier (115;215;315) from a graphical pattern representing the unique identifier (115;215;315).

14. Device (150;250;350) according to any of the claims 8-13,
wherein the authenticator (170;270;370) comprises a cryptographic key,
and
wherein the authenticator (170;270;370) is configured for using the cryptographic key for providing the authentication information (172;272;372) to the server (100;200;300).

15. Device (150;250;350) according to any of the claims 8-14,
wherein the authentication information (172;272;372) allows for an anonymized authenticating of the registered user against the server (100;200;300).

16. Server (100;200;300) for providing one or more data sets via a digital communication network (90), wherein the server (100;200;300) is configured for :

associating an unique identifier (115;215;315) with an identified data set (110;210;310), the unique identifier (115;215;315) representing a network address for accessing the identified data set (110;210;310) via the digital communication network (90), wherein the unique identifier (115;215;315) is specific to the identified data set (110;210;310),

validating an authentication information (172;272;372) provided by an authenticator (170;270;370) of a client (160;260;360) requesting access to the server (100;200;300) via the unique identifier (115;215;315), and

selectively providing the client (160;260;360) with an access right for one or more data sets, if the authentication information (172;272;372) identifies the authenticator (170;270;370) as being associated with a registered user,

wherein the authentication information does not comprise a user name, a password and personal data of the registered user so that the authentication information allows for an anonymized authenticating of the registered user against the server.

- 5 17. Server (100;200;300) according to claim 16, wherein the authentication information comprises an encrypted message which has been generated by using the authenticator,

 wherein the authenticator is represented by an information that does not comprise personal data or a hint on personal data of the registered user associated with the authenticator.

10

18. Method (500) for providing one or more data sets via a digital communication network (90), the method comprising:

 associating (501) an unique identifier (115;215;315) with an identified data set (110;210;310), the unique identifier (115;215;315) representing a network address for accessing the identified data set (110;210;310) via the digital communication network (90), wherein the unique identifier (115;215;315) is specific to the identified data set,

15

 validating (502) an authentication information (172;272;372) provided by an authenticator (170;270;370) of a client (160;260;360) requesting access to one or more data sets via the unique identifier (115;215;315), and

20

 selectively providing (503) the client (160;260;360) with an access right to one or more data sets, if the authentication information (172;272;372) identifies the authenticator (170;270;370) as being associated with a registered user.

- 25 19. Method (600) for obtaining a data set (110;210;310) via a digital communication network (90), the method comprising:

 obtaining (601) an unique identifier (115;215;315) of the data set (110;210;310), the unique identifier (115;215;315) representing a network address for accessing the data set (110;210;310) via the digital communication network (90), wherein the unique identifier (115;215;315) is specific to the data set (110;210;310),

30

using (602) the unique identifier (115;215;315) for sending a request for accessing a server (100;200;300) hosting the data set (110;210;310),

providing (603) the server (100;200;300) with an authentication information (172;272;372) of an authenticator (170;270;370) for authenticating the client (160;260;360) against the server (100;200;300), wherein the authenticator (170;270;370) is associated with a registered user.

5

20. A computer program for implementing any of the methods of claims 18 or 19 when being executed on a computer or signal processor.

10