

WHAT IS CLAIMED IS:

1. A computer-implemented method for performing offline authentication, comprising:

~~receiving, at an access device, a first public key associated with a certificate authority;~~

~~while operating in an offline mode:~~

obtaining, by the access device from a one-way communication, a data packet from a user device;

converting, at the access device, the data packet to obtain interaction data comprising a digital certificate certified by ~~the~~ a certificate authority, an index associated with the certificate authority, and a digital signature value generated by the user device;

obtaining, at the access device, a first public key associated with the certificate authority based on the index;

obtaining, at the access device, a second public key associated with the user device ~~utilizing the digital certificate and the~~ based on the first public key associated with the certificate authority and the digital certificate;

determining, at the access device, validity of the interaction data based at least in part on the digital signature value and the second public key associated with the user device;

in response to when the interaction data is being determined to be valid, ~~authorizing~~ verifying, at the access device, ~~an whether a first identifier of~~ associated with the interaction data satisfies a first condition; ~~and~~

in response to the first identifier satisfying the first condition, verifying, at the access device, whether a second identifier associated with the user device satisfies a second condition; and

providing, by the access device, access based at least in part on ~~determining that the identifier of the interaction data is authorized~~ the first condition and the second condition being satisfied.

2. The computer-implemented method of claim 1, wherein the data packet is obtained in the form of a quick response (QR) code presented via a display of the user device.

3. The computer-implemented method of claim 1, wherein the data packet is obtained in the form of a sound presented via a speaker of the user device.

4. The computer-implemented method of claim 1, wherein the digital certificate has been certified by the certificate authority within a threshold time period prior to the access device obtaining the data packet.

5. The computer-implemented method of claim 1, wherein the digital signature value is generated utilizing an elliptic curve cryptographic algorithm.

6. The computer-implemented method of claim 1, wherein providing, by the access device, access to the resource based at least in part on ~~determining that the identifier of the interaction data is authorized~~ the first condition and the second condition being satisfied, further comprises:

comparing, by the access device, the second identifier associated with the user device to a stored list of restricted identifiers; and

determining, by the access device, that the second identifier is excluded from the list of restricted identifiers, wherein providing access to the resource is based at least in part on the determining that the second identifier is excluded from the list of restricted identifiers.

7. The computer-implemented method of claim 1, further comprising:

extracting, by the access device, the first identifier from the interaction data, the first identifier corresponding to at least one a timestamp data field of the interaction data; and

comparing, by the access device, the ~~at least one timestamp data field~~ to a current time, wherein providing access to the resource is further based at least in part on comparing the ~~at least one timestamp data field~~ to the current time.

8. The computer-implemented method of claim 1, further comprising:

subsequent to providing access to the resource, performing, by the access device, an online authorization request procedure with a central server computer.

9. The computer-implemented method of claim 1, wherein the digital signature value is generated utilizing an elliptical curve cryptography algorithm, a private key associated with the user device, and at least one timestamp data field, a public key index data field, and a public key certificate of the interaction data.

10. The computer-implemented method of claim 1, further comprising:

obtaining, by the access device, ~~a certificate authority~~ the index by decrypting the from the decrypted interaction data; and

retrieving, by the access device, the first public key associated with the certificate authority based at least in part on the ~~certificate authority index~~.

11. An access device, comprising:

one or more processors; and

one or more memories storing computer-executable instructions, wherein executing the computer-executable instructions by the one or more processors, causes the access device to:

~~receive a first public key associated with a certificate authority;~~

~~while operating in an offline mode:~~

receive, in a one-way communication, a data packet from a user device;

convert the data packet to obtain interaction data comprising a digital certificate certified by ~~the~~ a certificate authority, an index associated with the certificate authority, and a digital signature value generated by the user device;

obtain a first public key associated with the certificate authority based on the index;

obtain a second public key associated with the user device ~~utilizing the digital certificate and~~ based on the first public key and the digital certificate associated with the certificate authority;

determine validity of the interaction data based at least in part on the digital signature value and the second public key associated with the user device;

~~when in response to the interaction data is being determined to be valid, authorize~~ verify whether an a first identifier of associated with the interaction data satisfies a first condition; ~~and~~

in response to the first identifier satisfying the first condition, verify whether a second identifier of the user device satisfies a second condition; and

provide access based at least in part on ~~determining that the identifier of the interaction data is authorized~~ the first condition and the second condition being satisfied.

12. The access device of claim 11, wherein the data packet is obtained in the form of a quick response (QR) code presented via a display of the user device.

13. The access device of claim 11, wherein the data packet is obtained in the form of a sound presented via a speaker of the user device.

14. The access device of claim 11, wherein the digital certificate has been certified by the certificate authority within a threshold time period prior to the access device obtaining the data packet.

15. The access device of claim 11, wherein the digital signature value is generated utilizing an elliptic curve cryptographic algorithm.

16. The access device of claim 11, wherein providing access to the resource based at least in part on ~~determining that the identifier of the interaction data is authorized~~ the first condition and the second condition being satisfied, further causes the access device to:

compare the second identifier associated with the user device to a stored list of restricted identifiers; and

determine that the second identifier is excluded from the list of restricted identifiers, wherein providing access to the resource is based at least in part on the determining that the second identifier is excluded from the list of restricted identifiers.

17. The access device of claim 11, wherein executing the computer-executable instructions by the one or more processors, further causes the access device to:

extract the first identifier from the interaction data, the first identifier corresponding to at least one a timestamp data field of the interaction data; and

compare the ~~at least one~~ timestamp data field to a current time, wherein providing access to the resource is further based at least in part on comparing the ~~at least one~~ timestamp data field to the current time.

18. The access device of claim 11, wherein executing the computer-executable instructions by the one or more processors, further causes the access device to:

perform an online authorization request procedure with a central server computer subsequent to providing access to the resource.

19. The access device of claim 11, wherein the digital signature value is generated utilizing an elliptical curve cryptography algorithm, a private key associated with the user device, and at least one timestamp data field, a public key index data field, and a public key certificate of the interaction data.

20. The access device of claim 11, wherein executing the computer-executable instructions by the one or more processors, further causes the access device to:

obtain ~~a certificate authority~~ the index from the decrypted by decrypting the interaction data; and

retrieve the first public key associated with the certificate authority based
at least in part on the ~~certificate authority~~ index.