

**CLAIMS**

1. A method for authenticating a client device in a communications network amongst a plurality of communications network access points, including:

providing a first authentication server apparatus for a first communications network and a further authentication server apparatus for each one of a plurality of respective further communications network access points;

storing in a first data store, by the first authentication server apparatus, a client identity data item identifying the client device and an expiry data item identifying an expiry time associated with the client identity data item, and transmitting the client identity data item and the expiry data item to the further authentication server apparatus of each of said further communications network access points;

storing in a further data store, by each further authentication server apparatus, the received client identity data item and expiry data item and deleting the stored client identity data item from the further data store upon expiry of a time period defined by said expiry data item;

receiving, by any given said further authentication server apparatus, a request from said client device for access to the first communications network and, on condition that said client identity data item remains stored in the further data store thereof, authenticating the client device by performing authentication communications with the first authentication server apparatus asynchronously with respect to authentication communications with the client device.

2. A method according to any preceding claim including receiving, by the given further authentication server apparatus, a password from the client device, wherein:

if said client identity data item remains stored in the further data store said authenticating the client device is not conditional upon verification of the password; and

if said client identity data item does not remain stored in the further data store said authenticating the client device is conditional upon verification of the password.

3. A method according to any preceding claim wherein said authenticating the client device includes performing authentication communications according to an AAA (Authentication,

Authorisation and Accounting) protocol or a RADIUS protocol (Remote Authentication Dial In User Service).

4. A method according to claim 3 wherein:

5           said authentication communications with the first authentication server apparatus include transmitting an Access Request communication to the first authentication server apparatus and receiving an Access Accept communication from the first authentication server.

- 10   5. A method according to claim 3 or claim 4 wherein:

          said authentication communications with the first authentication server apparatus include transmitting an Accounting Start communication to the first authentication server apparatus and receiving an Accounting Response communication from the first authentication server.

15

6. A method according to any of claims 3 to 5 wherein:

          said authentication communications with the client device include receiving an Access Request communication from the client device and transmitting an Access Accept communication to the client device.

20

7. A method according to any of claims 3 to 6 wherein:

          said authentication communications with the client device include receiving an Accounting Start communication from the client device and transmitting an Accounting Response communication to the client device.

25

8. A method according to any preceding claim wherein the client identity data item comprises any one or more of: a username; information identifying the client device (e.g. a calling-station-ID).

- 30   9. A method according to any preceding claim wherein the expiry data item comprises any one or more of: a value representing a time or time point; a value representing date; a value representing an interval of time.

10. A method according to claim 9 in which the expiry data item comprises a first time value which defines how much time the further authentication server apparatus must provide for performing the authentication communications with the first authentication server apparatus, asynchronously with respect to authentication communications with the client device.

11. A method according to claim 9 of claim 10 in which the expiry data item comprises a second time value which defines when the further authentication server apparatus must delete the stored client identity data item from the further data store thereof.

12. A method according to claim 11 wherein said deleting includes deleting the stored client identity data item from the further data store upon expiry of a time period defined by either one of, or both of: the first time value; the second time value.

13. A network communications apparatus for authenticating a client device in a communications network amongst a plurality of communications network access points, including:

a first authentication server apparatus for a first communications network arranged in communication with a further authentication server apparatus for each one of a plurality of respective further communications network access points;

a first data store arranged in communication with the first authentication server apparatus arranged for storing a client identity data item identifying the client device and an expiry data item identifying an expiry time associated with the client identity data item, the first authentication server apparatus being arranged to transmit the client identity data item and the expiry data item to the further authentication server apparatus of each of said further communications network access points;

a plurality of further data stores arranged in communication with a respective further authentication server apparatus for storing a client identity data item and an expiry data item transmitted from the first authentication server apparatus, each further authentication server apparatus being arranged for deleting a stored client identity data item from the respective further data store upon expiry of a time period defined by said expiry data item;

wherein each said further authentication server apparatus is operable to receive a request from said client device for access to the first communications network and, on condition that said client identity data item remains stored in the further data store thereof,

to authenticate the client device by performing authentication communications with the first authentication server apparatus asynchronously with respect to authentication communications with the client device.

- 5 14. A network communications apparatus according to claim 13 in which each further authentication server apparatus is arranged to receive a password from the client device, wherein:
  - if said client identity data item remains stored in the further data store said authenticating the client device is not conditional upon verification of the password; and
  - 10 if said client identity data item does not remain stored in the further data store said authenticating the client device is conditional upon verification of the password.
- 15 15. A network communications apparatus according to claim 13 in which said authenticating the client device includes performing authentication communications according to an AAA (Authentication, Authorisation and Accounting) protocol or a RADIUS protocol (Remote Authentication Dial In User Service).
- 20 16. A network communications apparatus according to claim 15 wherein:
  - said authentication communications with the first authentication server apparatus include transmitting an Access Request communication to the first authentication server apparatus and receiving an Access Accept communication from the first authentication server.
- 25 17. A network communications apparatus according to claim 15 or claim 16 wherein:
  - said authentication communications with the first authentication server apparatus include transmitting an Accounting Start communication to the first authentication server apparatus and receiving an Accounting Reponse communication from the first authentication server.
- 30 18. A network communications apparatus according to any of claims 15 to 17 wherein:
  - said authentication communications with the client device includes receiving an Access Request communication from the client device and transmitting an Access Accept communication to the client device.

