

**Claims**

1. A device pairing method comprising:
- generating, using a server, a user pairing identifier corresponding to a user profile;
- 5 sending, using the server, the generated user pairing identifier for use by a first user device of the user profile to pair a second user device with the user profile; and
- receiving, using the server, device information of the second user device.
- 10 2. The device pairing method of claim 1, further comprising:
- sending, using the first user device, the user pairing identifier to the second user device for replacement of a current pairing identifier of the second user device.
- 15 3. The device pairing method of claim 2, further comprising:
- sending, using the first user device, a signal to the second user device to cause the second user device to erase user related data of the second user device if the replaced current pairing identifier represents a non-default pairing identifier and is different from the user pairing identifier.
- 20 4. The device pairing method of any one of claims 1 to 3, further comprising:
- enabling communication of the first user device with the second user device if the first user device satisfies a predetermined condition relating to at least one of a geographic location and a time period.
- 25 5. The device pairing method of any one of claims 1 to 4, further comprising:
- sending, using the second user device to the first user device, a random number and an associated key identifier,
- receiving, using the second user device from the first user device, a
- 30 response hash-based message authentication code (HMAC) value,

computing, using the second user device, a verification HMAC value with the random number and one of a plurality of cryptographic keys of the second user device identified by the key identifier, and

controlling, using the second user device, communication of the second  
5 user device with the first user device based on a result of comparison of the response and verification HMAC values.

6. The device pairing method of claim 5, wherein the second user device is controlled to disconnect an existing connection with the first user device if the  
10 result of comparison indicates that the response and verification HMAC values do not match.

7. The device pairing method of claim 5 or 6, wherein the second user device is controlled to disregard communication from the first user device if the result of  
15 comparison indicates that the response and verification HMAC values do not match.

8. The device pairing method of any one of claims 5 to 7, further comprising:  
generating, using the second user device, the random number.  
20

9. The device pairing method of any one of claims 5 to 8, further comprising:  
generating, using the first user device, the response HMAC value with the random number and one of a plurality of cryptographic keys of the first user device identified by the key identifier.  
25

10. The device pairing method of any one of claims 1 to 9, wherein the user pairing identifier includes a unique combination of at least one of a number, an alphabet, and a character.

11. The device pairing method of any one of claims 1 to 10, wherein the server sends the generated user pairing identifier through the Internet.
12. The device pairing method of any one of claims 1 to 11, wherein the device  
5 information is received by the server from the first user device.
13. The device pairing method of claim 12, wherein the device information includes a serial number.
- 10 14. A device pairing system comprising:  
a server configured to:  
generating a user pairing identifier corresponding to a user profile;  
sending the generated user pairing identifier for use by a first user  
device of the user profile to pair a second user device with the user profile; and  
15 receiving device information of the second user device.
15. The device pairing system of claim 14, further comprising:  
the first user device.
- 20 16. The device pairing system of claim 15, wherein the first user device is configured to:  
send the user pairing identifier to the second user device for replacement  
of a current pairing identifier of the second user device.
- 25 17. The device pairing system of claim 16, wherein the first user device is further configured to:  
send a signal to the second user device to cause the second user device  
to erase user related data of the second user device if the replaced current  
pairing identifier represents a non-default pairing identifier and is different from  
30 the user pairing identifier.

18. The device pairing system of any one of claims 15 to 17, wherein communication of the first user device with the second user device is enabled if the first user device satisfies a predetermined condition relating to at least one  
5 of a geographic location and a time period.

19. The device pairing system of any one of claims 14 to 18, further comprising:  
the second user device.

10 20. The device pairing system of claim 19, wherein the second user device is configured to:

send, to the first user device, a random number and an associated key identifier,

15 receive, from the first user device, a response hash-based message authentication code (HMAC) value,

compute a verification HMAC value with the random number and one of a plurality of cryptographic keys of the second user device identified by the key identifier, and

20 control communication of the second user device with the first user device based on a result of comparison of the response and verification HMAC values.

21. The device pairing system of claim 20, wherein the second user device is controlled to disconnect an existing connection with the first user device if the  
25 result of comparison indicates that the response and verification HMAC values do not match.

22. The device pairing system of claim 20 or 21, wherein the second user device is controlled to disregard communication from the first user device if the

result of comparison indicates that the response and verification HMAC values do not match.

23. The device pairing system of any one of claims 20 to 22, wherein the  
5 second user device is further configured to:  
generate the random number.

24. The device pairing system of any one of claims 20 to 23 when dependent on  
claim 15, wherein the first user device is configured to generate the response  
10 HMAC value with the random number and one of a plurality of cryptographic  
keys of the first user device identified by the key identifier.

25. The device pairing system of any one of claims 14 to 24, wherein the user  
pairing identifier includes a unique combination of at least one of a number, an  
15 alphabet, and a character.

26. The device pairing system of any one of claims 14 to 25, wherein the server  
sends the generated user pairing identifier through the Internet.

20 27. The device pairing system of any one of claims 14 to 26, wherein the device  
information is received by the server from the first user device.

28. The device pairing system of claim 27, wherein the device information  
includes a serial number.

25

29. A device pairing method comprising:

using, by a user device, an associated user pairing identifier to pair  
another user device with a user profile of the user pairing identifier, the user  
pairing identifier being generated by a server.

30

30. A device communication control method comprising:
- sending, using a challenging computing device to a responding computing device, a random number and an associated key identifier;
  - receiving, using the challenging computing device from the responding computing device, a response hash-based message authentication code (HMAC) value;
  - computing, using the challenging computing device, a verification HMAC value with the random number and one of a plurality of cryptographic keys of the challenging computing device identified by the key identifier; and
  - controlling, using the challenging computing device, communication of the challenging computing device with the responding computing device based on a result of comparison of the response and verification HMAC values.
31. A device pairing system comprising:
- a user device configured to:
    - use an associated user pairing identifier to pair another user device with a user profile of the user pairing identifier, the user pairing identifier being generated by a server.
32. A device communication control system comprising:
- a challenging computing device configured to:
    - send, to a responding computing device, a random number and an associated key identifier,
    - receive, from the responding computing device, a response hash-based message authentication code (HMAC) value,
    - compute a verification HMAC value with the random number and one of a plurality of cryptographic keys of the challenging computing device identified by the key identifier, and

control communication of the challenging computing device with the responding computing device based on a result of comparison of the response and verification HMAC values.

5 33. A device pairing method comprising:

sending, using a server, a user pairing identifier for use by a first user device of the user profile to pair a second user device with the user profile, the user pairing identifier being generated independent of the first user device the and second user device; and

10 receiving, using the server, device information of the second user device.

34. A device pairing method comprising:

using, by a user device, an associated user pairing identifier to pair another user device with a user profile of the user pairing identifier, the user pairing identifier being generated independent of the user device and the another user device.

15

35. A device pairing method comprising:

sending, using a first user device, a signal to a second user device to cause the second user device to erase user related data of the second user device if a current pairing identifier of the second user device represents a non-default pairing identifier and is different from a user pairing identifier, the user pairing identifier being generated by a server.

20

25 36. A device pairing method comprising:

sending, using a first user device, a signal to a second user device to cause the second user device to erase user related data of the second user device if a current pairing identifier of the second user device represents a non-default pairing identifier and is different from a user pairing identifier, the user

pairing identifier being generated independent of the first user device and the second user device.