GBS

iQ.Suite Crypt Pro

- Serverbasierte E-Mail-Verschlüsselung -

Effiziente E-Mail-Verschlüsselung unter IBM Domino

Expertise matters

Inhalt

1 Einführung

Der Umfang der Kommunikation per E-Mail ist in den letzten Jahren stark gewachsen und wächst immer weiter. Mittlerweile gibt es kaum noch ein Unternehmen, welches E-Mail für die Abwicklung ihrer Geschäftsprozesse sowohl innerhalb des Unternehmens als auch mit externen Geschäftspartnern nicht verwendet. Neben schnellen Reaktionszeiten, ständiger Erreichbarkeit und kostengünstiger Kommunikation steht die Frage nach der Sicherheit von E-Mails im Vordergrund, u. A. die Sicherstellung der E-Mail-Vertraulichkeit. Viele Unternehmen setzen deshalb auf E-Mail-Sicherheitslösungen, die auch die Verschlüsselung von E-Mails beinhalten.

An diese Lösungen werden folgende Anforderungen gestellt:

- Serverbasierte E-Mail-Inhaltsprüfung (Virenschutz, Schutz vor Spam- und Junk-Mail, Schutz vor Industriespionage, etc.)
- E-Mail-Verschlüsselung (z.B. bei vertraulichen Angebotsdaten, Auftragsdaten, etc.)
- geringer Administrationsaufwand

Das vorliegende White Paper gibt einen Überblick über die Implementierung der beiden E-Mail-Verschlüsselungsstandards PGP und S/MIME in iQ.Suite Crypt Pro für Domino.

2 Implementierung in iQ.Suite Crypt Pro

iQ.Suite Crypt Pro ist ein Modul der iQ.Suite. Durch Einsatz weiterer Module der iQ.Suite ist eine Überprüfung verschlüsselter E-Mails auf Viren (durch iQ.Suite Watchdog) oder Inhaltsprüfung (durch iQ.Suite Wall) möglich. iQ.Suite Crypt Pro beinhaltet folgende wichtige Funktionen:

- iQ.Suite Crypt Pro ist wie alle Module der iQ.Suite serverbasiert. So ist eine sichere E-Mail-Kommunikation möglich, ohne dass der Endbenutzer aktiv eingreifen muss. Es ist nur ein Zertifikat/Schlüssel für das ganze Unternehmen erforderlich, das so genannte Company-Zertifikat bzw. der Company-Key[1]
- Mit iQ.Suite Crypt Pro ist die automatische Ver- und Entschlüsselung, Signatur und Signaturprüfung (Validierung, nur S/MIME) möglich.
- iQ.Suite Crypt Pro unterstützt den Verschlüsselungsstandard PGP/GnuPG für die Betriebssysteme Windows, Linux, AIX und Sun Solaris und den Standard S/MIME für Windows-, Linux- und SUN Solaris-Betriebssysteme.

[1] Bei S/MIME spricht man generell von Zertifikaten, bei PGP bzw. GnuPG spricht man von Schlüsseln oder Keys.

2.1 PGP-Implementierung

iQ.Suite Crypt Pro ermöglicht es, E-Mails durch Verwendung von PGP oder GnuPG zu verschlüsseln, durch PGP oder GnuPG verschlüsselte E-Mails zu empfangen und zu entschlüsseln und automatisch die öffentlichen Schlüssel aus eingehenden E-Mails zu extrahieren und in den Schlüsselring zu importieren.

Die folgenden Ausführungen für GnuPG sind analog für alle anderen PGP-Varianten anwendbar. Folgende Voraussetzungen sind für die Verwendung von GnuPG in iQ.Suite Crypt Pro notwendig:

1. GnuPG muss separat installiert sein.
2. Eine gültige Lizenz für das Modul iQ.Suite Crypt Pro muss vorhanden sein.
3. Der Pfad für die Systemumgebung muss das entsprechende GnuPG-Verzeichnis enthalten.

Die Konfiguration für iQ.Suite Crypt Pro zur Verwendung von GnuPG erfolgt richtlinienbasiert, d.h. die Regeln für Ver- und Entschlüsselung und Schlüsselimport können dediziert für Nutzer, Nutzergruppen und das Unternehmen konfiguriert werden.

2.1.1 Szenarien für GnuPG

Die einzelnen Ablaufszenarien für ein- und ausgehende E-Mails unter Verwendung von GnuPG zur Ver- und Entschlüsselung bzw. Schlüsselimport werden nachfolgend beschrieben.

