

the underlying transactions, known as the universal cardholder authentication field, or UCAF. In turn, this information is communicated to support the issuers in connection with payment authorization requests and to provide explicit evidence that authentication was completed by the issuers. Other payment networks utilize similar authentication services, which are generally based on the 3-D SecureTM protocol. And, each of these services typically requires the merchants' acquirers (or banks) to add the resulting authentication values into their standard authorization messages.

SUMMARY

[0004a] According to an aspect, the present disclosure refers to a system for use in authenticating users to accounts in connection with network transactions, the system comprising: a payment network, wherein the payment network is separate from a merchant, an acquirer associated with the merchant, and an issuer of a payment account; a directory server (DS) included in the payment network and coupled in communication with an access control server (ACS) and a digital service server (DSS); the ACS associated with the issuer and coupled in communication with the DS; and the DSS coupled in communication with the DS, wherein the DSS is separate from the merchant, the acquirer, and the issuer; wherein the DS is configured to: receive an authentication request for a transaction directed to the merchant from a merchant server plug-in (MPI) associated with the merchant, the transaction involving the payment account, the payment account associated with an account number, and the authentication request including at least one of a token associated with the payment account and the account number; and transmit the at least one of the token and the account number to the DSS; wherein, in response to receiving the at least one of the token and the account number, the DSS is configured to: generate a directory server nonce (DSN) for the authentication request; and transmit the DSN and the account number for the payment account to the DS; wherein, in response to receiving the DSN and the account number, the DS is configured to transmit the DSN and the account number to the ACS; wherein, in response to receiving the DSN and the account number, the ACS is configured to: generate an issuer authentication value (IAV); and transmit the IAV to the DS; wherein, in response to receiving the IAV from the ACS, the DS is configured to: compile an accountholder authentication value (AAV) as evidence of completed authentication for the

transaction, the AAV including the IAV, the DSN, and an amount of the transaction; and transmit the AAV to the MPI; wherein the payment network is configured to: receive an authorization request for the transaction from the MPI, the authorization request including the AAV; validate the AAV; and based on validation of the AAV, transmit the authorization request to the issuer; and wherein the issuer is configured to validate the IAV prior to approving or declining the transaction.

[0004b] According to an aspect, the present disclosure refers to a computer-implemented method for use in authenticating a user to a payment account in connection with a transaction, the method comprising: receiving, by a directory server (DS), an authentication request for a transaction directed to a merchant and associated with a payment account, the authentication request including a token associated with the payment account and a cryptogram, wherein the DS is included in a payment network, and wherein the payment network is separate from the merchant, an acquirer associated with the merchant, and an issuer of the payment account; transmitting, by the DS, the token and the cryptogram to a digital service server (DSS), the DSS separate from the merchant, the acquirer, and the issuer; mapping, by the DSS, the token to a primary account number (PAN) for the payment account; validating, by the DSS, the cryptogram; in response to validating the cryptogram, generating, by the DSS, a directory server nonce (DSN) for the authentication request; transmitting, by the DSS, the DSN and the PAN to the DS; in response to receiving the DSN and the PAN, transmitting, by the DS, the DSN and the PAN to an access control server (ACS) associated with the issuer of the payment account; generating, by the ACS, an issuer authentication value (IAV); transmitting, by the ACS, the IAV to the DS; in response to receiving the IAV from the ACS, compiling, by the, an accountholder authentication value (AAV) as evidence of completed authentication, the AAV including the IAV, the DSN, and an amount of the transaction; transmitting, by the DS, the AAV to one of the merchant and a merchant server plug-in (MPJ) associated with the merchant; receiving, by the payment network, an authorization request for the transaction including the AAV from one of the merchant and the MPI; validating, by the payment network, the AAV; based on validating the AAV, transmitting, by the payment network, the authorization request to the issuer of the payment account; and validating, by the issuer, the IAV prior to approving or declining the transaction.

