GBS

iQ.Suite Crypt Pro

- Server-based email encryption -

Efficient email encryption for IBM Domino

Expertise matters

Contents

1 Executive Summary

The amount of communication handled via email has strongly increased in the last couple of years and is still growing. There is hardly a company that does not use email to run its business processes both within the company and with external business partners. In addition to short response times, constant reachability and cost-efficient communication, major issues also include the security of emails and the protection of confidential email contents. Many companies therefore rely on email security solutions that also include encrypting emails.

To be efficient, these solutions must meet the following requirements:

- Server-based email content checking (virus protection, protection against spam/junk mail, protection against industrial espionage, etc.)
- Email encryption (e.g. for confidential offers, contract data, etc.)
- Low administration requirements

The present whitepaper provides an overview of the issues related to the implementation of the PGP and S/MIME encryption standards within iQ.Suite Crypt Pro for Domino.

2 Implementation in iQ.Suite Crypt Pro

iQ.Suite Crypt Pro is one of the iQ.Suite modules. When used in combination with further iQ.Suite modules, it is possible to check encrypted mails for viruses (using iQ.Suite Watchdog) or specific contents (using iQ.Suite Wall). iQ.Suite Crypt Pro includes the following functionalities:

- As all of the iQ.Suite modules, iQ.Suite Crypt Pro is a server-based software. This ensures secure email communication without active actions required from the end user. Only a single certificate/key is required for the entire company, the company certificate or company key.[1]
- iQ.Suite Crypt Pro enables automatic encryption/decryption as well as signing and signature verification (validation with S/MIME only).
- iQ.Suite Crypt Pro supports the PGP/GnuPG encryption standard for Windows, Linux, AIX and Sun Solaris as well as the S/MIME standard for Windows, Linux and SUN Solaris.

[1] **S/MIME usually refers to certificates while PGP or GnuPG typically use the term "key".**

2.1 PGP Implementation

iQ.Suite Crypt Pro allows to encrypt mails with PGP or GnuPG, to receive and decrypt PGP or GnuPGP-encrypted mails and to automatically extract public keys from incoming emails and install them into the key ring.

By analogy, all of the information provided for GnuPG also applies to any other PGP variant. To use GnuPGP within iQ.Suite Crypt Pro, the following requirements have to be met:

1. GnuPGP has been installed separately.
2. A valid license for the iQ.Suite Crypt Pro module is available.
3. The system environment path includes the appropriate GnuPG directory.

To use GnuPGP, the configuration for iQ.Suite Crypt Pro is based on policies, i.e. the rules for encryption, decryption and importing keys can be configured specifically for each user, user group or the entire company.

2.1.1 Scenarios for GnuPG

This section describes various application scenarios for importing keys and encrypting/decrypting outgoing/incoming mails using GnuPG.

2.1.1.1 Encrypting Outgoing Emails

- Prerequisites:

  1. The recipient's public key is available in the key ring and is "ultimately" trusted to or it is signed with the standard or company key. For further information on confidence levels, types of signatures and their meaning, please refer to the GnuPGP Documentation.
  2. The iQ.Suite Crypt Pro-Job "Encryption with GnuPG" is enabled for the applicable operating system.
  3. Appropriate rules have been configured for all recipients in the "Encryption with GnuPG" iQ.Suite Crypt Pro-Job. If required, create and activate multiple jobs to do so.
  4. The program path for calling cmd.exe has been set. Attention: The different Windows versions use different names for the subdirectories.
  5. The path for calling gpg.exe has been set.
  6. The path to the public key ring must have been set in the parameters (Home directory).
  7. A detailed description of the parameters and settings is to be found in the Online Help or Administration Manual.

- Encryption procedure:
  1. The user sends his mail in the usual way.
  2. On the server, iQ.Suite Crypt Pro fetches the public key for the mail's recipient from the GnuPGP key ring.
  3. The mail is encrypted (scenario for S/MIME see 2.2.1.1 Encrypting Outgoing Mail).
  4. The mail is delivered to the recipient.

In the iQ.Suite Crypt Pro-Job configuration document, a number of additional options are available:

- Provided the communication partner also runs iQ.Suite Crypt Pro or another server-based encryption module that uses GnuPG for encryption, the recipient-to-key mapping can be explicitly specified.
- Also a selection between PGP/MIME and PGP/Inline is possible. With PGP/Inline message text and attachment of an email are encrypted separately. You can indicate whether the encryption is performed within the email's body text or if the encrypted data is sent as attachment. The name of the attachment is freely selectable. PGP/MIME enables the encryption of the whole email content as one complete block (with exception of the email header).

