CLAIMS:

1. A method, comprising:

receiving, at a server computer via a first communication channel, a first provisioning request to provision a first payment credential to a first mobile device, wherein the first payment credential is associated with a first account of a first user;

determining a first risk level associated with the first provisioning request;

responsive to the first risk level being within a predetermined risk threshold range, causing an authentication process to be performed with the first user;

responsive to a successful performance of the authentication process, causing the first payment credential to be provisioned onto the first mobile device;

receiving, at the server computer via the first communication channel, a second provisioning request to provision a second payment credential to a second mobile device, wherein the second payment credential is associated with a second account of a second user;

determining a second risk level associated with the second provisioning request; and

responsive to the second risk level being below the predetermined risk threshold range, causing the second payment credential to be provisioned onto the second mobile device.

2. The method of claim 1, further comprising:

receiving, at the server computer via the first communication channel, a third provisioning request to provision a third payment credential to a third mobile device, wherein the third payment credential is associated with a third account of a third user;

determining a third risk level associated with the third provisioning request; and

responsive to the third risk level meeting or exceeding the predetermined risk threshold range, transmitting, by the server computer, a provisioning

request denial message indicating that the third provisioning request is denied.

3. The method of claim 1, further comprising:

further responsive to the first risk level being within the predetermined risk threshold range, transmitting a first set of provisioning scripts to be executed by the first mobile device to cause the first payment credential to be stored at the first mobile device in an inactive state, wherein the inactive state does not allow the first mobile device to utilize the first payment credential for financial transactions,

wherein said causing the first payment credential to be provisioned onto the first mobile device comprises transmitting, by the server computer, an activation script to be executed by the first mobile device to switch the first payment credential from the inactive state to an active state that allows the first mobile device to use the first payment credential for financial transactions.

4. The method of claim 3, wherein said activation script, when executed by the first mobile device, causes the first payment credential to be switched to the active state by one or more of:

disabling a protection flag associated with the first payment credential within a secure element of the first mobile device; and

decrypting the first payment credential.

5. The method of claim 1, wherein:

said causing the authentication process to be performed with the first user comprises causing a dynamic verification value to be provided to the first user via a second communication channel; and

said successful performance of the authentication process comprises receiving, at the server computer, a consumer verification response that includes the dynamic verification value.

6. The method of claim 5, wherein said causing the dynamic verification value to be provided to the first user via the second communication channel comprises:

generating, by the server computer, the dynamic verification value; and

transmitting, by the server computer, the dynamic verification value to an issuer computer of an issuer of the first account to cause the issuer to provide the dynamic verification value to the first user.

7. The method of claim 5, further comprising:

receiving, at the server computer, a message transmitted by the issuer computer that includes the dynamic verification value; and

comparing, by the server computer, the received dynamic verification value of the consumer verification response with a stored copy of the dynamic verification value received from the issuer computer,

wherein said causing the dynamic verification value to be provided to the first user via the second communication channel comprises transmitting, by the server computer to an issuer computer of an issuer of the first account, a request for the dynamic verification value.

8. The method of claim 5, further comprising:

determining, by the server computer, whether the received dynamic verification value of the consumer verification response has a same value as an output of a validation algorithm utilizing at least two input values, wherein the at least two input values comprise an account identifier of the first account and a time value,

wherein said causing the dynamic verification value to be provided to the first user via the second communication channel comprises transmitting, by the server computer, a request for the dynamic verification value to be generated and provided to the first user.

9. The method of claim 1, further comprising:

generating a set of one or more consumer-specific encryption keys;

causing at least one of the set of consumer-specific encryption keys to be provided to the first mobile device;

encrypting a communication message using one of the set of consumer-specific encryption keys to yield an encrypted communication message; and

transmitting the encrypted communication message to a wallet application provider, wherein the wallet application provider provides the encrypted

communication message to the first mobile device and does not have any of the set of consumer-specific encryption keys.