DRAWINGS

[0005] The drawings described herein are for illustrative purposes only of selected embodiments and not all possible implementations, and are not intended to limit the scope of the present disclosure:

[0006] FIG. 1 illustrates an exemplary system for use in providing full accountholder authentication values (AAVs) for transactions, based on authentication of consumers in connection with the transactions and based on validation codes for associated cryptograms, and including one or more aspects of the present disclosure;

[0007] FIG. 2 is a block diagram of an exemplary computing device that may be used in the system of FIG. 1;

[0008] FIG. 3 illustrates an exemplary method that may be implemented via the system of FIG. 1 for use in providing a full AAV, including an issuer authentication value (IAV), for a transaction, based on authentication of a consumer; and

[0009] FIG. 4 is a block diagram of an exemplary format of a full AAV, including an IAV, that may be used in connection with the system of FIG. 1 and/or the method of FIG. 3.

[0010] Corresponding reference numerals indicate corresponding parts throughout the several views of the drawings.

DETAILED DESCRIPTION

[0011] Exemplary embodiments will now be described more fully with reference to the accompanying drawings. The description and specific examples included herein are intended for purposes of illustration only and are not intended to limit the scope of the present disclosure.

CLAIMS

What is claimed is:

1. A system for use in authenticating users to accounts in connection with network transactions, the system comprising:
 - a payment network, wherein the payment network is separate from a merchant, an acquirer associated with the merchant, and an issuer of a payment account;
 - a directory server (DS) included in the payment network and coupled in communication with an access control server (ACS) and a digital service server (DSS);
 - the ACS associated with the issuer and coupled in communication with the DS; and
 - the DSS coupled in communication with the DS, wherein the DSS is separate from the merchant, the acquirer, and the issuer;wherein the DS is configured to:
 - receive an authentication request for a transaction directed to the merchant from a merchant server plug-in (MPI) associated with the merchant, the transaction involving the payment account, the payment account associated with an account number, and the authentication request including at least one of a token associated with the payment account and the account number; and
 - transmit the at least one of the token and the account number to the DSS; wherein, in response to receiving the at least one of the token and the account number, the DSS is configured to:
 - generate a directory server nonce (DSN) for the authentication request; and
 - transmit the DSN and the account number for the payment account to the DS;
 - wherein, in response to receiving the DSN and the account number, the DS is configured to transmit the DSN and the account number to the ACS;
 - wherein, in response to receiving the DSN and the account number, the ACS is configured to:
 - generate an issuer authentication value (IAV); and
 - transmit the IAV to the DS;
 - wherein, in response to receiving the IAV from the ACS, the DS is configured to:

compile an accountholder authentication value (AAV) as evidence of completed authentication for the transaction, the AAV including the IAV, the DSN, and an amount of the transaction; and

transmit the AAV to the MPI;

wherein the payment network is configured to:

receive an authorization request for the transaction from the MPI, the authorization request including the AAV;

validate the AAV; and

based on validation of the AAV, transmit the authorization request to the issuer; and

wherein the issuer is configured to validate the IAV prior to approving or declining the transaction.

2. The system of claim 1, wherein the authentication request includes the token for the payment account; and

wherein the DSS is further configured to map the token to the account number for the payment account prior to transmitting the account number to the DS.

3. The system of claim 1, wherein the authentication request includes a cryptogram; and wherein the DSS is configured to validate the cryptogram prior to transmitting the DSN to the DS.

4. The system of claim 1, wherein the authentication request includes a cryptogram; and wherein the DSS is configured to:

store the cryptogram in a memory prior to transmitting the DSN to the DS;

locate the cryptogram in the memory based on the DSN; and

validate the cryptogram in response to the authorization request including the AAV.

5. The system of claim 1, wherein the amount of the transaction includes a logarithmic amount of the transaction; and

wherein the AAV further includes a merchant ID.

6. The system of claim 1, wherein the DS is further configured to generate a message authentication code (MAC) based on at least the DSN, the AAV including the MAC;
wherein the payment network is configured, in connection with validating the AAV, to validate the MAC based on a shared key with the directory server; and
wherein the payment network is further configured to transmit the authorization request, or part thereof, to the DSS.
7. The system of claim 6, wherein the DSS is further configured to validate a digital secure remote payment (DSRP) cryptogram included in the authentication request and to provide a validation result for the DSRP cryptogram to the payment network; and
wherein the payment network is configured to transmit the authorization request, including the validation result, to the issuer of the payment account.
8. The system of claim 1, wherein the DSN includes at least an application transaction count (ATC) and a randomly generated value.
9. The system of claim 1, wherein the amount of the transaction includes a logarithmic amount of the transaction; and
wherein the AAV includes the IAV, the DSN, the logarithmic amount, a truncated hash of a merchant ID for the merchant, a currency code, a key ID for a shared key and a MAC generated by the shared key.
10. The system of claim 1, wherein the DS is further configured to:
calculate a logarithm of the amount of the transaction;
calculate a truncated hash of a merchant ID of the merchant; and
transmit the logarithm of the amount of the transaction and the truncated hash of the merchant ID, along with the DSN and the account number, to the ACS.
11. The system of claim 1, wherein the authentication request includes a cryptogram; and

wherein the DSS is configured to map the token to the account number and to validate the cryptogram prior to transmitting the DSN to the DS.

