American Express cards) retrieved from the mobile wallet application, is dynamically computed at the time of request, is entered into the checkout web site or application. The masked EXP also retrieved from the mobile wallet application, to be entered also uses a date far in the future indicating that this is a dCVV CNP transaction. This way both the original CVV-2 and EXP are hidden from an attacker monitoring the transaction. Moreover, intercepting a particular CNP transaction does not lead to an attacker using the information in another transaction, because the CVV code is computed in real-time and changes between CNP transactions, and is time stamped so that it would expire after a short time.

[0013] In order to convert existing static card data into dynamic card data for mobile users without requiring each card issuer to change their provisioning infrastructure, the devices, systems, and methods effectively allow cardholders to convert existing magnetic stripe card data into dynamic tokenized dynamic card data using mobile devices without requiring the card issuers to setup a separate remote mobile provisioning system. The card issuer, the issuer's processor, or the issuer's payment network may host the Provisioning Authentication Server (PAS) to authenticate the dCVV packaged in the MST transmission, or dCVV2 for online transactions, and either validate for the issuer the dynamic payment data is authentic, or validate and return the original track data (in the case of the payment network,) or original CVV2 back to the issuer or its processor so that the payment network can do the authentication service (or tokenization service) on behalf of the card issuer. This can dramatically speed up the conversion from static card data in the field to dynamic tokenized card data to enhance security for CP and CNP transactions.

[0013a] In view of the above and in accordance with a first aspect of the present application, there is provided a method of creating and transmitting dynamic card data, comprising: receiving, by a device, card track data; encrypting, by the device, the card track data using a first key; sending, by the device, the encrypted card track data to a server; receiving, by the device, a working key for the card track data from the server; generating, by the device, modified card track data including a time-dependent CVV using the working key; and sending, by the device, the modified card track data to a point of sale terminal or causing the modified card track data to be displayed to a user for use in an e-commerce transaction.

[0013b] In accordance with a second aspect of the present application, there is provided a method for provisioning dynamic financial card data by issuer, comprising: receiving, by a server, a request for provisioning a working key, the request comprising card track data; requesting, by the server, an authentication of a user corresponding to the card track data from a card issuer server, wherein the card issuer server corresponds to a card issuer of the card track data; receiving, by the server, an authentication result from the card issuer server; and generating, by the server in response to the authentication result, the working key for the card track data received with the request, for the generation of dynamic card track data.

[0013c] In accordance with a third aspect of the present application, there is provided a method for performing dynamic-CVV (dCVV) verification, comprising: generating, by a server, a working key for card track data; receiving, by a magnetic stripe storage and transmission device (MST), the working key; generating, by the MST, modified card track data including a dCVV component based on original card track data, a time-stamp or counter and the working key; sending the modified card track data to a point of sale terminal or e-commerce website for payment processing; receiving, by the server, a request for verification of the dCVV from a card issuer server or a third party service provider in response to initiation of the payment processing, wherein the request includes the modified card track data; performing, by the server, a verification of the dCVV component; and sending, by the server, a verification failure or final verification based on the verification of the dCVV component to the card issuer sever or the third party service provider.

BRIEF DESCRIPTION OF THE DRAWINGS

[0014] Embodiments of devices, systems, and methods are illustrated in the figures of the accompanying drawings which are meant to be exemplary and not limiting, in which like references are intended to refer to like or corresponding parts, and in which:

[0015] FIG. I is a functional diagram of an overview of a system according to aspects of the disclosure;

[0016] FIG. 2 is a flow diagram of a method of operation of initializing an MST according to aspects of the disclosure;

[0017] FIG. 3 is a flow diagram of a method of provisioning a static card based on a user

CLAIMS

What is claimed is:

1. A method for creating and transmitting dynamic card data, comprising:

receiving, by a device, card track data;

encrypting, by the device, the card track data using a first key;

sending, by the device, the encrypted card track data to a server;

receiving, by the device, a working key for the card track data from the server;

generating, by the device, modified card track data including a time-dependent CVV using the working key; and

sending, by the device, the modified card track data to a point of sale terminal or causing the modified card track data to be displayed to a user for use in an e-commerce transaction.

