GBS

PKI Fundamentals

- iQ.Suite Crypt Pro Basics -

Public-Key Infrastructures and the Encryption Methods PGP and S/MIME

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. With its Crypt module, iQ.Suite from GBS Software offers a comprehensive and complete policy-based solution to these issues.

The present documentation provides an overview of public-key infrastructures as well as the encryption methods PGP und S/MIME.

2 Public-Key Infrastructures

This section deals with the management of public keys. If these public keys are kept and managed in a publicly accessible database or a directory. one speaks of a public-key infrastructure (PKI).

2.1 Basic Terms and Definitions

A PKI is a combination of hardware/software components, policies and different procedures. it is based on objects that are called certificates and serve as digital identification. Certificates associate users to their public keys.

A PKI consists of:

- a security policy – Defines the level of security, the processes and the use of cryptography; includes information on how to handle keys and valuable information;
- a Certification Authority (CA) – As the PKI's trust basis, this is where the certificates are created;
- a Registration Authority (RA) – Interface between the users and the CA; registers and authenticates the users' identity and forwards requests for certificates to the CA;
- a distribution system for the certificates – for instance distribution by users themselves or a directory server such as LDAP. The distribution depends on the PKI environment.
- PKI applications, e.g. emails, communication between web server and web browser.

Also called Trust Center, a CA and RA combination is used for the authentication of individual persons and their messages.

2.2 Alternatives to PKI

Depending on the number of users involved, building a public-key infrastructure can be quite time-consuming and expensive. Typically, a PKI is set up when multiple applications such as email encryption, access control to facilities, areas or buildings and single sign-on functionality is to be implemented on a single smart card. When secure (encrypted) transmission via the Internet is the issue, a server-based solution is an alternative (also refer to the "PKI Alternative" whitepaper). Within companies, a secure connection from any client to the server is ensured through other means, e.g. VPN. To encrypt an email while they are transmitted over the Internet or to ensure the authenticity of a message by way of an electronic signature, a server-based approach is a very good solution, in particular in terms of cost-benefit.

2.3 LDAP

LDAP (Lightweight Directory Access Protocol) is an open standard for global or local directory services, for instance in networks and/or in the Internet. A directory can be best compared to a telephone book. An LDAP is normally used to associate names to telephone numbers and emails addresses, but it can also contain other information. Provided the data in the directory does not change very often, LDAPs are designed to ensure high performance when dealing with a large number of requests.

LDAP features the following properties:

- LDAP is a client/server system. The LDAP client supplies information to or receives information from the LDAP server. The LDAP server manages the information in the directory, forwards requests to another LDAP server where required or includes the information supplied in the directory.
- LDAP is sometimes called X.500 Lite. X.500 is an international standard for directories. X.500 is equipped with comprehensive functions, it is very complex, it requires high computing power and includes the complete OSI layer model[1]. By contrast, LDAP can be easily run on a PC and via TCP/IP. LDAP is able to access X.500 directories, but does not support all of the X.500 functions.
- The main advantage of LDAP is the more condensed nature of certain information and, compared to X.500, a much easier implementation.
- LDAP can only be used in conjunction with LDAP-capable application programs or LDAP gateways. Though it supports access control functions to a certain extent, LDAP does not have as many security features as X.500.
- LDAP an open, configurable protocol. It is able to store virtually any information related to specific organizational structures.

[1] Open Systems Interconnection (OSI – an ISO working group). The OSI layer model serves as international reference model for data transmission in networks. It consists of seven layers.

- LDAP is often used as central authentication service. Users thus have a common login interface, e.g. for console login, POP server, IMAP server, network computers, etc. With LDAP, a user ID and the corresponding password can be used for all login procedures, which greatly simplifies the administration tasks.

LDAP terminology:

- Each entry in an LDAP directory is a unit, identified or referenced by its unique name (Distinguished Name, DN).
- Each entry has attributes, i.e. pieces of information directly related to the entry. For instance, an organization could be an LDAP entry and the fax number, the address, etc. the entry's attributes. Staff members can also be LDAP entries. Typical staff attributes include telephone numbers and email addresses.
- Certain attributes are compulsory, while others are optional. An object class defines the attributes and whether they are compulsory or optional.
- The LDAP data exchange format (LDAP Data Interchange Format, LDIF) is an ASCII text format for LDAP entries. Files that import data from or export data to an LDAP server must be provided in LDIF format.

