

Claims

1. A payment authentication system for authenticating a card-not-present payment transaction initiated using a user electronic device, the payment authentication system comprising:

an authentication server comprising an authentication server processor, an authentication server data storage device and an authentication server database, the authentication server database storing a plurality of authentication records, each authentication record comprising a payment card identifier, a mobile number and a secure element identifier, the authentication server data storage device storing computer program instructions operable to cause the authentication server processor to:

receive, from the user electronic device, an authentication request comprising a payment amount, a payment card identifier, a mobile number and a secure element identifier associated with the user electronic device; and

validate a combination of the payment card identifier, the mobile number and the secure element identifier of the authentication request by determining if the combination of the payment card identifier, the mobile number and the secure element identifier matches an authentication record of the plurality of authentication records;

a directory server comprising a directory server processor and a directory server data storage device, the directory server data storage device storing computer program instructions operable to cause the directory server processor to:

compare the payment amount with a threshold amount, the card-not-present payment transaction is a high-value transaction if the payment amount is greater than the threshold amount;

generate a network authentication value (AV) if the payment amount is less than the threshold and the combination of the payment card identifier, the mobile number and the secure element identifier has been validated;

store a combination of the network AV and the payment card identifier; and

transmit, to the user electronic device, an authentication response comprising the network AV; and

a payment network server comprising a payment network server processor and a payment network server data storage device, the payment network server data storage device storing computer program instructions operable to cause the payment network server processor to:

receive, from the user electronic device, a transaction request comprising a received payment card identifier and a received network AV;

determine if the received payment card identifier and the received network AV match the stored payment card identifier and the stored network AV; and

transmit, to an issuer server, an authorization request comprising an authentication indication indicating that the card-not-present payment transaction has been authenticated if the received payment card identifier and the received network AV match the stored payment card identifier and the stored network AV;

wherein the directory server data storage device further stores computer program instructions operable to cause the directory server processor to:

transmit, to the issuer server, a request to provide an issuer AV if the payment amount is greater than the threshold amount, the request comprising the payment card identifier, the mobile number and the secure element identifier;

receive, from the issuer server, the issuer AV; and

transmit, to the user electronic device, the issuer AV.

2. The system of claim 1, wherein the payment network server data storage device further stores computer program instructions operable to cause the payment network server processor to:

receive, from the user electronic device, a high-value transaction request comprising a received issuer AV, a received payment card identifier and an indication of a high-value payment amount;

transmit, to the issuer server, a high-value authorization request comprising the received issuer AV and the received payment card identifier; and

receive, from the issuer server, an authorization response indicating whether the card-not-present payment transaction is authorised to proceed, the card-not-present payment transaction is authorised to proceed if the received issuer AV and the received payment card identifier match a stored issuer AV and the stored payment card identifier at the issuer server.

3. The system of claim 2, wherein the payment card identifier or the received payment card identifier is a tokenized payment card identifier.

4. The system of claim 3, wherein the transaction request or the high-value transaction request further comprises a device-generated cryptogram, the payment network server data storage device further stores computer program instructions operable to cause the payment network server processor to authenticate a combination of the device-generated cryptogram and the tokenized payment card identifier.

5. A payment authentication system for authenticating a card-not-present payment transaction initiated using a user electronic device, the payment authentication system comprising:

an authentication server comprising an authentication server processor and an authentication server data storage device, the authentication server data storage device storing computer program instructions operable to cause the authentication server processor to:

receive, from the user electronic device, an authentication request comprising a payment card identifier, a mobile number and a secure element identifier associated with the user electronic device;

a directory server comprising a directory server processor and a directory server data storage device, the directory server data storage device storing computer program instructions operable to cause the directory server processor to:

transmit, to an issuer server, a request to provide an issuer AV, the request comprising the payment card identifier, the mobile number and the secure element identifier;

receive, from the issuer server, the issuer AV indicating that a combination of the payment card identifier, the mobile number and the secure element identifier matches a stored authentication record comprising the payment card identifier, the mobile number and the secure element identifier; and

transmit, to the user electronic device, an authentication response comprising the issuer AV; and

a payment network server comprising a payment network server processor and a payment network server data storage device, the payment network server data storage device storing computer program instructions operable to cause the payment network server processor to:

receive, from the user electronic device, a transaction request comprising a received payment card identifier, a device-generated cryptogram associated with the received payment card identifier and a received issuer AV;

validate the device-generated cryptogram; and

transmit, to the issuer server, an authorization request comprising the received payment card identifier and the received issuer AV for authenticating the received payment card identifier and the received issuer AV if the device-generated cryptogram is validated.

6. The system of claim 5, wherein the authentication server further comprises an authentication server database storing a plurality of authentication records, each authentication record comprising a payment card identifier, a mobile number and a secure element identifier, the authentication server data storage device further stores computer program instructions operable to cause the authentication server processor to:

validate the combination of the payment card identifier, the mobile number and the secure element identifier by determining if the combination of the payment card identifier,

the mobile number and the secure element identifier matches an authentication record of the plurality of authentication records,

wherein the request to provide the issuer AV is transmitted to the issuer server if the combination of the payment card identifier, the mobile number and the secure element identifier is validated.

7. The system of claim 5 or claim 6, wherein the payment card identifier or the received payment card identifier is a tokenized payment card identifier, the payment network server data storage device further stores computer program instructions operable to cause the payment network server processor to authenticate a combination of the device-generated cryptogram and the tokenized payment card identifier.

