The first device may include a communication interface. The first device may include one or more processors in communication with the memory and communication interface. The one or more processors may be 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. The one or more processors may be configured to transmit the cryptogram via the communication interface. The one or more processors may be configured to update the counter value after transmission of the cryptogram. The one or more processors may be configured to receive an encrypted access token via the communication interface. ~~The one or more processors may be configured to decrypt the encrypted access token. The one or more processors may be configured to store the decrypted access token in the memory.~~ The one or more processors may be configured to 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~~, wherein the access token is encrypted~~.

[0006] Embodiments of the present disclosure provide an authentication method. The method may include creating a cryptogram using at least one key and counter value, wherein the cryptogram includes the counter value and transmission data. The method may include transmitting, via a communication interface, the cryptogram. The method may include updating the counter value. The method may include receiving, via the communication interface, an encrypted access token. ~~The method may include decrypting the encrypted access token. The method may include storing the decrypted access token in memory.~~ The method may include 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~~, wherein the access token is encrypted~~.

[0007] Embodiments of the present disclosure provide a computer readable non-transitory medium comprising ~~computer-~~executable instructions that ~~are~~, when executed on a processor, ~~and~~ 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; ~~receiving an encrypted access token; decrypting the encrypted access token;~~ transmitting, after entry of a communication interface into a communication field, the encrypted 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

BRIEF DESCRIPTION OF THE DRAWINGS

[0008] Various embodiments of the present disclosure, together with further objects and advantages, may best be understood by reference to the following description taken in conjunction with the accompanying drawings.

[0009] Figure 1 depicts an authentication system according to an exemplary embodiment.

[00010] Figure 2A is an illustration of a contactless card according to an exemplary embodiment.

[00011] Figure 2B is an illustration of a contact pad of a contactless card according to an exemplary embodiment.

[00012] Figure 3 depicts a method of authentication according to an exemplary embodiment.

[00013] Figure 4 depicts a sequence diagram of a process for authentication according to an exemplary embodiment.

[00014] Figure 5 depicts an authentication system according to an exemplary embodiment.

[00015] Figure 6 depicts a method of authentication according to an exemplary embodiment.