CLAIMS

1. A computing device, comprising:

a memory configured to store instructions; and

processing circuitry coupled with the memory, the processing circuitry configured to execute the instructions, and when executed, the instructions to cause processing circuitry to:

determine to establish a communication connection with a second computing device;

~~generate~~detect a contactless card within in wireless communication range of the computing device;

receive, from the contactless card, an encrypted payload ~~with~~ comprising an identifier, wherein the encrypted payload is generated by the contactless card utilizing a key and a cryptographic algorithm, and the ~~encrypted payload comprising an~~ identifier to uniquely identify a customer associated with the contactless card, the computing device, or both;

send the encrypted payload and a call number to service provider system to initiate establishment the communication connection with the second computing device; and

establish the communication connection with the second computing device based on a successful authentication performed by the service provider system utilizing the encrypted payload including the identifier.

2. The computing device of claim 1, wherein the identifier comprises on one or more of password information, answers to pre-stored queries, biometric information, an image, or combination thereof.

3. The computing device of claim 1, wherein the identifier comprises audio data, and the audio data is unique to an expected user of the computing device.

4. The computing device of claim 1, wherein the call number is associated with the second computing device to establish the call communication connection with the second computing device.

5. The computing device of claim 1, wherein the key is a private key of a key pair, and the service provider system to decrypt the encrypted payload with a public key of the key pair to authenticate the identifier.

~~6. The computing device of claim 1, wherein the memory further comprises the key and the identifier, and the processing circuitry to retrieve the key and the identifier from the memory to generate the encrypted payload.~~

6~~7~~. The computing device of claim 1, wherein the service provider system comprises a Voice over Internet Protocol (VoIP) network, a Public Switched Telephone Network (PSTN), or a combination thereof.

8~~7~~. A computer-implemented method, comprising:

a memory configured to store instructions; and

determining, by a processor of a computing device, to establish a communication connection with a second computing device;

~~determining encrypted payload,~~detecting a contactless card within in wireless communication range of the computing device;

receiving, from the contactless card, an encrypted payload comprising an identifier ~~to uniquely identify~~, wherein the ~~computing device~~ encrypted ~~with~~payload is generated by the contactless card utilizing a key and a cryptographic algorithm, and the identifier to uniquely identify a customer associated with the contactless card, the computing device, or both;

sending the encrypted payload and a call number to service provider system to initiate establishment the communication connection with the second computing device, wherein the call number is associated with the second computing device; and

communicating, via the communication connection, with the second computing device based on a successful authentication performed by the service provider system utilizing the encrypted payload including the identifier.

9. 8. The computer-implemented method of claim 8~~7~~, wherein the identifier comprises on one or more of password information, answers to pre-stored queries, biometric information, an image, or combination thereof.

10~~9~~. The computer-implemented method of claim 7~~8~~, wherein the identifier comprises audio data, and the audio data is unique to an expected user of the computing device.

~~11. The computer-implemented method of claim 8, wherein the identifier comprises data received from a contactless card.~~

~~12. The computer-implemented method of claim 8, comprising receiving, from a contactless card, the encrypted payload comprising the identifier, wherein the encrypted payload is generated by the contactless card utilizing the key and the cryptographic algorithm.~~

~~13~~10. The computer-implemented method of claim 7~~12~~, wherein the encrypted payload is received in a message authentication code (MAC) cryptogram.

~~14~~11. The ~~computing~~computer-implemented method of claim ~~12~~7, wherein the encrypted payload is received via near-field communication (NFC) interface as part of an NFC exchange with the contactless card.

~~15.~~12 The computer-implemented method of claim ~~14~~11, comprising sending an NFC read to the contactless card to request the encrypted payload and cause generation of a message authentication (MAC) cryptogram to communicate the encrypted payload.

~~16~~13. The computer-implemented method of claim ~~8~~7, wherein the key is a private key of a key pair, and the service provider system to decrypt the encrypted payload with a public key of the key pair to authenticate the identifier.

~~17. The computer-implemented method of claim 8, comprising:~~

~~storing, in a memory of the computing device, the key and the identifier;~~

~~retrieving, by a processor of the computing device, the key and the identifier; and~~

~~generating the encrypted payload by applying the cryptographic algorithm and the key to the identifier.~~

~~18~~14. The computer-implemented method of claim 7~~8~~, wherein the service provider system comprises a voice over Internet Protocol (VoIP) network, a public switched telephone network (PSTN), or a combination thereof.

~~19~~15. A computer-readable medium storing instructions, the instructions configured to, when executed, cause one or more processors of a first computing device to:

determine to establish a communication connection with a second computing device;

~~determine encrypted payload,~~detect a contactless card within in wireless communication range of the computing device;

receive, from the contactless card, an encrypted payload comprising an identifier ~~to uniquely identify~~, wherein the ~~computing device~~ encrypted ~~with~~payload is generated by the contactless card utilizing a key and a cryptographic algorithm, and the identifier to uniquely identify a customer associated with the contactless card, the computing device, or both;

send the encrypted payload and a call number to service provider system to initiate establishment the communication connection with the second computing device, wherein the call number is associated with the second computing device; and

communicate, via the communication connection, with the second computing device based on a successful authentication performed by the service provider system utilizing the encrypted payload including the identifier.

~~20. The computer-readable medium of claim 19, further comprising instructions to cause the one or more processors to:~~

~~retrieve the key and the identifier from memory; and~~

~~generate the encrypted payload by applying the cryptographic algorithm and the key to the identifier.~~