2.1.1.1 Ausgehende E-Mail verschlüsseln

- Voraussetzung:
  a) Der öffentliche Schlüssel des Empfängers ist im Schlüsselring vorhanden und es wird ihm absolut („ultimately“) vertraut oder er ist durch den standardisierten Unternehmensschlüssel signiert. Nähere Informationen über die verschiedenen Vertrauensstufen, Signaturarten und deren Bedeutung entnehmen Sie bitte der Dokumentation zu GnuPG.
  b) Der iQ.Suite Crypt Pro-Job „Encryption with GnuPG“ für das gewünschte Betriebssystem ist aktiv.
  c) Im iQ.Suite Crypt Pro-Job „Encryption with GnuPG“ müssen die jeweiligen Regeln für die Empfänger konfiguriert sein. Gegebenenfalls erstellen und aktivieren Sie dazu mehrere Jobs.
  d) Der Programmpfad für den Aufruf von cmd.exe ist gesetzt. Achtung: Die verschiedenen Windows-Versionen haben unterschiedliche Namen für die Unterverzeichnisse.
  e) Der Pfad zum Aufruf von gpg.exe muss gesetzt sein.
  f) Der Pfad zum öffentlichen Schlüsselring muss in den Parametern gesetzt sein (Home Directory).
  g) Eine genaue Beschreibung der notwendigen Parameter und Einstellungen finden Sie in der Online-Hilfe und im Administrationshandbuch.

- Ablauf der Verschlüsselung:

  a) Der Benutzer versendet seine E-Mail wie gewohnt.

  b) Auf dem Server holt sich iQ.Suite Crypt Pro den öffentlichen Schlüssel (Public-Key) für den Empfänger der E-Mail aus dem Schlüsselring von GnuPG

  c) Die E-Mail wird verschlüsselt (Szenario für S/MIME siehe 2.1.1.1 Ausgehende E-Mail verschlüsseln).

  d) Die E-Mail wird dem Empfänger zugestellt.

Im Konfigurationsdokument für den iQ.Suite Crypt Pro-Job können Sie zusätzliche Optionen angeben:

- Setzt der Kommunikationspartner ebenfalls iQ.Suite Crypt Pro oder ein anderes serverbasiertes Verschlüsselungsmodul ein, welches mit GnuPG verschlüsselt, so können Sie die Zuordnung von Empfängern zu Schlüsseln explizit angeben.
- Ebenso ist eine Auswahl zwischen PGP/MIME und PGP/Inline möglich. Bei PGP/Inline werden Nachrichtentext und Dateianhang einer E-Mail separat verschlüsselt. Zudem können Sie angeben, ob die verschlüsselten Inhalte direkt in den Nachrichtentext einer E-Mail integriert werden soll oder ob die verschlüsselten Daten als Dateianhang versandt werden. Den Name des Anhangs können Sie wählen. PGP/MIME ermöglicht dagegen eine Verschlüsselung des gesamten E-Mail-Inhalts als kompletter Block (mit Ausnahme des E-Mail-Headers).

2.1.1.2 Eingehende E-Mail entschlüsseln

- Voraussetzung:

  a) Der iQ.Suite Crypt Pro-Job „Decryption with GnuPG“ ist aktiv.

  b) Im iQ.Suite Crypt Pro-Job „Decryption with GnuPG“ müssen die jeweiligen Regeln für die Empfänger konfiguriert sein. Gegebenenfalls erstellen und aktivieren Sie dazu mehrere Jobs.

  c) Der Programmpfad für den Aufruf von cmd.exe ist gesetzt. **Achtung**: Die verschiedenen Windows-Versionen haben unterschiedliche Namen für die Unterverzeichnisse.

  d) Der Pfad zum Aufruf von gpg.exe muss gesetzt sein. Wichtig ist der Parameter „echo %PASSWORD%“

  e) Der Pfad zum privaten Schlüsselring muss in den Parametern gesetzt sein (Home Directory).

  f) Das Passwort des Standardschlüssels bzw. des privaten Unternehmensschlüssels muss gesetzt sein.

  g) Eine genaue Beschreibung der notwendigen Parameter und Einstellungen finden Sie in der Online-Hilfe und im Administrationshandbuch.

- Ablauf der Entschlüsselung:

  a) Es erfolgt eine Identifikation des in der eingehenden E-Mail verwendeten Schlüssels über die E-Mail-Adresse.

  b) Die eingehende E-Mail wird mittels des privaten Unternehmensschlüssels (Private Key) entschlüsselt.

  c) Die entschlüsselte E-Mail wird zugestellt.

2.1.1.3 Automatischer Schlüsselimport

Mit iQ.Suite Crypt Pro ist es möglich, die öffentlichen Schlüssel von Kommunikationspartnern, die mit der verschlüsselten E-Mail zusammen ihren öffentlichen Schlüssel versenden, automatisch in den Schlüsselring zu importieren.