10. The method of claim 1, further comprising:

receiving, at the server computer, an authorization request message for a transaction involving the first account of the first user;

generating, by the server computer, a unique transaction identifier for the transaction; and

transmitting, by the server computer, the unique transaction identifier and additional transaction information for the transaction, wherein the first mobile device, upon receipt of the unique transaction identifier and the additional transaction information:

identifies a record of a transaction log based upon the unique transaction identifier, and

updates the record based upon the additional transaction information.

11. The method of claim 1, wherein the first provisioning request does not include a primary account number (PAN) of the first account but does include a reference identifier of the PAN, and wherein the method further comprises identifying, by the server computer, the first account using the reference identifier.

12. A non-transitory computer readable storage medium storing instructions which, when executed by one or more processors of a server computer, cause the server computer to perform operations comprising:

receiving, at a server computer via a first communication channel, a first provisioning request to provision a first payment credential to a first mobile device, wherein the first payment credential is associated with a first account of a first user;

determining a first risk level associated with the first provisioning request;

responsive to the first risk level being within a predetermined risk threshold range, causing an authentication process to be performed with the first user;

responsive to a successful performance of the authentication process, causing the first payment credential to be provisioned onto the first mobile device;

receiving, at the server computer via the first communication channel, a second provisioning request to provision a second payment credential to a second mobile device, wherein the second payment credential is associated with a second account of a second user;

determining a second risk level associated with the second provisioning request; and

responsive to the second risk level being below the predetermined risk threshold range, causing the second payment credential to be provisioned onto the second mobile device.

13. The non-transitory computer readable storage medium of claim 12, wherein the operations further comprise:

receiving, at the server computer via the first communication channel, a third provisioning request to provision a third payment credential to a third mobile device, wherein the third payment credential is associated with a third account of a third user;

determining a third risk level associated with the third provisioning request; and

responsive to the third risk level meeting or exceeding the predetermined risk threshold range, transmitting, by the server computer, a provisioning request denial message indicating that the third provisioning request is denied.

14. The non-transitory computer readable storage medium of claim 12, wherein the operations further comprise:

further responsive to the first risk level being within the predetermined risk threshold range, transmitting a first set of provisioning scripts to be executed by the first mobile device to cause the first payment credential to be stored at the first mobile device in an inactive state, wherein the inactive state does not allow the first mobile device to utilize the first payment credential for financial transactions,

wherein said causing the first payment credential to be provisioned onto the first mobile device comprises transmitting, by the server computer, an activation script to be executed by the first mobile device to switch the

first payment credential from the inactive state to an active state that allows the first mobile device to use the first payment credential for financial transactions.

15. The non-transitory computer readable storage medium of claim 12, wherein:

said causing the authentication process to be performed with the first user comprises causing a dynamic verification value to be provided to the first user via a second communication channel; and

said successful performance of the authentication process comprises receiving, at the server computer, a consumer verification response that includes the dynamic verification value.

16. The non-transitory computer readable storage medium of claim 12, further comprising:

generating a set of one or more consumer-specific encryption keys;

causing at least one of the set of consumer-specific encryption keys to be provided to the first mobile device;

encrypting a communication message using one of the set of consumer-specific encryption keys to yield an encrypted communication message; and

transmitting the encrypted communication message to a wallet application provider, wherein the wallet application provider provides the encrypted communication message to the first mobile device and does not have any of the set of consumer-specific encryption keys.

17. A server computer, comprising:

one or more processors; and

a non-transitory computer readable storage medium communicatively coupled with the one or more processors and storing instructions which, when executed by the one or more processors, cause the server computer to perform operations comprising:

receiving, at a server computer via a first communication channel, a first provisioning request to provision a first payment credential to a first mobile device, wherein the first payment credential is associated with a first account of a first user;

determining a first risk level associated with the first provisioning request;

responsive to the first risk level being within a predetermined risk threshold range, causing an authentication process to be performed with the first user;

responsive to a successful performance of the authentication process, causing the first payment credential to be provisioned onto the first mobile device;

receiving, at the server computer via the first communication channel, a second provisioning request to provision a second payment credential to a second mobile device, wherein the second payment credential is associated with a second account of a second user;

determining a second risk level associated with the second provisioning request; and

responsive to the second risk level being below the predetermined risk threshold range, causing the second payment credential to be provisioned onto the second mobile device.