12. A computer-implemented method for use in authenticating a user to a payment account in connection with a transaction, the method comprising:

- receiving, by a directory server (DS), an authentication request for a transaction directed to a merchant and associated with a payment account, the authentication request including a token associated with the payment account and a cryptogram, wherein the DS is included in a payment network, and wherein the payment network is separate from the merchant, an acquirer associated with the merchant, and an issuer of the payment account;

- transmitting, by the DS, the token and the cryptogram to a digital service server (DSS), the DSS separate from the merchant, the acquirer, and the issuer;

- mapping, by the DSS, the token to a primary account number (PAN) for the payment account;

- validating, by the DSS, the cryptogram;

- in response to validating the cryptogram, generating, by the DSS, a directory server nonce (DSN) for the authentication request;

- transmitting, by the DSS, the DSN and the PAN to the DS;

- in response to receiving the DSN and the PAN, transmitting, by the DS, the DSN and the PAN to an access control server (ACS) associated with the issuer of the payment account;

- generating, by the ACS, an issuer authentication value (IAV);

- transmitting, by the ACS, the IAV to the DS;

- in response to receiving the IAV from the ACS, compiling, by the, an accountholder authentication value (AAV) as evidence of completed authentication, the AAV including the IAV, the DSN, and an amount of the transaction;

- transmitting, by the DS, the AAV to one of the merchant and a merchant server plug-in (MPJ) associated with the merchant;

- receiving, by the payment network, an authorization request for the transaction including the AAV from one of the merchant and the MPI;

- validating, by the payment network, the AAV;

based on validating the AAV, transmitting, by the payment network, the authorization request to the issuer of the payment account; and
validating, by the issuer, the IAV prior to approving or declining the transaction.

13. The computer-implemented method of claim 12, wherein the DSN includes at least an application transaction count (ATC) and a randomly generated value.

14. The computer-implemented method of claim 12, further comprising:
compressing, by the DS, at least one of the amount of the transaction and a merchant ID associated with the merchant;
transmitting, by the DS, the compressed at least one of the amount of the transaction and the merchant ID to the ACS; and
wherein the AAV includes the compressed at least one of the amount of the transaction and the merchant ID.

15. The computer-implemented method of claim 12, further comprising:
generating, by the DS, a message authentication code (MAC), the AAV including the MAC; and
wherein validating the AAV includes validating the MAC in response to the authorization request including the AAV.

16. The computer-implemented method of claim 15, further comprising:
mapping, by the payment network, the token to the PAN after validating the MAC; and
transmitting, by the payment network, the authorization request with the PAN and a validation result to the issuer of the payment account prior to the issuer validating the IAV.

17. The computer-implemented method of claim 16, wherein the AAV includes the IAV, the DSN, a logarithmic value of the amount of the transaction, a truncated hash of a merchant ID for the merchant, a currency code, a key ID for a shared key used to generate the MAC, and the MAC.

18. The computer-implemented method of claim 17, further comprising:
generating, by the ACS, the IAV based on a key and at least the PAN and the DSN; and
wherein validating the IAV includes validating the IAV based on the shared key and at least the PAN and the DSN.
19. The computer-implemented method of claim 12, further comprising:
calculating, by the DS, a logarithm of the amount of the transaction;
calculating, by the DS, a truncated hash of a merchant ID of the merchant; and
transmitting, by the DS, the logarithm of the amount of the transaction and the truncated hash of the merchant ID, along with the DSN and the account number, to the ACS.
20. The computer-implemented method of claim 12, wherein the authentication request includes a cryptogram; and wherein the method further comprises:
mapping, by the DSS, the token to the account number; and
validating, by the DSS, the cryptogram prior to transmitting the DSN to the DS.