- Voraussetzungen

  a) Der öffentliche Schlüssel des Senders ist im Nachrichtentext der E-Mail enthalten, z.B. als eindeutiger Block im Nachrichtentext oder als Anhang.

  b) Der iQ.Suite Crypt Pro-Job „Import Key for GnuPG“ (Betriebssystemversion beachten!) ist aktiv.

  c) Der Programmpfad für den Aufruf von cmd.exe ist gesetzt. **Achtung**: Die verschiedenen Windows-Versionen haben unterschiedliche Namen für die Unterverzeichnisse.

  d) Das Programm newkey.cmd muss im Programmpfad von GnuPG liegen. Newkey.cmd ist eine Batchdatei. Für die in dieser Batchdatei enthaltenen Programmaufrufe muss der Pfad gesetzt sein. Ein Beispiel für die Datei newkey.cmd finden Sie unter der Registerkarte Misc im Jobdokument.

  e) Der Pfad zum öffentlichen Schlüsselring muss in den Parametern gesetzt sein (Home Directory).

  f) Nach erfolgreichem Import müssen im iQ.Suite Crypt Pro-Job „Encryption with GnuPG“ die jeweiligen Regeln für die Empfänger konfiguriert sein, damit die importierten Schlüssel verwendet werden und erfolgreich verschlüsselt werden kann. Gegebenenfalls erstellen und aktivieren Sie dazu mehrere Jobs. Neu importierte Schlüssel müssen über den Administrator den Vertrauensstatus erhalten.

  g) Eine genaue Beschreibung der notwendigen Parameter und Einstellungen finden Sie in der Online-Hilfe und im Administrationshandbuch.

- Ablauf des Key Imports

  a) Der in der E-Mail enthaltene öffentliche Schlüssel des Senders wird aus der E-Mail heraus gelöst.

  b) Der öffentliche Schlüssel wird in den Schlüsselring importiert.

  c) Der Administrator erhält, wenn gewünscht, eine Benachrichtigung über den erfolgreichen Import des Schlüssels.

  d) Die verschlüsselte E-Mail kann anschließend entschlüsselt werden, falls sie verschlüsselt übertragen wurde.

  e) Die E-Mail wird dem Empfänger zugestellt.

  f) Dem importierten Schlüssel muss anschließend durch den Administrator „absolut“ vertraut werden oder er muss mit dem Standard-(Unternehmens)-Schlüssel signiert werden.

  g) Es erfolgt weder eine automatische Definition der Vertrauensstellung noch eine Signatur.

2.2 S/MIME Implementierung

In iQ.Suite Crypt Pro ist ein S/MIME-Interface implementiert. Folgende Voraussetzungen sind für die Verwendung von S/MIME in iQ.Suite Crypt Pro notwendig:

- Betriebssystem ist Windows 2000/2003, XP, Linux oder SUN Solaris.
- Eine gültige Lizenz für das Modul „iQ.Suite Crypt Pro with S/MIME“.
- Der Pfad für die Systemumgebung muss das Verzeichnis smime enthalten, da während des Setups alle nötigen Programme in dieses smime-Verzeichnis installiert werden.
- Ein Zertifikat (pkcs12-Format) einer Zertifizierungsstelle (Certification Authority - CA), das Benutzerzertifikate ausstellen und signieren kann, die zur E-Mail-Verschlüsselung eingesetzt werden können. Es wird in diesem Zusammenhang im Folgenden auch mit Aussteller-Zertifikat (root.pfx) bezeichnet. Es dient iQ.Suite Crypt Pro zur Erstellung der internen privaten Benutzerzertifikate, mit denen ausgehende E-Mails signiert werden können. Das Aussteller-Zertifikat muss als pfx-Datei (pkcs12-Format) im smime-Verzeichnis stehen. Hinweis: Bei der Installation wird ein Testzertifikat in das Verzeichnis …\smime\TestCertificates abgelegt.
- Ein Unternehmens-Zertifikat (pkcs12-Format), mit dem E-Mails verschlüsselt werden können, erstellt und signiert von o. g. CA. (company.pfx). Es dient iQ.Suite Crypt Pro als Vorlage für die internen privaten Benutzertifikate. Des Weiteren werden eingehende, verschlüsselte E-Mails mit dem Unternehmens-Zertifikat entschlüsselt. Das Unternehmens-Zertifikat muss als pfx-Datei (pkcs12-Format) im smime-Verzeichnis stehen.
- Hinweis: Bei der Installation wird ein Testzertifikat in das Verzeichnis …`\smime\TestCertificates` abgelegt.

- Die Schlüsseldatenbank g_cert.nsf muss für die Verwaltung öffentlicher Zertifikate auf dem lokalen Server vorhanden sein. Bei der Bearbeitung eingehender, signierter E-Mails werden die Zertifikatsdaten der Signatur auf Wunsch automatisch in die Schlüsseldatenbank abgelegt und stehen für spätere Aufgaben zur Verfügung.
- Wird ein Zertifikat benötigt, das noch unbekannt ist, kann über einen LDAP-Server in einem entsprechenden Verzeichnis gesucht werden. Das Zertifikat wird anschließend in der Datenbank gespeichert. Ein Eintrag in einem LDAP-Verzeichnis muss mindestens die E-Mail-Adresse und das Zertifikat der entsprechenden Person enthalten. IBM Domino kann als LDAP-Server benutzt werden.

