

portion using the parameters received in the parameter portion, manage key material for security of the data, and transmit the encrypted data back to the calling application.

[0007a] In yet another embodiment, a computer-based method for remote cryptographic services to a client application in a service call to a service system in a service provider computer system, said method comprising: storing identity information for a plurality of client applications; generating, by a key management services module associated with the service provider computer system, an encryption key, wherein the encryption key is associated with at least one client application of the plurality of client applications, wherein the encryption key is used by a cryptography provider to encrypt application data; exposing a cryptography service provider API to the plurality of client applications, wherein the cryptography service provider API is configured to i) deliver encryption requests and decryption requests to the cryptography provider, and ii) deliver encrypted data and decrypted data to the plurality of client applications; receiving, via the cryptography service provider API, an encryption request from the at least one client application, wherein the encryption request includes data for an end-user of the at least one client application, wherein the encryption request includes at least one encryption parameter specified by the at least one client application for use in encrypting the data, and wherein the at least one encryption parameter identifies an encryption type and an encryption strength; encrypting the data using the generated encryption key, the encryption type specified by the at least one client application, and the encryption strength specified by the at least one client application; transmitting, via the cryptography service provider API, the encrypted data to the at least one client application without transmitting the encryption key to the at least one client application; receiving, from the at least one client application, a decryption request comprising at least a parameter portion and the encrypted data, wherein the parameter portion defines the encryption type associated with the encrypted data and the encryption strength associated with the encrypted data; determining an identity of the at least one client application transmitting the received message based on the identity information and the parameter portion; decrypting the encrypted data based on the generated encryption key, the encryption type, and the encryption strength; and transmitting the decrypted data back to the at least one client application.

[0007b] In yet another embodiment, a computer system for processing data, the computer system comprising a memory device and a processor in communication with

the memory device, the computer system programmed to: store identity information for a plurality of client applications; generate, by a key management services module associated with the service provider computer system, an encryption key, wherein the encryption key is associated with at least one client application of the plurality of client applications, wherein the encryption key is used by a cryptography provider to encrypt application data; expose a cryptography service provider API to the plurality of client applications, wherein the cryptography service provider API is configured to i) deliver encryption requests and decryption requests to the cryptography provider, and ii) deliver encrypted data and decrypted data to the plurality of client applications; receive, via the cryptography service provider API, an encryption request from the at least one client application, wherein the encryption request includes data for an end-user of the at least one client application, wherein the encryption request includes at least one encryption parameter specified by the at least one client application for use in encrypting the data, and wherein the at least one encryption parameter identifies an encryption type and an encryption strength; encrypt the data using the generated encryption key, the encryption type specified by the at least one client application, and the encryption strength specified by the at least one client application; transmit, via the cryptography service provider API, the encrypted data to the at least one client application without transmitting the encryption key to the at least one client application; receive from the at least one client application, a decryption request comprising at least a parameter portion and the encrypted data, wherein the parameter portion defines the encryption type associated with the encrypted data and the encryption strength associated with the encrypted data; determine an identity of the at least one client application transmitting the received message based on the identity information and the parameter portion; decrypt the encrypted data based on the generated encryption key, the encryption type, and the encryption strength; and transmit the decrypted data back to the at least one client application.

[0007c] In yet another embodiment, one or more non-transitory computer-readable storage media having computer-executable instructions embodied thereon, wherein when executed by at least one processor, the computer-executable instructions cause the processor to: store identity information for a plurality of client applications; generate, by a key management services module associated with the service provider computer system, an encryption key, wherein the encryption key is associated with at least

one client application of the plurality of client applications, wherein the encryption key is used by a cryptography provider to encrypt application data; expose a cryptography service provider API to the plurality of client applications, wherein the cryptography service provider API is configured to i) deliver encryption requests and decryption requests to the cryptography provider, and ii) deliver encrypted data and decrypted data to the plurality of client applications; receive, via the cryptography service provider API, an encryption request from the at least one client application, wherein the encryption request includes data for an end-user of the at least one client application, wherein the encryption request includes at least one encryption parameter specified by the at least one client application for use in encrypting the data, and wherein the at least one encryption parameter identifies an encryption type and an encryption strength; encrypt the data using the generated encryption key, the encryption type specified by the at least one client application, and the encryption strength specified by the at least one client application; transmit, via the cryptography service provider API, the encrypted data to the at least one client application without transmitting the encryption key to the at least one client application; receive from the at least one client application, a decryption request comprising at least a parameter portion and the encrypted data, wherein the parameter portion defines the encryption type associated with the encrypted data and the encryption strength associated with the encrypted data; determine an identity of the at least one client application transmitting the received message based on the identity information and the parameter portion; decrypt the encrypted data based on the generated encryption key, the encryption type, and the encryption strength; and transmit the decrypted data back to the at least one client application.

