

as illustrative and not restrictive, and the intention is not to be limited to the details given herein, but may be modified within the scope of the appended claims along with their full scope of equivalents. For example, the various elements or components may be combined or integrated in another system or certain features may be omitted, or not implemented.

Also, techniques, systems, subsystems and methods described and illustrated in the various embodiments as discrete or separate may be combined or integrated with other systems, modules, techniques, or methods without departing from the scope of the present disclosure. Other items shown or discussed as directly coupled or communicating with each other may be coupled through some interface or device, such that the items may no longer be considered directly coupled to each other but may still be indirectly coupled and in communication, whether electrically, mechanically, or otherwise with one another. Other examples of changes, substitutions, and alterations are ascertainable by one skilled in the art and could be made without departing from the spirit and scope disclosed herein.

What is claimed is:

1. A method for securing enterprise data, comprising: receiving unencrypted data by an encryption gateway service stored in a memory and executed by a processor, wherein the encryption gateway service includes an encryption/decryption component stored in a memory and executed by a processor, an identity management component stored in a memory and executed by a processor, a notification component stored in a memory and executed by a processor, and a logging/auditing component stored in a memory and executed by a processor; authenticating and authorizing, by the identity management component, a user attempting to send the unencrypted data to the encryption gateway service by communicating with an enterprise identity management system; encrypting, by the encryption/decryption component, the unencrypted data; sending, by the notification component, a notification that the unencrypted data has been encrypted to an entity from which the unencrypted data was received within an enterprise operating the encryption gateway service; logging, by the logging/auditing component, that the unencrypted data has been encrypted; and sending, by the encryption gateway service, the encrypted data to a destination.
2. The method of claim 1 wherein the encryption gateway service further includes a key management component stored in a memory and executed by a processor, wherein encrypting the unencrypted data is based on using a key obtained by the key management component through communication with an enterprise key management data store.
3. The method of claim 1 wherein sending the notification that the unencrypted data has been encrypted comprises sending the notification via an enterprise messaging system.
4. The method of claim 1, wherein the notification is sent via one of an email message, an instant message, a text message, and a voice message.

5. The method of claim 1 further comprising sending, by the notification component, a notification that the encrypted data has been sent to the destination.

6. The method of claim 1 further comprising:

receiving, by the encryption gateway service, second encrypted data from the destination;

sending, by the notification component, a notification to an appropriate entity within the enterprise that the second encrypted data has been received;

decrypting, by the encryption/decryption component, the second encrypted data using a key obtained through communication with an enterprise key management data store; and

sending, by the encryption gateway service, the decrypted data to the appropriate entity.

7. The method of claim 6 wherein decrypting the second encrypted data comprises determining whether a user input from the appropriate entity indicates to decrypt the second encrypted data, and decrypting the second encrypted data in response to a determination that the user input from the appropriate entity indicates to decrypt the second encrypted data.

8. The method of claim 1 further comprising logging, by the logging/auditing component, the sending to the destination and the receiving from the destination.

9. The method of claim 1 wherein the encryption/decryption component uses a PGP encryption/decryption system to encrypt the data.

10. The method of claim 1 wherein the encryption gateway service is accessible to a plurality of client computers within the enterprise, wherein the plurality of client computers lack locally resident versions of the encryption/decryption component.

11. The method of claim 1 wherein sending the encrypted data to the destination comprises sending the encrypted data to the entity from which the unencrypted data was received, determining whether a user input from the entity indicates to send the encrypted data to the destination, and sending the encrypted data to the destination in response to a determination that the user input from the entity indicates to send the encrypted data to the destination.

12. The method of claim 1 further comprising sending, by the notification component, a notification to the entity from which the unencrypted data was received that the encrypted data has been sent to the destination.

13. The method of claim 1 further comprising:

providing, by the identity management component, enrollment services to a new communication partner;

providing, by the identity management component, expiration and renewal services to an existing communication partner; and

providing, by the identity management component, revocation services to the enterprise for communication partner access to the identity management component.

14. The method of claim 1 further comprising sending, by the encryption gateway service, the encrypted data to a retention repository.

15. The method of claim 14 further comprising, deleting, by the encryption gateway service, one of the encrypted data from the retention repository and the unencrypted data.

\* \* \* \* \*