Die Konfiguration für iQ.Suite Crypt Pro zur Verwendung von S/MIME erfolgt richtlinienbasiert, d.h. die Regeln für Ver- und Entschlüsselung, Signatur und Signaturprüfung können dediziert für Nutzer, Nutzergruppen und das Unternehmen konfiguriert werden.

2.2.1 Szenarien für S/MIME

Die einzelnen Ablaufszenarien für ein- und ausgehende E-Mails unter Verwendung von S/MIME zur Ver- und Entschlüsselung bzw. Signatur und Signaturprüfung werden nachfolgend beschrieben.

2.2.1.1 Ausgehende E-Mail verschlüsseln

- Voraussetzung:
  a) Das Empfänger-Zertifikat ist in der Schlüsseldatenbank g_cert.nsf vorhanden oder via LDAP erreichbar und mittels E-Mail-Adresse identifizierbar
  b) Der iQ.Suite Crypt Pro-Job „Encrypt with S/MIME“ ist aktiv.
  c) Im iQ.Suite Crypt Pro-Job „Encrypt with S/MIME“ müssen die jeweiligen Regeln für die Empfänger konfiguriert sein. Gegebenenfalls erstellen und aktivieren Sie dazu mehrere Jobs.
  d) Die Namen des Unternehmens- und des Aussteller-Zertifikates sind in den Parametern des Jobs explizit anzugeben. Bei der Verschlüsselung ist nur das Passwort für das Unternehmens-Zertifikat notwendig, welches mit der Variablen %password% gesetzt werden kann. Das Passwort des Aussteller-Zertifikates muss nur bei S/MIME Signaturen angegeben werden und kann mit der Variable %issuerpassword% gesetzt werden.
  e) Bei Verwendung eines LDAP-Servers müssen die Adresse (IP oder DNS-Name) und der Port für den LDAP-Server stimmen, d.h. die Parameter „ldapserver“ und „ldapserverport“ müssen korrekt konfiguriert sein.
  f) Als Option kann über den Parameter „--signmessage“ angegeben werden, ob jede verschlüsselte E-Mail auch automatisch signiert werden soll.
  g) Eine genaue Beschreibung der notwendigen Parameter und Einstellungen finden Sie in der Online-Hilfe und im Administrationshandbuch.

- Ablauf der Verschlüsselung:

  a) Der Benutzer versendet seine E-Mail wie gewohnt.

  b) Auf dem Server holt sich das iQ.Suite Crypt Pro S/MIME-Interface den öffentlichen Schlüssel (Public-Key) für den Empfänger der E-Mail aus der Schlüsseldatenbank bzw. dem LDAP-Server (oder dem lokalen Puffer [der Cache-DB], falls mehrere E-Mails in kurzen Abständen versendet werden).

  c) Die E-Mail wird verschlüsselt (für das PGP-Szenario siehe auch 2.1.1.1 Ausgehende E-Mail verschlüsseln).

  d) Die E-Mail wird dem Empfänger zugestellt.

Im Konfigurations-Dokument für den iQ.Suite Crypt Pro-Job können zusätzliche Optionen angegeben werden:

- Setzt der Kommunikationspartner ebenfalls iQ.Suite Crypt Pro oder ein anderes serverbasiertes Verschlüsselungsmodul ein, das auf Basis eines Unternehmens-Zertifikates verschlüsselt, so können Sie die Zuordnung von Empfängern zu Schlüsseln explizit angeben (siehe auch Vorgehensweise am Beispiel von S/MIME).

2.2.1.2 Ausgehende E-Mail signieren

- Voraussetzung:

  a) Das Unternehmens-Zertifikat und das zugehörige Aussteller-Zertifikat sind als *.pfx Datei im **smime**-Verzeichnis vorhanden, z.B. **company.pfx** und **root.pfx**. Die Passwörter für beide Zertifikate sind mit den Variablen %Password% und %Issuerpassword% gesetzt.

  b) Der iQ.Suite Crypt Pro-Job „Sign S/MIME Outgoing Message“ ist konfiguriert und aktiv.

  c) Wichtig ist, dass im Job-Dokument die Parameter *--from = %FROM%* und *--outputformat=CLEARSIGNED* gesetzt sind.

  d) Im iQ.Suite Crypt Pro-Job „Sign S/MIME Outgoing Message“ müssen die jeweiligen Regeln für die Empfänger konfiguriert sein. Gegebenenfalls erstellen und aktivieren Sie dazu mehrere Jobs.

  e) Eine genaue Beschreibung der notwendigen Parameter und Einstellungen finden Sie in der Online-Hilfe und im Administrationshandbuch.