19. A network communications apparatus according to any of claims 15 to 18 wherein:

said authentication communications with the client device includes receiving an Accounting Start communication from the client device and transmitting an Accounting Response communication to the client device.

20. A network communications apparatus according to any of claims 13 to 19 wherein the client identity data item comprises any one or more of: a username; information identifying the client device (e.g. a calling-station-ID).

21. A network communications apparatus according to any of claims 13 to 20 wherein the expiry data item comprises a first time value which defines how much time the further authentication server apparatus must provide for performing the authentication communications with the first authentication server apparatus, asynchronously with respect to authentication communications with the client device.

22. A network communications apparatus according to any of claims 13 to 21 wherein the expiry data item comprises a second time value which defines when the further authentication server apparatus must delete the stored client identity data item from the further data store thereof.

23. A network communications apparatus according to claim 22 wherein said deleting includes deleting the stored client identity data item from the further data store upon expiry of a time period defined by either one of, or both of: the first time value; the second time value.

24. A network communications apparatus for authenticating a client device in a communications network amongst a plurality of communications network access points, including:

a first authentication server apparatus for a first communications network adapted and arranged for network communication with a further authentication server apparatus for each one of a plurality of respective further communications network access points;

a first data store arranged in network communication with the first authentication server apparatus arranged for storing a client identity data item identifying the client

device and an expiry data item identifying an expiry time associated with the client identity data item for use in deleting the client identity data item from a further data store upon expiry of a time period defined by said expiry data item, the first authentication server apparatus being arranged to transmit the client identity data item and the expiry data item to a said further authentication server apparatus of each of said further communications network access points for storage in a said further data store thereof;

wherein the first authentication server is arranged to authenticate the client device via a said further authentication server apparatus by performing authentication communications with the further authentication server apparatus asynchronously with respect to authentication communications between the client device and the further authentication server while said client identity data item remains stored in the further data store thereof.

25. A network communications apparatus according to claim 24 in which said authenticating the client device includes performing authentication communications according to an AAA (Authentication, Authorisation and Accounting) protocol or a RADIUS protocol (Remote Authentication Dial In User Service).

26. A network communications apparatus according to any of claims 24 to 25 wherein the client identity data item comprises any one or more of: a username; information identifying the client device (e.g. a calling-station-ID).

27. A network communications apparatus according to any of claims 24 to 26 wherein the expiry data item comprises a first time value which defines how much time the further authentication server apparatus must provide for performing the authentication communications with the first authentication server apparatus, asynchronously with respect to authentication communications with the client device.

28. A network communications apparatus according to any of claims 24 to 27 wherein the expiry data item comprises a second time value which defines when the further authentication server apparatus must delete the stored client identity data item from the further data store thereof.

29. A network communications apparatus for authenticating a client device in a communications network amongst a plurality of communications network access points, including:

a first authentication server apparatus for a communications network access point adapted and arranged for network communication with a second authentication server apparatus for a second communications network access point;

a data store arranged in communication with the first authentication server apparatus and arranged for storing a client identity data item identifying the client device and an expiry data item identifying an expiry time associated with the client identity data item, the first authentication server apparatus being arranged for deleting a stored client identity data item from the data store upon expiry of a time period defined by said expiry data item;

the first authentication server apparatus is arranged to receive the client identity data item and the expiry data item transmitted from said second authentication server apparatus for storage in said data store;

wherein the first authentication server is arranged to obtain authentication of the client device via said second authentication server apparatus by performing authentication communications with the second authentication server apparatus asynchronously with respect to authentication communications between the client device and the first authentication server while said client identity data item remains stored in the data store.

30. A network communications apparatus according to claim 29 in which the first authentication server apparatus is arranged to receive a password from the client device, wherein:

if said client identity data item remains stored in the data store said authenticating the client device is not conditional upon verification of the password; and

if said client identity data item does not remain stored in the data store said authenticating the client device is conditional upon verification of the password.

31. A network communications apparatus according to claim 29 or 30 in which said authenticating the client device includes performing authentication communications according to an AAA (Authentication, Authorisation and Accounting) protocol or a RADIUS protocol (Remote Authentication Dial In User Service).

32. A network communications apparatus according to any of claims 29 to 31 wherein the client identity data item comprises any one or more of: a username; information identifying the client device (e.g. a calling-station-ID).

5 33. A network communications apparatus according to any of claims 29 to 32 wherein the expiry data item comprises a first time value which defines how much time the first authentication server apparatus must provide for performing the authentication communications with the second authentication server apparatus, asynchronously with respect to authentication communications with the client device.

10

34. A network communications apparatus according to any of claims 29 to 33 wherein the expiry data item comprises a second time value which defines when the first authentication server apparatus must delete the stored client identity data item from the data store thereof.

15

35. A network communications apparatus according to claim 34 wherein said deleting includes deleting the stored client identity data item from the further data store upon expiry of a time period defined by either one of, or both of: the first time value; the second time value.

20

36. A computer program product, or data carrier/store containing a computer program including instructions executable on a computer(s) to implement the method according to any of claims 1 to 12.

25 37. One or more computers programmed with computer program including instructions arranged, when executed, to implement the method according to any of claims 1 to 12.

38. A network of computers programmed with a computer program including instructions arranged, when executed, to implement the method according to any of claims 1 to 12.

30