CLAIMS

1. A computer-readable media embodied with programming code, that when executed by a processor of a client device cause the processor to:

provide, by the client device, a support request to access call center services of a service provider system;

determine a first multifactor authentication process for the client device has occurred;

in response to the determination, populate a client interface of thea client device with customer service web content delivered to the client device by the service provider system;

present on the client interface a prompt from the customer service web content that requests a connection with a contactless card;

establish a connection with the contactless card via a communication link between the client device and the contactless card;

receive customer information from the contactless card, wherein the customer information includes a number for the call center services and a pre-authentication number, wherein the pre-authentication number is a unique number associated with pre-authentication of the client device;

generate, using the number for the call center services, a call to the call center services of the service provider system, wherein the generated call includes the pre-authentication number; and

obtain, based on the pre-authentication number included in the generated call to the call center services, an advanced position in a call handling queue of incoming calls that bypasses an authentication queue.

2. The computer-readable media of claim 1, wherein the programming code, that when executed by the processor of the client device, further causes the processor to: generate the pre-authentication number in response to a communication with the contactless card.

3. The computer-readable media of claim 1, wherein the programming code, that when executed by the processor of the client device, further causes the processor to:

in response to a subsequent customer support request, change the preauthentication number from a previous pre-authentication number.

4. The computer-readable media of claim 1, wherein the programming code, that when executed by the processor of the client device, further causes the processor to:

generate a prompt requesting re-authorization of the client device.

5. The computer-readable media of claim 1, wherein the programming code, that when executed by the processor of the client device, further causes the processor to:

communicate with the contactless card; and

in response to communicating with the contactless card, receive authentication information.

6. The computer-readable media of claim 5, wherein the authentication information includes the pre-authentication number.

7. The computer-readable media of claim 1, wherein the programming code, that when executed by the processor of the client device further causes the processor, when generating the call to the call center services, to:

append the pre-authentication number to the number for the call center services.

8. A method, comprising:

providing, by a processor of a client device, a support request to access call center services of a service provider system;

determining a first multifactor authentication process for the client device has occurred;

in response to the determination, populating a client interface of the~~a~~ client device with customer service web content delivered to the client device by the service provider system;

presenting on the client interface a prompt from the customer service web content that requests a connection with a contactless card;

establishing a connection with the contactless card via a communication link between the client device and the contactless card;

receiving customer information from the contactless card, wherein the customer information includes a number for the call center services and a pre-authentication number, wherein the pre-authentication number is a unique number associated with pre-authentication of the client device;

generating, using the number for the call center services, a call to the call center services of the service provider system, wherein the generated call includes the pre-authentication number; and

obtaining, based on the pre-authentication number included in the generated call to the call center services, an advanced position in a call handling queue of incoming calls that bypasses an authentication queue.

9. The method of claim 8, further comprising:

generating the pre-authentication number in response to a communication with the contactless card.

10. The method of claim 8, further comprising:

in response to a subsequent customer support request, changing the pre-authentication number from a previous pre-authentication number.

11. The method of claim 8, further comprising:

generating a prompt requesting re-authorization of the client device.

12. The method of claim 8, further comprising:

communicating by the client device with the contactless card; and

in response to communicating the contactless card, receiving authentication information by the client device.

13. The method of claim 11, wherein the authentication information includes the pre-authentication number.

14. The method of claim 11, when generating the call, further comprises:

appending, by the processor, the pre-authentication number to the number for the call center services.

15. A computer-implemented method, comprising:

receiving, by a service provider system, a support request from a client device, the support request being a request to access a service provider application executing call center services;

in response to the support request, sending to the client device by the service provider system, a request for second authentication information of a contactless card;

receiving, by the service provider system from the client device, the second authentication information including a cryptogram;

obtaining a validation of the cryptogram based on an authentication process performed by the service provider system, which validates the client device;

responsive to the validation of the client device,

receiving by the service provider system an incoming call from the client device, wherein the incoming call includes a pre-authentication number that is a unique number associated with pre-authentication of the client device;

filtering, by the service provider system the incoming call for the pre-authentication number; and

based on the filtering indicating the incoming call is pre-authenticated, advancing the incoming call to a position in a call handling queue that bypasses an authentication queue.

16. The method of claim 15, wherein the first authentication information includes one of credentials, biometric information, a key, or combination thereof.

17. The method of claim 15, further comprising:

maintaining by the authentication server a copy of a master key used to generate a diversity key which is used to validate the cryptogram.

18. The method of claim 17, further comprising:

decrypting, by the authentication server, information in the cryptogram received from the client device using the diversified key generated from the copy of the master key maintained by the authentication server to expose the counter value from the contactless card, wherein the counter value is included with the second authentication information of the contactless card;

comparing a counter value included in the cryptogram received from the client device to a counter value retrieved by the authentication server; and

in response to the comparison indicating a match, generating the validation.

19. The method of claim 16, further comprising:

authorizing the client device for access to the customer relationship management server upon receipt of a previously-received cryptogram from the client device.

20. The method of claim 15, wherein the service provider system comprises a customer relationship management server to process the incoming call including filtering the incoming call and advancing the incoming call and an authentication server to perform the authentication process.