

WHAT IS CLAIMED IS:

1 1. A method comprising:
2 receiving, by a second computer, from a first computer, a request for a
3 verification value associated with a transaction, the request including a token;
4 generating, by the second computer, a random value;
5 storing, by the second computer, a record including the random value
6 and the token;
7 generating, by the second computer, a first verification value based on
8 the random value and the token;
9 providing, by the second computer, the first verification value to the first
10 computer;
11 receiving, by the second computer, from a third computer, a request to
12 validate the first verification value, the request including the first verification value
13 and the token;
14 identifying, by the second computer, the record including the random
15 value based on the token;
16 generating, by the second computer, a second verification value based
17 on the random value and the token;
18 determining, by the second computer, that the second verification value
19 matches the first verification value; and
20 providing, by the second computer, to the third computer, a value
21 credential associated with the token.

1 2. The method of claim 1, wherein the random value is a unique
2 hexadecimal value, and wherein the first verification value is a dynamic value.

1 3. The method of claim 1, wherein the transaction is an access
2 request, wherein the third computer sends the value credential to an authorizing
3 entity computer, and wherein the authorizing entity computer allows access to a
4 physical space based on the value credential.

1 4. The method of claim 1, wherein the random value is not
2 provided to the first computer, and wherein the first verification value is not stored at
3 the second computer.

1 5. The method of claim 1, wherein the request for the verification
2 value further includes a token requestor identifier, wherein the stored record further
3 includes the token requestor identifier, wherein the request to validate the first
4 verification value further includes the token requestor identifier, wherein the record
5 including the dynamic data is identified further based on the token requestor
6 identifier.

1 6. A second computer comprising:
2 a processor; and
3 a computer readable medium, the computer readable medium
4 comprising code, executable by the processor, for implementing a method
5 comprising:
6 receiving, from a first computer, a request for a verification value
7 associated with a transaction, the request including a token;
8 generating a random value;
9 storing a record including the random value and the token;
10 generating a first verification value based on the random value and the
11 token;
12 providing the first verification value to the first computer;
13 receiving, from a third computer, a request to validate the first
14 verification value, the request including the first verification value and the token;
15 identifying the record including the random value based on the token;
16 generating a second verification value based on the random value and
17 the token;
18 determining that the second verification value matches the first
19 verification value; and

20 providing, to the third computer, a value credential associated with the
21 token.

1 7. The second computer of claim 6, wherein the random value is a
2 unique hexadecimal value, and wherein the first verification value is a dynamic
3 value.

1 8. The second computer of claim 6, wherein the transaction is an
2 access request, wherein the third computer sends the value credential to an
3 authorizing entity computer, and wherein the authorizing entity computer allows
4 access to a physical space based on the value credential.

1 9. The second computer of claim 6, wherein the random value is
2 not provided to the first computer, and wherein the first verification value is not
3 stored at the second computer.

1 10. The second computer of claim 6, wherein the request for the
2 verification value further includes a token requestor identifier, wherein the stored
3 record further includes the token requestor identifier, wherein the request to validate
4 the first verification value further includes the token requestor identifier, wherein the
5 record including the dynamic data is identified further based on the token requestor
6 identifier.

1 11. A method comprising:
2 receiving, by a third computer, from a first computer, an authorization
3 request message for a transaction, the authorization request message including a
4 token and a first verification value;
5 sending, by the third computer, the token and the first verification value
6 to a second computer, wherein the second computer identifies a random value
7 based on the token, wherein the second computer generates a second verification
8 value based on the random value and the token, and wherein the second computer
9 determines that the second verification value matches the first verification value;

10 receiving, by the third computer, from the second computer, a value
11 credential associated with the token; and

12 sending, by the third computer, the authorization request message and
13 the value credential to an authorizing entity computer, wherein the authorizing entity
14 computer authorizes the transaction based on the value credential.

1 12. The method of claim 11, wherein the random value is a unique
2 hexadecimal value, and wherein the first verification value is a dynamic value.

1 13. The method of claim 11, wherein the transaction is an access
2 request, and wherein the authorizing entity computer allows access to a physical
3 space based on the value credential.

1 14. The method of claim 11, wherein the random value is stored
2 privately at the second computer, and wherein the first verification value is not stored
3 at the second computer.

1 15. The method of claim 11, wherein the authorization request
2 message also includes a token requestor identifier, wherein a token requestor
3 identifier is also sent to the second computer, and wherein the second computer
4 identifies the random value further based on the token requestor identifier.

1 16. A third computer comprising:
2 a processor; and
3 a computer readable medium, the computer readable medium
4 comprising code, executable by the processor, for implementing a method
5 comprising:
6 receiving, from a first computer, an authorization request message for
7 a transaction, the authorization request message including a token and a first
8 verification value;
9 sending the token and the first verification value to a second computer,
10 wherein the second computer identifies a random value based on the token, wherein
11 the second computer generates a second verification value based on the random

12 value, the token, and wherein the second computer determines that the second
13 verification value matches the first verification value;
14 receiving, from the second computer, a value credential associated
15 with the token; and
16 sending the authorization request message and the value credential to
17 an authorizing entity computer, wherein the authorizing entity computer authorizes
18 the transaction based on the value credential.

1 17. The third computer of claim 16, wherein the random value is a
2 unique hexadecimal value, and wherein the first verification value is a dynamic
3 value.

1 18. The third computer of claim 16, wherein the transaction is an
2 access request, and wherein the authorizing entity computer allows access to a
3 physical space based on the value credential.

1 19. The third computer of claim 16, wherein the random value is
2 stored privately at the second computer, and wherein the first verification value is not
3 stored at the second computer.

1 20. The third computer of claim 16, wherein the authorization
2 request message also includes a token requestor identifier, wherein a token
3 requestor identifier is also sent to the second computer, and wherein the second
4 computer identifies the random value further based on the token requestor identifier.