

WE CLAIM:

1. 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.
2. The method for secure data communication of claim 1, further comprising:
 - transmitting, by the server in response to a successful first factor authentication, a retrieval message to the application,
 - wherein the retrieval message initiates a retrieval of the data set by the application.
3. The method for secure data communication of claim 1, wherein the authentication message is indicative of a two factor authentication.
4. The method for secure data communication of claim 1, further comprising:
 - transmitting, by the server, the authentication message to the application,
 - wherein the authentication message instructs the application to perform one or more actions.
5. The method for secure data communication of claim 5, wherein the one or more actions comprise at least one selected from the group of a conversion of a first type of operation to a second type of operation.

6. The method for secure data communication of claim 5, wherein:
the first type of operation comprises a card-not-present transaction, and
the second type of operation comprises a card-present transaction.
7. The method of claim 4, further comprising performing, by the server, a third factor authentication by verifying one or more user-provided data retrieved via the device, the one or more user-provided data being retrieved in response to the authentication message generated by the server.
8. The method of claim 7, wherein the one or more user-provided data comprises at least one selected from the group of a primary account number and a cardholder identifier.
9. The method of claim 1, wherein:
the cryptogram is retrieved from a memory of a contactless card, via near-field communication (NFC), by the device, and
a retrieval of the cryptogram corresponds to a first NFC read of the contactless card by the device.
10. The method of claim 7, wherein:
the data set is stored on the memory of the contactless card, and
the data set is retrieved from the memory of the contactless card by performing a second NFC read of the contactless card by the device.
11. The method of claim 1, wherein verifying the data set comprises matching, by the server, the data set with one or more reference sets of data associated with prior transactions conducted with a contactless card.
12. 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.

13. The authentication server of claim 12, wherein:

the processor performs a third factor authentication by verifying one or more user-provided
data retrieved via the device, and

the one or more user-provided data being retrieved in response to the authentication
message transmitted by the server.

14. The authentication server of claim 12, wherein:

the processor transmits the authentication message to the application, and
the authentication message instructs the application to perform one or more actions.

15. The authentication server of claim 14, wherein the one or more actions comprise at least
one selected from the group of a conversion of a first type of operation to a second type of
operation.

16. 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.

17. The computer readable non-transitory medium of claim 17, the procedures further comprising:

transmitting, in response to a successful first factor authentication, a retrieval message to the application,

wherein the retrieval message initiates a retrieval of the data set by the application.

18. The computer readable non-transitory medium of claim 17, wherein the cryptogram is retrieved from a memory of a contactless card by performing a first NFC read of the contactless card by the device.

19. The computer readable non-transitory medium of claim 18, wherein the data set is stored on the memory of the contactless card and retrieved by performing a second NFC read of the contactless card by the device.

20. The computer readable non-transitory medium of claim 19, wherein the data set comprises one or more sets of data associated with prior transactions conducted with the contactless card.