WHAT IS CLAIMED

1. A method comprising:

determining, by a user device, data including an electronic identifier associated with the user;

determining, by the user device, a key stored in a secure element of the user device;

digitally signing, by the user device, the data using the key;

determining, by the user device, a cryptogram; and

providing, by the user device, the signed data and the cryptogram to a reader device, wherein the reader device sends a request to include the signed data in an electronic ledger upon verifying the cryptogram.

2. The method of claim 1, wherein determining the cryptogram comprises:

determining, by the user device, a session key based on at least an intermediary key and a counter value; and

encrypting, by the user device, the data using the session key.

3. The method of claim 2, wherein the intermediary key is a limited use key.

4. The method of claim 2, wherein the intermediary key is a static key.

5. The method of claim 1, wherein providing the signed data and the cryptogram to the reader device comprises:

detecting, by the user device, that the reader device is proximate; and

sending, by the user device, the signed data and the cryptogram to the reader device over a short-range wireless connection.

6. A method comprising:

receiving, by a reader device from a user device, signed data and a cryptogram, wherein the signed data is determined by digitally signing data including an electronic identifier associated with the user using a key stored in a secure element of the user device;

determining, by the reader device, whether the cryptogram can be verified; and

upon verifying the cryptogram, sending, by the reader device, a request to a remote server computer to include the signed data in an electronic ledger.

7. The method of claim 6, wherein the cryptogram is determined using a session key that is determined based on at least an intermediary key and a counter value.

8. The method of claim 7, wherein verifying the cryptogram comprises:

determining, by the reader device, the session key;

decrypting, by the reader device, the cryptogram using the session key to determine a first value;

decrypting, by the reader device, the signed data to determine a second value; and

determining, by the reader device, that the first value and the second value match.

9. The method of claim 8, further comprising:

receiving, by the reader device, one or more dynamic values utilized to generate the session key from the user device.

10. The method of claim 6, wherein receiving the signed data and the cryptogram from the user device comprises:

detecting, by the reader device, that the user device is proximate; and

receiving, by the reader device, the signed data and the cryptogram from the user device over a short-range wireless connection.

11. A user device comprising:

a processor; and

a computer readable medium coupled to the processor, the computer readable medium comprising code, executable by the processor, to perform a method comprising:

determining data including an electronic identifier associated with the user;

determining a key stored in a secure element of the user device;

digitally signing the data using the key;

determining a cryptogram; and

providing the signed data and the cryptogram to a reader device, wherein the reader device sends a request to include the signed data in an electronic ledger upon verifying the cryptogram.

12. The user device of claim 11, wherein the step of determining the cryptogram in the method comprises:

determining a session key based on at least an intermediary key and a counter value; and

encrypting the data using the session key.

13. The user device of claim 12, wherein the intermediary key is a limited use key.

14. The user device of claim 12, wherein the intermediary key is a static key.

15. The user device of claim 11, wherein the step of providing the signed data and the cryptogram to the reader device in the method comprises:

detecting that the reader device is proximate; and

sending the signed data and the cryptogram to the reader device over a short-range wireless connection.

16. A reader device comprising:

a processor; and

a computer readable medium coupled to the processor, the computer readable medium comprising code, executable by the processor, to perform a method comprising:

receiving, from a user device, signed data and a cryptogram, wherein the signed data is determined by digitally signing data including an electronic identifier associated with the user using a key stored in a secure element of the user device;

determining, by the reader device, whether the cryptogram can be verified; and

upon verifying the cryptogram, sending, by the reader device, a request to a remote server computer to include the signed data in an electronic ledger.

17. The reader device of claim 16, wherein the cryptogram is determined using a session key that is determined based on at least an intermediary key and a counter value.

18. The reader device of claim 16, wherein the step of verifying the cryptogram in the method comprises:

determining the session key;

decrypting the cryptogram using the session key to determine a first value;

decrypting the signed data to determine a second value; and

determining that the first value and the second value match.

19. The reader device of claim 18, wherein the method further comprises:

receiving, by the reader device, one or more dynamic values utilized to generate the session key from the user device.