2.4 Certificates

2.4.1 Basics

Certificates are documents that testify to a certain identity. A certificate can be compared to an official document or a passport.

iQ.Suite Crypt Pro is a software that deals with electronic/digital certificates. To simplify matters, digital certificates will simply be referred to as certificates in this document.

A certificate issued by the CA guarantees that a public key actually belongs to the person, group or company that claims to be the owner of the key. To that end, the information needed to identify the public key holder is registered in the certificate. Once the identity has been confirmed by the Registration Authority (RA), the certificate is (digitally) signed by the Certification Authority (CA), thus guaranteeing the identity. The CA signs with its own private key.

Certificates can be issued for persons, groups, companies or servers. Accordingly, one speaks of personal certificates, group certificates, company certificates or server certificates.

Depending on individual requirements, different methods can be used to verify an identity. Applications range from a simple verification of a person's email address to situations where a person has to personally present his or her identity card in order to obtain a certificate.

Certificates can be created by way of software, e.g. S-Trust, PGP, Microsoft CA Server. The most widely used certificates are:

- PGP certificate (see PGP Certificate Types)
- X.509 certificate (see Certificate X.509 v3)

2.4.2 Necessity of Certificates

The problems related to the distribution of keys when using asymmetric cryptosystems are often underestimated or not really recognized. With public keys knowingly exchanged over an insecure channel, many people seem to think that “intercepting” these keys is the only threat to communication security.

However, a variety of active attacks have to be taken into account:

- User A’s public key KA is intercepted by user B and replaced with another key KA*.
- The database now contains the “fake” key KA*. This key is used by another user to encrypt a message addressed to A.
- User B intercepts the message and decrypts it using the private key associated with the public key KA*, i.e. he is able to read and modify the message.
- Then, user B encrypts the message (whether modified or not) with user A’s public key and sends it to user A, who decrypts it with his own private key.

Neither user A nor the sender are likely to have noticed the attack.

Certificates are used to protect oneself against this kind of attack, as they allow to exchange keys securely.

Just like identity cards, certificates have to be protected against:

- Counterfeiting: through the signature of the competent authority
- Abuse: through a validity range. This range can be very short, as issuing new certificates is relatively easy.

A database containing a list of blocked (invalid) certificates is called Certificate Revocation List (CRL).

2.4.3 Certificate X.509 v3

The CCITT and the ISO have agreed on a standardization of digital certificates, the Directory Authentication Framework [CITT509], also called X.509 protocol.

Currently available in version 3, the X.509 protocol describes the structure of certificates and has been adopted in ANSI and ISO standards. Currently, X.509 is the most widely used standard.

A certificate must at least contain the following information:

- the owner
- the owner's public key
- the signature of the CA

An X.509 certificate must additionally contain the following information:

- the version
- the series number
- the algorithm
- the issuer's name
- the expiry date
- the user's name
- the user's public key
- the issuer's unique identifier
- the user's unique identifier
- any extensions
- the signature

Extensions essentially include:

- Certificate Policies – the terms and conditions under which the CA works (e.g. security measures related to certificates, etc.).
- CRL Distribution Points – designates the point (IP address) where information on revoked certificates can be found.

When compared to PGP certificates (see S/MIME), there are a number of differences:

- X.509 certificates are provided by a CA, while PGP certificates are issued (signed) by “normal” people.
- X.509 certificates support one name only as owner of the key.
- X.509 certificates support one signature only to confirm the key.

2.4.4 Certificate Revocation

Any abused certificates need to be recognized and revoked, visibly for all. All revoked certificates are listed in a so-called Certificate Revocation List (CRL). Certificates are revoked by the Certification Authority for the following reasons: the password has become known, the certificate has been abused, the certificate owner leaves the company for which the certificate has been issued, etc. A CRL version 2 contains the following:

- Version
- Algorithm
- Issuer’s name
- Issuing date of the current CRL
- Issuing date of a new CRL
- Series numbers of the revoked certificates
- Extensions
- Signature

Any revoked certificate has to remain in the revocation list at least until its original validity period has expired. The latest revocation list must be made available to the participants of the security infrastructure on a periodical basis, in order to ensure they can verify the trustworthiness of a certifi-cate at any time and to prevent abuse by attackers who have illegally obtained someone else’s cer-tificate and related key.

Any revoked certificate has to remain in the revocation list at least until its original validity period has expired. The latest revocation list must be made available to the participants of the security infrastructure on a periodical basis, in order to ensure they can verify the trustworthiness of a certifi-cate at any time and to prevent abuse by attackers who have illegally obtained someone else’s cer-tificate and related key.