2. The method of claim 1, wherein an expiration date, a registered primary account number, or a portion of a discretionary field of the modified track data indicates to a card issuer or a third party service provider that the modified card track data is dynamic-CVV (dCVV) card track data and authorization is to be performed in a dCVV mode.

3. The method of claim 1, wherein the sending of the modified card track data to the point of sale terminal includes sending the time-dependent CVV, and a dynamic mode indicator.

4. The method of claim 3, wherein the dynamic mode indicator is a primary account number, an expiration date, or a separate dynamic mode indicator of the modified track data.

5. The method of claim 4, wherein the dynamic mode indicator indicates to a card issuer or third party service provider, that the modified card track data is dynamic-CVV (dCVV) card track data and authorization is to be performed in a dCVV mode.

6. The method of claim 1, wherein the device is a magnetic stripe storage and transmission device or a mobile communication device.

7. A method for provisioning dynamic financial card data by issuer, comprising:

receiving, by a server, a request for provisioning a working key, the request comprising card track data;

requesting, by the server, an authentication of a user corresponding to the card track data from a card issuer server, wherein the card issuer server corresponds to a card issuer of the card track data;

receiving, by the server, an authentication result from the card issuer server; and

generating, by the server in response to the authentication result, the working key for the card track data received with the request, for the generation of dynamic card track data.

8. The method of claim 7, wherein the requesting the authentication of the user from the card issuer server includes sending a primary account number and at least one of a CVV-2, a name, a date of birth, a username and password, and an answer to a challenge question to the card issuer server for authentication.

9. The method of claim 7, further comprising securely sending the working key to a wallet server.

10. The method of claim 7, further comprising receiving a request for verification of a dynamic CVV (dCVV) in response to initiation of payment transaction, wherein the dCVV is based on the working key.

11. The method of claim 10 wherein the receiving the request for verification of the dCVV includes receiving a primary account number, an expiration date, a service code, a time-stamp, and a mode indicator.

12. The method of claim 11, further comprising comparing the received time-stamp with a stored time-stamp or current time on the server for verifying a transaction.

13. The method of claim 12, further comprising sending an authorization failure in response to the stored time-stamp or current time corresponding to a time greater than the

received time-stamp.

14. A method for performing dynamic-CVV (dCVV) verification, comprising:

generating, by a server, a working key for card track data;

receiving, by a magnetic stripe storage and transmission device (MST), the working key;

generating, by the MST, modified card track data including a dCVV component based on original card track data, a time-stamp and counter and the working key;

sending the modified card track data to a point of sale terminal or e-commerce website for payment processing;

receiving, by the server, a request for verification of the dCVV from a card issuer server or a third party service provider in response to initiation of the payment processing, wherein the request includes the modified card track data;

performing, by the server, a verification of the dCVV component; and

sending, by the server, a verification failure or final verification based on the verification of the dCVV component to the card issuer server or the third party service provider.

15. The method of claim 14, wherein the modified card track data includes the dCVV component, a primary account number, an expiration date, a service code, the time-stamp or counter, and optionally a separate mode indicator when the expiry date or the primary account number is not used to indicate that authorization is to be performed in a dCVV mode.

16. The method of claim 15 wherein the mode indicator indicates to the card issuer server that the modified card track data is dCVV card track data and authorization is to be performed in a dCVV mode.

17. The method of claim 15, wherein the performing the verification includes comparing a received time-stamp or received counter with a stored time-stamp or a current time of the server or stored counter.

18. The method of claim 17, wherein the sending the verification failure or final verification includes sending the verification failure in response to the stored time-stamp or

current time of the server corresponding to a time greater than the received time-stamp.

19. The method of claim 15, wherein the performing the verification includes:

independently computing, by the server, a dCVV value using the working key; and

comparing the computed dCVV value with the dCVV component.

20. The method of claim 19, wherein the sending the verification failure or final verification includes sending the final verification in response to the computed dCVV value matching the received dCVV component.

21. The method of claim 14, further comprising sending, by the server, the original card track data to the card issuer server for processing via the card issuer server's normal processing methods to complete a transaction, wherein the original card track data corresponds to data of a card issuer corresponding to the card issuer server.