2.1.1.2 Decrypting Incoming Emails

- Prerequisites:
  a) The iQ.Suite Crypt Pro-Job "Decryption with GnuPG" is active.
  b) Appropriate rules have been configured for all recipients in the "Decryption with GnuPG" iQ.Suite Crypt Pro job. If required, create and activate multiple jobs to do so.
  c) The program path for calling **cmd.exe** has been set. **Attention**: The different Windows versions use different names for the subdirectories.
  d) The path for calling **gpg.exe** has been set. The important parameter is "echo %PASSWORD%".
  e) The path to the private key ring must have been set in the parameters (Home directory).
  f) The password for the standard key or the private company key must have been set.
  g) A detailed description of the parameters and settings is to be found in the Online Help or Administration Manual.
- Decryption procedure:
  a) The key used in the incoming email is identified through the email address.
  b) The incoming mail is decrypted with the private company key.
  c) The decrypted mail is delivered.

2.1.1.3 Automatic Key Import

For encrypted emails from a communication partner who sends his public key along with the mail, iQ.Suite Crypt Pro allows to automatically extract this public key from the mail and import it into the key ring.

- Prerequisites:
  a) The sender's public key is included in the body text of the mail, e.g. as clearly identifiable text block, or as attachment.
  b) The iQ.Suite Crypt Pro-Job "Import Key for GnuPG" (check for appropriate operating system version!) is active.
  c) The program path for calling **cmd.exe** has been set. **Attention**: The different Windows versions use different names for the subdirectories.
  d) The program **newkey.cmd** must be located in the GnuPGP program path. **newkey.cmd** is a batch file. The program calls included in this batch file require the corresponding path to have been set. A sample newkey.cmd file is to be found in the job document under the **Misc.** tab.
  e) The path to the public key ring must have been set in the parameters (Home directory).
  f) After successful import, the corresponding rules must have been configured for the recipients in the "Encryption with GnuPG" iQ.Suite Crypt Pro-Job so that the imported keys can be used for encryption. If required, create and activate multiple jobs to do so. The trust status for newly imported keys has to be set by the Administrator.
  g) A detailed description of the parameters and settings is to be found in the Online Help or Administration Manual.
- Key import procedure:
  a) The sender's public key included in the mail is extracted from the mail.
  b) The public key is imported into the key ring.
  c) Where set accordingly, the Administrator receives a notification of the successful completion of the key import procedure.
  d) If sent encrypted, the mail can now be decrypted.
  e) The mail is delivered to the recipient.
  f) The imported key has to be assigned "ultimate trust" by the Administrator or it has to be signed with the standard (company) key.
  g) Neither the signature nor the definition of the trust status is performed automatically.

2.2 S/MIME Implementation

iQ.Suite Crypt Pro includes a built-in S/MIME interface. To use S/MIME within iQ.Suite Crypt Pro, the following requirements have to be met:

- The operating system is Windows 2000/2003, XP, Linux or SUN Solaris.
- A valid license for the "iQ.Suite Crypt Pro with S/MIME" module is available.
- The system environment path contains the **smime** directory, as all programs required are copied to that directory by the Setup procedure.
- A certificate (pkcs12 format) from a CA (Certification Authority) that is entitled to issue and sign user certificates to be used for email encryption. In that context, this certificate is also referred to as Issuer Certificate (**root.pfx**). It is used by iQ.Suite Crypt Pro to create the internal private user certificates that can be used to sign outgoing emails. The issuer certificate has to be located as pfx file (pkcs12 format) in the **smime** directory. **Note**: During installation, a test certificate is stored in the `…\smime\TestCertificates` directory.
- A company certificate (pkcs12 format) that can be used to encrypt emails, created and signed by the CA above (**company.pfx**). It is used by iQ.Suite Crypt Pro as template for the internal private user certificates. The company certificate is also used to decrypt incoming encrypted emails. The company certificate has to be located as pfx file (pkcs12 format) in the **smime** directory. **Note**: During installation, a test certificate is stored in the `…\smime\TestCertificates` directory.
- For the administration of public certificates, the key database **g_cert.nsf** must be available on the local server. When processing incoming signed mails, the signature's certificate data can be automatically stored in the key database for further use if required.
- If a yet unknown certificate is required, it can be searched for in an appropriate directory using an LDAP server. The certificate is then stored in the database. An entry in the LDAP directory has to include at least the email address and the certificate of the corresponding person. IBM Domino can be used as LDAP server.

