transmit magnetic stripe card data to merchants' conventional point of sale (POS) terminals and other devices with magnetic stripe readers (MSRs) or online checkout systems, in physical and virtual environments.

[0009] The present disclosure also relates to devices, systems, and methods for converting static card data (for example, the CVVI or CVV2) into dynamic cryptograms that can only be used one time, and cannot be replayed by fraudsters, and leveraging mobile devices to deliver payment information that includes the cryptograms back to the card issuer for authentication, without changing the existing merchant acceptance infrastructure whether it is for physical payment via POS or remote payment via online checkout. The devices, systems, and methods allow users to automatically convert the static card data into dynamic one time use card data that can be authenticated by the payment network or processor on behalf of the thousands of card issuers as a service, without infrastructure change and integration by each issuer.

[0010] In an ~~aspect~~embodiment, a dynamic cryptogram which can be called a dynamic-CVV (dCVV) is used to secure card payments. A dCVV is generated freshly with a key plus primary account number (PAN), expiration or expiry date (EXP), timestamp and counter, when the card is used for payment in both Card-Not-Present (CNP) and Card-Present (CP) transactions. The dCVV, which is cryptographically generated, cannot be generated without the knowledge of the card data and a secret key. Also, each dCVV is only valid for a short period of time. This prevents the replaying attack described above, since re-use of the dCVV from a previously monitored transaction will result in an authorization error.

[0011] In another ~~aspect~~embodiment, the card issuer or a stand-in service provider may differentiate CP transactions that use dCVV technology, because the validation algorithm used is different for dCVV transaction as opposed to ordinary magnetic stripe CP transactions. The dCVV transactions may be identified by replacing the EXP of the card data with a number equivalent to a date far into the future recognizable by the issuer or service provider. This obscures the EXP in a payment transaction while providing the card issuer with a convenient flag to recognize the card as being in dCVV mode. Other flags can be used to indicate the card is in dCVV mode, such as a flag in a discretionary field of the track data used to indicate dCVV mode. The PAN can also be registered in the issuer or service provider's database as a dCVV card.

[0012] The concept of dCVV in the domain of MST also naturally applies to CNP transactions. In CNP transactions, a dynamically generated 3 digit code (or 4 digit code in the case of

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; 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 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, a working key 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), 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.

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. 1 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