WE CLAIM:

1. A trusted device comprising:

authentication circuitry configured to authenticate with an authentication operation a user having physical possession of said trusted device and thereby switch said trusted device to an authenticated state;

retention monitoring circuitry configured to monitor physical possession of said trusted device by said user following said authentication operation and to switch said trusted device out of said authenticated state if said trusted device is not in physical possession of said user;

communication triggering circuitry configured to detect a request to establish communication received from a target device that is one of a plurality of different target devices; and

communication circuitry configured to communicate with said target device if said trusted device is in said authenticated state.

2. A trusted device as claimed in claim 1, wherein said communication with said target device includes presentation to said target device of credentials including one or more of: an application-program-interface key, a digital certificate, a user identity, a password and cryptographically signed data.

3. A trusted device as claimed in any one of claims 1 and 2, wherein communication with said target device includes creation of credentials usable in subsequent authentications.

4. A trusted device as claimed in any one of claims 1, 2 and 3, wherein said communication with said target device includes the transfer of information including at least one of configuration data, personalisation preferences, network settings, contracts, receipts, computer programs, data logs, transaction records and credentials.

5. A trusted device as claimed in claim 2, wherein said trusted device automatically selects which credentials to use.

6. A trusted device as claimed in claim 4, wherein said trusted device automatically selects which information to use.

7. A trusted device as claimed in claims 5 or 6, wherein automatic selection criteria used in said automatic selection are subject to user configuration.

8. A trusted device as claimed in claims 5 or 6, wherein said trust device permits a user to manually alter a selection that has been made automatically.

9. A trusted device as claimed in any one of the preceding claims, wherein said retention monitoring circuitry includes one or more detection circuits comprising at least one of:

a clasp configured to hold said trusted device attached to said user when said clasp is in a closed state, said retention monitoring circuitry switching said trusted device out of said authenticated state if said clasp changes out of said closed state;

contact detecting circuitry configured to detect contact between said trusted device and said user using one of more of: electrical signals detected from said user; temperature of a contact area between said trusted device and said user;

proximity detecting circuitry configured to detect proximity said trusted device and a proximity device worn by said user;

a photo-detector shielded from light when said trusted device is physical possession of said user;

a chemical detector configured to detect a chemical characteristic of said user;

biometric detector circuitry configured to recognise one or more biometric characteristics of said user;

a motion sensor configured to detect motion of said trusted device as said user moves while said trusted device is in physical possession of said trusted device;

implant detection circuitry configured to detect proximity of an implant within said user; and

heat flux detection circuitry having a plurality of temperature sensors and configured to detect heat flux through said trusted device.

10. A trusted device as claimed in claim 9, wherein retention monitoring circuitry comprises a plurality of detection circuits and is configured to combine detection results from said plurality of detection circuits to determine a retention probability that said trusted device is in physical possession of said user and to switch said trusted device out of said authenticated state if said retention probability falls below a threshold probability level.

11. A trusted device as claimed in claim 10, wherein said retention monitoring circuitry is configured to reduce said retention probability as a time since said authentication operation increases.

12. A trusted device as claimed in any one of the preceding claims, wherein said authentication circuitry comprises at least one of:

biometric recognition circuitry configured to recognise one or more biometric characteristics of said user;

fingerprint recognition circuitry configured to recognise a fingerprint of said user;

face recognition circuitry configured to recognise a face of said user;

chemical recognition circuitry configured to recognise one or more chemical characteristics of said user;

ECG recognition circuitry configured to recognise ECG signals of said user;

bioimpedance circuitry configured to recognise one or more bioimpedance characteristics of said user;

gait recognition circuitry configured to recognise a gait of said user; and

implant recognition circuitry configured to recognise an implant within said user.

13. A trusted device as claimed in claim 12, wherein said authentication circuitry is configured accept an authentication operation with an accepted probability of a false positive in identifying said user and said accepted probability increases as a time since a previous positive authentication operation decreases.

14. A trusted device as claimed in any one of claims 12 and 13, wherein said retention monitoring circuitry generates a retention probability to indicate a

probability that said trusted device has remained in physical possession of said user since a previous positive authentication operation, said authentication circuitry is configured accept an authentication operation with an accepted probability of a false positive in identifying said user and said accepted probability decreases as a retention probability increases.

15. A trusted device as claimed in any one of the preceding claims, wherein said communication triggering circuitry is configured to trigger communication with said target device in response to at least one of:

detection of a distance of less than a threshold distance between said target device and said trusted device;

detection of said user touching said target device;

receipt of a message specifying said target device;

said user selecting said target device from a list of devices.

16. A trusted device as claimed in any one of the preceding claims, wherein said communication circuitry is configured to communicate with said target device independently of availability of communication between said trusted device and any other device.

17. A trusted device as claimed in any one of the preceding claims, wherein said communication circuitry is configured to communicate with said target device independently of availability of communication between said target device and any other device.

