

WHAT IS CLAIMED IS:

1. A method comprising:

managing, by an authorizing server computer, a first token vault storing a first set of data associated with a token representing an account identifier associated with a user account, wherein the first token vault is synchronized with a second token vault storing a second set of data associated with the token, the second token vault in communication with a transaction processing computer;

receiving, by the authorizing server computer, an authorization request message associated with a transaction from the transaction processing computer, the authorization request message including the token and at least a portion of the second set of data associated with the token including at least the account identifier;

retrieving, by the authorizing server computer, additional data associated with the token from the first token vault;

determining, by the authorizing server computer, to approve or decline the transaction based on a combination of the additional data retrieved from the first token vault and the portion of the second set of data retrieved from the second token vault;

transmitting, by the authorizing server computer to the transaction processing computer, an authorization response message authorizing or declining the transaction.

2. The method of claim 1, further comprising:

synchronizing, by the authorizing server computer, the first token vault with the second token vault.

3. The method of claim 1, wherein the transaction processing computer

manages the second token vault.

4. The method of claim 1, wherein a token generator service computer

manages the second token vault.

5. The method of claim 1, wherein the first set of data and the second set of

data are mutually exclusive.

6. The method of claim 1, wherein the first set of data and the second set of data are non-mutually exclusive.

7. The method of claim 1, wherein the second set of data associated with the token stored in the second token vault includes one or more of a token status indicator, a device identifier associated with the token, a token expiration date, an account identifier expiration date, a token assurance level, a token type, and a token requestor identifier.

8. The method of claim 1, wherein the additional data is only stored at the first token vault.

9. The method of claim 1, wherein the additional data includes a domain restriction associated with the token, wherein the domain restriction limits use of the token to a particular domain.

10. The method of claim 1, wherein the first token vault stores override data associated with the token.

11. The method of claim 1, wherein the first token vault is continuously synchronized with the second token vault immediately after content of the first token vault is modified.

12. The method of claim 1, further comprising:
receiving, by the authorizing server computer, the token and the first set of data associated with the token; and

storing, by the authorizing server computer, the first set of data at the first token vault.

13. The method of claim 1, further comprising:
generating, by the authorizing server computer, the token and the first set of data associated with the token; and

storing, by the authorizing server computer, the token, a mapping between the token and the account identifier, and the first set of data at the first token vault.

14. The method of claim 1, further comprising:

receiving, by the authorizing server computer, a token update message including the token and an updated information associated with the token; and

storing, by the authorizing server computer, the updated information associated with the token at the first token vault thereby updating the first token vault.

15. An authorizing server computer comprising:

a processor; and

a computer readable medium, the computer readable medium comprising code that, when executed by the processor, causes the processor to:

manage a first token vault storing a first set of data associated with a token representing an account identifier associated with a user account, wherein the first token vault is synchronized with a second token vault storing a second set of data associated with the token, the second token vault in communication with a transaction processing computer;

receive, from the transaction processing computer, an authorization request message associated with a transaction, the authorization request message including the token and at least a portion of the second set of data associated with the token including at least the account identifier;

retrieve additional data associated with the token from the first token vault;

determine to approve or decline the transaction based on a combination of the additional data retrieved from the first token vault and the portion of the second set of data retrieved from the second token vault;

transmit, to the transaction processing computer, an authorization response message authorizing or declining the transaction.

16. The authorizing server computer of claim 15, wherein the first set of data and the second set of data are non-mutually exclusive, wherein the code, when executed by the processor, further causes the processor to:

synchronize the first token vault with the second token vault.

17. The authorizing server computer of claim 15, wherein the transaction processing computer or a token service server computer manages the second token vault.

18. The authorizing server computer of claim 15, wherein the first set of data and the second set of data are non-mutually exclusive, wherein the code, when executed by the processor, further causes the processor to:

- send a token update request message to a token service provider server computer;
- receive, from the token server provider server computer, a token update message including the token and an updated information associated with the token; and
- store the updated information associated with the token at the first token vault thereby updating the first token vault.

19. The authorizing server computer of claim 15, wherein the additional data is only stored at the first token vault, and wherein the additional data includes one or more of override data, or a domain restriction associated with the token, wherein the domain restriction limits use of the token to a particular domain.

20. The authorizing server computer of claim 15, wherein the code, when executed by the processor, further causes the processor to:

- receive a token update message including the token and an updated information associated with the token;
- store the updated information associated with the token at the first token vault thereby updating the first token vault; and
- synchronizing the first token vault with the second token vault immediately after content of the first token vault is modified.