Problems with CRLs:

1. When a certificate is revoked, one has to wait until the next CRL issue to make this fact public. This delay may range from a few hours to several weeks.
2. The size of the CRL depends on the number of users of a Certification Authority as well as on the validity period of the certificates.

2.5 Certification Authority

Security infrastructures with a central Certification Authority (CA) have the following tasks:

- Issue certificates/certify keys,
- maintain and publish revocation lists.

By issuing a certificate, the CA links the name of a user to his public key. The structure of an x.509 certificate is described under Certificates, Basics. The CA guarantees that the name and the public key in the certificate belong to the same person. The CA ensures that any applicants for a certificate provide evidence of their identity to the CA.

It is therefore necessary that all persons involved trust the CA’s public key. If the CA’s private key is compromised, all user certificates have to be newly issued.

Any certified public keys have to be published, usually in an LDAP directory service (see Alternatives to PKI).

A CA can be compared to an identity card authority. If unauthorized persons had the possibility to create identity cards, they could cause a lot of damage. Accordingly, a CA environment also needs to be appropriately protected.

A CA can be represented by a tree structure, however complex this tree structure may be. The “Root CA” is the root of the tree, while its leaves are the certified users. In between, there may be additional CAs, each certified by the next higher CA in the hierarchy. The root CA is not certified by any authority, i.e. it is trustworthy for all others by definition.

There are two different ways to link two different public key infrastructures:

1. The first is to set up a third, higher-ranking CA.
2. The second is that both CAs certify each other and, in so doing, also all user certificates issued by the other CA.

2.6 Certification Procedure

Essentially, a certificate consists of one's own public key. In order to have that key certified by the competent CA, one first has to create the pair of keys; then the public key has to be signed by the Certification Authority

A CA may use one of two ways to issue a certificate:

1. The user generates the pair of keys himself and provides the public key to the CA for certification.
2. The CA generates the pair of keys for the user.

Both of these options have advantages and drawbacks.

Case 1 – User creates keys:

Advantages:

- The user generates the pair of keys himself and only sends the public key to the CA. The later signs the key and returns the certificate thus created to the user. Before signing the key and issuing the certificate, the CA has to make sure that the public key obtained really belongs to the user. To do so, the CA may ask the user to present himself personally with an identity card or other piece of identification. A verification of the applicant's identity by phone or email is not appropriate. With this procedure, the user can be sure that nobody else can possibly own his private key.
- The information transmitted, i.e. the public key and the certificate, do not cause any security-relevant problems, as all information communicated is public anyhow. Any sensitive information, such as password or private key, remains with the user. All that is needed is a verification of the public key in order to make sure it has not been altered.

Drawbacks:

- The user has to make sure that a copy of his pair of keys is stored at a safe place (e.g. in a safe deposit box), if he needs them again in case they are lost (e.g. following a hard disk crash). Otherwise, a new pair of keys has to be generated and the new public key has to be certified again by the CA.
- In one way or another, the public key has to be transported from the user to the CA and the certificate has to be returned from the CA to the user.

Case 2 – CA creates keys:

Advantages:

- The CA creates the keys. This makes it possible to keep the keys at the CA. Should the user ever need his pair of keys again (e.g. due to loss of data following a hard disk crash), he can obtain them from the CA.
- The user has no safeguarding tasks to take care of.
- The CA can create the certificate in a single operation, which makes it much easier.

Drawbacks:

- The members of the security infrastructure and the CA must fully trust each other, as the user's private key is also kept at the CA.
- When delivering certificates to users, the CA has to ensure that all certificates are assigned correctly.

3 PGP

PGP was implemented by Phil Zimmerman, a US programmer, and made available in the public domain, i.e. free for all Internet users. For commercial users, the program was licensed by PGP Corporation.

3.1 Encryption and Signature

PGP is a hybrid cryptographic method. When a user encrypts a message with PGP, the program performs the following steps:

1. PGP compresses the message (plaintext). Many plaintexts have a file pattern that cryptanalysis methods can use to analyze and identify the key. Compressing the text makes it much more difficult to analyze the key.
2. PGP creates a session key that is used only once. This session key, created on a random basis, serves as key for a powerful conventional encryption algorithm. Once this algorithm has been applied, the message is encrypted.
3. The session key is encrypted with the recipient's public key.
4. The encrypted session key and the encrypted message are sent to the recipient.

The recipient decrypts the session key with is private key and then the message with the decrypted session key.

