Claims:

1. A method, implemented by a computer-implemented authentication system, for authenticating a user attempting to access a target component of a computer system from a first user system, the first user system being connectable to a first communications network, the method comprising:
- receiving user authentication information entered by the user via a first user-interface of the first user system;
- obtaining via the first communications network at least one item of contextual information chosen from information indicative of the first user system or a property of the first communications network and a session identifier;
- verifying the user authentication information, and responsive to successful verification of the user authentication information, sending a message from the computer-implemented authentication system via a second communications network to a second user system, the message comprising at least one item of contextual information or derived information of this collected contextual information, allowing the second user system to present at least the at least one item of contextual information to the user via a second user interface so as to allow the user to verify the at least one item of contextual information, and a real-time session-specific one-time passcode associated with the session idenitifier;
- receiving via the first user system and the first communications network a passcode entered by the user into the first user system;
- verifying the entered passcode against the real-time session-specific one-time passcode and/or the session identifier; and responsive to a successful verification of the entered passcode, granting to the first user system access to the target component.

2. A method according to claim 1 wherein the target component is chosen from a computer, a computer program, computer program functionality, a computer resource, a computer network.

3. A method according to claim 1 or 2, wherein the first and second user systems are different devices.

4. A method according to claim 3, wherein the second user system is a portable communications device configured to receive and display the message.

5. A method according to claim 1 or 2 wherein the first and second user systems are embodied as a single user system adapted to provide the first and second user interfaces, and wherein the method comprises presenting at least the at least one item of contextual information by the single user system via a second user interface of the single user system different from the first user interface

6. A method according to any one of the preceeding claims, wherein the first and second communications networks are different communications networks.

7. A method according to any one of the preceeding claims, further comprising communicating the passcode from the computer-implemented authentication system to the user.

8. A method according to any one of the preceeding claims, further comprising communicating gathered contextual information from the computer-implemented authentication system to the user via a second passcode window displayed by the first user system.

9. A method according to any one of the preceeding claims where the authentication system creates a passcode in real-time that is only valid for the session ID created by the login attempt that invokes the code being created and sent.

10. A computer-implemented authentication system comprising program code means adapted to cause the computer-implemented authentication system to perform the steps of the method according to any one of claim 1 through 9 when the program code means are executed by the computer-implemented authentication system.

11. A computer-implemented authentication system according to claim 10 comprising an authentication server and wherein the program code comprises a login program configured to provide the first user-interface on the first user system.

12. A computer program comprising program code means adapted to cause the data processing system to perform the steps of the method according to any one of claim 1 through 9 when the program code means are executed by the data processing system.

Claims:

1. A method, implemented by a computer-implemented authentication system, for authenticating a user attempting to access a target component of a computer system from a first user system, the first user system being connectable to a first communications network, the method comprising:

receiving, by at least one computing device, user authentication information entered by the user via a first user-interface of the first user system;

obtaining, by the at least one computing device, via the first communications network a session identifier and at least one item of contextual information identifying the first user system or a property of the first communications network;

verifying, by the at least one computing device, the user authentication information, and responsive to successful verification of the user authentication information, sending a message from the computer-implemented authentication system via a second communications network to a second user system, the message comprising

(a) at least one item of said obtained contextual information or derived information of said obtained contextual information, allowing the second user system to present at least the at least one item of contextual information to the user via a second user interface so as to allow the user to verify the at least one item of contextual information, and

(b) a real-time session-specific one-time passcode, different from the at least one item of said obtained contextual information, and associated with the session identifier;

receiving, by the at least one computing device, via the first user system and the first communications network a passcode entered by the user into the first user system;

verifying, by the at least one computing device, the entered passcode against the real-time session-specific one-time passcode and/or the session identifier; and responsive to a successful verification of the entered passcode, granting to the first user system access to the target component.

2. The method according to claim 1 wherein the target component is chosen from a

computer, a computer program, computer program functionality, a computer resource, a computer network.

3. The method according to claim 1, wherein the first and second user systems are different devices.

4. The method according to claim 3, wherein the second user system is a portable communications device configured to receive and display the message.

5. The method according to claim 1 wherein the first and second user systems are embodied as a single user system adapted to provide the first and second user interfaces, and wherein the method comprises presenting at least the at least one item of contextual information by the single user system via a second user interface of the single user system different from the first user interface.

6. The method according to claim 1, wherein the first and second communications networks are different communications networks.

7. The method according to claim 1, further comprising communicating the passcode from the computer-implemented authentication system to the user.

8. The method according to claim 1, further comprising communicating gathered contextual information from the computer-implemented authentication system to the user via a second passcode window displayed by the first user system.

9. The method according to claim 1, wherein the authentication system creates a passcode in real-time that is only valid for the session ID created by the login attempt that invokes the code being created and sent.

10. The method according to claim 1, wherein the at least one item of contextual information comprises a computer identifier of a computer used as the first user system, or approximate regional information about a location of the first user system.

11. A non-transitory computer readable medium encoded with instructions for authenticating a user attempting to access a target component of a computer system from a first user system, the instructions executable by a processor, comprising:

receiving user authentication information entered by the user via a first user-interface of the first user system;

obtaining via the first communications network a session identifier and at least one item of contextual information identifying the first user system or a property of the first communications network;

verifying the user authentication information and, responsive to successful verification of the user authentication information, sending a message from the computer-implemented authentication system via a second communications network to a second user system, the message comprising:

a) at least one item of said obtained contextual information or derived information of said obtained contextual information, allowing the second user system to present at least the at least one item of contextual information to the user via a second user interface so as to allow the user to verify the at least one item of contextual information, and

b) a real-time session-specific onetime passcode, different from the at least one item of said obtained contextual information, and associated with the session identifier;

receiving via the first user system and the first communications network a passcode entered by the user into the first user system; and

verifying the entered passcode against the real-time session-specific one-time passcode and/or the session identifier; and responsive to a successful verification of the entered passcode, granting to the first user system access to the target component.

12. A system for authenticating a user attempting to access a target component of a computer system from a first user system, the first user system being connectable to a first communications network, the system comprising:

a first user system to receive user authentication information entered by the user via a first user-interface of the first user system;

a communications network to obtain a session identifier and at least one item of contextual information identifying the first user system or a property of the first communications network; and

an authentication system comprising at least one microprocessor, the at least one microprocessor to:

verify the user authentication information and, responsive to successful verification of the user authentication information, sending a message from the computer-implemented authentication system via a second communications network to a second user system, the message comprising:

a) at least one item of said obtained contextual information or derived information of said obtained contextual information, allowing the second user system to present at least the at least one item of contextual information to the user via a second user interface so as to allow the user to verify the at least one item of contextual information, and

b) a real-time session-specific onetime passcode, different from the at least one item of said obtained contextual information, and associated with the session identifier;

receive via the first user system and the first communications network a passcode entered by the user into the first user system; and

verify the entered passcode against the real-time session-specific one-time passcode and/or the session identifier; and responsive to a successful verification of the entered passcode, grant to the first user system access to the target component.

13. The system according to claim 12 further comprising an authentication server, and wherein the at least one microprocessor further to provide the first user-interface on the first user system.