- Ablauf der Signatur:

  a) Der Benutzer versendet seine E-Mail wie gewohnt.

  b) Es wird für den Absender der E-Mail „on-the-fly“ ein Zertifikat erzeugt, d.h. mit folgenden Schritten:

     I. Öffne Unternehmens-Zertifikat.

     II. Ändere die E-Mail-Adresse im Zertifikat, d.h. die vorhandene E-Mail-Adresse des Unternehmens wird durch die E-Mail-Adresse des Absenders ersetzt.

III. Zusätzlich wird die im Unternehmens-Zertifikat enthaltene Seriennummer geändert.

IV. Das neue Zertifikat wird mit dem Aussteller-Zertifikat (im smime-Verzeichnis vorhanden) unterzeichnet.

c) Das neue Zertifikat wird als neue Datei im pkcs12-Format gespeichert: <from>_<Domainpart des Aussteller-Zertifikates>.pfx

   Der Name „from“ leitet sich aus dem Parameter --from = %FROM% im Jobdokument ab.

   Beispiel: john.smith_belle.view.pfx

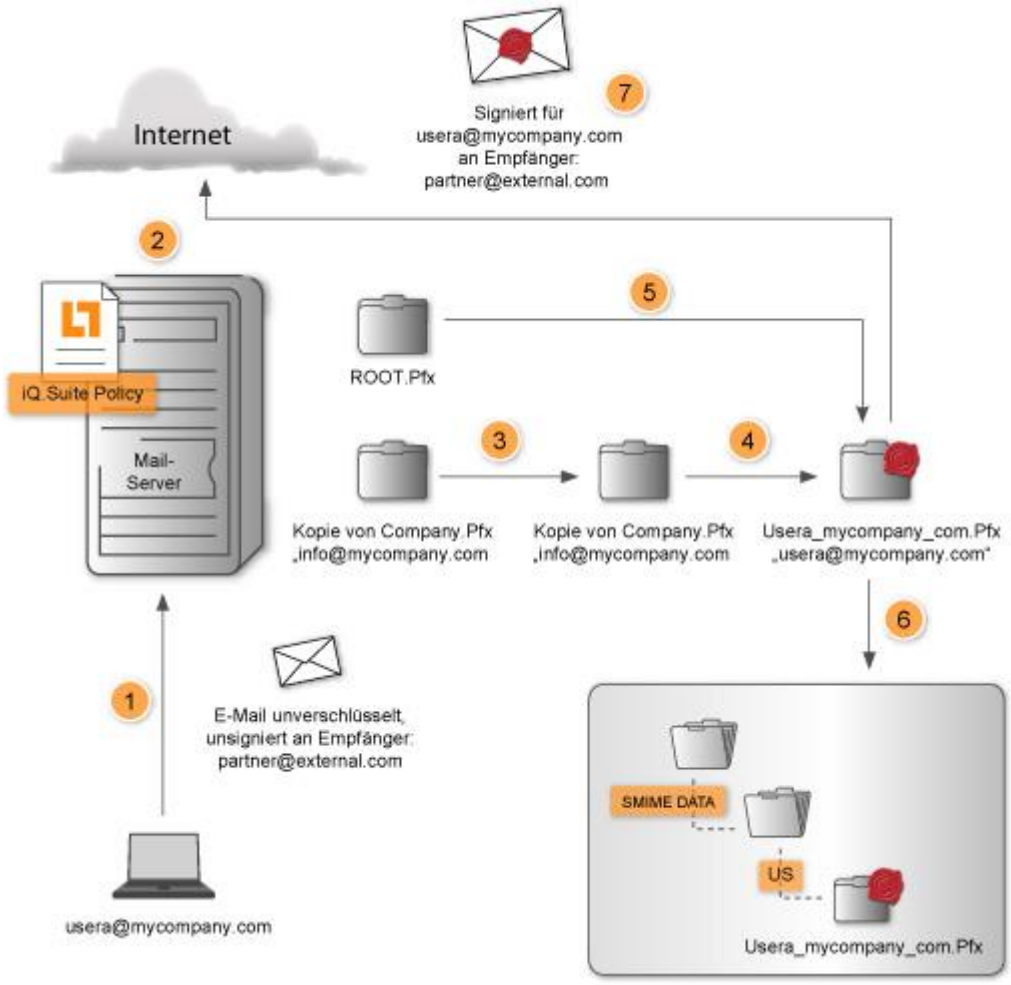
   Ist bereits eine pfx-Datei desselben Namens vorhanden, so wird diese verwendet. Die Ablage der neuen Zertifikate erfolgt im smime-Verzeichnis. Für jedes neue Zertifikat wird ein eigenes Unterverzeichnis angelegt, wobei die ersten beiden Buchstaben des Benutzernamens als Bezeichnung für das Unterverzeichnis verwendet werden. Haben verschiedene Benutzer die gleichen zwei ersten Buchstaben, so werden die neuen Zertifikate im gleichen Unterverzeichnis abgelegt.

d) Die Daten des Absenders werden mit dem neuen bzw. dem bereits vorhandenen Zertifikat unterzeichnet.

e) Die Daten werden versendet.