18. A trusted device as claimed in any one of the preceding claims, wherein said communication circuitry is configured to provide bi-directional communication between said trusted device and said target device.

19. A trusted device as claimed in any one of the preceding claims, further comprising a display configured to display information from said target device.

20. A trusted device as claimed in any one of the preceding claims, wherein said communication circuitry is configured to receive information from said target device

and further comprising target authentication circuitry configured to authenticate said target device using said information received from said target device.

21. A trusted device as claimed in any one of the preceding claims, wherein said communication circuitry includes confirmation circuitry configured to require receipt of a confirmation input from said user before permitting communication with said target device.

22. A trusted device as claimed in any one of the preceding claims, wherein said trusted device is at least one of:

a wearable device; and

a wrist watch.

23. A trusted device as claimed in any one of the preceding claims, comprising identity storage circuitry configured to store identity data for use in said communication using said authenticated identity, said identity data comprising one of more public identity identifiers each having associated secret data.

24. A trusted device as claimed in any one of the preceding claims, wherein said target device communicates with one or more levels of further devices.

25. A trusted device as claimed in 24, wherein said communication with said one or more levels of further devices uses credentials stored in said trusted devices.

26. A trusted device as claimed in claim 25, wherein a maximum permitted number of levels of said one or more further devices is a function of one or more of:

a credential used; and

a user input to said trusted device.

27. A trusted device comprising:

authentication means for authenticating with an authentication operation a user having physical possession of said trusted device and thereby switch said trusted device to an authenticated state;

retention monitoring means for monitoring physical possession of said trusted device by said user following said authentication operation and for switching said trusted device out of said authenticated state if said trusted device is not in physical possession of said user;

communication triggering means for detecting a request to establish communication received from a target device that is one of a plurality of different target devices; and

communication means for communicating with said target device if said trusted device is in said authenticated state.

28. A method of trusted processing comprising the steps of:

authenticating with an authentication operation a user having physical possession of said trusted device and thereby switch said trusted device to an authenticated state;

monitoring physical possession of said trusted device by said user following said authentication operation and switching said trusted device out of said authenticated state if said trusted device is not in physical possession of said user;

detecting a request to establish communication received from a target device that is one of a plurality of different target devices; and

communicating with said target device if said trusted device is in said authenticated state.

CLAIMS

We claim:

1. A trusted device comprising:

authentication circuitry configured to authenticate with an authentication operation a user having physical possession of said trusted device and thereby switch said trusted device to an authenticated state;

retention monitoring circuitry configured to monitor physical possession of said trusted device by said user following said authentication operation and to switch said trusted device out of said authenticated state if said trusted device is not in physical possession of said user;

communication triggering circuitry configured to detect a request to establish communication received from a target device that is one of a plurality of different target devices; and communication circuitry configured to communicate with said target device if said trusted device is in said authenticated state.

2. The trusted device as claimed in claim 1, wherein said communication with said target device includes presentation to said target device of credentials including one or more of: an application-program-interface key, a digital certificate, a user identity, a password and cryptographically signed data.

3. The trusted device as claimed in claim 2, wherein said trusted device automatically selects which credentials to use.

4. The trusted device as claimed in claim 3, wherein automatic selection criteria used in said automatic selection are subject to user configuration.

5. The trusted device as claim 3, wherein said trust device permits a user to manually alter a selection that has been made automatically.

6. The trusted device as claimed in claim 1, wherein communication with said target device includes creation of credentials usable in subsequent authentications.

7. The trusted device as claimed in claim 1, wherein said communication with said target device includes the transfer of information including at least one of configuration data, personalisation preferences, network settings, contracts, receipts, computer programs, data logs, transaction records and credentials.

8. The trusted device as claimed in claim 7, wherein said trusted device automatically selects which information to use.

9. The trusted device as claimed in claim 1, wherein said retention monitoring circuitry includes one or more detection circuits comprising at least one of: a clasp configured to hold said trusted device attached to said user when said clasp is in a closed state, said retention monitoring circuitry switching said trusted device out of said authenticated state if said clasp changes out of said closed state; contact detecting circuitry configured to detect contact between said trusted device and said user using one of more of: electrical signals detected from said user; temperature of a contact area between said trusted device and said user; proximity detecting circuitry configured to detect proximity said trusted device and a proximity device worn by said user; a photo-detector shielded from light when said trusted device is physical possession of said user; a chemical detector configured to detect a chemical characteristic of said user; biometric detector circuitry configured to recognise one or more biometric characteristics of said user; a motion sensor configured to detect motion of said trusted device as said user moves while said trusted device is in physical possession of said trusted device; implant detection circuitry configured to detect proximity of an implant within said user; and heat flux detection circuitry having a plurality of temperature sensors and configured to detect heat flux through said trusted device.

