

CLAIMS

1. A method, implemented by a computer-Implemented authentication system (104), for authenticating a user (101) attempting to access a target component (114) of a computer system, the method comprising:
 - 5 a) Receiving (S402), from a first user system (102) via a computer network (111), user authentication information and a network address identifying the first user system within the computer network;
 - b) obtaining (S407, S607) at least one data item of contextual information indicative of a property of an environment of a wireless communications device (113) associated with the user authentication information, the wireless communication device and the first user system being different devices;
 - 10 c) authenticating (S403, S409) the user based on at least the user authentication information; and
 - d) subject to successful authentication, granting (S415) access to the target component and maintaining (S411) a data record indicative of a security context comprising the received network address and the received contextual information;
 - 20 wherein the method further comprises:
 - determining (S414), after repeated successful access attempts from one or more recurring network addresses, and with a given recurring set of contextual information, and based on one or more selection criteria, at least one recurrent security context from a plurality of stored data records, each data record being indicative of a stored security context comprising one or more network addresses of a user system and received contextual information associated with said one or more network addresses, and each stored security context having associated with it data about one or more previous occurrences of said stored security context; wherein the recurrent security context comprises one or more recurring network addresses and the recurring contextual information which have repeatedly been associated with successful access attempts; and
 - 25
 - 30

- using (S410, S412) the determined recurrent security context in a subsequent decision whether to grant a subsequent request by said user to access the target component.

- 5 2. A method according to claim 1, wherein the contextual information comprises one or more of a service set identifier of a wireless local network to which the wireless communications device is connected; a service set identifier of a wireless local network (105) detected by the wireless communications device, a network address of a node of a network (112) to which the wireless
10 communications device is connected, geographical coordinates of a current position of the wireless communications device; a public internet protocol address of the wireless communications device.
- 15 3. A method according to any one of the preceding claims, wherein obtaining at least one data item of contextual information comprises causing the wireless communications device to execute a software application configured to cause the wireless communications device to collect (S407) the contextual information and to forward the collected contextual information to the computer-implemented authentication system.
20
- 25 4. A method according to any one of the preceding claims, wherein obtaining at least one data item of contextual information comprises obtaining (S607), from a software application (532) executed on a server computer (531) configured to provide a service to wireless communications devices, a network address from which the wireless communications device has previously accessed said server computer to obtain said service and/or other data indicative of a property of the wireless communications device and/or at least one property of an environment of the wireless communications device.
- 30 5. A method according to any one of the preceding claims wherein authenticating the user comprises:
 - sending (S404), via a communications network (112), challenge data to said wireless communications device;
 - receiving (S408), via the computer network, a one-time passcode
35 from the first user system;

- verifying (S409) the received one-time passcode.

6. A method according to claim 5, further comprising causing the wireless communications device to compute (S406) the passcode from at least the challenge data and a secret key of the wireless communications device.
5
7. A method according to claim 6, wherein verifying the received passcode comprises using the challenge data, the received passcode and a digital key stored by the computer-implemented authentication system and associated with the wireless communications device.
10
8. A method according to any one of the preceding claims, further comprising: if the received network address matches the network address of a previously determined recurrent security context (S410), granting access to the target component without further authentication only if the obtained contextual information corresponds to the contextual information of said previously determined recurrent security context (S412).
15
9. A method according to any one of the preceding claims, further comprising: if the obtained contextual information corresponds to the contextual information of a previously determined recurrent security context, and if the received network address does not match the network address of said previously determined recurrent security context, granting access to the target component only subject to an additional user authentication process.
20
25
10. A data processing system (104) configured to perform the steps of the method defined in any one of claims 1 through 9.
11. A computer program product comprising computer program code adapted to cause a data processing system to perform the steps of the method defined in any one of claims 1 through 9 when said computer program code is executed on said data processing system.
30