CLAIMS:

1. An authentication method of encoding and/or decoding an identifier using a scrambled configuration of keys in an operable keypad and/or image of a keypad, comprising the steps:

   using biometric data relating to a user to provide an encoded or decoded version of an identifier by using the biometric data to provide one or more strings, arrays or series of values, each corresponding to a keypad configuration for the creation of a keypad or image of a keypad; and

   using the one or more strings, arrays or series of values as input to a subroutine call, wherein the subroutine comprises instructions to generate the operable keypad and/or the keypad image; and the biometric data determines or is used to supply a scrambled configuration of keys in the operable keypad and/or a scrambled configuration of keys depicted in the keypad 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 claims 1, 2 or 3 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 any preceding claim, wherein:
   the subroutine forms part of a keypad generation component arranged to generate the at least one keypad and/or keypad image on or at an electronic device operated by the user.

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

7. A method according to claim 6, 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.

8. A method according to any preceding claim and comprising the step:
generating at least one operable keypad and at least one keypad image, wherein:
the configuration of keys in the operable keypad is different relative to the configuration of keys depicted in the keypad image.

9. A method according to any preceding claim and comprising the step of:
using the biometric data to compute a decoded version of the encoded identifier,
wherein the decoding step is performed as part of an authentication session initiated when the user wishes to gain access to a controlled resource or service, or perform a transaction.

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

11. 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.

12. A method according to claim 11 wherein:
the biometric data is sent to the remote computing resource to enable an encoded version of the identifier to be decoded using the biometric data or data derived therefrom.

13. A method according to any preceding claim, wherein:
the order of keys in the scrambled configuration of keys in the operable keypad and/or

the scrambled configuration of keys depicted in the keypad image is scrambled relative to a default or reference keypad configuration.

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 use biometric data relating to a user to provide an encoded or decoded version of an identifier by:

using the biometric data to provide one or more strings, arrays or series of values, each corresponding to a keypad configuration for the creation of a keypad or image of a keypad; and

using the one or more strings, arrays or series of values as input to a subroutine call, wherein the subroutine comprises instructions to generate the operable keypad and/or the keypad image; such that the biometric data determines or is used to supply a scrambled configuration of keys in the operable keypad and/or a scrambled configuration of keys depicted in the keypad 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 claim 14, 15 or 16 , wherein the system is arranged to:

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 .