To use S/MIME, the configuration for iQ.Suite Crypt Pro is based on policies, i.e. the rules for encryption, decryption, signatures and the verification of signatures can be configured specifically for each user, user group or the entire company.

2.2.1 Scenarios for S/MIME

This section describes various application scenarios for outgoing/incoming mails where S/MIME is used for encryption/decryption, signing and the verification of signatures.

2.2.1.1 Encrypting Outgoing Mails

- Prerequisites:
  a) The recipient certificate is available in the key database **g_cert.nsf** or accessible via LDAP and identifiable through the email address.
  b) The iQ.Suite Crypt Pro-Job "Encrypt with S/MIME“ is active.
  c) Appropriate rules have been configured for all recipients in the "Encrypt with S/MIME" iQ.Suite Crypt Pro-Job. If required, create and activate multiple jobs to do so.
  d) The names of the company and issuer certificates are to be explicitly specified in the job parameters. For encryption, only the company certificate's password is needed (can be set with the %password% variable). The issuer certificate's password is needed for S/MIME signatures only and can be set with the %issuerpassword% variable.
  e) When using an LDAP server, make sure the address (IP or DNS name) and the port for the LDAP server are set correctly (ldapserver and ldapserverport parameters).
  f) As an option, the "-signmessage" parameter can be used to set whether or not an encrypted email is also to be automatically signed.
  g) A detailed description of the parameters and settings is to be found in the Online Help or Administration Manual.
- Encryption procedure:
  a) The user sends his mail in the usual way.
  b) On the server, the iQ.Suite Crypt Pro S/MIME interface fetches the public key for the mail's recipient from the key database or the LDAP server (or the local [Cache DB] buffer in case multiple mails are sent at short intervals).
  c) The mail is encrypted (for the PGP scenario, also refer to 2.1.1.1 Encrypting Outgoing Emails).
  d) The email is delivered to the recipient.

Additional options are available in the configuration document for the iQ.Suite Crypt Pro-Job:

- Provided the communication partner also runs iQ.Suite Crypt Pro or another server-based encryption module that uses a company certificate for encryption, the recipient-to-key mapping can be explicitly specified (also refer to Procedure with S/MIME).

2.2.1.2 Signing Outgoing Mails

- Prerequisites:

  a) The company certificate and the associated issuer certificate are located in the **smime** directory as *.pfx files, e.g. **company.pfx** and **root.pfx**. The passwords for both certificates have been set with the %Password% and %Issuerpassword% variables.

  b) The iQ.Suite Crypt Pro-Job "Sign S/MIME Outgoing Message" is configured and active.

  c) Important: In the job document, both the parameters *--from = %FROM%* and *--outputformat=CLEARSIGNED* have been set.

  d) In the "Sign S/MIME Outgoing Message" iQ.Suite Crypt Pro-Job, the corresponding rules must have been configured for the recipients. If required, create and activate multiple jobs to do so.

  e) A detailed description of the parameters and settings is to be found in the Online Help or Administration Manual.

- Signing procedure:

  a) The user sends his mail in the usual way.

  b) A certificate for the sender of the email is created "on the fly", i.e. in the following steps:

     i) Open company certificate.

     ii) Change email address in the certificate, i.e. the existing company email address is replaced with sender's email address.

     iii) In addition, the series number in the company certificate is changed.

     iv) The new certificate is signed with the issuer certificate (to be found in the **smime** directory).