18. The server computer of claim 17, wherein the operations further comprise:

receiving, at the server computer via the first communication channel, a third provisioning request to provision a third payment credential to a third mobile device, wherein the third payment credential is associated with a third account of a third user;

determining a third risk level associated with the third provisioning request; and

responsive to the third risk level meeting or exceeding the predetermined risk threshold range, transmitting, by the server computer, a provisioning request denial message indicating that the third provisioning request is denied.

19. The server computer of claim 17, wherein the operations further comprise:

further responsive to the first risk level being within the predetermined risk threshold range, transmitting a first set of provisioning scripts to be

executed by the first mobile device to cause the first payment credential to be stored at the first mobile device in an inactive state, wherein the inactive state does not allow the first mobile device to utilize the first payment credential for financial transactions,

wherein said causing the first payment credential to be provisioned onto the first mobile device comprises transmitting, by the server computer, an activation script to be executed by the first mobile device to switch the first payment credential from the inactive state to an active state that allows the first mobile device to use the first payment credential for financial transactions.

20. The server computer of claim 17, wherein:

said causing the authentication process to be performed with the first user comprises causing a dynamic verification value to be provided to the first user via a second communication channel; and

said successful performance of the authentication process comprises receiving, at the server computer, a consumer verification response that includes the dynamic verification value.

CLAIMS

1. A method for provisioning a mobile device with a payment credential, comprising:

transmitting, from the mobile device to a server computer, a provisioning request to provision the payment credential on the mobile device, wherein the payment credential is associated with an account of a user;

when a risk level associated with the provisioning request is within a predetermined risk threshold range:

receiving, by the mobile device, a first set of provisioning scripts;

executing, by the mobile device, the first set of provisioning scripts to cause the payment credential to be stored at the mobile device in an inactive state;

storing, by the mobile device, the payment credential in the inactive state, wherein the inactive state does not allow the mobile device to utilize the payment credential for financial transactions prior to an authentication process being performed with the user;

responsive to a successful performance of the authentication process, receiving by the mobile device, an activation script;

executing, by the mobile device, the activation script to switch the payment credential from the inactive state to an active state that allows the mobile device to use the payment credential for financial transactions;

when the risk level associated with the provisioning request is below the predetermined risk threshold range:

receiving, by the mobile device, a second set of provisioning scripts;

executing, by the mobile device, the second set of provisioning scripts to cause the payment credential to be stored at the mobile device in the active state without requiring the authentication process with the user; and

initiating, by the mobile device, a financial transaction using the payment credential.

2. The method of claim 1, further comprising:

when the risk level meets or exceeds the predetermined risk threshold range,

receiving, by the mobile device, a provisioning request denial message indicating that the provisioning request is denied.

3. The method of claim 1, wherein executing the activation script further comprises:

storing, by the mobile device, a protection flag associated with the payment credential in a memory of the mobile device based on executing the first set of provisioning scripts, the protection flag representing the inactive state of the payment credential; and

disabling, by the mobile device, the protection flag associated with the payment credential within a secure element of the mobile device.

4. The method of claim 1, wherein:

the authentication process comprises a dynamic verification value being provided to the user via a separate communication channel; and

said successful performance of the authentication process comprises the user providing a consumer verification response that includes the dynamic verification value.

5. The method of claim 1, further comprising:

receiving, by the mobile device from the server computer, at least one of a set of consumer-specific encryption keys in the first set of provisioning scripts or the second set of provisioning scripts;

receiving, by the mobile device from a wallet application provider, an encrypted communication message encrypted by the server computer using one of the set of consumer-specific encryption keys, wherein the wallet application provider does not have any of the set of consumer-specific encryption keys; and

decrypting, by the mobile device, the encrypted communication message using the at least one of the set of consumer-specific encryption keys.

6. The method of claim 1, wherein the first set of provisioning scripts or the second set of provisioning scripts is encrypted using a secure element key associated with a secure memory area on a secure element of the mobile device.

