iQ.Suite Crypt Pro Basics

- Central email encryption -

Server-based encryption for comprehensive email content security

Expertise matters

Contents

1 Executive Summary

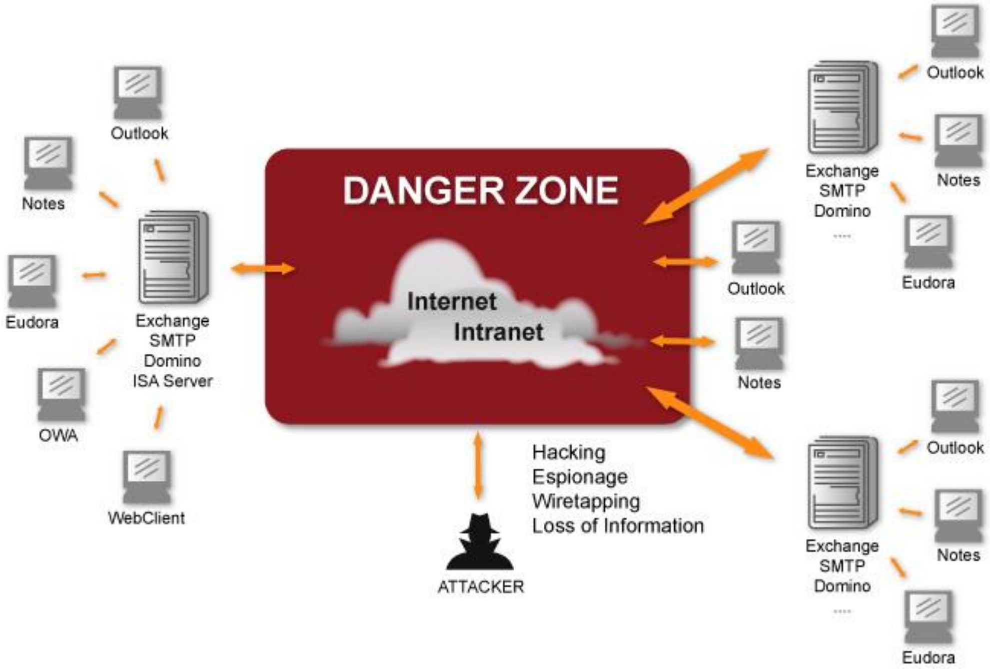
Of the world's population, over 2.5 billion people are registered email users, with business documents making up for a significant part of the email traffic. A vast majority of companies have connected to the Internet and make use of the web's global information exchange information in order to maintain their competitive edge.

However, the greater the number of participants in a communication network, the greater is the need for protecting the individual's rights. This protection particularly applies to the data which the individual distributes and/or processes in the network. Especially in the commercial sector, no multinational company would even consider transporting sensitive internal information such as corporate finances, business and sales reports through the Internet unless it could be guaranteed that such information will arrive safely and securely.

Safe and secure in this context means that only authorized persons have access to and can view the data. There are many ways of transporting data in a network. It can, for example, be stored in a local database, where users can access it as required. Sometimes, however, it is necessary to actually send information. This can, among other methods, be done by electronic mail.

On its way from the sender to the recipient, an email passes through numerous computer systems, both on the Internet and in the intranet. The route an email takes is not predetermined, but rather depends on factors such as network traffic and bandwidth. Like a postcard, the content of an email is unprotected on its way to its recipient and can be read and changed by anyone.

Insecure email communication:



The use of email encryption turns the electronic postcard into an encrypted letter with a seal of authenticity. The present whitepaper deals with the alternative to a public-key infrastructure (PKI).

For further information on cryptography, please refer to the whitepaper entitled “Cryptography”. The “PKI Fundamentals” whitepaper deals with PKI basics. Both whitepapers are available for download on our Whitepaper Website.

2 Client-based Encryption

With client-based encryption (also called end-to-end encryption), the email is encrypted from the sender’s PC to the recipient’s PC. This means that it cannot be read by third parties along its entire route.

At first sight, this type of encryption may seem like a good solution; in practice, however, client-based encryption often does not achieve the desired results. Why?

There are a number of reasons for this:

2.1 User-tied Keys

In client-based encryption, every email user receives an individual pair of keys for email communication. This pair of keys applies to this user’s entire encrypted email traffic.

