

token or the issuer of the token. On the one hand, the token is intended to hide information. On the other hand, it would be useful to identify, from the payment token, the origin or the issuer of the token, a level of confidence that the user attempting to use the token is in fact the actual cardholder and data used to determine the level of confidence. Currently, techniques for identifying this information do not exist.

[0005] Moreover, tokens have traditionally been restricted to a particular network or payment processing system and have not supported interoperability between payment networks. Accordingly, the adoption and integration of tokens with various payment systems has been limited.

[0006] Embodiments of the present invention seek to solve these problems and other problems, individually and collectively.

BRIEF SUMMARY

[0007] Embodiments of the present invention are directed to providing, along with a token, a token assurance level and data used to generate the token assurance level. At the time a token is issued, steps may be taken to ensure that the token is replacing a PAN that was legitimately being used by a token requestor. This process is known as Identification and Verification (ID&V) and may be performed each time a token is requested. A token assurance level may be assigned to a given token in light of the type of ID&V that is performed and the entity performing the ID&V. Different ID&Vs may result in different token assurance levels. An issuer may wish to know the level of assurance and the data used in generating the level of assurance associated with a token prior to authorizing a payment transaction that uses the token. The assurance level that is assigned to a given token may change over time and be re-calibrated based upon factors that influence its confidence levels such as any association with fraudulent transactions or fraud-related chargebacks, etc.

[0007a] A first aspect of the invention provides a method comprising: receiving, by a computer, an authorization request message from a requestor, the authorization request message comprising a payment token representing a primary account number, the primary account number assigned by an issuer, wherein the authorization request message is for conducting a payment transaction using the primary account number; receiving, by the computer, a token assurance level associated with the token along with data used to generate the token assurance level; modifying, by the computer, the authorization request message to include the token assurance level and the data used

to generate the token assurance level; and transmitting, by the computer, the modified authorization request message to the issuer for approval, wherein the token assurance level is based on an identification and verification method used when the payment token is generated.

[0008] The token assurance level may represent a level of trust in an association between the payment token and the primary account number represented by the payment token. In some embodiments, the token assurance level is based on an entity performing the identification and verification method.

[0009] According to various embodiments, the method further includes, prior to receiving the authorization request message, receiving, by the computer, a token generation message for generation of the payment token to represent the primary account number. The token generation message may include a requested token assurance level associated with the payment token. The method may further include generating, by the computer, the payment token and the token assurance level associated with the payment token, and storing the payment token, the token assurance level and the primary account number associated with the payment token at a repository.

[0010] In some embodiments, the method may also include interacting with a repository storing a one-to-one mapping between one or more primary account numbers and one or more payment tokens generated for the one or more primary account numbers.

[0011] Another embodiment is directed to apparatuses, systems, and computer-readable media configured to perform the method described above.

[0011a] A second aspect of the present invention provides a system comprising: a processor; and a non-transitory computer readable medium coupled to the processor, the computer readable medium comprising code, that when executed by the processor, causes the processor to: receive an authorization request message from a requestor, the authorization request message comprising a payment token representing a primary account number, the primary account number assigned by an issuer, wherein the authorization request message is for conducting a payment transaction using the primary account number; receive a token assurance level associated with the token along with data used to generate the token assurance level; modifying the authorization request message to include the token assurance level and the data used to generate

the token assurance level; and transmit the modified authorization request message to the issuer for approval, wherein the token assurance level is based on an identification and verification method used when the payment token is generated.

[0012] A third aspect of the present invention is directed to a method including generating, by a computer, a payment token and a token assurance level associated with the payment token, the payment token representing a primary account number assigned by an issuer. The method also includes sending, by the computer, the payment token to a requestor and receiving, by the computer, an authorization request message from the requestor. The authorization request message may comprise the payment token. The authorization request message is for conducting a payment transaction using the primary account number. The method may further include modifying, by the computer, the authorization request message to include the token assurance level and data used to generate the token assurance level, and transmitting, by the computer, the modified authorization request message to the issuer for approval. The token assurance level may be based on an identification and verification method used when the payment token is generated.

[0013] These and other embodiments are described in further detail below.

BRIEF DESCRIPTION OF THE DRAWINGS

[0014] FIG. 1 shows a system and a flow diagram providing an overview of the various entity interactions in a tokenization ecosystem environment, according to an exemplary embodiment of the present invention.

[0015] FIG. 2 shows a system and a flow diagram providing an overview of the various entity interactions in a tokenization ecosystem environment where a payment network serves as a token service provider, according to an exemplary embodiment of the present invention.

[0016] FIG. 3 shows a system and flow diagram for an authorization flow for a mobile device at a merchant terminal transaction, according to an exemplary embodiment of the present invention.

