CLAIMS

What is claimed is:

1. A method of communicating with a transaction card having a card data processor, a communication interface, and a card memory having a unique card identifier stored therein, the method comprising:

transmitting, by an application executing on a communication device to the transaction card, a write command including session-specific challenge information;

transmitting, by the application to the transaction card, read command;

receiving, by the application from the transaction card, card-specific challenge response information; and

authenticating the transaction card using the challenge response information.

2. The method of claim 1, wherein the card-specific challenge response information comprises card-encrypted information.

3. The method of claim 2, wherein the card-specific challenge response information further comprises a digital authentication certificate.

4. The method of claim 2, wherein the action of authenticating the transaction card includes:

attempting to decrypt the card-encrypted information using at least one card-unique key associated with the unique card identifier; and

responsive to a successful decryption of the card-encrypted information, establishing a positive authentication result.

5. The method of claim 1, wherein the session-specific challenge information comprises a random number.

6. The method of claim 1, wherein:

the session-specific challenge information is generated by the application, and

authenticating the transaction card is performed by the application.

7. The method of claim 1, wherein authenticating the transaction card comprises:

transmitting, by the application to the authentication server, challenge response information; and

receiving, by the application from the authentication server, an authentication result.

8. The method of claim 1, further comprising receiving, by the application from an authentication server, the session-specific challenge information.

9. The method of claim 1, wherein:

the communication interface comprises a near field communication (NFC) interface,

the write command comprises an NFC data exchange format (NDEF) WRITE TAG command, and

the read command comprises an NDEF READ TAG command.

10. The method of claim 9, further comprising, prior to transmitting the write command, establishing, by the application, a first NFC session with the transaction card.

11. The method of claim 10, further comprising, prior to the action of transmitting the NDEF READ TAG command:

terminating the first NFC session; and

establishing, by the communication device within a predetermined time interval after termination of the first NFC session, a second NFC session with the transaction card.

12. A communication device, comprising:

a communication device data processor;

a communication interface in communication with the data processor and configured for communication with one or more transaction cards; and

a communication device memory accessible by the data processor and containing a communication device application comprising instructions to be carried out by the data processor,

wherein, upon execution by the communication device data processor, the communication device application:

transmits, to the transaction card, write command including session-specific challenge information,

transmits, to the transaction card, read command,

receives, from the transaction card, card-specific challenge response information, and

authenticates the transaction card.

13. The communication device of claim 10 wherein:

the card-specific challenge response information comprises card-encrypted information, and

as part of authenticating the transaction card, the communication application:

attempts to decrypt the card-encrypted information using at least one card-unique key associated with the transaction card, and

responsive to a successful decryption of the card-encrypted information, establishes a positive authentication result.

14. The communication device of claim 10, further comprising:

a network communication interface in communication with the communication device data processor and configured for selective communication with an authentication server via a network,

wherein the communication application receives the session-specific challenge information from the authentication server.

15. The communication device of claim 14, wherein, as part of authenticating the transaction card, the communication application:

transmits the challenge response information to the authentication server; and

receives an authentication result from the authentication server.

16. The communication device of claim 10, wherein communication application:

determines a time interval between the action of transmitting the read command and receiving the card-specific challenge response information, and

authenticates the transaction card if the time interval is less than a predetermined maximum communication interval.

17. The communication device of claim 10, wherein the session-specific challenge information comprises a pseudo-random number.

18. A transaction card, comprising:

a card microprocessor;

a communication interface; and

a card memory storing one or more applets including instructions for execution by the card microprocessor,

wherein, upon execution by the card microprocessor, the one or more applets:

receive, from a communication device via the communication interface, a write command including challenge information,

generate a digital signature using the challenge information,

receive, from the communication device via the communication interface, a read command, and

transmit, to the communication device, the digital signature.

19. The transaction card of claim 18, wherein:

the card memory has at least one card-unique encryption key stored therein, and

the digital signature comprises a cryptogram encrypted using at least a portion of the challenge information and the at least one card-unique encryption key.

20. The transaction card of claim 19, wherein:

the card memory stores a card identifier and at least one public key certificate, and

the one or more applets transmit the at least one public key certificate and the card identifier with the digital signature.