Der Empfänger kann die E-Mail lesen und bekommt einen Hinweis, dass die E-Mail signiert ist. Um dem Sender verschlüsselt zu antworten, muss das Zertifikat dem Empfänger-Mailsystem so zur Verfügung gestellt werden, dass dieses damit verschlüsseln kann. Das ist im Fall von Outlook der Zertifikatsspeicher von Windows, kann aber auch ein LDAP-Directory sein. Details sind den entsprechenden Handbüchern der Mailclients zu entnehmen.

Die nachfolgende Grafik beschreibt den Ablauf der Signatur.



1. Interner Sender verschickt E-Mail.
2. iQ.Suite erkennt auf Basis Sender/Empfänger-Konstellation, dass die E-Mail signiert werden soll.
3. Das Unternehmenszertifikat wird dupliziert.
4. Die E-Mail Adresse im duplizierten Unternehmenszertifikat wird durch die des Absenders ersetzt.
5. Das veränderte, duplizierte Unternehmenszertifikat wird mit dem ROOT Zertifikat signiert.
6. Dieses angepasste Zertifikat wird unterhalb des Unternehmenszertifikates im Dateisystem abgelegt.

Dieser Prozess läuft nur einmal für jeden internen Benutzer, dessen E-Mails signiert werden sollen.

Um eine E-Mail zu signieren und / oder zu entschlüsseln, benötigt der Sender ein Zertifikat mit seiner eigenen E-Mailadresse. Das Unternehmenszertifikat dient als Vorlage, um mit Hilfe der Root-CA ein solches individuelles Benutzerzertifikat zu erstellen:

Es wird eine Kopie des Unternehmenszertifikates erstellt, die E-Mailadresse ausgetauscht und von der Root-CA signiert. Wenn der Parameter *--newserialnr* mitgegeben wird, wird zusätzlich eine neue Seriennummer für das Zertifikat erstellt. Dies verhindert beim Empfänger Fehlermeldungen.

Dieser Prozess läuft genau dann ab, wenn der interne Benutzer das erste Mal eine E-Mail an einen externen Empfänger schickt. Wenn bereits ein Zertifikat für den Benutzer vorhanden ist, ist es nicht nötig, ein weiteres zu erstellen. Die E-Mail wird dann mit dem passenden Zertifikat signiert und/oder entschlüsselt.

2.2.1.3 Ausgehende E-Mail verschlüsseln und signieren

Es gibt zwei Vorgehensweisen:

- Ausgehende E-Mails werden mit einem Job verschlüsselt und signiert. Eine ausgehende verschlüsselte E-Mail wird automatisch auch signiert, siehe Ausgehende E-Mail signieren in S/MIME. Unter Operations muss der Modus von Signieren auf Verschlüsseln umgestellt werden. Das ist die empfohlene Variante.
- Alternativ können zwei Jobs für unterschiedliche Benutzergruppen für den Empfang der E-Mails definiert werden: Eine Benutzergruppe mit dem entsprechenden Job, die nur signierte E-Mails empfängt, siehe Ausgehende E-Mail signieren in S/MIME und eine Benutzergruppe, die nur verschlüsselte und nicht signierte E-Mails empfängt, siehe Ausgehende E-Mail verschlüsseln. Beide Benutzergruppen müssen disjunkt sein. Falls es Benutzer geben sollte, die in beiden Gruppen enthalten sind, wählen Sie die erste Vorgehensweise.

2.2.1.4 Eingehende E-Mail entschlüsseln

- Voraussetzung:

a) Der iQ.Suite Crypt Pro-Job „Decrypt S/MIME Message“ ist aktiv.

b) Im iQ.Suite Crypt Pro-Job „Decrypt S/MIME Message“ müssen die jeweiligen Regeln für die Empfänger konfiguriert sein. Gegebenenfalls erstellen und aktivieren Sie dazu mehrere Jobs.

c) Eine genaue Beschreibung der notwendigen Parameter und Einstellungen finden Sie in der Online-Hilfe und im Administrationshandbuch.

- Ablauf der Entschlüsselung:

a) Es erfolgt eine Identifikation des in der eingehenden E-Mail verwendeten Zertifikates über den Ausstellernamen.

b) Bei der Entschlüsselung erfolgt automatisch eine Signaturprüfung (siehe Schritte a bis d im Ablauf „Eingehende E-Mail-Signatur prüfen – Ablauf der Signaturprüfung“). Ist die E-Mail mit einem Zertifikat signiert, welches in der Schlüsseldatenbank g_cert.nsf noch nicht vorhanden ist, wird es in diese importiert und verifiziert.

c) Ab sofort können an den Absender verschlüsselte E-Mails versandt werden. Ist das Zertifikat vorhanden, wird es verifiziert.

d) Im Anschluss wird die E-Mail mit dem Zertifikat des Unternehmens (company.pfx) entschlüsselt.

e) Die entschlüsselte E-Mail wird zugestellt.

f) Der Empfänger der E-Mail erhält am Ende des Nachrichtentextes einen Report über die erfolgreiche Entschlüsselung und Signaturprüfung.