BRIEF DESCRIPTION OF THE DRAWINGS

[0008] Figures 1-9 show exemplary embodiments of the methods and systems described herein.

[0009] Figure 1 is a schematic diagram illustrating an exemplary multi-party transaction card industry system for enabling ordinary payment-by-card transactions in which merchants and card issuers do not need to have a one-to-one special relationship.

[0010] Figure 2 is a simplified block diagram of an exemplary processing system including a plurality of computer devices in accordance with one embodiment of the present invention.

[0011] Figure 3 is an expanded block diagram of an exemplary embodiment of a server architecture of a processing system including other computer devices in accordance with one embodiment of the present invention.

[0012] Figure 4 illustrates an exemplary configuration of a user system operated by a user, such as the cardholder shown in Figure 1.

[0013] Figure 5 illustrates an exemplary configuration of a server system such as the server system shown in Figures 2 and 3.

[0014] Figure 6 illustrates a data flow diagram of a security services system in accordance with an exemplary embodiment of the present disclosure.

[0015] FIG. 7 is a block diagram of the centralized web services platform shown in FIG. 6 in accordance with an exemplary embodiment of the present disclosure.

[0016] FIG. 8 is a flow diagram of a method of handling a call for services from the centralized web services platform shown in FIG. 6 by an application in accordance with an exemplary embodiment of the present disclosure.

CLAIMS

1. A computer-based method for providing bundled services to a client application in a service call to a service system in a service provider computer system, said method comprising:

5 receiving a message defining an API service request comprising at least a parameter portion and a payload portion;

determining at the gateway system an identity of an application transmitting the received message using identity information that has been established within the service provider computer system;

10 providing, by a services platform, at least one of encryption services and decryption services for data contained in the payload portion using the parameters received in the parameter portion;

managing key material for security of the data; and

transmitting the encrypted data back to the calling application.

2. The computer-based method of Claim 1, further comprising selecting at least one encryption algorithm from a library of encryption algorithms to apply to the received data based on the received parameters.

3. The computer-based method of Claim 2, further comprising storing an encryption key generated during the encryption in the services platform.

4. The computer-based method of Claim 2, further comprising selecting a decryption algorithm from a library of decryption algorithms corresponding to the selected encryption algorithm to apply to the received data based on the received parameters.

5. The computer-based method of Claim 1, wherein receiving a message defining an API service request comprises receiving a message defining an API

service request from at least one of an application external to the service provider computer system and an application internal to the service provider computer system.

6. The computer-based method of Claim 1, wherein receiving a message defining an API service request comprises receiving a message defining an API service request from a website associated with the service provider computer system.

7. The computer-based method of Claim 1, wherein receiving a message defining an API service request comprises receiving a message defining an API service request from an application not associated with the service provider computer system.

8. A computer system for processing data, the computer system comprising a memory device and a processor in communication with the memory device, the computer system programmed to:

5 receive a message defining an API service request comprising at least a parameter portion and a payload portion;

determine at the gateway system an identity of an application transmitting the received message using identity information that has been established within the service provider computer system;

10 provide, by a services platform, at least one of encryption services and decryption services for data contained in the payload portion using the parameters received in the parameter portion;

manage key material for security of the data; and

transmit the encrypted data back to the calling application.

9. The computer system of Claim 8, wherein said computer system is programmed to select at least one encryption algorithm from a library of encryption algorithms to apply to the received data based on the received parameters.

10. The computer system of Claim 9, wherein said computer system is programmed to store an encryption key generated during the encryption in the services platform.

11. The computer system of Claim 9, wherein said computer system is programmed to select a decryption algorithm from a library of decryption algorithms corresponding to the selected encryption algorithm to apply to the received data based on the received parameters.

12. The computer system of Claim 8, wherein said computer system is programmed to receive a message defining an API service request from at least one of an application external to the service provider computer system and an application internal to the service provider computer system.

13. The computer system of Claim 8, wherein said computer system is programmed to receive a message defining an API service request from a website associated with the service provider computer system.

14. The computer system of Claim 8, wherein said computer system is programmed to receive a message defining an API service request from an application not associated with the service provider computer system.

