Internal and external encryption with iQ.Suite Exchange

Description of the method and possible configurations
# Table of contents

1. Background 3
2. Case study 4
   2.1 End-to-end vs. server-based encryption 5
   2.2 Encryption management 5
   2.3 Method 5
3. iQ.Suite Module 6
   3.1 Crypt Pro 6
   3.2 KeyManager 7
   3.3 PDFCrypt 7
   3.4 WebCrypt Pro 8
4. Implementation 9
   4.1 Certificates and KeyManager 9
   4.2 Internal encryption 9
   4.3 iQ.Suite configuration 10
5. About GBS 12
1. Background

Internet has dramatically changed the communication between people and organizations and the transformation won’t stop here. Despite instant messaging and team collaboration tools, e-mail remains the only universal technology that enables scheduled communication with nearly any content. E-mail can be used just as easily on any end device in complex company networks as it can on a single system in a household. However, this general application also brings challenges in terms of the required security of communication. Protective mechanisms are necessary, especially when it comes to confidential communication. At the same time, the widespread use of e-mail communication requires simple operation in complex situations. Usually, the individual users in a company infrastructure are not fully aware of the legal and internal regulations. The rapid change in these requirements makes it almost impossible to communicate updates to everyone involved in a timely manner.

This whitepaper describes the different technologies and their joint use in a corporate infrastructure for internal and external encryption. Encryption can be used to achieve one or more goals.

- **Confidentiality**
  The message can only be read by the author and the recipient.

- **Authentication**
  The message was written by the person specified in the sender address

- **Authenticity**
  The message was not changed in transit.
  Different methods can be used for encryption

- **Symmetric encryption**
  The method for decryption is the exact reverse of the encryption, e.g. five letters ahead or back in the alphabet. In symmetric encryption methods, encryption and decryption are performed with the same key. This means that the sender and receiver must have agreed on this secret key in advance, and the key must of course be kept secret. There is only one key, which is needed for both encryption and decryption.

- **Asymmetric encryption**
  The procedures for encryption and decryption are related, but not identical. The key for encryption can therefore be distributed as desired. Only the key for decryption must be protected.

- **Combined methods**
  Asymmetric methods are much more computationally intensive than symmetric methods. A symmetric method is used to encrypt the message. The key for decryption is protected with an asymmetric procedure.

For e-mail encryption, S/MIME and PGP are the most widely used implementations of asymmetric encryption. While PGP certificates are always self-generated, S/MIME certificates can be signed by the creator or by a public certification authority. The latter has the advantage that a recipient can verify a certificate with the help of the certification authority. For self-signed certificates, another way must be found to verify the authenticity. Self-signed certificates are therefore often used in communication between companies, while publicly signed certificates are ideal for communication with individuals. Certificate-based encryption is often regarded as complicated and therefore rejected. Alternative procedures are usually limited in functionality because they are based on symmetrical methods and thus cannot achieve all three goals - confidentiality, authentication and authenticity. However, they often satisfy the requirements if, for example, only encryption of the message is needed.
2. Case study

For illustration purposes, let’s consider a company that consists of several subsidiaries in one country and various sales companies in other countries. The company intends to provide development services for various customers, some of which also need to be protected in-house. The following communication paths should be possible in encrypted form:

- Communication between subsidiaries
- Communication of the employees with the personnel department and the personnel council
- Communication with customers
- Communication with individuals, e.g. applicants

In addition, various internal company security measures must be observed, for example:

- Legally compliant archives
- Prohibition of certain file formats
- Data Leakage Prevention
- Automatic signatures
- Delegable absence management

In addition to traditional computer systems, the company also uses mobile devices for e-mail communication.
2.1 End-to-end vs. server-based encryption

In the business environment, server-based encryption is usually preferable, since secure communication can be combined with the requirements of company-wide processes. Communication between the user and the mail system is almost always protected by transport encryption. This prevents a potential attacker with access to the network from reading any communication. The unencrypted message content can be checked, archived and, if necessary, blocked on the mail system in accordance with the guidelines. After the check, the messages can be encrypted and delivered.

