In accordance with another embodiment of the present disclosure, there is provided a method comprising: upon authenticating a user to an application for a secure file transfer of a file using a user authentication ID, obtaining a passphrase from a secure repository based upon the user authentication ID for authenticating a user to an application requiring the secure file transfer of the file; upon authenticating the passphrase, establishing a first connection with a first server to retrieve an authentication key from a secure key store; sending the authentication key and the passphrase to a second server; and upon validating the authentication key and the passphrase, establishing a second connection with the second server to initiate the secure file transfer of the file between the second server and a file recipient; wherein the first server comprises a secure file transfer protocol (SFTP) remote method invocation (RMI) server; and wherein the authentication key remains hidden from the application requiring the secure file transfer of the file.

In accordance with a second embodiment, a method comprises receiving a file transfer request and validating parameters for initiating the file transfer request including a file transfer authentication key and a passphrase for accessing the file transfer authentication key. Upon determining existence of the passphrase and authentication key, the method further comprises providing the passphrase and authentication key to a file transfer server to authenticate the file transfer request.

In accordance with a third embodiment of the present disclosure, there is provided an application server comprising: a secure file transfer protocol (SFTP) remote method invocation (RMI) client component; and a vault accessible by the SFTP RMI client to obtain a passphrase for authenticating a file transfer request by the application server, upon authenticating a user to an application using a user authentication ID and obtaining the passphrase based upon the user authentication ID; an SFTP RMI server, and a secure authentication key store from which the SFTP RMI server obtains an authentication key determined upon authentication of the obtained passphrase; wherein the SFTP RMI server is communicatively connected to an SFTP server, the SFTP server being communicatively connected to an intended file recipient initiating a file transfer upon validating the authentication key and the obtained passphrase, wherein the authentication key and the obtained passphrase are sent to the SFTP server by the SFTP RMI server; wherein the application server comprises a processing device to

implement an authorization and clearance of the file transfer request; and wherein the authentication key is owned by the SFTP RMI server and is hidden from the application server.

BRIEF DESCRIPTION OF THE DRAWINGS

Further aspects of the present disclosure will be more readily appreciated upon review of the detailed description of its various embodiments, described below, when taken in conjunction with the accompanying drawings.

FIG. 1 illustrates an example payment card transaction processing system.

FIG. 2A illustrates an example application and application server architecture for implementing secure file transfer with secure SSH key authentication.

FIG. 2B is an example message flow diagram illustrating the message flow between system entities to achieve secure file transfer with secure SSH key authentication in the application and application server architecture of FIG. 2.

FIG. 3A is a flowchart illustrating example processes performed by a client to initiate a secure file transfer in accordance with various embodiments of the present disclosure.

FIG. 3B is a flowchart illustrating example processes performed by a server to initiate a secure file transfer in accordance with various embodiments of the present disclosure.

FIG. 4 illustrates an example computing component that may be used in implementing features of various embodiments of the present disclosure.

CLAIMS

What is claimed is:

1. A method for supporting secure file transfer, the method comprising:

upon authenticating a user to an application for a secure file transfer of a file using a user authentication ID, obtaining a passphrase from a secure repository based upon the user authentication ID for authenticating a user to an application requiring the secure file transfer of the file;

upon authenticating the passphrase, establishing a first connection with a first server to retrieve an authentication key from a secure key store;

sending the authentication key and the passphrase to a second server; and

upon validating the authentication key and the passphrase, establishing a second connection with the second server to initiate the secure file transfer of the file between the second server and a file recipient;

wherein the first server comprises a secure file transfer protocol (SFTP) remote method invocation (RMI) server; and

wherein the authentication key remains hidden from the application requiring the secure file transfer of the file.

2. The method of claim 1, wherein the second server comprises an SFTP server communicatively connected to the file recipient.

3. The method of claim 1, wherein establishing the first connection with the first server comprises sending a file transfer request to the first server including a plurality of required arguments including a passphrase argument containing a value indicative of the passphrase.

4. The method of claim 1, wherein the authentication key comprises a secure shell (SSH) key.

5. The method of claim 1, wherein the first connection is established between the first server and an SFTP RMI client.

6. The method of claim 1, wherein the second connection is established between the second server and the first server.

7. An application server, comprising:

a secure file transfer protocol (SFTP) remote method invocation (RMI) client component;

a vault accessible by the SFTP RMI client to obtain a passphrase for authenticating a file transfer request by the application server, upon authenticating a user to an application using a user authentication ID and obtaining the passphrase based upon the user authentication ID;

an SFTP RMI server; and

a secure authentication key store from which the SFTP RMI server obtains an authentication key determined upon authentication of the obtained passphrase; [[and]]

wherein the SFTP RMI server is communicatively connected to an SFTP server, the SFTP server being communicatively connected to an intended file recipient initiating a file transfer upon validating the authentication key and the obtained passphrase, wherein the authentication key and the obtained passphrase are sent to the SFTP server by the SFTP RMI server;

wherein the application server comprises a processing device to implement an authorization and clearance of the file transfer request; and

wherein the authentication key is owned by the SFTP RMI server and is hidden from the application server.

8. The application server of claim 7, wherein the SFTP RMI server is communicatively connected to an SFTP server for effectuating a file transfer based on the file transfer request between the application server and an intended file recipient.

9. The application server of claim 7, wherein the vault is automatically accessed by the SFTP RMI client based upon an authentication ID for authenticating a user to the application server.