16. The method as claimed in any one of claims 11 to 15, wherein the second source is a centralised management server that stores a plurality of second secret keys for a plurality of apparatuses.

17. The method as claimed in any preceding claim, wherein the first and second apparatuses are Bluetooth enabled apparatus, and the secure wireless connection is a secure Bluetooth connection.

18. An apparatus, comprising:

a memory, the memory comprising a first partial link key;

a user input module for receiving a first secret key from a user;

a first communications module for receiving a second secret key from a second source; and

a link key generator for generating a first link key based upon the stored first partial link key, the first secret key and the second secret key or a second link key based upon the stored first partial link key and the first secret key;

a secure wireless communications module for establishing a secure wireless connection with a second apparatus using either the first link key or the second link key, wherein in use, if the first link key is used to establish the wireless connection with the second apparatus, the first apparatus is granted a first level of access to the second apparatus, and if the second link key is used to establish the wireless connection with the second apparatus, the first apparatus is granted a second level of access to the second apparatus, the second level of access having less access than the first level of access.

19. The apparatus as claimed in claim 18, wherein the user input module is a keypad.

20. The apparatus as claimed in claim 18, wherein the first communications module receives the second secret key over a wired communications link.

21. The apparatus as claimed in claim 18, wherein the second source is a supervisor apparatus and the first communications module receives the second secret key over a near field or short range wireless communications link from thea supervisor apparatus when the apparatus is within a first communication range of the supervisor apparatus.

22. The apparatus as claimed in claim 18, wherein the second source is a supervisor apparatus and when the apparatus is no longer within a first communication range of thea supervisor apparatus, the apparatus is configured to tear down a secure wireless communications link established using the first link key.

23. The apparatus as claimed in claim 21 or 22, wherein the first communications module receives the second secret key over a secure wireless communications link.

24. The apparatus as claimed in claim 18, wherein the first communications module is a wireless communications module configured for communicating over a mobile phone or long range radio communications protocol with the second source.

25. The apparatus as claimed in claim 24, wherein the apparatus further comprises a location estimator module, and wherein the apparatus is configured to send a location estimate of the first apparatus to the second source over a wireless communication link between the first apparatus and the second source.

26. The apparatus as claimed in 25, wherein the apparatus further receives an approved area with the second secret key, and the apparatus is configured to tear down a secure wireless connection between the apparatus and the second apparatus established using the first link key when the location estimate of the apparatus is no longer within the approved area.

27. The apparatus as claimed in claim 25, wherein a secure wireless connection established between the apparatus and the second apparatus established using the first link key is only maintained whilst a wireless connection is maintained between the apparatus and the second source, and the apparatus is configured to tear down the secure wireless connection in response to a command from the second source received over the wireless connection.

28. The apparatus as claimed in any one of claims 18 to 27, wherein the first communications module comprises the secure wireless communications module.

29. The apparatus as claimed in any one of claims 18 to 28, wherein the secure wireless communications module is a Bluetooth enabled communications module and the secure wireless connection is a secure Bluetooth connection.

30. An apparatus, comprising:

a memory, the memory comprising at least a first link key and a second link key;

a wireless communications module for establishing a secure wireless connection with a second apparatus using either the first link key or the second link key;

an access control module for granting access to the one or more functions or resources of the apparatus to the second apparatus, wherein the access control module grants a first level of access to the second ~~Bluetooth enabled~~ apparatus if the secure wireless connection was established with first link key value, and grants a second level of access if the secure wireless connection was established with second link key value, the second level of access having less access than the first level of access, wherein in use, the first link key is generated in the second apparatus based upon a stored partial link key, a first secret key received from a first source and a second secret key received from a second source, and the second link key value is generated using the stored partial link key and the first secret key received from the first source.

31. The apparatus as claimed in claim 30, wherein the apparatus is a weapon, and the one or more functions or resources comprise firing the weapon.

32. The apparatus as claimed in claims 30 or 31, wherein the wireless communications module is a Bluetooth enabled communications module, and the secure wireless connection is a secure Bluetooth connection.

33. A supervisor apparatus, comprising:

a memory, the memory for storing a secret key;

a communications module for establishing a communication link with a first apparatus, and providing the secret key to the first apparatus for use in generating a link key for generating a secure wireless connection with a second apparatus, wherein in use, the first apparatus generates the link key using a stored partial link key, a first secret key from a first source and the secret key provided by the supervisor apparatus, and the first apparatus is granted a first level of access to the second apparatus if the generated link key is used to establish the secure wireless communications link between the first apparatus and the second apparatus, and if the first apparatus generates the link key using the stored partial link key and the first secret key the first apparatus is granted a second level of access to the second apparatus, the second level of access having less access than the first level of access.

34. The supervisor apparatus as claimed in claim 33, further comprising:

a user input module for receiving the secret key from a user.

35. The supervisor apparatus as claimed in claim 33, wherein the apparatus is a portable apparatus.

36. The supervisor apparatus as claimed in claim 33, wherein the apparatus is mounted in a fixed location.

37. The supervisor apparatus as claimed in claim 33, wherein the communications module provides the secret key to the first apparatus over a wired connection.

38. The supervisor apparatus as claimed in claim 33, wherein the communications module provides the secret key to the first apparatus using a near field or short range communications protocol.

39. The supervisor apparatus as claimed in claim 33, wherein the communications module provides the secret key to the first apparatus over a secure wireless connection.

40. The supervisor apparatus as claimed in claim 33, wherein the memory stores an approved area for use of the secret key, and further comprising a location verification module that is configured to receive a location estimate of the first apparatus and the secret key is only sent to the first apparatus if the location estimate of the first apparatus is within the approved area.

41. The supervisor apparatus as claimed in claim 40, wherein the location estimate is a location estimate received from the first apparatus via the communications module.

42. The supervisor apparatus as claimed in claim 40, wherein the memory stores a plurality of approved areas and a plurality of second secret keys, and each of the plurality of second secret keys is associated with at least one of the approved areas, and the location verification module is configured such