

WHAT IS CLAIMED IS:

1 1. A method comprising:
2 receiving, by a primary device, credential data of a secondary device;
3 generating, by the primary device, a cryptogram using the credential
4 data of the secondary device; and
5 transmitting, by the primary device, the cryptogram to an access device
6 to request for authorization to use an account associated with a user of the primary
7 device, wherein the authorization is granted based on verification of the cryptogram
8 and an interaction activity pattern of interactions between the primary device and a
9 set of communication devices of the user including the secondary device.

1 2. The method of claim 1, further comprising:
2 for each communication device in the set of communication devices:
3 establishing, by the primary device, a communication channel
4 between the primary device and the communication device;
5 receiving, by the primary device, device data from the
6 communication device including at least one of a device identifier identifying
7 the communication device, sensor data sensed by the communication device,
8 or user data captured by the communication device; and
9 sending, by the primary device, the device data received from
10 the communication device to an authorization server, wherein the device data
11 is used for establishing the interaction activity pattern.

1 3. The method of claim 2, wherein the interaction activity pattern is
2 established further based on a time of day of when the primary device interacted with
3 each communication device.

1 4. The method of claim 2, wherein the authorization is granted
2 based on a comparison of the interaction activity pattern with recent interactions
3 between the primary device and one or more of the communication devices.

1 5. The method of claim 1, wherein the credential data of the
2 secondary device includes a device identifier of the secondary device, and the
3 method further comprises:

1 17. The method of claim 16, wherein the cryptogram is generated by
2 encrypting the second intermediate cryptogram using the first intermediate key,
3 decrypting the encrypted second intermediate cryptogram using the second
4 intermediate key, and re-encrypting the decrypted second intermediate cryptogram
5 using the first portion of the cryptogram key.

1 18. The method of claim 1, wherein the request for authorization is
2 initiated from a tertiary device acting as a user interface device that is
3 communicatively coupled to the primary device.

1 19. A communication device comprising:
2 a processor; and
3 a memory storing computer readable instructions, which when
4 executed by the processor, cause the communication device to implement the
5 method of any of claims 1-18.

1 20. The communication device of claim 19, wherein the
2 communication device is a portable communication device or a network-connected
3 communication device.