15. One or more non-transitory computer-readable storage media having computer-executable instructions embodied thereon, wherein when executed by at least one processor, the computer-executable instructions cause the processor to:

5 receive a message defining an API service request comprising at least a parameter portion and a payload portion;

determine at the gateway system an identity of an application transmitting the received message using identity information that has been established within the service provider computer system;

provide, by a services platform, at least one of encryption services and
10 decryption services for data contained in the payload portion using the parameters received
in the parameter portion;

manage key material for security of the data; and

transmit the encrypted data back to the calling application.

16. The computer-readable storage media of Claim 15, wherein the
computer-executable instructions further cause the processor to select at least one
encryption algorithm from a library of encryption algorithms to apply to the received data
based on the received parameters.

17. The computer-readable storage media of Claim 16, wherein the
computer-executable instructions further cause the processor to store an encryption key
generated during the encryption in the services platform.

18. The computer system of Claim 16, wherein said computer system is
programmed to select a decryption algorithm from a library of decryption algorithms
corresponding to the selected encryption algorithm to apply to the received data based on
the received parameters.

19. The computer-readable storage media of Claim 15, wherein the
computer-executable instructions further cause the processor to receive a message defining
an API service request from at least one of an application external to the service provider
computer system and an application internal to the service provider computer system.

20. The computer-readable storage media of Claim 15, wherein the
computer-executable instructions further cause the processor to receive a message defining
an API service request from a website associated with the service provider computer
system.

CLAIMS

1. A computer-based method for remote cryptographic services to a client application in a service call to a service system in a service provider computer system, said method comprising:

storing identity information for a plurality of client applications;

generating, by a key management services module associated with the service provider computer system, an encryption key, wherein the encryption key is associated with at least one client application of the plurality of client applications, wherein the encryption key is used by a cryptography provider to encrypt application data;

exposing a cryptography service provider API to the plurality of client applications, wherein the cryptography service provider API is configured to i) deliver encryption requests and decryption requests to the cryptography provider, and ii) deliver encrypted data and decrypted data to the plurality of client applications;

receiving, via the cryptography service provider API, an encryption request from the at least one client application, wherein the encryption request includes data for an end-user of the at least one client application, wherein the encryption request includes at least one encryption parameter specified by the at least one client application for use in encrypting the data, and wherein the at least one encryption parameter identifies an encryption type and an encryption strength;

encrypting the data using the generated encryption key, the encryption type specified by the at least one client application, and the encryption strength specified by the at least one client application;

transmitting, via the cryptography service provider API, the encrypted data to the at least one client application without transmitting the encryption key to the at least one client application;

receiving, from the at least one client application, a decryption request comprising at least a parameter portion and the encrypted data, wherein the parameter portion defines the encryption type associated with the encrypted data and the encryption strength associated with the encrypted data;

determining an identity of the at least one client application transmitting the received message based on the identity information and the parameter portion;

decrypting the encrypted data based on the generated encryption key, the encryption type, and the encryption strength; and

transmitting the decrypted data back to the at least one client application.

2. The computer-based method of Claim 1, further comprising selecting at least one encryption algorithm to apply to the encrypted data based on the parameter portion.

3. The computer-based method of Claim 2, further comprising storing the generated encryption key and the association in a cryptographic key material module.

4. The computer-based method of Claim 2, further comprising selecting a decryption algorithm corresponding to the selected encryption algorithm to apply to the received data based on the parameter portion.

5. The computer-based method of Claim 1, wherein receiving the encryption request further comprises receiving the encryption request from at least one of an application external to the service provider computer system and an application internal to the service provider computer system, and wherein receiving the decryption request further comprises receiving the decryption request from at least one of an application external to the service provider computer system and an application internal to the service provider computer system.

6. The computer-based method of Claim 1, wherein receiving the encryption request comprises receiving a message defining an API service request from a website associated with the service provider computer system.

7. The computer-based method of Claim 1, wherein receiving the encryption request comprises receiving a message defining an API service request from an application not associated with the service provider computer system.

