BROWSER INTEGRATION WITH CRYPTOGRAM

CROSS-REFERENCES TO RELATED APPLICATIONS

[0001] The present application is a non-provisional application of and claims priority to U.S. Provisional Application No. 62/146,100, filed on April 10, 2015 (Attorney Docket No.: 79900-941691), the entire contents of which are herein incorporated by reference for all purposes.

BACKGROUND

[0002] Transactions often require that a user provide sensitive data to execute the transaction. Sensitive data may be an access code to a building or payment details, for example. In some cases, personal user information may be handled by multiple entities, including third parties. When the sensitive data is in electronic form, multiple computing devices, networks, and/or entities are sometimes given access to the sensitive information. Thus, it is desirable that the number of networks, computing devices, and/or entities that have access to such sensitive data be reduced in order to limit the access to the sensitive data.

[0003] Embodiments of the invention address this and other problems, individually and collectively.

BRIEF SUMMARY

[0004] Embodiments of the present invention relate to systems and methods for conducting a transaction a browser configured to be integrated with a token cryptogram. According to one embodiment of the invention, a server computer receives authentication credentials from a user. The authentication credentials may be from a web-browser or an operating system (OS) that a user is utilizing in a computing environment. The server computer may identify that the website accessed by the user is "token-aware." The server computer may provide a transaction data identifier

[0045] At step 5, server computer 105 may identify that the website operated by gateway service provider 104 (or merchant 103) is "token-aware" and therefore enabled to accept a token cryptogram (S303). In the context of this disclosure, a "token-aware" website is configured to accept a token cryptogram in field of a webpage of the website. In some embodiments, the data field is a hidden field in that it is not viewable to the user. In one embodiment, the website includes a unique identifier and the website is identified as a token-aware website by transmitting the unique identifier to payment processing network to verify the unique identifier. In one embodiment, a "token-aware" website identifies itself by including a HyperText Markup Language (HTML) tag within the website. In one embodiment, the HTML tag functions as the unique identifier. The HTML tag may also verifies the identity of the website and establish the website as a trusted website. In yet another embodiment, identifying the website as token-aware includes receiving an Extended Validation Certificate (EVC) from the website.

[0046] Still referring to step 5, server computer 105 may provide one or more transaction data identifiers associated with the authentication credentials of the user account to gateway service provider 104 after identifying that the website is token-aware. In one embodiment, the transaction data identifier can be the last four digits of a PAN and identifies that particular account for use in the pending transaction.

[0047] Referring to FIG. 3, website webpage 301 includes a transaction completion interface 303 that includes transaction data identifiers 307 and 309, which are the last four digits of different PANs that are associated with the user account 305 and the authentication credentials of the user account 305. Server computer 105 may store the last four digits of a PAN, but not store the complete PAN. User 101 can choose to select one of the transaction data identifiers to complete the pending transaction. The user may also choose to enter a new PAN 311 that has not been linked to the user account. If user 101 selects one of the transaction data identifiers 307/309, the website sends server computer 105 a confirmation of which transaction data identifier was approved by user 101 to complete the pending transaction.

WHAT IS CLAIMED

1. A method of performing a transaction comprising:

assigning, by a server computer, a unique identifier to a website

receiving, by the server computer, authentication credentials of a user accessing the website;

identifying, by the server computer, that the website accessed by the user is token-aware by identifying the unique identifier of the website and transmitting the unique identifier of the website to a processing network to verify the unique identifier of the website, wherein the token-aware website is configured to accept a token cryptogram in data fields of a webpage of the website;

providing, by the server computer, a transaction data identifier to the website, wherein the transaction data identifier identifies underlying transaction data and is associated with the authentication credentials;

receiving, by the server computer, a confirmation that the transaction data identified by the transaction data identifier is approved by the user to complete a transaction;

transmitting, by the server computer, a token and a cryptogram request comprising the unique identifier of the website to a processing network, wherein the token is linked to the transaction data identified by the transaction data identifier;

receiving from the processing network, a token cryptogram based on the token; and

providing, by the server computer, tokenized credentials and the token cryptogram to the data fields of the webpage of the website to conduct a transaction.

2. The method of claim 1 further comprising:

providing the unique identifier of the website to the data fields of the webpage, wherein the data fields are hidden fields not visible to the user viewing the website.

3. The method of claim 1, wherein identifying that the website is token-aware includes analyzing an html (HyperText Markup Language) tag of the website.