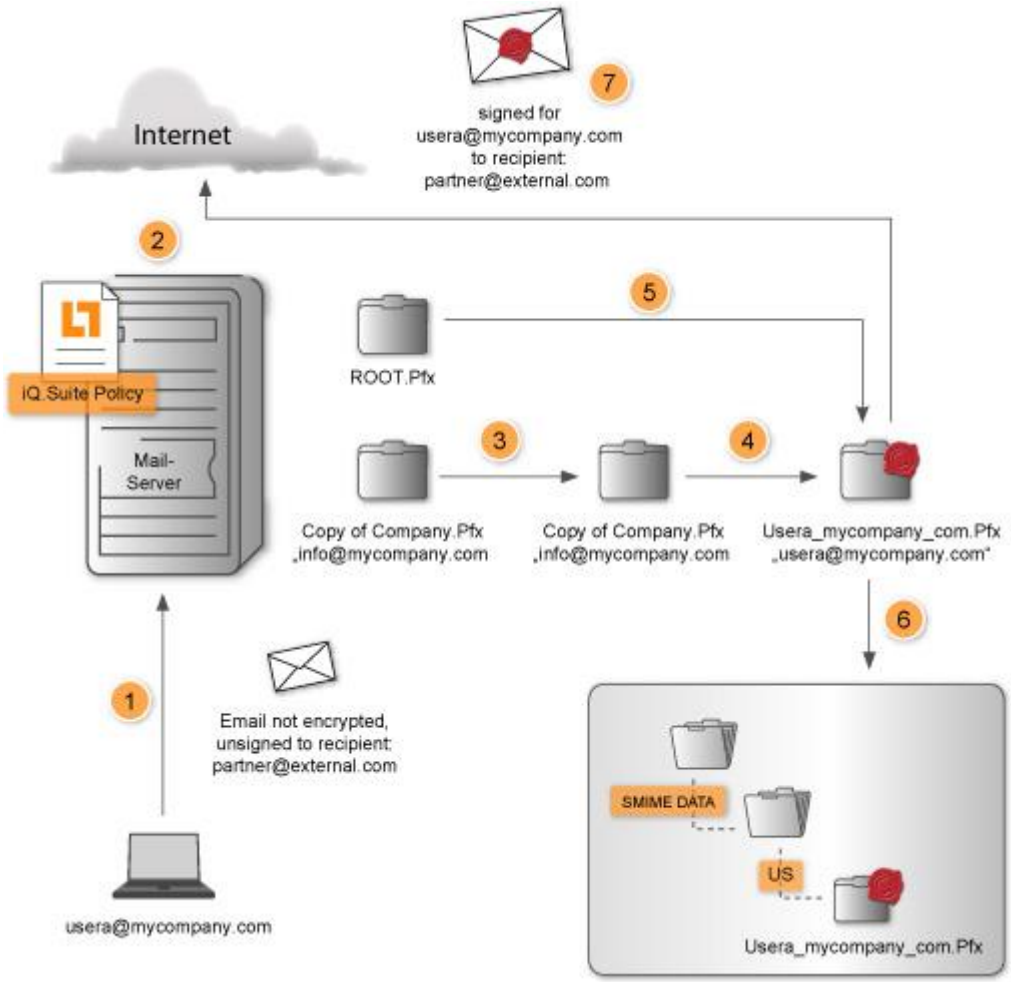
  c) The new certificate is saved as new file in pkcs12 format:
  <from>_<domain part of the issuer certificate>.pfx
  The name "from" is derived from the --from = %FROM% parameter in the job document.
  Example: john.smith_belle.view.pfx
  If a pfx file with the same name already exists, that file is used.

  The new certificates are stored in the **smime** directory. A separate subdirectory is created for each new certificate, with the two first letters of the user name used as subdirectory name. If these two letters are the same for several users, the new certificates are stored in a common subdirectory.

  d) The sender's data is signed with the new certificate or the existing one.

  e) The data is sent.

The recipient is able to read the mail and receives a message that the mail has been signed. To return an encrypted answer to the sender, the certificate needs to be made available to the recipient's mail system in such a way that it can be used for encryption. In the case of Outlook, this is the Windows Certificate store, but it can also be an LDAP directory. For details, please refer to the corresponding mail client manuals.



1. Internal sender sends email.
2. Based on sender/recipient constellation iQ.Suite recognises that the email should be signed.
3. The company certificate will be duplicated.
4. The email address in the duplicated company certificate will be replaced by senders email address.
5. The modified duplicated company certificate will be signed with a ROOT certificate.
6. The modified certificate will be stored in the file system, next to the company´s certificate.
7. The modified certificate will be used to sign the email.

2.2.1.3 Encrypting and Signing Outgoing Mails

There two possible procedures:

- The outgoing mail is encrypted and signed with a single job. An outgoing encrypted email is also automatically signed; see Signing Outgoing Mails with S/MIME. Under Operations, the mode has to be changed from **Sign** to **Encrypt**. This is the recommended procedure.
- Alternatively, it is possible to define two mail reception jobs for different user groups: one job for a user group that receives signed mails only (see Signing Outgoing Mails with S/MIME) and another one for a user group that only receives encrypted but unsigned mails (see Encrypting Outgoing Mail). Both of the user groups have to be disjoint from each other. If there are users included in both groups, use the first procedure.

