

[0006] These and other deficiencies exist. Accordingly, there is a need for systems and methods for authentication that overcome these deficiencies by protecting communications from interception and unauthorized access in a secure and reliable manner.

SUMMARY OF THE DISCLOSURE

[0006a] According to an aspect of the present disclosure, there is provided a method for secure data communication, comprising: receiving, by a server, a cryptogram, the cryptogram comprising user identification information; performing, by the server, a first factor authentication, wherein the first factor authentication comprises: decrypting the cryptogram, and verifying the user identification information; receiving, by the server, a data set from an application executing on a device; performing, by the server, a second factor authentication comprising verifying the data set; and generating, by the server, an authentication message.

[0006b] According to another aspect of the present disclosure, there is provided an authentication server, comprising: a memory; and a processor, wherein the processor: receives a cryptogram comprising a first set of identification data, performs a first factor authentication of the cryptogram, receives a second set of identification data comprising one or more metadata, performs, after the first factor authentication, a second factor authentication based on the one or more metadata, and generates an authentication message indicative of an outcome of the second factor authentication, and transmits the authentication message to a device.

[0006c] According to another aspect of the present disclosure, there is provided a computer readable non-transitory medium comprising computer executable instructions that, when executed by a processor, perform procedures comprising the steps of: receiving a cryptogram, the cryptogram comprising user identification information; performing a first factor authentication, wherein the first factor authentication comprises: decrypting the cryptogram,

and verifying by the server, the user identification information in the cryptogram; receiving a data set from the application executing on a device; performing a second factor authentication comprising verifying the data set; and generating an authentication message.

[0007] Embodiments of the present disclosure provide an authentication server. The authentication server may include a processor and a memory. The processor may be configured to receive a cryptogram associated with a first near field communication data exchange format (NDEF) read. The processor may be configured to perform a first factor authentication of the cryptogram. The processor may be configured to receive a first data set, wherein the first data set is associated with a second NDEF read. The processor may be configured to extract metadata from the first data set. The processor may be configured to perform, after the first factor authentication, a second factor authentication based on the metadata. The processor may be configured to generate a message indicative of an outcome of the second factor authentication. The processor may be configured to transmit the message that instructs the processor to effectuate one or more actions.

[0008] Embodiments of the present disclosure provide a method of authentication. The method may include receiving a cryptogram associated with a first near field communication data exchange format (NDEF) read. The method may include performing a first factor authentication. The method may include receiving a first data set, wherein the first data set is associated with a second NDEF read. The method may include extracting metadata from the first data set. The method may include performing, after the first factor authentication, a second factor authentication based on the metadata. The method may include generating a message indicative of an outcome of the second factor authentication. The method may include transmitting the message that instructs the processor to effectuate one or more actions.