If, for instance, the user leaves the company, the latter can no longer access the user’s emails. This could conceivably present a serious problem for the company, unless the pair of keys has been stored centrally together with the password, in which case both pieces of information can still be accessed.

2.2 Complexity

Introducing company-wide client-based encryption is a complicated undertaking. First of all, every mail user needs a unique key or pair of keys, quickly resulting in hundreds or thousands of keys to be created, distributed and managed. As the number of users increases, so does the required administrative work. Keys are normally requested from an authorized certification body. Here, too, there is a correlation between the number of keys generated and the costs incurred.

Also, the creation and allocation of keys is not the only cost factor in setting up client-based encryption: First of all, the required encryption software has to be installed on every email user’s PC, which is both costly and time-consuming. In addition to the difficulties in using their email software, the email users then have to learn to use the encryption software as well to encrypt their messages. And when they receive messages, they need to know the correct steps to decrypt them again. Even extensive user training – beside being a costly undertaking – does not guarantee problem-free encryption and decryption: user mistakes can never be excluded.

Added to that are costs of ongoing support and software maintenance, such as updating the encryption software on all user PCs.

Because of the need for user interaction, there is a general lack of acceptance of encryption, users regarding the required work associated with encryption as an additional burden placed on them by Management or the IT department. Lack of acceptance, in turn, often means that email traffic security cannot be guaranteed to the extent required.

2.3 No Server-based, Corporate Email Content Security

For many companies, security in email communication is not limited to encryption of mail messages. Top priorities for IT departments and security officers include issues such as virus protection, protection from spam and junk mail, data loss and undesirable content.

Looking at client-based encryption, we have to conclude that:

Client-based encryption prevents comprehensive email content security.

The reason is that an encrypted message cannot be protected by antivirus programs and other email security tools on the mail servers, as encrypted messages cannot be read by these programs and the associated protective mechanisms therefore do not work. This is a precarious situation. To save costs and simplify administration in many ways, most companies have decided to install email security applications on their servers. Client-based encryption goes against the need for standardized, centrally implemented and managed email infrastructures with appropriate security mechanisms.

3 Server-based Encryption

A server-based solution for email encryption offers good possibilities to avoid the problems described under 2 Client-based Encryption.

3.1 Easy Implementation

Unlike client-based encryption, server-based solutions can be implemented very quickly.

Server-based encryption does not require individual pairs of keys for each user, but only a central key or pair of keys belonging to the company.

Thus, a single corporate key or pair of keys can be used for all email communications, making the administration of keys much simpler. Also, the costs of requesting, distributing and managing the keys are much lower than those associated with client-based encryption. With this concept, the focus is on the company as legal person. The corporate key used protects the emails sent by any employee of the company and guarantees to third parties that the mail was sent from that company. Because, ultimately, the company is liable for the content of its employees' emails, it does not matter in this case, which employee has sent a particular message. We can therefore conclude that a corporate key provides sufficient legal protection for the company. It is, of course, still possible to assign personal keys to individual employees, although for most employees, encryption with a corporate key will provide sufficient security.

A further advantage of server-based encryption is that it eliminates the need for the complicated implementation of a public-key infrastructure (PKI). Through encryption between two dedicated email servers, an equally secure “partial” PKI solution for encrypting emails can be implemented. Thus, to implement encryption between two companies, only a few issues have to be taken care of:

- one key per company ,
- the exchange of these keys between the companies,
- the entry of these keys in the central key management.

With these few steps, it is possible to protect the entire email communication between two companies.

3.2 No Client Software Distribution

Where client-based encryption requires comprehensive software distribution measures, deployment of the server-based solution is much simpler and therefore less costly, as all of the software components required are installed on the mail servers. Compared to numerous client installations, the server installation is quick, simple and inexpensive. Besides saving on initial costs, the maintenance costs are also much lower.

3.3 User-transparent Encryption

With server-based encryption, no interaction with the email users is necessary. The email users send and receive emails in the same ways as they would normally do. They do not have to carry out any additional operations or be familiar with software other than their mail clients. As the encryption and decryption of their mails is handled on the server, unnoticed by the users, no user training is needed, which also saves costs. The acceptance of server-based encryption is, of course, also higher among email users, since nothing changes for them from a practical point of view.

In addition, the encryption methods used can be easily – and transparently for the user – combined or changed on the mail servers. This flexibility is especially useful when new corporate or industry standards are introduced.

