ENCRYPTION GATEWAY SERVICE

CROSS-REFERENCE TO RELATED APPLICATIONS

None.

STATEMENT REGARDING FEDERALLY SPONSORED RESEARCH OR DEVELOPMENT

Not applicable.

REFERENCE TO A MICROFICHE APPENDIX

Not applicable.

FIELD OF THE INVENTION

The present disclosure relates to data security. More specifically, but not by way of limitation, a system and a method are provided for the centralized encryption and decryption of data.

BACKGROUND OF THE INVENTION

The increasing number of computer systems that are interconnected with other computer systems in computer networks and the increasing complexity of such networks have made the task of protecting computer systems from vulnerabilities increasingly difficult and costly. Data security-related issues that an enterprise might face include authentication and authorization of users, encryption of files and messages, digital rights management, filtering of unwanted content, and compliance with regulations and other standards. The encryption of files and messages, in particular, is seen as an effective means of protecting sensitive data.

SUMMARY OF THE INVENTION

In one embodiment, an encryption management system of an enterprise is provided. The system includes an encryption/decryption component operable for enterprise messages to be secured by receiving and encrypting the messages received from enterprise applications. The encryption/decryption component further decrypts messages received from enterprise partners that are encrypted. The system includes an identity management component to manage access to the encryption management system, and a key management component to manage keys used by the encryption/decryption component. The system includes a notification component that initiates sending messages regarding events occurring in the encryption management system through communication with an enterprise messaging system. The system also includes a logging/auditing component to log events occurring in the encryption management system. A server computer whereon at least the encryption/decryption component resides, the server computer accessible to a plurality of applications.

In another embodiment, a method for securing enterprise data is provided. The method includes sending unencrypted data to an encryption gateway service that includes an encryption/decryption component, an identity management component, a key management component, a notification component, and a logging/auditing component. The method includes the encryption gateway service encrypting the data. The method includes the encryption gateway service sending a notification that the data has been encrypted. The method provides for the encryption gateway service logging that the data has been encrypted. The method also includes the encryption gateway service sending a first encrypted data to a destination.

These and other features and advantages will be more clearly understood from the following detailed description taken in conjunction with the accompanying drawings and claims.

BRIEF DESCRIPTION OF THE DRAWINGS

For a more complete understanding of the presentation and the advantages thereof, reference is now made to the following brief description, taken in connection with the accompanying drawings in detailed description, wherein like reference numerals represent like parts.

FIG. **1** illustrates an encryption system according to an embodiment of the present disclosure.

FIG. **2** illustrates an encryption method according to an embodiment of the present disclosure.

FIG. **3** is a block diagram of a computer system operable for some of the various embodiments of the present disclosure.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

It should be understood at the outset that although an exemplary implementation of one embodiment of the present invention is illustrated below, the present system may be implemented using any number of techniques, whether currently known or in existence. The present disclosure should in no way be limited to the exemplary implementations, drawings, and techniques illustrated below, including the exemplary design and implementation illustrated and described herein, but may be modified within the scope of the appended claims along with their full scope of equivalents.

In an embodiment of the present disclosure, an Encryption Gateway Service (EGS) acts as a common encryption and decryption service provider for applications within an enterprise that send data to or receive data from external trading partners. Encryption and decryption activities are centralized on a server computer rather than distributed on multiple desktop computers. The EGS delivers an enterprise wide, file-level encryption and decryption management system for all external and internal data transfers, including both automated and manual transactions. The EGS centralizes the management of trading partners and their associated keys and certificates. Additionally, the enterprise can gain an increased level of control on file encryption and data traffic by auditing transactions that involve encryption or decryption. The EGS can communicate with an enterprise's existing identity management system to authenticate and authorize users for access to the encryption and decryption services. The EGS notifies users whether or not a message has successfully been sent to a trading partner and also notifies users when a message has arrived from a trading partner.

Use of the EGS minimizes the requirements for licenses for encryption software, reduces the proliferation of encryption software and related keys across application servers and desktops, standardizes encryption and decryption on a single version of a single encryption/decryption product, reduces the number of security exposures related to file encryption, creates a standardized integration guide for the EGS infrastructure, manages the keys used in exchanges with trading partners, makes cryptographic activity and exchanges with