2.2.1.5 Eingehende E-Mail-Signatur prüfen

- Voraussetzung:

  a) Der iQ.Suite Crypt Pro-Job „Verify S/MIME Signatur“ ist aktiv.

  b) Im iQ.Suite Crypt Pro-Job „Verify S/MIME Signatur“ sind die entsprechenden Regeln für die Empfänger konfiguriert. Gegebenenfalls erstellen und aktivieren Sie dazu mehrere Jobs.

  c) Eine genaue Beschreibung der notwendigen Parameter und Einstellungen finden Sie in der Online-Hilfe und im Administrationshandbuch.

- Ablauf der Signaturprüfung:

  a) Zertifikat/Signatur wird aus der eingehenden E-Mail gelöst. Falls das Absender-Zertifikat nicht Bestandteil der E-Mail ist, kann es von einem verfügbaren LDAP-Server oder aus der Cache-DB geholt werden.

  b) Sollte das Zertifikat noch nicht in der Schlüsseldatenbank g_cert.nsf vorhanden sein, so wird es in diese importiert. Ab sofort können an den Absender verschlüsselte E-Mails versandt werden (siehe Ausgehende E-Mail verschlüsseln in S/MIME).

  c) Die signierten Daten werden anhand des Absender-Zertifikates verifiziert:

  d) Es wird überprüft, ob das Zertifikat zur Signatur passt (über E-Mailadresse und Zertifikatsnummer).

  e) Es wird überprüft, ob der Absender zum Zertifikat passt.

  f) Es wird ein Report über die Signaturprüfung (Schritte c - e) erzeugt.

  g) In der E-Mail wird die Signatur des Absenders entfernt und die E-Mail wird um den Report ergänzt.

  h) Die E-Mail wird dem Empfänger zugestellt.

2.2.1.6 E-Mail eingehend entschlüsseln und Signaturprüfung

Bei der Entschlüsselung eingehender E-Mails erfolgt automatisch eine Signaturprüfung, siehe Eingehende E-Mail entschlüsseln in S/MIME. Trotzdem sollte zusätzlich ein separater Job für die Signaturprüfung vorhanden sein. Eingehende E-Mails können unverschlüsselt und unsigniert oder nur verschlüsselt oder auch nur signiert sein.

Wichtig ist hierbei, dass die iQ.Suite Jobs in der entsprechenden Reihenfolge angesprochen werden, d.h. der Entschlüsselungs-Job muss vor dem Signaturprüfungs-Job erfolgen. Mit dem Parameter „–noverify“ kann auch ein reiner Entschlüsselungsjob ohne Signaturprüfung konfiguriert werden.

2.3 Vorgehensweise am Beispiel von S/MIME

Die Herstellung einer Verbindung mit S/MIME zu einem zukünftigen Kommunikationspartner kann mit folgenden Schritten vorgenommen werden:

- Aktivieren des entsprechenden Crypt Pro-Jobs „Verify S/MIME Signatur“ oder / und „Decrypt S/MIME Message“.
- Der zukünftige Kommunikationspartner sendet eine signierte E-Mail an der das Zertifikat angehängt ist.
- Import des Zertifikates in die Zertifikatsdatenbank g_cert.nsf (automatisch) oder in das LDAP-Verzeichnis.
- Aktivieren des entsprechenden Crypt Pro-Jobs „Encrypt S/MIME Message“.
- Zuordnung des Empfängers zur entsprechenden Richtlinien-Liste für die Verwendung der Verschlüsselung, d.h. Ergänzung der Auswahlregel „EncryptionRecipients S/MIME“ um den jeweiligen Empfänger.

Der Import eines Zertifikates in ein LDAP-Verzeichnis ist betriebssystemabhängig.

Der Kommunikationspartner muss entsprechend auf seiner Seite die Zertifikate, die Sie ihm zukommen lassen, importieren und verifizieren.

- Notes/Domino
- Der Import des Zertifikates erfolgt über die Standard Domino-Funktion. Eine genaue Beschreibung der Vorgehensweise kann dem Domino-Handbuch entnommen werden. Voraussetzung für den Import ist das Vorhandensein des Benutzers im Namens- und Adressbuch (nicht registriert).
- Outlook-User
- Der Import des Zertifikates erfolgt in den Zertifikatsspeicher des Windows-Betriebssystems. Zusätzlich muss die Aussteller-ID (stammt vom Aussteller-Zertifikat des Unternehmens-Zertifikates) durch den Zertifikatsmanager des Outlookclients der Status „Vertrauenswürdig“ verliehen werden. Im Betriebssystem sind eine Reihe von vertrauenswürdigen Ausstellern, u. A. Verisign, enthalten. Bei der Erstellung eigener Zertifikate muss der Status vertrauenswürdig separat verliehen werden. Ist dieser Status nicht verliehen, so werden

eingehende E-Mails in Outlook zwar entschlüsselt und die Signatur wird ebenfalls verifiziert, aber bei jeder E-Mail kommt der Hinweis auf die nicht vorhandene Vertrauenswürdigkeit des Zertifikates.