End-to-end encryption requires all public certificates to be distributed to the end devices and updated. Encryption takes place as soon as the message is created. Central processing is no longer possible; archives contain only encrypted messages.

For our case study, server-based encryption is selected.

2.2 Encryption management

Encryption management should ideally be automatic. If a central rule can be defined, this typically leads to better results. The following are available as decision criteria:

- Address rules
- Detection of file type
- Content analyses

Implementing manual control on top of that enables individual encryption of internal mails and increases user acceptance.

2.3 Method

For external communication should be used PGP and publicly signed certificates. These certificates are created or purchased only for those users who engage in external confidential communication. In most cases, this is about 30% of the users. The S/MIME certificates can be obtained and renewed automatically by a certification authority.

The internal encryption takes place via self-signed S/MIME certificates and is provided to all employees. PDFCrypt is used for confidential external communication if no public PGP or S/MIME keys are available from the communication partner. Alternatively, WebCrypt Pro could also be used here.
3. iQ.Suite Module

3.1 Crypt Pro

Crypt Pro provides encryption and decryption with S/MIME and PGP certificates. The certificates are provided in the KeyManager.

Incoming mails can be decrypted with the private keys of the recipients. The public keys of the senders are used for the subsequent certificate check. Crypt Pro can thus fulfill all three requirements - confidentiality, authentication and authenticity.

Outgoing mails are signed with the sender’s private certificates and encrypted with the recipient’s public certificates. The recipient of the message can thus meet all three requirements as well.

Incoming mails can optionally be re-encrypted with the recipient’s public internal certificate after decryption and central processing by iQ.Suite. This means that information that needs to be protected in your own infrastructure can also be securely stored.

Internal mails that are to be transmitted encrypted are subsequently stored in the sent folder of the sender encrypted with the sender’s public key.
3.2 KeyManager

KeyManager manages the S/MIME and PGP certificates for use with Crypt Pro. Own PGP certificates can be imported and managed. Foreign public PGP keys can be recognized with Crypt Pro and automatically imported into the KeyManager. S/MIME certificates can be automatically created and renewed by KeyManager for users if a root certificate is available. Alternatively, certificates can be imported from Active Directory. Publicly signed S/MIME certificates can be automatically requested, imported, and renewed by specific certificate authorities. For installations with several legally independent entities, the certificates can be split into different tenants.

3.3 PDFCrypt

PDFCrypt provides an alternative to certificate-based encryption. It allows a message to be encrypted without knowing the recipient’s infrastructure. The only requirement is a PDF reader that can open encrypted PDF documents. The email is printed to a PDF and file attachments are inserted into the PDF as comments. The PDF is then encrypted with a password. The password can be saved for later emails so that the recipient does not need a new password for each message. The password complexity can be defined as desired. Preferred passwords of the recipients can be saved.

The challenge is the transmission of the password to the recipient. The password can be sent automatically via SMS, but the recipient’s current mobile phone number must be known. Alternatively, the password can be transmitted by telephone or requested by the recipient from the sender’s service desk. It is also possible to send it in an unencrypted e-mail. However, this method should be used only in very special situations.
3.4 WebCrypt Pro

WebCrypt Pro is another alternative that is technically comparable to PDFCrypt. However, the message and any file attachments are saved in an encrypted HTML file. The recipient can upload the file to a web portal and decrypt it there. Access to the portal is protected by a username and password.
4. Implementation

Several iQ.Suite modules have to be combined for the described case study.