7. The method of claim 1, further comprising:

transmitting, by the mobile device, the payment credential in the active state to a transacting entity during the financial transaction with the transacting entity.

8. The method of claim 1, wherein the first set of provisioning scripts or the second set of provisioning scripts are received by the mobile device prior to the account of the user being activated.

9. The method of claim 1, further comprising:

receiving, by the mobile device from the server computer, a unique transaction identifier and additional transaction information for the financial transaction involving the payment credential associated with the account of the user;

identifying, by the mobile device, a record of a transaction log based upon the unique transaction identifier; and

updating, by the mobile device, the record based upon the additional transaction information.

10. The method of claim 1, wherein the provisioning request includes a reference identifier of a primary account number (PAN) of the account of the user instead of the PAN.

11. A mobile device, comprising:

one or more processors; and

a non-transitory computer readable storage medium communicatively coupled with the one or more processors and storing instructions which, when executed by the one or more processors, cause the mobile device to perform operations comprising:

transmitting, to a server computer, a provisioning request to provision a payment credential on the mobile device, wherein the payment credential is associated with an account of a user;

when a risk level associated with the provisioning request is within a predetermined risk threshold range:

receiving a first set of provisioning scripts;

executing the first set of provisioning scripts to cause the payment credential to be stored at the mobile device in an inactive state;

storing the payment credential in the inactive state, wherein the inactive state does not allow the mobile device to utilize the payment credential for financial transactions prior to an authentication process being performed with the user;

responsive to a successful performance of the authentication process, receiving an activation script;

executing the activation script to switch the payment credential from the inactive state to an active state that allows the mobile device to use the payment credential for financial transactions;

when the risk level associated with the provisioning request is below the predetermined risk threshold range:

receiving a second set of provisioning scripts;

executing the second set of provisioning scripts to cause the payment credential to be stored at the mobile device in the active state without requiring the authentication process with the user; and

initiating a financial transaction using the payment credential.

12. The mobile device of claim 11, wherein the operations further comprise:

when the risk level meets or exceeds the predetermined risk threshold range,

receiving a provisioning request denial message indicating that the provisioning request is denied.

13. The mobile device of claim 11, wherein executing the activation script further comprises:

storing a protection flag associated with the payment credential in a memory of the mobile device based on executing the first set of provisioning scripts, the protection flag representing the inactive state of the payment credential; and

disabling the protection flag associated with the payment credential within a secure element of the mobile device.

14. The mobile device of claim 11, wherein:

the authentication process comprises a dynamic verification value being provided to the user via a separate communication channel; and

said successful performance of the authentication process comprises the user providing a consumer verification response that includes the dynamic verification value.

15. The mobile device of claim 11, wherein the operations further comprise:

receiving, from the server computer, at least one of a set of consumer-specific encryption keys in the first set of provisioning scripts or the second set of provisioning scripts;

receiving, from a wallet application provider, an encrypted communication message encrypted by the server computer using one of the set of consumer-specific encryption keys, wherein the wallet application provider does not have any of the set of consumer-specific encryption keys; and

decrypting the encrypted communication message using the at least one of the set of consumer-specific encryption keys.

16. The mobile device of claim 11, wherein the first set of provisioning scripts or the second set of provisioning scripts is encrypted using a secure element key associated with a secure memory area on a secure element of the mobile device.

17. The mobile device of claim 11, wherein the operations further comprise:

transmitting the payment credential in the active state to a transacting entity during the financial transaction with the transacting entity.

18. The mobile device of claim 11, wherein the first set of provisioning scripts or the second set of provisioning scripts are received by the mobile device prior to the account of the user being activated.

19. The mobile device of claim 11, wherein the operations further comprise:

receiving, from the server computer, a unique transaction identifier and additional transaction information for the financial transaction involving the payment credential associated with the account of the user;

identifying a record of a transaction log based upon the unique transaction identifier; and

updating the record based upon the additional transaction information.

20. The mobile device of claim 11, wherein the provisioning request includes a reference identifier of a primary account number (PAN) of the account of the user instead of the PAN.