

WHAT IS CLAIMED IS:

1. A method, comprising:

identifying, by a protocol management computer, presence of a reader device utilizing a near field communications channel;

obtaining, by the protocol management computer from a remote server computer, a first initialization key associated with the reader device, wherein a second initialization key corresponding to the first initialization key was previously stored at the reader device during a manufacturing process of the reader device, wherein the first initialization key and the second initialization key are static keys;

storing, at the protocol management computer, the first initialization key;

receiving, by the protocol management computer via the near field communications channel, first encrypted data comprising a first public key associated with the reader device, the first encrypted data having been encrypted by the reader device based at least in part on the second initialization key stored at the reader device;

decrypting, by the protocol management computer based at least in part on the first initialization key stored at the protocol management computer, the first encrypted data to obtain the first public key associated with the reader device;

encrypting, by the protocol management computer based at least in part on the first initialization key stored at the protocol management computer, data comprising a second public key associated with the protocol management computer to generate second encrypted data; and

transmitting, by the protocol management computer via the near field communications channel, the second encrypted data for decryption by the reader device, the decryption being based at least in part on the second initialization key stored at the reader device.

2. The method of claim 1, wherein the first initialization key includes

an asymmetric key of an asymmetric key pair.

3. The method of claim 1, further comprising obtaining, by the protocol management computer, an identifier associated with the reader device, wherein obtaining the first initialization key comprises transmitting a request for the first initialization key, wherein the request for the first initialization key comprises the identifier, and wherein the identifier is utilized to retrieve the first initialization key.

4. The method of claim 1, wherein the remote server computer is configured to perform terminal processing operations.

5. The method of claim 1, wherein the first initialization key and the second initialization key are symmetric keys, and wherein the method further comprises:

transmitting, by the protocol management computer, a first encrypted message and a first initialization vector, the first encrypted message being encrypted with the symmetric key;

receiving, by the protocol management computer, a second encrypted message, the second encrypted message comprising the second encrypted data comprising the first public key associated with the reader device, the second encrypted message being encrypted using a second initialization vector generated from the first initialization vector;

decrypting, by the protocol management computer, the second encrypted message utilizing the second initialization vector;

verifying, by the protocol management computer, the second encrypted message as decrypted; and

transmitting, by the protocol management computer to the reader device, a third encrypted message comprising the second public key associated with the protocol management computer, the third encrypted message being encrypted utilizing a third initialization vector generated from the second initialization vector.

6. The method of claim 5, further comprising generating a unique identifier for the reader device and a nonce, wherein the first initialization key, the unique identifier, and the nonce are included in the first encrypted message.

7. The method of claim 6, wherein the second encrypted message, as decrypted, further comprises the symmetric key, one or more unique identifiers for the reader device, and the nonce.

8. The method of claim 7, wherein verifying the second encrypted message as decrypted comprises comparing the nonce received in the second encrypted message to the nonce as transmitted in the first encrypted message.

9. The method of claim 5, further comprising generating the second public key and a second private key associated with the protocol management computer in response to verifying the second encrypted message.

10. A protocol management computer, comprising:
a processor; and

a computer readable medium coupled to the processor, the computer readable medium comprising code that, when executed by the processor, causes the protocol management computer to perform operations comprising:

identifying presence of a reader device utilizing a near field communications channel;

obtaining, from a remote server computer, a first initialization key associated with the reader device, wherein a second initialization key corresponding to the first initialization key was previously stored at the reader device during a manufacturing process of the reader device, wherein the first initialization key and the second initialization key are static keys;

storing the first initialization key;

receiving, via the near field communications channel, first encrypted data comprising a first public key associated with the reader device, the first encrypted data having been encrypted by the reader device based at least in part on the second initialization key stored at the reader device;

decrypting, based at least in part on the first initialization key stored at the protocol management computer, the first encrypted data to obtain the first public key associated with the reader device;

encrypting, based at least in part on the first initialization key stored at the protocol management computer, data comprising a second public key associated with the protocol management computer to generate second encrypted data; and

transmitting, via the near field communications channel, the second encrypted data for decryption by the reader device, the decryption being based at least in part on the second initialization key stored at the reader device.

11. The protocol management computer of claim 10, wherein the operations further comprise negotiating, with the reader device, utilizing the first public key and the second public key, one or more session keys.

12. The protocol management computer of claim 11, wherein the one or more session keys are utilized to establish a secure connection between the protocol management computer and the reader device.

13. The protocol management computer of claim 12, wherein the secure connection conforms to a Bluetooth communications protocol.

14. The protocol management computer of claim 10, wherein the protocol management computer is configured to operate as a contactless card.

15. A reader device, comprising:
a processor; and
a computer readable medium coupled to the processor, the computer readable medium comprising code that, when executed by the processor, causes the reader device to perform operations comprising:

storing, during a manufacturing process of the reader device, a second initialization key at the reader device, the second initialization key corresponding to a first initialization key stored at a protocol management computer, wherein the first initialization key and the second initialization key are static keys;

receiving, from the protocol management computer, a communication via a near field communications channel;

in response to receiving the communication, transmitting, via the near field communications channel, first encrypted data comprising a first public key associated with the reader device, the first encrypted data having been encrypted by the reader device based at least in part on the second initialization key stored at the reader device;

receiving, from the protocol management computer, via the near field communications channel, second encrypted data comprising a second public key associated with protocol management computer; and

decrypting the second encrypted data based at least in part on the second initialization key stored at the reader device.

16. The reader device of claim 15, wherein the first initialization key and the second initialization key are symmetric keys, and wherein the operations further comprise:

receiving, from the protocol management computer, a first encrypted message comprising a first initialization vector, the first encrypted message being encrypted utilizing the symmetric key;

decrypting the first encrypted message utilizing the first initialization vector;

transmitting a second encrypted message comprising the first public key associated with the reader device, the second encrypted message being encrypted using a second initialization vector generated from the first initialization vector; and

receiving a third encrypted message comprising the second public key associated with the protocol management computer, the third encrypted message being encrypted utilizing a third initialization vector generated by the protocol management computer from the second initialization vector.

17. The reader device of claim 16, wherein the operations further comprise generating the second initialization vector from the first initialization vector, wherein the second initialization vector comprises twelve left-most bytes of the first initialization vector.

18. The reader device of claim 16, wherein the first encrypted message, the second encrypted message, and the third encrypted message are Application Protocol Data Unit messages defined by ISO/IEC 7816-4 communications standard.

19. The reader device of claim 15, wherein the operations further comprise generating the first public key as part of a public-private key pair.

20. The reader device of claim 16, wherein the operations further comprise transmitting, by the reader device to the protocol management computer, a fourth message, the fourth message indicating the third encrypted message was received successfully.