[0005] To address these security concerns, the Payment Card Industry Security Standards Council (PCI SSC) manages the ongoing evolution of the Payment Card Industry (PCI) security standards. Service providers are responsible for enforcing compliance with PCI standards to protect sensitive customer data. For example, the PCI standards may dictate authentication standards to be followed prior to permitting a client to access and/or modify customer account information. Call centers may require client authentication in the form of exchange of passwords, answers to personal questions, biometric data or the like. Customers may be prompted multiple times to provide authentication information in various forms during the handling of a call. Not only can this authentication and re-authentication process frustrate a client and degrade the service provider goodwill, each authentication instance potentially exposes sensitive customer information to potentially malicious parties.

SUMMARY

[0005a] According to a first aspect of the present invention, there is provided 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 a 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.

[0005b] According to a second aspect of the present invention, there is provided 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 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.

[0005c] According to a third aspect of the present invention, there is provided 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.

[0006] There is disclosed a method for pre-authenticating support requests received by a service provider from one or more coupled devices includes the steps of receiving a support request from a client operating a client device that has been authorized to access a service provider application in response to

first authentication information provided by the client. In response to the support request, the method includes requesting second authentication information from the client, the second authentication information including a cryptogram and receiving the second authentication information including the cryptogram from the client device. The method includes selectively validating the client by decrypting at least a portion of the second authentication information using a copy of a key associated with the client and maintained by the service provider. The method includes the steps of, responsive to validation of the client, initiating a call with the client device and directing a call center support service to bypass an authorization step of a call center support process to expedite handling of the initiated call. With such an arrangement, multi-factor authentication

mechanisms of the service provider may be leveraged for use with customer support services, thereby increasing the efficiency of client issue resolution and increasing customer information security.

[0007] There is disclosed a system for pre-authenticating customer service support requests received at a service provider from one or more coupled client devices includes a client interface adapted to exchange information with one or more coupled client devices. The system also includes a storage device and a diversified key table stored in the storage device and comprising an entry for at least one client of the service provider, the entry including first and second authentication information for the client. The system further includes an authentication unit, coupled to the client interface and the diversified key table, for retrieving one of the first or second authentication information upon receipt of a client request by the client interface and for authorizing the client request in response to the retrieved first or second authentication information. A customer call center interface is coupled to the authentication unit, for selectively forwarding a support request, received from a client device, to a call center service, the support request forwarded following authorization of the support request by the authentication unit, the customer call center interface augmenting the support request to direct the call center service to bypass authentication of the support request by a call center service process.

[0008] There is disclosed a method for pre-authenticating support requests received by a service provider from one or more coupled client devices includes the steps of receiving a support request from a client device that has been authorized to access a service provider application in response to first authentication information provided by the client. In response to receiving the support request, the method includes prompting a client to engage a card with the client device to retrieve second authentication information from the card, the second authentication information including a cryptogram and receiving the second authentication information. The method includes selectively validating the support request by decrypting at least a portion of the

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 a 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 pre-authentication 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 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.