3.4 Central, Rule-based Encryption

Shifting encryption from the clients to the server allows to set up a centrally controlled, rule-based encryption scheme. Rule-based encryption uses a set of “if-then” conditions, where the “if” may contain multiple conditions and the “then” multiple actions to be executed. Regarding encryption, the following rules could, for instance, be defined:

If ...,	*then ...*
an email is sent to abc@xyz.com,	encrypt the mail with the PGP key abc.
an email is received by *@test.com,	decrypt the mail with PGP company key.
an email is sent to tom@jerry.com with “S/MIME“ in the Subject line,	encrypt the mail with S/MIME certificate 4711.

Such a rule-based approach ensures maximum flexibility for the company, with a central user interface used for the administration of the rules.

3.5 Central Key Administration

Key administration is performed on the email servers within the corresponding encryption applications (PGP and/or S/(MIME), with PGP keys automatically imported into the key ring. This centralized approach not only simplifies implementation, but also reduces maintenance costs.

3.6 Solution with iQ.Suite Crypt Pro

3.6.1 Flexible Server-based Encryption and Decryption

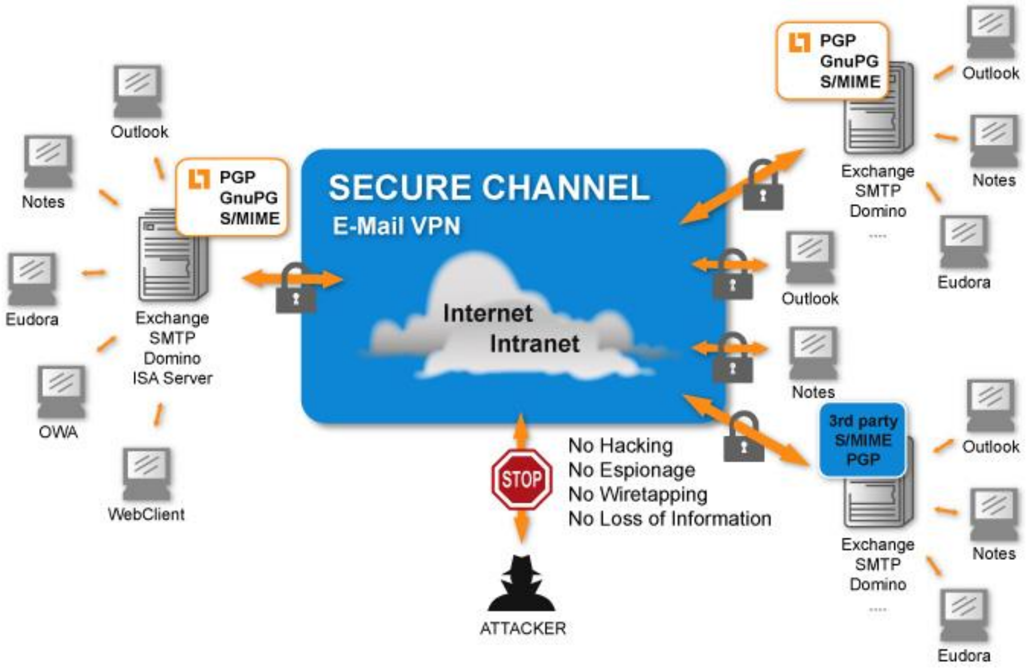
iQ.Suite Crypt Pro as well as PGP and/or S/MIME are installed on the corresponding mail servers. A client-side installation is not required [see 3.2 No Client Software Distribution].

Notwithstanding server-based encryption in the company using iQ.Suite Crypt Pro, the communication partners may, of course, decide to use both server-based and client-based encryption. The decisive point is that both partners have to use the same encryption methods. iQ.Suite Crypt Pro supports the industry standards PGP and S/MIME.