8. A computer system for processing data, the computer system comprising a memory device and a processor in communication with the memory device, the computer system programmed to:

store identity information for a plurality of client applications;

generate, by a key management services module associated with the service provider computer system, an encryption key, wherein the encryption key is associated with at least one client application of the plurality of client applications, wherein the encryption key is used by a cryptography provider to encrypt application data;

expose a cryptography service provider API to the plurality of client applications, wherein the cryptography service provider API is configured to i) deliver encryption requests and decryption requests to the cryptography provider, and ii) deliver encrypted data and decrypted data to the plurality of client applications;

receive, via the cryptography service provider API, an encryption request from the at least one client application, wherein the encryption request includes data for an end-user of the at least one client application, wherein the encryption request includes at least one encryption parameter specified by the at least one client application for use in encrypting the data, and wherein the at least one encryption parameter identifies an encryption type and an encryption strength;

encrypt the data using the generated encryption key, the encryption type specified by the at least one client application, and the encryption strength specified by the at least one client application;

transmit, via the cryptography service provider API, the encrypted data to the at least one client application without transmitting the encryption key to the at least one client application;

receive from the at least one client application, a decryption request comprising at least a parameter portion and the encrypted data, wherein the parameter portion defines the encryption type associated with the encrypted data and the encryption strength associated with the encrypted data;

determine an identity of the at least one client application transmitting the received message based on the identity information and the parameter portion;

decrypt the encrypted data based on the generated encryption key, the encryption type, and the encryption strength; and

transmit the decrypted data back to the at least one client application.

9. The computer system of Claim 8, wherein said computer system is programmed to select at least one encryption algorithm to apply to the encrypted data based on the parameter portion.

10. The computer system of Claim 9, wherein said computer system is programmed to store the generated encryption key and the association in a cryptographic key material module.

11. The computer system of Claim 9, wherein said computer system is programmed to select a decryption algorithm corresponding to the selected encryption algorithm to apply to the received data based on the parameter portion.

12. The computer system of Claim 8, wherein receiving the encryption request further comprises receiving the encryption request from at least one of an application external to the service provider computer system and an application internal to the service provider computer system, and wherein receiving the decryption request further comprises receiving the decryption request from at least one of an application external to the service provider computer system and an application internal to the service provider computer system.

13. The computer system of Claim 8, wherein said computer system is programmed to receive the encryption request from a website associated with the service provider computer system.

14. The computer system of Claim 8, wherein said computer system is programmed to receive a message defining an API service request from a website associated with the service provider computer system.

15. One or more non-transitory computer-readable storage media having computer-executable instructions embodied thereon, wherein when executed by at least one processor, the computer-executable instructions cause the processor to:

store identity information for a plurality of client applications;

generate, by a key management services module associated with the service provider computer system, an encryption key, wherein the encryption key is associated with at least one client application of the plurality of client applications, wherein the encryption key is used by a cryptography provider to encrypt application data;

expose a cryptography service provider API to the plurality of client applications, wherein the cryptography service provider API is configured to i) deliver encryption requests and decryption requests to the cryptography provider, and ii) deliver encrypted data and decrypted data to the plurality of client applications;

receive, via the cryptography service provider API, an encryption request from the at least one client application, wherein the encryption request includes data for an end-user of the at least one client application, wherein the encryption request includes at least one encryption parameter specified by the at least one client application for use in encrypting the data, and wherein the at least one encryption parameter identifies an encryption type and an encryption strength;

encrypt the data using the generated encryption key, the encryption type specified by the at least one client application, and the encryption strength specified by the at least one client application;

transmit, via the cryptography service provider API, the encrypted data to the at least one client application without transmitting the encryption key to the at least one client application;

receive from the at least one client application, a decryption request comprising at least a parameter portion and the encrypted data, wherein the parameter portion defines the encryption type associated with the encrypted data and the encryption strength associated with the encrypted data;

determine an identity of the at least one client application transmitting the received message based on the identity information and the parameter portion;

decrypt the encrypted data based on the generated encryption key, the encryption type, and the encryption strength; and

transmit the decrypted data back to the at least one client application.

16. The computer-readable storage media of Claim 15, wherein the computer-executable instructions further cause the processor to select at least one encryption algorithm to apply to the encrypted data based on the parameter portion.

17. The computer-readable storage media of Claim 16, wherein the computer-executable instructions further cause the processor to store the generated encryption key and the association in a cryptographic key material module.

18. The computer-readable storage media of Claim 16, wherein the computer-executable instructions further cause the processor to select a decryption algorithm corresponding to the selected encryption algorithm to apply to the received data based on the parameter portion.

19. The computer-readable storage media of Claim 15, wherein the computer-executable instructions further cause the processor to receive the encryption request from at least one of an application external to the service provider computer system and an application internal to the service provider computer system.

20. The computer-readable storage media of Claim 15, wherein the computer-executable instructions further cause the processor to receive the encryption request from a website associated with the service provider computer system.