CLAIMS:

1. An authentication method of using biometric data relating to a user to provide an encoded or decoded version of an identifier; the method comprising the steps:
   using the biometric data to generate at least one operable keypad and/or at least one keypad image by using the biometric data to specify the order or position of keys in the operable keypad and/or a keypad image; and
   generating a mapping between the operable keypad or keypad image and a further operable keypad and/or image.

2. A method according to claim 1 and further comprising the step:
   generating the biometric data at or on an electronic device.

3. A method according to claim 2 wherein the electronic device is a handheld, portable or mobile computing device.

4. A method according to any preceding claim and comprising the step of:
   using the biometric data to encode the identifier such that the biometric data becomes the key to decode the identifier.

5. A method according to claim any preceding claim and comprising the step:
   wherein the biometric data comprises, or is processed to provide, one or more strings, arrays or sequences of values.

6. A method according to any preceding claim wherein:
   the biometric data is used to specify a keypad configuration.

7. A method according to any preceding claim wherein the method further comprises the step of using the mapping to encode or decode the identifier.

8. A method according to any preceding claim and further comprising the step:
   storing an encoded version of the identifier.

9. A method according to claim 8 wherein:
the encoded version is generated using a keypad configuration specified by the biometric data; and/or
the encoded version of the identifier is stored on a server.

10. A method according to any preceding claim and further comprising the step of:
using at least a portion of the biometric data as input into a subroutine call, wherein the subroutine comprises instructions to generate an operable keypad or a keypad image.

11. A method according to any preceding claim and further comprising the step:
verifying the identifier by comparing it to a previously stored version.

12. A method according to any preceding claim and further comprising the step of:
sending the biometric data, or data derived from the biometric data, from an electronic device operated by the user to a remote computing resource.

13. A method according to Claim 12, wherein sending the biometric data, or data derived from the biometric data, from an electronic device operated by the user to a remote computing resource is to enable an encoded version of the identifier to be decoded using the biometric data or data derived therefrom.

14. An authentication system comprising:
an electronic device operated by a user; and
a remote computing resource;
wherein the system is arranged and configured to provide an encoded or decoded version of an identifier using biometric data relating to a user; by:
using the biometric data to generate at least one operable keypad and/or at least one keypad image by using the biometric data to specify the order or position of keys in the operable keypad and/or a keypad image; and
generating a mapping between the operable keypad or keypad image and a further operable keypad and/or image.

15. A system according to claim 14 wherein;
the biometric data is generated or captured at or on the electronic device.

16. A system according to claim 15 wherein the electronic device is a handheld, portable or mobile computing device.

17. A system according to claims 14 to 16, wherein the system is arranged to:
i) use the biometric data to specify a keypad configuration; and/or
ii) encode the identifier using the biometric data such that the biometric data becomes the key to decode the identifier.

18. A system according to any of claims 14 to 17 wherein the system is arranged and configured to perform the method of any of claims 1 to 13.

19. An authentication method comprising the steps:
capturing biometric data relating to a user;
using the biometric data as input to a software-implemented component which is arranged and configured to use the biometric data to encode an identifier associated with the user such that the biometric data is required to decode the identifier by:
using the biometric data to generate at least one operable keypad and/or at least one keypad image and to specify the order or position of keys in the operable keypad and/or a keypad image; and
generating a mapping between the operable keypad or keypad image and a further operable keypad and/or image.