20. The reader device of claim wherein the step of receiving the signed data and the cryptogram from the user device in the method comprises:

detecting that the user device is proximate; and

receiving the signed data and the cryptogram from the user device over a short-range wireless connection.

WHAT IS CLAIMED

1. A method comprising:
determining, by a user device, data including an electronic identifier associated with the user;
determining, by the user device, a key stored in a secure element of the user device;
digitally signing, by the user device, the data using the key;
determining, by the user device, a cryptogram; and
providing, by the user device, the signed data and the cryptogram to a reader device, wherein the reader device sends a request to include the signed data in an electronic ledger upon verifying the cryptogram.

2. The method of claim 1, wherein providing the signed data and the cryptogram to the reader device comprises:
detecting, by the user device, that the reader device is proximate; and
sending, by the user device, the signed data and the cryptogram to the reader device over a short-range wireless connection.

3. A method comprising:
receiving, by a reader device from a user device, signed data and a cryptogram, wherein the signed data is determined by digitally signing data including an electronic identifier associated with the user using a key stored in a secure element of the user device;
determining, by the reader device, whether the cryptogram can be verified; and
upon verifying the cryptogram, sending, by the reader device, a request to a remote server computer to include the signed data in an electronic ledger.

4. The method of claim 3, wherein verifying the cryptogram comprises:
determining, by the reader device, a session key;
decrypting, by the reader device, the cryptogram using the session key to determine a first value;
decrypting, by the reader device, the signed data to determine a second value; and
determining, by the reader device, that the first value and the second value match.

5. The method of claim 4, further comprising:
receiving, by the reader device, one or more dynamic values utilized to generate the session key from the user device.

6. The method of claim 3, wherein receiving the signed data and the cryptogram from the user device comprises:
detecting, by the reader device, that the user device is proximate; and
receiving, by the reader device, the signed data and the cryptogram from the user device over a short-range wireless connection.

7. A user device comprising:
a processor; and

a computer readable medium coupled to the processor, the computer readable medium comprising code, executable by the processor, to perform a method comprising:

determining data including an electronic identifier associated with the user;

determining a key stored in a secure element of the user device;

digitally signing the data using the key;

determining a cryptogram; and

providing the signed data and the cryptogram to a reader device, wherein the reader device sends a request to include the signed data in an electronic ledger upon verifying the cryptogram.

8. The user device of claim 7, wherein the step of providing the signed data and the cryptogram to the reader device in the method comprises:

detecting that the reader device is proximate; and

sending the signed data and the cryptogram to the reader device over a short-range wireless connection.

9. A reader device comprising:

a processor; and

a computer readable medium coupled to the processor, the computer readable medium comprising code, executable by the processor, to perform a method comprising:

receiving, from a user device, signed data and a cryptogram, wherein the signed data is determined by digitally signing data including an electronic identifier associated with the user using a key stored in a secure element of the user device;

determining, by the reader device, whether the cryptogram can be verified; and

upon verifying the cryptogram, sending, by the reader device, a request to a remote server computer to include the signed data in an electronic ledger.

10. The reader device of claim 9, wherein the step of verifying the cryptogram in the method comprises:

determining the session key;

decrypting the cryptogram using the session key to determine a first value;

decrypting the signed data to determine a second value; and

determining that the first value and the second value match.

11. The reader device of claim 10, wherein the method further comprises:

receiving, by the reader device, one or more dynamic values utilized to generate the session key from the user device.

12. The reader device of claim 9 wherein the step of receiving the signed data and the cryptogram from the user device in the method comprises:

detecting that the user device is proximate; and

receiving the signed data and the cryptogram from the user device over a short-range wireless connection.

13. The method of claim 1, wherein the ledger is in the form of a blockchain.

14. The user device of claim 7, wherein the ledger is in the form of a blockchain.

15. The method of claim 3, wherein the reader device is operated by a resource provider, and the ledger is in the form of a blockchain.

16. The reader device of claim 9, wherein the reader device is operated by a resource provider, and the ledger is in the form of a blockchain.