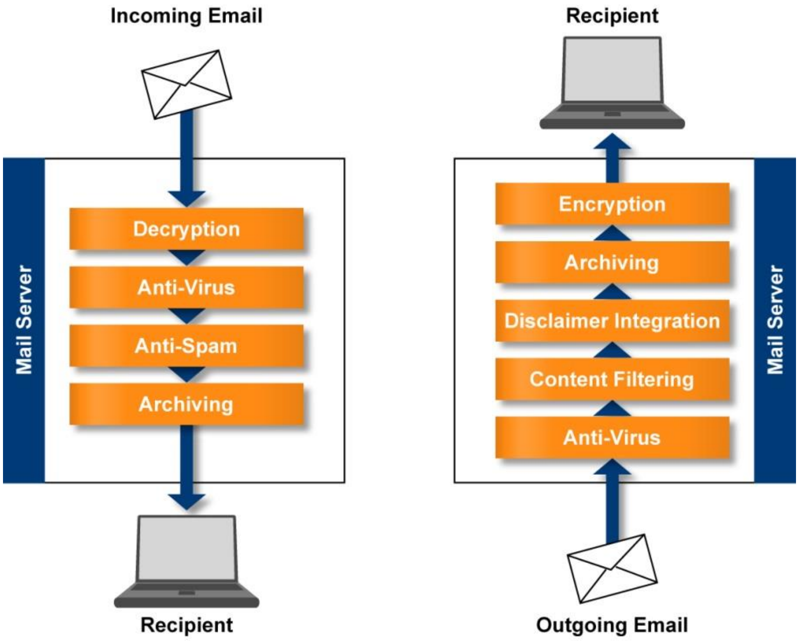
3.6.2 Integrated Encryption and Content Security

Encryption alone is not enough to ensure comprehensive security of all email traffic. Central virus protection, protection from spam and junk mails, protection against loss of information and undesired content are also central issues. iQ.Suite Crypt Pro is the only server-based encryption product that fulfils both encryption and content security requirements.

Secure email communication with iQ.Suite Crypt Pro



By combining iQ.Suite Crypt Pro with further iQ.Suite modules, multi-layered security measures can be implemented:



With iQ.Suite Crypt Pro, companies do not have to decide whether they use encryption **or** server-based virus protection, anti-spam protection, etc. With iQ.Suite Crypt Pro, the answer is both: encryption **and** comprehensive, server-based content protection.

3.7 Server-based Encryption vs. Client-based Encryption

	Server-based encryption with iQ.Suite Crypt Pro	***Client-based end-to-end encryption***
Initial software distribution expenses	Low	High
Support needs	Low	High
Software maintenance needs	Low	High
Central, server-based key management	Yes	No
Key management needs within company	Low	High
Implementation needs	Low	High
User acceptance	High	Low
User transparency	Yes	No
Training needs	Low	High
Server-based virus protection	Yes	No
Server-based protection against spam / junk mail	Yes	No
Rule-based email security, based on domains, business units, groups and users	Yes	Yes, but unreasonably expensive
Installation of encryption software	On mail server only	On all clients
PKI infrastructure required	No	Yes
Total implementation costs	Low	High
Ongoing operation costs	Low	High
Support for email substitute schemes	Yes	No
Central archiving, encrypted and/or not encrypted	Yes	No

4 Scenarios

4.1 Client-to-Server Encryption

In addition to full-time employees, many companies engage the services of self-employed people at various geographic locations. Self-employed people generally do not work on the company's premises but, for instance, at home. From there, they can communicate by email with the company using any Internet provider they choose. In fact, email is often the primary means of communication. Beside general information, critical data, such as price lists, contracts, and customer and supplier data may be exchanged via email.

In the following section, we will look at suitable solutions to provide comprehensive protection of all email communications. Beside security along the paths of communication, virus protection and content checking are also given high priority.

Requirements

1. As self-employed people communicate with the company using many different email programs and Internet providers, encryption must take place on the communication partners' PCs. The encryption standards supported by the company must, however, be taken into account.
2. The company does not want to complicate the use of email for its on-site employees through the use of encryption, and therefore prefers a solution that is transparent to the users.
3. Cost is a major issue, as is ease of implementation, and the company therefore wants to avoid complex software distributions and expensive user training. At the same time, it wants to keep key administration as simple as possible.
4. In parallel with the introduction of email encryption, the implementation of a server-based solution for virus protection and content checking is planned. The encryption solution must therefore fit into the overall email security concept, so that server-based protection of encrypted emails is also possible.

Solution approaches

1. Self-employed correspondents are equipped with the PGP encryption program. PGP is available for various email clients and can therefore be used by all independent partners. Each partner receives a PGP key.
2. A corporate key for the company is generated. The public key is made available to all self-employed partners.
3. The self-employed partners enter the public key in their PGP program.
4. iQ.Suite Crypt Pro and PGP are installed on the company's email server. **No** software installation is necessary on the company's client PCs.
5. The self-employed partners' public keys are entered in PGP on the email server.
6. Appropriate encryption rules are created in iQ.Suite Crypt Pro:

If ...,	*then ...*
an email is received from self.employee1@t-online.de,	decrypt the mail with PGP company key.
an email is received from self.employee2@aol.com,	decrypt the mail with PGP company key.
an email is sent to self.employee3@hotmail.com,	encrypt the mail with the PGP key FM3.
etc.	etc.