10. The trusted device as claimed in claim 9, wherein retention monitoring circuitry comprises a plurality of detection circuits and is configured to combine detection results from said plurality of detection circuits to determine a retention probability that said trusted device is in physical possession of said user and to switch said trusted device out of said authenticated state if said retention probability falls below a threshold probability level.

11. The trusted device as claimed in claim 10, wherein said retention monitoring circuitry is configured to reduce said retention probability as a time since said authentication operation increases.

12. The trusted device as claimed in claim 1, wherein said authentication circuitry comprises at least one of: biometric recognition circuitry configured to recognise one or more biometric characteristics of said user; fingerprint recognition circuitry configured to recognise a fingerprint of said user; face recognition circuitry configured to recognise a face of said user; chemical recognition circuitry configured to recognise one or more chemical characteristics of said user; ECG recognition circuitry configured to recognise ECG signals of said user; bioimpedance circuitry configured to recognise one or more bioimpedance characteristics of said user; gait recognition circuitry configured to recognise a gait of said user; and implant recognition circuitry configured to recognise an implant within said user.

13. The trusted device as claimed in claim 12, wherein said authentication circuitry is configured accept an authentication operation with an accepted probability of a false positive in identifying said user and said accepted probability increases as a time since a previous positive authentication operation decreases.

14. The trusted device as claimed in claim 12, wherein said retention monitoring circuitry generates a retention probability to indicate a probability that said trusted device has remained in physical possession of said user since a previous positive authentication operation, said authentication circuitry is configured accept an authentication operation with an accepted probability of a false positive in identifying said user and said accepted probability decreases as a retention probability increases.

15. The trusted device as claimed in claim 1, wherein said communication triggering circuitry is configured to trigger communication with said target device in response to at least one of: detection of a distance of less than a threshold distance between said target device and said trusted device; detection of said user touching said target device; receipt of a message specifying said target device; said user selecting said target device from a list of devices.

16. The trusted device as claimed in claim 1, wherein said communication circuitry is configured to communicate with said target device independently of availability of communication between said trusted device and any other device.

17. The trusted device as claimed in claim 1, wherein said communication circuitry is configured to communicate with said target device independently of availability of communication between said target device and any other device.

18. The trusted device as claimed in claim 1, wherein said communication circuitry is configured to provide bi-directional communication between said trusted device and said target device.

19. The trusted device as claimed in claim 1, further comprising a display configured to display information from said target device.

20. The trusted device as claimed in claim 1, wherein said communication circuitry is configured to receive information from said target device and further comprising target authentication circuitry configured to authenticate said target device using said information received from said target device.

21. The trusted device as claimed in claim 1, wherein said communication circuitry includes confirmation circuitry configured to require receipt of a confirmation input from said user before permitting communication with said target device.

22. The trusted device as claimed in claim 1, wherein said trusted device is at least one of: a wearable device; and a wrist watch.

23. The trusted device as claimed in claim 1, comprising identity storage circuitry configured to store identity data for use in said communication using said authenticated identity, said identity data comprising one of more public identity identifiers each having associated secret data.

24. The trusted device as claimed in claim 1, wherein said target device communicates with one or more levels of further devices.

25. The trusted device as claimed in 24, wherein said communication with said one or more levels of further devices uses credentials stored in said trusted devices.

26. The trusted device as claimed in claim 25, wherein a maximum permitted number of levels of said one or more further devices is a function of one or more of: a credential used; and a user input to said trusted device.

27. The trusted device as claimed in claim 1 comprising a data store configured to store identity data for each of a plurality of identities for a said user of the trusted device, wherein said identity data is for use in said communication using said authenticated identity.

28. The trusted device as claimed in claim 27 wherein after said authentication operation, said communication with said target device comprises: presenting said user with the stored identity data for each of the plurality of identities for selection, and using the selected identity data to control the identity data that is sent to said target device.

29. A trusted device comprising:

authentication means for authenticating with an authentication operation a user having physical possession of said trusted device and thereby switch said trusted device to an authenticated state;

retention monitoring means for monitoring physical possession of said trusted device by said user following said authentication operation and for switching said trusted device out of said authenticated state if said trusted device is not in physical possession of said user; communication triggering means for detecting a request to establish communication received from a target device that is one of a plurality of different target devices; and communication means for communicating with said target device if said trusted device is in said authenticated state.

30. A method of trusted processing comprising the steps of:

authenticating, using authentication circuitry, with an authentication operation a user having physical possession of said trusted device and thereby switch said trusted device to an authenticated state;

monitoring, using retention monitoring circuitry, physical possession of said trusted device by said user following said authentication operation and switching said trusted device out of said authenticated state if said trusted device is not in physical possession of said user;

detecting, using communication triggering circuitry, a request to establish communication received from a target device that is one of a plurality of different target devices; and communicating, using communication circuitry, with said target device if said trusted device is in said authenticated state.