- **Watchdog**
  - File type detection and regulation; Virus and malware detection
- **Wall**
  - Content analysis; Anti-Spam
- **Convert**
  - Converting of undesired file types
- **Bridge**
  - Legally compliant e-mail archiving
- **Crypt Pro**
  - Encryption with S/MIME and PGP
- **KeyManager**
  - Key management for CryptPro
- **PDFCrypt or WebCrypt**
  - Alternative encryption methods
- **Trailer**
  - Automated adding of standardized signatures, advertising banners, event notices and legal requirements to outgoing mails.
  - Internal messages can be tagged with key location and contact information
- **Clerk**
  - Automated, delegatable, and template-based absence notification.

The list of modules represents a typical, but not required combination. The mail system can be operated in a local and optionally distributed installation or in the cloud. The iQ.Suite installation can be operated locally or in the cloud, or via GBS as iQ.Suite as a Service.

### 4.1 Certificates and KeyManager

The self-signed S/MIME certificates for internal encryption are stored in a separate tenant in KeyManager. The certificates can be calculated automatically by the KeyManager. Alternatively, certificates can be imported from a third-party system or synchronized with Active Directory or Azure Active Directory.

The S/MIME and PGP certificates for external communication are stored in a second tenant. The public S/MIME and PGP keys of the communication partners are also collected in this tenant.

### 4.2 Internal signature and encryption

It should be possible to encrypt and sign internal e-mails. Encryption is optional and can be managed by the sender of the message. Internal encryption is typically used for confidential communications with the HR department, works council, etc. For defined user groups, encryption can be automatic.

The internal signature should be used for all internal emails to provide additional protection against external attacks. These attacks are called CEO Fraud, Business Email Compromise or Fake President Fraud. Users can use the signature for better detection of forged mails, e.g. if external senders replicate emails to influence employees, the signature provides the recipient with an additional recognition feature for internal messages.
4.3 iQ.Suite Configuration

A possible mail processing flow could consist of the following jobs:

- Incoming messages are decrypted
- New public keys are imported into the KeyManager
- All messages are scanned for viruses, spam and other threats, as well as for undesired file types and blocked or converted to other formats, e.g. PDF
- All messages are checked for confidential content and provided with an encryption feature
  - All messages from or to defined mail addresses are provided with a feature for encryption
- Depending on the company, mails are stored in the legally secure archives
- Incoming and internal messages for absent users are answered individually using the configured templates
- Outgoing and internal messages are provided with the defined signatures of the respective company
- All internal messages are S/MIME signed
- Internal messages for defined user groups or with a freely definable processing instruction are
Incoming messages that have been received in encrypted form and given an encryption feature in the content analysis are sent to the user in encrypted form.

Outgoing messages that have been provided with an encryption feature in the content analysis are sent encrypted.

Encryption takes place according to the recipient's public key with S/MIME, PGP or as an encrypted PDF.

All messages that were sent encrypted are subsequently stored in the sender's sent folder in encrypted form.

This list represents an implementation example that can easily be adapted to real needs.
5. About GBS

GBS Europa GmbH is a leading vendor of solutions and services in the fields of messaging security and workflow for Domino and Microsoft collaboration platforms. Over 5,000 customers and more than 4 million users worldwide trust in GBS expertise. The company operates in Europe, North America and Asia.

© 2021 GBS Europa GmbH

Our product descriptions are of a general and descriptive nature only. They do not stipulate any specific features nor do they represent any form of warranty or guarantee. We reserve the right to change the specifications and design of our products without notice at any time, in particular in order to keep abreast of technical developments. The information contained in this document presents the topics from the viewpoint of GBS Europa GmbH (hereafter ‘GBS’) at the time of publishing. Since GBS needs to be able to react to changing market requirements, this is not an obligation for GBS and GBS cannot guarantee that the information presented in it is accurate after the publication date. This document is intended for information purposes only. GBS does not extend warranty for this document, in either explicit or implied form. This also applies to quality, execution, standard commercial practice or suitability for a particular purpose. All the product and company names that appear in this document may be trademarks of their respective owners.

Website: www.gbs.com
E-mail: info@gbs.com
Locations: www.gbs.com/en/locations