

WHAT IS CLAIMED IS:

1. A method comprising:

receiving, by a resource provider computer that is a merchant computer from a first user device that is an appliance configured to initiate a payment transaction and is not configured to store payment credential information for processing the

5 payment transaction and is not configured with an interface to receive an authentication input from a user, a transaction request comprising a device credential or a token, wherein the device credential or the token is previously associated with a second user device based on an enrollment process with an enrollment module, wherein the first user device is associated with the user;

10 retrieving, from a mapping stored in a memory of the resource provider computer, an association between the device credential or token and the second user device, wherein the mapping indicates an association between payment credentials or tokens and a plurality of user devices, and wherein the mapping identifies a user device configured to act as an authenticating device;

15 identifying, by the resource provider computer, the second user device associated with the device credential or the token in the transaction request from the first user device based on the retrieved mapping, wherein the second user device acts as an authenticating device for the first user device according to the mapping to perform the authentication with the resource provider computer for the transaction request
20 received from the first user device, wherein the first user device and second user device are associated with a same payment credential or token;

based on the second user device associated with the device credential or token being identified based on the retrieved mapping, transmitting, by the resource provider computer to the second user device, an authentication request to authenticate
25 the resource provider computer with the first user device;

receiving, by the resource provider computer from the second user device, an authentication response, the authentication response comprising an indication that the first user device is authenticated;

transmitting, by the resource provider computer, an authorization request message to an authorizing entity computer in response to receiving the indication that the first user device is authenticated;

receiving an authorization response message authorizing the transaction request; and

receiving from the first user device a subsequent transaction request, authenticating the subsequent transaction request without requiring authentication with the second user device.

2. The method of claim 1, wherein the device credential is an identifier for the second user device.

3. The method of claim 1, wherein the resource provider computer receives the device credential associated with the user from the first user device, and the method further comprises:

obtaining, by the resource provider computer from a token provider computer, the token corresponding to the device credential and a cryptogram; and generating, by the resource provider computer, the authorization request message to include the token and the cryptogram, and exclude the device credential.

4. The method of claim 3, wherein the cryptogram includes data about an authentication method used in the authentication request.

5. The method of claim 1, wherein the authorization request message further includes a first identifier for the first user device and a second identifier for the second user device, wherein transmitting the authorization request message causes the authorizing entity computer to maintain an association between the payment credential, the first identifier for the first user device, and the second identifier for the second user device, the association allowing subsequent transactions initiated by the first user device to be conducted.

6. The method of claim 1, wherein prior to receiving the transaction request from the first user device, the method comprises:

receiving, by the resource provider computer, a first identifier of the first user device and a second identifier of the second user device;

associating, by the resource provider computer, the first user device with the second user device; and

storing, by the resource provider computer, the first identifier of the first user device with the second identifier of the second user device in a database.

7. The method of claim 6, wherein identifying the second user device comprises retrieving the identifier of the second user device from the database.

8. The method of claim 1, wherein the first user device does not have a user interface that includes an alphanumeric key pad.

9. The method of claim 1, wherein the authentication request includes a biometric authentication request.

10. The method of claim 1, wherein the first user device is a household appliance and the second user device is a mobile phone.

11. A resource provider computer comprising:
one or more processors; and
one or more computer-readable media comprising code, when executed
by the one or more processors, cause the resource provider computer to perform a
5 method comprising:
receiving, by the resource provider computer that is a merchant computer
from a first user device that is an appliance configured to initiate a payment transaction
and is not configured to store payment credential information for processing the
payment transaction and is not configured with an interface to receive an authentication
10 input from a user, a transaction request comprising a device credential or a token,
wherein the device credential or the token is previously associated with a second user
device based on an enrollment process with an enrollment module, wherein the first
user device is associated with the user;
retrieving, from a mapping stored in a memory of the resource provider
15 computer, an association between the device credential or token and the second user
device, wherein the mapping indicates an association between payment credentials or
tokens and a plurality of user devices, and wherein the mapping identifies a user device
configured to act as an authenticating device;
identifying the second user device associated with the device credential in
20 the transaction request from the first user device based on the retrieved mapping,
wherein the second user device acts as an authenticating device for the first user device
according to the mapping to perform the authentication with the resource provider
computer for the transaction request received from the first user device, wherein the first
user device and second user device are associated with a same payment credential or
25 token;
based on the second user device associated with the device credential or
token being identified based on the retrieved mapping, transmitting, to the second user
device, an authentication request to authenticate the resource provider computer with
the first user device;
30 receiving, from the second user device, an authentication response, the
authentication response comprising an indication that the first user device is
authenticated;

transmitting an authorization request message to an authorizing entity computer in response to receiving the indication that the first user device is authenticated;

5 receiving an authorization response message authorizing the transaction request; and

receiving from the first user device a subsequent transaction request, authenticating the subsequent transaction request without requiring authentication with the second user device.

12. The resource provider computer of claim 11, wherein the method further comprises:
receiving, from the authorizing entity computer, the authorization response message.

13. The resource provider computer of claim 11, wherein the resource provider computer grants access to a secure location if the authorization request message is approved.

14. The resource provider computer of claim 11, wherein the device credential is a first identifier of the first user device.

15. The resource provider computer of claim 11, wherein the resource provider computer stores an association between the first user device and the payment credential, and wherein the method further comprises:

receiving a de-enrollment message comprising a first identifier of the first user device; and

5 removing the association between the first user device and the payment credential.

16. The resource provider computer of claim 15, wherein the transaction request is a first transaction request and the authorization request message is a first authorization request message and wherein the method further comprises:

receiving, from the first user device, a second transaction request comprising the device credential associated with the user; and

10 determining that the first user device is authenticated, and that communication with the second user device is not needed; and

transmitting a second authorization request message in response to determining that the first user device is authenticated.

17 . The resource provider computer of claim 11, wherein the resource provider computer receives the device credential associated with the user from the first device, and the method further comprises:

obtaining, by the resource provider computer from a token provider computer, and a cryptogram; and

generating, by the resource provider computer, the authorization request message to include the token and the cryptogram, and exclude the device credential.

18. The method according to claim 1, further comprising sending, by
5 the resource provider computer, a token request message to a token service provider computer, the token request message requesting a cryptogram for the transaction,
wherein the cryptogram comprises encrypted authentication method data,
an encrypted account identifier, an encrypted transaction channel indicator, and
encrypted expiration information.

10

19. The method according to claim 1, wherein the payment credential information is sensitive credential information.

20. The method according to claim 1, wherein the device credential or token is a device identifier.