[0017] FIG. 4 shows a system and a flow diagram for an authorization flow for a mobile/digital wallet e-Commerce transaction, according to an exemplary embodiment of the present invention.

CLAIMS

1. A method comprising:

receiving, by a computer, an authorization request message from a requestor, the authorization request message comprising a payment token representing a primary account number, the primary account number assigned by an issuer, wherein the authorization request message is for conducting a payment transaction using the primary account number;

receiving, by the computer, a token assurance level associated with the token along with data used to generate the token assurance level;

modifying, by the computer, the authorization request message to include the token assurance level and the data used to generate the token assurance level; and

transmitting, by the computer, the modified authorization request message to the issuer for approval,

wherein the token assurance level is based on an identification and verification method used when the payment token is generated.

2. The method of claim 1, further comprising:

prior to receiving the authorization request message:

receiving, by the computer, a token generation message for generation of the payment token to represent the primary account number, the token generation message including a requested token assurance level associated with the payment token;

generating, by the computer, the payment token and the token assurance level associated with the payment token; and

storing the payment token, the token assurance level and the primary account number associated with the payment token at a repository.

3. The method of claim 2, wherein the requested token assurance level is different from the token assurance level that is generated and stored at the repository.

4. The method of claim 1, wherein the token assurance level represents a level of trust in an association between the payment token and the primary account number represented by the payment token.

5. The method of claim 1, wherein the token assurance level is based on an entity performing the identification and verification method.

6. The method of claim 1, wherein the token assurance level is updated when additional identification and verification method is performed on the payment token.

7. The method of claim 1, wherein a first identification and verification method results in a first token assurance level and a second identification and verification method results in a second token assurance level different than the first token assurance level.

8. The method of claim 1, further comprising:
receiving, by the computer, an authorization response message from the issuer, the authorization response message generated in response to the authorization request message; and

transmitting, by the computer, the authorization response message including the token assurance level to the requestor.

9. The method of claim 1, further comprising:
interacting with a repository storing a one-to-one mapping between one or more primary account numbers and one or more payment tokens generated for the one or more primary account numbers.

10. A system comprising:
a processor; and
a non-transitory computer readable medium coupled to the processor, the computer readable medium comprising code, that when executed by the processor, causes the processor to:

receive an authorization request message from a requestor, the authorization request message comprising a payment token representing a primary account number, the primary account number assigned by an issuer, wherein the authorization request message is for conducting a payment transaction using the primary account number;

receive a token assurance level associated with the token along with data used to generate the token assurance level;

modifying the authorization request message to include the token assurance level and the data used to generate the token assurance level; and

transmit the modified authorization request message to the issuer for approval,

wherein the token assurance level is based on an identification and verification method used when the payment token is generated.

11. The system of claim 10, wherein the code, when executed by the processor, further causes the processor to:

prior to receiving the authorization request message:

receive a token generation message for generation of the payment token to represent the primary account number, the token generation message including a requested token assurance level associated with the payment token;

generate the payment token and the token assurance level associated with the payment token; and

store the token assurance level and the primary account number associated with the payment token at a repository.

12. The system of claim 11, wherein the requested token assurance level is different from the token assurance level that is generated and stored at the repository.

13. The system of claim 10, wherein the token assurance level represents a level of trust in an association between the payment token and the primary account number represented by the payment token.

14. The system of claim 10, wherein the token assurance level is further based on an entity performing the identification and verification method.

15. The system of claim 14, wherein the token assurance level is updated when additional identification and verification method is performed on the payment token.

16. The system of claim 14, wherein a first identification and verification method results in a first token assurance level and a second identification and verification method results in a second token assurance level different than the first token assurance level.

17. The system of claim 10, wherein the code, when executed by the processor, further causes the processor to:

receive an authorization response message from the issuer, the authorization response message generated in response to the authorization request message; and

transmit the authorization response message including the token assurance level to the requestor.

18. The system of claim 10, further comprising:

a repository storing a one-to-one mapping between one or more primary account numbers and one or more payment tokens generated for the one or more primary account numbers

wherein the code, when executed by the processor, further causes the processor to:

interact with the repository.

19. A method comprising:

- generating, by a computer, a payment token and a token assurance level associated with the payment token, the payment token representing a primary account number assigned by an issuer;
- sending, by the computer, the payment token to a requestor;
- receiving, by the computer, an authorization request message from the requestor, the authorization request message comprising the payment token, wherein the authorization request message is for conducting a payment transaction using the primary account number;
- modifying, by the computer, the authorization request message to include the token assurance level and data used to generate the token assurance level; and
- transmitting, by the computer, the modified authorization request message to the issuer for approval,

wherein the token assurance level is based on an identification and verification method used when the payment token is generated.