8. The system of any one of the preceding claims, further comprising a registration server, the registration server comprises a registration server processor and a registration server data storage device, the registration server data storage device storing computer program instructions operable to cause the registration server processor to:

receive, from the user electronic device, a registration request comprising the payment card identifier, the mobile number and the secure element identifier;

store, using a registration server database, a registration record comprising the payment card identifier, the mobile number and the secure element identifier;

transmit, to the issuer server, the registration record for registering with the issuer server; and

transmit, to the user electronic device, a registration response indicating that the payment card identifier, the mobile number and the secure element identifier have been registered.

9. A payment authentication method for authenticating a card-not-present payment transaction initiated using a user electronic device, the method comprising:

receiving, from the user electronic device, an authentication request comprising a payment amount, a payment card identifier, a mobile number and a secure element identifier associated with the user electronic device;

validating, a combination of the payment card identifier, the mobile number and the secure element identifier of the authentication request by determining if the combination of the payment card identifier, the mobile number and the secure element identifier matches an authentication record, the authentication record being one of a plurality of authentication records stored in an authentication server database, each of the plurality of authentication records comprising a payment card identifier, a mobile number and a secure element identifier;

comparing the payment amount with a threshold amount, the card-not-present payment transaction is a high-value transaction if the payment amount is greater than the threshold amount;

generating, a network authentication value (AV) if the payment amount is less than the threshold amount and the combination of the payment card identifier, the mobile number and the secure element identifier has been validated;

storing, a combination of the network AV and the payment card identifier;

transmitting, to the user electronic device, an authentication response comprising the network AV;

receiving, from the user electronic device, a transaction request comprising a received payment card identifier and a received network AV;

determining, if the received payment card identifier and the received network AV match the stored payment card identifier and the stored network AV; and

transmitting, to an issuer server, an authorization request comprising an authentication indication indicating that the card-not-present payment transaction has been authenticated if the received payment card identifier and the received network AV match the stored payment card identifier and the stored network AV;

transmitting, to the issuer server, a request to provide an issuer AV if the payment amount is greater than the threshold amount, the request comprising the payment card identifier, the mobile number and the secure element identifier;

receiving, from the issuer server, the issuer AV; and

transmitting, to the user electronic device, the issuer AV.

10. The method of claim 9, further comprising:

receiving, from the user electronic device, a high-value transaction request comprising a received issuer AV, a received payment card identifier and an indication of a high-value payment amount;

transmitting, to the issuer server, a high-value authorization request comprising the received issuer AV and the received payment card identifier; and

receiving, from the issuer server, an authorization response indicating whether the card-not-present payment transaction is authorised to proceed, the card-not-present payment transaction is authorised to proceed if the received issuer AV and the received payment card identifier match a stored issuer AV and the stored payment card identifier at the issuer server.

11. The method of any one of claims 9 and 10, wherein the payment card identifier or the received payment card identifier is a tokenized payment card identifier and the transaction

request or the high-value transaction request further comprises a device-generated cryptogram, the method further comprises authenticating a combination of the device-generated cryptogram and the tokenized payment card identifier.

12. A payment authentication method for authenticating a card-not-present payment transaction initiated using a user electronic device, the method comprising:

- receiving, from the user electronic device, an authentication request comprising a payment card identifier, a mobile number and a secure element identifier associated with the user electronic device;

- transmitting, to an issuer server, a request to provide an issuer AV, the request comprising the payment card identifier, the mobile number and the secure element identifier;

- receiving, from the issuer server, the issuer AV indicating that a combination of the payment card identifier, the mobile number and the secure element identifier matches a stored authentication record comprising the payment card identifier, the mobile number and the secure element identifier;

- transmitting, to the user electronic device, an authentication response comprising the issuer AV;

- receiving, from the user electronic device, a transaction request comprising a received payment card identifier, a device-generated cryptogram associated with the received payment card identifier and a received issuer AV;

- validating the device-generated cryptogram; and

- transmitting, to the issuer server, an authorization request comprising the received payment card identifier and the received issuer AV for authenticating the received payment card identifier and the received issuer AV if the device-generated cryptogram is validated.

13. The method of claim 12, further comprising:

- validating the combination of the payment card identifier, the mobile number and the secure element identifier by determining if the combination of the payment card identifier, the mobile number and the secure element identifier matches an authentication record, the authentication record being one of a plurality of authentication records stored in an authentication server database, each of the plurality of authentication records comprising a payment card identifier, a mobile number and a secure element identifier,

- wherein the request to provide the issuer AV is transmitted to the issuer server if the combination of the payment card identifier, the mobile number and the secure element identifier is validated.

14. The method of claim 12 or claim 13, wherein the payment card identifier or the received payment card identifier is a tokenized payment card identifier, the method further comprises authenticating a combination of the device-generated cryptogram and the tokenized payment card identifier.

15. The method of any one of claims 9 to 14, further comprising:

receiving, from the user electronic device, a registration request comprising the payment card identifier, the mobile number and the secure element identifier;

storing, using a registration server database, a registration record comprising the payment card identifier, the mobile number and the secure element identifier;

transmitting, to the issuer server, the registration record for registering with the issuer server; and

transmitting, to the user electronic device, a registration response indicating that the payment card identifier, the mobile number and the secure element identifier have been registered.

16. The method of claim 15, further comprising:

tokenizing the payment card identifier; and

storing the tokenized payment card identifier in the registration record,

wherein the payment card identifier comprised in the registration response for transmission to the user electronic device is the tokenized payment card identifier.

17. The method of claim 16, further comprising:

receiving, from the user electronic device, transaction authentication data comprising the tokenized payment card identifier, the mobile number and the secure element identifier.

18. A non-transitory computer-readable medium having stored thereon program instructions for causing at least one processor to perform the method according to any one of claims 9 to 17.