4. The method of claim 3, wherein the html tag also verifies a trusted identity of the website.

5. The method of claim 1 wherein the tokenized credentials are provided to the data fields of the webpage only when the website is identified as token-aware.

6. The method of claim 1, wherein the transaction data is the tokenized credentials.

7. The method of claim 1, wherein the transaction data identifier is a last four digits of a Primary Account Number (PAN).

8. A computer comprising:

processing logic;

a network interface coupled to the processing logic; and

a computer readable medium accessible to the processing logic, the computer readable medium comprising code, executable by a processor, for implementing a method comprising:

assigning, by a server computer, a unique identifier to a website;

receiving, by the server computer, authentication credentials of a user accessing the website;

identifying, by the server computer, that the website accessed by the user is token-aware by identifying the unique identifier of the website and transmitting the unique identifier of the website to a processing network to verify the unique identifier of the website, wherein the token-aware website is configured to accept a token cryptogram in data fields of a webpage of the website;

providing, by the server computer, a transaction data identifier to the website, wherein the transaction data identifier identifies underlying transaction data and is associated with the authentication credentials;

receiving, by the server computer, a confirmation that the transaction data identified by the transaction data identifier is approved by the user to complete a transaction;

transmitting, by the server computer, a token and a cryptogram request comprising the unique identifier of the website to a processing network, wherein the token is linked to the transaction data identified by the transaction data identifier;

receiving from the processing network, a token cryptogram based on the token; and

providing, by the server computer, tokenized credentials and the token cryptogram to the data fields of the webpage of the website to conduct a transaction.

9. A method of performing a transaction comprising:

receiving a transaction data identifier from a server computer, wherein the transaction data identifier is associated with authentication credentials verified by the server computer;

providing a transaction completion interface of a website to a computing device, the transaction completion interface making the transaction data identifier viewable to a user of the transaction completion interface, wherein the transaction data identifier identifies underlying transaction data;

receiving a confirmation from the user that the transaction data identified by the transaction data identifier is approved to complete a transaction;

transmitting the confirmation to the server computer;

providing an indication to the server computer that the website is token-aware, wherein the token-aware website is configured to accept a token cryptogram in data fields of a webpage of the website;

receiving, from the server computer, tokenized credentials, a unique identifier of the website, and a token cryptogram in the data fields of the webpage of the website; and

transmitting an authorization request to conduct a transaction to an acquirer computer, wherein the authorization request includes the tokenized credentials, the token cryptogram, and the unique identifier of the website.

10. The method of claim 9 further comprising:

receiving an authorization response from the acquirer computer, the authorization response either approving or declining the transaction.

11. The method of claim 10 further comprising:

sending a transaction completion message to the computing device when the authorization response approves the transaction.

12. The method of claim 9, wherein the token-aware indication includes an html (HyperText Markup Language) tag.

13. The method of claim 12, wherein the token-aware indication also serves to verify the website as a trusted website.

14. The method of claim 9, wherein the token-aware indication includes an Extended Validation Certificate.

15. The method of claim 9, wherein the data fields are hidden fields that are not rendered for viewing by the user.

16. The method of claim 9, wherein the transaction data identifier is a last four digits of a social security number.

17. The method of claim 9, wherein the authentication credentials are associated with a browser publisher of a browser that the website is rendered in.

18. A computer comprising:

processing logic;

a network interface coupled to the processing logic; and

a computer readable medium accessible to the processing logic, the computer readable medium comprising code, executable by a processor, for implementing a method comprising:

receiving a transaction data identifier from a server computer, wherein the transaction data identifier is associated with authentication credentials verified by the server computer;

providing a transaction completion interface of a website to a computing device, the transaction completion interface making the transaction data identifier viewable to a user of the transaction completion interface, wherein the transaction data identifier identifies underlying transaction data;

receiving a confirmation from the user that the transaction data identified by the transaction data identifier is approved to complete a transaction;

transmitting the confirmation to the server computer;

providing an indication to the server computer that the website is token-aware, wherein the token-aware website is configured to accept a token cryptogram in data fields of a webpage of the website;

receiving, from the server computer, tokenized credentials, a unique identifier of the website, and a token cryptogram in the data fields of the webpage of the website; and

transmitting an authorization request to an acquirer computer, wherein the authorization request includes the tokenized credentials, the token cryptogram, and the unique identifier of the website.