- Details für den Import-Vorgang der Herstellung der Vertrauenswürdigkeit eines Zertifikates sind dem Windows-Handbuch zu entnehmen.

Die Herstellung einer Verbindung zu einem anderen Server funktioniert entsprechend. Das kann zum Beispiel dann der Fall sein, wenn zwei verschiedene Firmen mittels Unternehmenszertifikaten sicher kommunizieren wollen, aber die E-Mails automatisch den entsprechenden Empfängern und Sendern zugeordnet werden sollen. Die Schritte sind:

- Anforderung des Zertifikates des anderen Servers durch Empfang einer signierten E-Mail oder als Datei im p7b-Format.
- Senden des eigenen Zertifikates an den anderen Server - d.h. entweder versenden Sie eine signierte E-Mail mit dem Zertifikat als Anhang oder senden das Zertifikat auf anderen Wegen (z.B. per Diskettenaustausch) im p7b-Format dem Kommunikationspartner zu.
- Import des Zertifikates in das LDAP-Verzeichnis (z.B. Domino)
- Zuordnung des Empfängers zur entsprechenden Richtlinien-Liste für die Verwendung der Verschlüsselung.

Die Interoperabilität von iQ.Suite Crypt Pro S/MIME ist mit Systemen gegeben, die nach dem S/MIME Standard arbeiten.

3 iQ.Suite Crypt Pro auf einen Blick

Highlights

- Unternehmensweite Verschlüsselungs-Richtlinien

  Die flexible Konfiguration von Absender-Empfänger-Kombinationen und E-Mail-Domänen erlaubt gezielte Verschlüsselungsbeziehungen zwischen Personen, Gruppen und Unternehmen. Zentrale Richtlinien ermöglichen beispielsweise das Einrichten permanenter E-Mail-Verschlüsselung oder deren Begrenzung auf bestimmte Personengruppen.

- Transparente Wirkungsweise

  Der Einsatz standardisierter Verfahren und die zentrale Verarbeitung auf dem Server stellt Transparenz gegenüber dem Benutzer und Unabhängigkeit vom E-Mail-Client sicher. Alle Kombinationen der Verschlüsselungspartner, wie Client-Client, Server-Server und Client-Server, sind frei konfigurierbar.

- Unterschiedliche Verschlüsselungsstandards

  Die gleichzeitige Verwendung von unterschiedlichen Verschlüsselungsverfahren wie PGP/GnuPG und S/MIME bietet höchste Sicherheit für unterschiedliche Einsatzzwecke und Kommunikationspartner.

- Flexibles Regelwerk

  Durch den Einsatz eines intelligenten, frei definierbaren Regelwerks zur gezielten Verschlüsselung von E-Mail-Inhalten bietet iQ.Suite Crypt Pro höchste Flexibilität und Sicherheit.

- Integrierte und zentrale Administration

Features

- Vergabe zentraler Verschlüsselungs-Richtlinien für die Kommunikation über Internet und öffentliche Netze
- Transparente E-Mail-Verschlüsselung unabhängig vom E-Mail-Client für den Benutzer
- Gezieltes Verschlüsseln durch Adressprüfung beliebiger Absender-Empfänger-Kombinationen, Empfängergruppen und Internetdomänen
- Integrierbar in jede Schlüsselverwaltung und Public Key Infrastructure (PKI)
- Zentrale Ablage von personen- und firmenbezogenen Public-Keys auf dem Server
- Keine Schlüsselverwaltung beim Endbenutzer
- Gleichzeitige Verwendung unterschiedlicher Verfahren mit langen Schlüsseln, z.B. PGP, GnuPG, S/MIME
- Detaillierte Protokollfunktionen
- Integrierte Zertifikatsdatenbank
- Konfigurierbare Benachrichtigungen an Absender, Empfänger und Administrator
- Multiplattformsupport für alle Betriebssysteme
- Optimiertes Multiprozessing und Multithreading auch für Partitioned Server und Cluster
- Skalierbare Architektur
- Einfache Erweiterung mit weiteren iQ.Suite Produkten

Über GBS

GROUP Business Software ist führender Anbieter von Lösungen und Services in den Bereichen Messaging Security und Workflow für die IBM und Microsoft Collaboration Plattformen. Weltweit vertrauen mehr als 5.000 Kunden und 4 Millionen Anwender auf die Expertise von GBS. Der Konzern ist in Europa, Nordamerika sowie Asien tätig.

Weitere Informationen unter www.gbs.com