2.2.1.4 Decrypting Incoming Mails

- Prerequisites:
  a) The iQ.Suite Crypt Pro-Job "Decrypt S/MIME Message" is active.
  b) Appropriate rules have been configured for all recipients in the "Decrypt S/MIME Message" iQ.Suite Crypt Pro-Job. If required, create and activate multiple jobs to do so.
  c) A detailed description of the parameters and settings is to be found in the Online Help or Administration Manual.
- Decryption procedure:
  a) The issuer name is used to identify the certificate used in the incoming mail.
  b) The decryption procedure automatically includes a verification of the signature (see Steps a through d under Verifying Incoming Mail Signature – Signature verification procedure). If the mail has been signed with a certificate not yet included in the g_cert.nsf key database, it is imported into the database and then verified.
  c) From then on, it is possible to send encrypted mails to the sender. If the certificate already exists, it is verified.
  d) Then, the mail is decrypted with the company certificate (company.pfx).
  e) The decrypted mail is delivered.
  f) At the end of the body text, the recipient of the mail is provided with a report on the successful decryption and signature verification.

2.2.1.5 Verifying Incoming Mail Signature

- Prerequisites:
  a) The iQ.Suite Crypt Pro-Job "Verify S/MIME Signature" is active.
  b) Appropriate rules have been configured for the recipients in the "Verify S/MIME Signature" iQ.Suite Crypt Pro-Job. If required, create and activate multiple jobs to do so.
  c) A detailed description of the parameters and settings is to be found in the Online Help or Administration Manual.

- Signature verification procedure:

  a) The certificate/signature is extracted from the incoming mail. In case the sender certificate is not part of the email, it can be retrieved from an LDAP server (if available) or the Cache DB.

  b) If the certificate is not found in the **g_cert.nsf**, it is imported into the database. From then on, it is possible to send encrypted mails to the sender (see Encrypting Outgoing Mail with S/MIME).

  c) The sender certificate is used to verify the signed data:

  d) The systems first checks whether the certificate matches the signature (using mail address and certificate number).

  e) It then checks whether the sender matches the certificate.

  f) Finally, it creates a report on the signature verification (Steps c to e).

  g) The sender's signature is removed from the mail and the report is added to the mail.

  h) The mail is delivered to the recipient.

2.2.1.6 Decrypting Incoming Mails with Signature Verification

The decryption of incoming emails automatically includes the verification of the signature, see Decrypting Incoming Mails with S/MIME. Nonetheless, a separate signature verification job should also be available. Incoming mails can be both unencrypted and unsigned or encrypted only or signed only. The important point is to run the corresponding iQ.Suite jobs in the appropriate order, i.e. the decryption job before the signature verification job. The "–noverify" parameter can be used to configure an encryption-only job, i.e. without signature verification.

2.3 Procedure with S/MIME

Perform the following steps to set up an S/MIME-based connection with a future communication partner:

- Activate the corresponding Crypt Pro-Job "Verify S/MIME Signature" or / and "Decrypt S/MIME Message".
- The future communication partner sends a signed mail and attaches the certificate.
- The certificate is (automatically) imported into the **g_cert.nsf** certificate database or the LDAP directory.
- Activate the corresponding Crypt Pro-Job "Encrypt S/MIME Message".
- The recipient is assigned to the appropriate encryption policy list, i.e. the corresponding recipient is added to the "EncryptionRecipients S/MIME" selection rule.

Importing a certificate into an LDAP directory depends on the operating system. Similarly, on his side, the communication partner has to import and verify the certificates provided by you.

- Notes/Domino

  To import the certificate, the standard Domino function is used. For a detailed description of the procedure, please refer to the Domino Manual. The procedure requires the user to be entered in the name and address book (not registered).

- Outlook users

  The certificate is imported into the Certificate Store of the Windows operating system. In addition, the Issuer ID (from the issuer certificate of the company certificate) has to be set to "Trustworthy" by the Outlook client Certificate Manager. The operating system includes a number of trustworthy issuers such as, among others, Verisign. When creating your own certificates the Trustworthy status has to bet separately. Otherwise, incoming mails will be decrypted in Outlook and their signature will also be verified, but for each mail a message will point out that the certificate is not trustworthy.

- For more details on the import procedure and setting a certificate to trustworthy, please refer to your Windows Manual.

To set up a connection to another server is performed in a similar way. This may be the case when two different companies wish to communicate securely by way of company certificates, but with mails automatically assigned to the corresponding recipients and senders. In this case, perform the following steps:

- Get the certificate from the other server through the reception of a signed mail or as file in p7b format.
- Send your own certificate to the other server – i.e. send a signed mail with the certificate attached or transmit the certificate in p7b format to the partner by some other means (e.g. by floppy disk).
- Import the certificate into the LDAP directory (e.g. Domino)
- Assign the recipient to the appropriate encryption policy list.

iQ.Suite Crypt Pro S/MIME is interoperable with systems working on a S/MIME Standard.

3 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 e mail 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
- Integrated certificate database
- 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
- 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