WE CLAIM:

1. A first device, comprising:

a memory including a counter value, transmission data, and at least one key;

a communication interface; and

one or more processors in communication with the memory and communication interface, wherein the one or more processors are configured to:

create a cryptogram using the at least one key and counter value, wherein the cryptogram includes the counter value and the transmission data;

transmit the cryptogram via the communication interface;

update the counter value after transmission of the cryptogram;

receive an encrypted access token via the communication interface;

decrypt the encrypted access token;

store the decrypted access token in the memory; and

transmit, after entry of the communication interface into a communication field, the access token via the communication interface for access to one or more resources, wherein the access token is encrypted.

2. The first device of claim 1, wherein the one or more processors are further configured to receive a challenge via the communication interface, wherein the challenge includes a public key and an encrypted test.

3. The first device of claim 2, wherein the one or more processors are further configured to transmit, responsive to the challenge, a challenge response via the communication interface.

4. The first device of claim 2, wherein the one or more processors are further configured to

generate a decrypted test by decrypting the encrypted test.

5. The first device of claim 4, wherein the one or more processors are further configured to include the decrypted test in a challenge response transmitted via the communication interface.

6. The first device of claim 2, wherein the one or more processors are further configured to encrypt the access token using the public key.

7. The first device of claim 6, wherein the encrypted access token is decrypted using a private key.

8. The first device of claim 1, wherein each entry of the communication interface into the communication field generates a challenge.

9. The first device of claim 1, wherein the access token comprises a limited use token.

10. The first device of claim 1, wherein the access token includes an access identifier.

11. An authentication method, comprising:

creating a cryptogram using at least one key and counter value, wherein the cryptogram includes the counter value and transmission data;

transmitting, via a communication interface, the cryptogram;

updating the counter value;

receiving, via the communication interface, an encrypted access token;

decrypting the encrypted access token;

storing the decrypted access token in memory; and

transmitting, after entry of the communication interface into a communication field, the access token via the communication interface to receive access to one or more resources, wherein the access token is encrypted.

12. The authentication method of claim 11, further comprising:

receiving, via the communication interface, a challenge, wherein the challenge includes a public key and an encrypted test.

13. The authentication method of claim 12, further comprising:

transmitting, responsive to the challenge, a challenge response via the communication interface.

14. The authentication method of claim 12, further comprising:

generating a decrypted test by decrypting the encrypted test.

15. The authentication method of claim 14, further comprising:

including the decrypted test in a challenge response transmitted via the communication interface.

16. The authentication method of claim 12, further comprising:

encrypting the access token using the public key.

17. The authentication method of claim 16, wherein the encrypted access token is decrypted using a private key.

18. The authentication method of claim 11, further comprising receiving a challenge based on each entry of the communication interface into the communication field.

19. The authentication method of claim 11, further comprising invalidating the access token after expiration of a predetermined time period.

20. A computer readable non-transitory medium comprising computer executable instructions that are executed on a processor and comprising the steps of:

creating a cryptogram using one or more keys and a counter value, wherein the cryptogram includes the counter value and transmission data;

transmitting the cryptogram;

~~updating the counter value;~~

~~receiving an encrypted access token;~~

~~decrypting the encrypted access token;~~

~~transmitting, after entry of a communication interface into a communication field, the access token via the communication interface, wherein the access token is encrypted; and~~

~~receiving, after authentication of the access token, access to one or more resources.~~

1. A first device, comprising:

a memory including a counter value, transmission data, and at least one key;

a communication interface; and

one or more processors in communication with the memory and communication interface, wherein the one or more processors are configured to:

create a cryptogram using the at least one key and counter value, wherein the cryptogram includes the counter value and the transmission data,

transmit the cryptogram via the communication interface,

update the counter value after transmission of the cryptogram,

receive an encrypted access token via the communication interface, and

transmit, after entry of the communication interface into a communication field, the encrypted access token via the communication interface for access to one or more resources.

2. The first device of claim 1, wherein the one or more processors are further configured to:

receive a challenge via the communication interface,

wherein the challenge includes a public key and an encrypted test.

3. The first device of claim 2, wherein the one or more processors are further configured to transmit, responsive to the challenge, a challenge response via the communication interface.

4. The first device of claim 2, wherein the one or more processors are further configured to:

generate a decrypted test in a challenge response transmitted via the communication interface, and

include the decrypted test in a challenge response transmitted via the communication interface.

5. The first device of claim 2, wherein, prior to transmitting the encrypted access token via the communication interface, the one or more processors are further configured to:

decrypt the encrypted access token,

store the decrypted access token in the memory, and

encrypt the decrypted access token using the public key to yield the encrypted access token that is transmitted.

6. The first device of claim 5, wherein the encrypted access token is decrypted using a private key.

7. The first device of claim 1, wherein each entry of the communication interface into the communication field generates a challenge.

8. The first device of claim 1, wherein the access token comprises a limited use token.

9. The first device of claim 1, wherein the access token includes an access identifier.

10. An authentication method, comprising:

creating a cryptogram using at least one key and counter value, wherein the cryptogram includes the counter value and transmission data;

transmitting, via a communication interface, the cryptogram;

updating the counter value;

receiving, via the communication interface, an encrypted access token; and

transmitting, after entry of the communication interface into a communication field, the encrypted access token via the communication interface to receive access to one or more resources.

11. The authentication method of claim 10, further comprising:

receiving, via the communication interface, a challenge,

wherein the challenge includes a public key and an encrypted test.

12. The authentication method of claim 11, further comprising, prior to transmitting the encrypted access token via the communication interface:

decrypting the encrypted access token;

storing the decrypted access token in memory; and

encrypting the decrypted access token using the public key to yield the encrypted access token that is transmitted.

13. The authentication method of claim 12, wherein the encrypted access token is decrypted using a private key.

14. The authentication method of claim 11, further comprising transmitting, responsive to the challenge, a challenge response via the communication interface.

15. The authentication method of claim 11, further comprising generating a decrypted test by decrypting the encrypted test.

16. The authentication method of claim 15, further comprising including the decrypted test in a challenge response transmitted via the communication interface.

17. The authentication method of claim 11, further comprising receiving a challenge based on each entry of the communication interface into the communication field.

18. The authentication method of claim 11, further comprising invalidating the access token after expiration of a predetermined time period.

19. A computer readable non-transitory medium comprising executable instructions that, when executed on a processor, cause the processor to perform procedures comprising the steps of:

creating a cryptogram using one or more keys and a counter value, wherein the cryptogram includes the counter value and transmission data;

transmitting the cryptogram;

updating the counter value;

transmitting, after entry of a communication interface into a communication field, the encrypted access token via the communication interface; and

receiving, after authentication of the access token, access to one or more resources.

20. The computer readable non-transitory medium of claim 19, the procedures, prior to transmitting the encrypted access token via the communication interface, further comprising the steps of:

receiving an encrypted access token;

decrypting the encrypted access token; and

encrypting the decrypted access token using a public key to yield the encrypted access token that is transmitted.