7. To enable virus protection and content checking for encrypted mails, two additional modules – iQ.Suite Watchdog (for virus protection) and iQ.Suite Wall (for content checking) – are installed on the email server and incorporated in the existing set of rules.

	If ...,	*then ...*
STAGE 1:	an email is received from self.employee1@t-online.de,	decrypt the mail with PGP company key.
	an email is received from self.employee2@aol.com,	decrypt the mail with PGP company key.
	etc.	etc.
STAGE 2 and 3	mails are received from the Internet, regardless of senders,	start antivirus program and content checking.

4.2 Server-to-Server Encryption

A company has relations with a large number of suppliers. Because of its speed and low associated costs, email is now used for more than 80 percent of communication. All business partners use the email platforms IBM Notes/Domino or Microsoft Exchange. Email communication includes the exchange of critical information, such as orders, technical drawings, analyses and pricing agreements. If this kind of information were to get into the wrong hands, the consequences for the company could be fatal.

As a consequence, all future email correspondence with the business partners is to be encrypted.

Requirements

1. No additional hardware costs should arise through the implementation of encryption.
2. To minimize costs and required time, a central encryption solution is to be implemented.
3. Because the participating companies favor different encryption methods, the encryption solution must support the PGP and S/MIME industry standards.

Solution approaches

1. The companies involved install iQ.Suite Crypt Pro and the required encryption programs (PGP or S/MIME) on their email servers.
2. A company key is generated for each business partner.
3. The company keys are entered in the encryption programs (PGP or S/MIME) on the email servers.
4. Appropriate encryption rules are created in iQ.Suite Crypt Pro:

If ...	*then …*
an email is received from supplier1@supplier.com,	decrypt the mail with PGP company key.
an email is received from supplier2@supplierxyz.com,	decrypt the mail with PGP company key.
an email is sent to supplier3@suppliernet.com,	encrypt the mail with S/MIME certificate LF3

5 Facts and Data

iQ.Suite Crypt Pro Support	
Supported email systems	■ IBM Notes / Domino ■ Microsoft Exchange / SMTP
Supported encryption methods	■ PGP ■ PGP/MIME[1] ■ S/MIME
Supported modes	■ Encrypt ■ Decrypt ■ Sign ■ Verify signature ■ Import key

[1] **iQ.Suite for Exchange**

6 iQ.Suite Crypt Pro in a Nutshell

Highlights

- Company-wide encryption guidelines
  The flexible configuration of sender-recipient combinations and email domains allows the definition of specific encryption relationships between different persons, groups and companies. Thus, centralized guidelines enable email encryption for all users or selected groups of people.
- Transparent efficiency
  The use of standardized methods and the central processing on the server ensure transparency for the user as well as independence from the email client used. Any combination of encryption partners, such as client-client, server-server and client-server, is freely configurable.
- Different encryption standards
  The simultaneous use of different encryption methods, such as PGP and S/MIME, offers the highest security for a wide variety of application purposes and communication partners.
- Flexible rule sets
  Using an intelligent and freely definable rule-based mechanism for selective encryption of email contents, iQ.Suite Crypt Pro provides high-level flexibility and security.
- Integrated central administration

Features

- Definition of centralized encryption policies for communication via Internet and public networks
- Transparency of email encryption for users, independent of email client used
- Selective encryption through address checks for any sender-recipient combinations, recipient groups and Internet domains
- Integration into any encryption administration and public-key infrastructure (PKI)
- Centralized archival of personal and company-related public keys on the server
- No encryption key management required from end users
- Simultaneous use of different methods with long keys, e.g. PGP, S/MIME
- Detailed logging functions
- Configurable messages to sender, recipient and Administrator
- Multiple platform support for all operating systems
- Optimized multi-processing and multi-threading, including for partitioned servers and clusters
- Scaleable architecture
- "Ready to go" for Application Service Providing (ASP)
- Seamless integration with additional iQ.Suite products

About GBS

GROUP Business Software is a leading vendor of solutions and services in the fields of messaging security and workflow for the IBM 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.

Further information at www.gbs.com

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 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.