PGP can also be used to sign messages. PGP uses a secure hash function[2] to generate the hash value from a message text. The hash value has a fixed length, regardless of the message. Together with the user's private key, this hash value is used to sign the message. PGP transmits both the message and the signature to the recipient.

If the recipient also uses PGP, he may verify the signature with the sender's public key.

3.2 PGP Certificate Types

PGP distinguishes between two types of certificates for keys:

- PGP certificates
- X.509 certificates (see Certificate X.509 v3)

The PGP certificate contains (not exclusively):

- the PGP version;
- the user's public key – together with his algorithm: RSA, Diffie-Hellman or DSS3;
- information on the certificate use – e.g. name, user ID, etc.;
- the certificate's digital signature;
- the certificate's validity period;
- the preferred symmetric encryption algorithm – supported algorithms include, among others, CAST, IDEA or Triple-DES[4].

PGP offers a number of functions. It creates one or more pairs of keys for the user. It integrates and manages new public keys from recipients and enables the use of encryption and authentication procedures for messages.

The length of the key can be 512, 768,1024 or 2048 bit, depending on the PGP version. The creation and assignment of the keys is performed as follows:

- To ensure originality and randomness, the user is prompted for a random input. This input is used to generate the public key and the private key. Both are given a timestamp (exact time of creation by time zones) and an identifier, which represents the 64 least significant bits.
- A user ID is assigned to the public key, which associates the key to a specific mail recipient. Typically, this will be the name, followed by the email address between angle brackets.

[2] **See whitepaper Cryptography – iQ.Suite Crypt Pro Basics**

[3] **See whitepaper Cryptography – iQ.Suite Crypt Pro Basics**

[4] **See whitepaper Cryptography – iQ.Suite Crypt Pro Basics**

- The keys are integrated into so-called key rings. A distinction is made between public key rings and private key rings. Within both rings, the keys are sorted by timestamp, key ID and user ID. The private key ring additionally contains the user's public key as well as the private key in an encrypted form. The private key is protected by a password or passphrase, which has to be entered each time the key is to be used. The public key ring contains the known keys of the partners and for each of these keys a trust indicator (Owner Trust), an originality indicator (Key Legitimacy) as well as two additional security fields (Signature, Signature Trust).
- As a rule, both local key ring files and public key servers can be used to store the public keys.

3.3 PGP Variants

This section provides a short description of a few programs/products based on PGP methods.

- OpenPGP
  - Specification for an open encryption standard, adopted as IETF standard in 1998
  - No implementation, specification only
  - Backwards compatible with older PGP versions
- GnuPG
  - Developed due to incompatibility between PGP 6.0 and previous versions
  - New implementation of the OpenPGP standard
  - Command line program (actual encryption program)
  - Supports communication with both older and new PGP versions
  - Under GPL license
  - Further development promoted by BMWi
  - Possible front-ends include, for instance, GnuPP for Windows with plug-ins, e.g. for MS-Outlook, Pegasus, Mozilla/Netscape
- Commercial versions
  - From PGP Inc.
  - Subject to license and fee

4 S/MIME

S/MIME is an extension of the email standard MIME. The MIME standard (Multimedia Internet Mail Extension) allows to attach binary information (pictures, sounds, programs).

S/MIME stands for Secure Multipurpose Internet Mail Extension. In its version 3, it has been validated as encryption standard by the Internet Engineering Task Force (IETF). The development was ensured by a manufacturer's consortium around RSA Security.

This encryption standard is supported, among others, in the email components of Netscape, Microsoft and Opensoft web browsers.

4.1 Encryption

S/MIME uses a hybrid encryption technology, i.e. a quick symmetric encryption of the actual message with a session key, followed by an asymmetric encryption of the session key with the recipient's public key.

For S/MIME in version 3, this means that the asymmetric part of the key exchange procedure is handled with Diffie-Hellman algorithms, while Triple DES is used for the symmetric part. RSA and MD5 are also supported[5].

Though using the same algorithms, there is no compatibility between S/MIME and PGP versions.

To create the keys, an appropriate software can be used on the client. The software creates a so-called certificate, which contains the public key, the private key as well as the certificate issuer's signature. The same software can be used to extract the individual keys from this certificate. If exported, the certificate can also be used for other programs, such as the email client Outlook or Thunderbird, the mail component in Mozilla.

4.2 Certificates

Two different ways are available in order to provide the public key to others for encryption and for verification of the signature:

1. Request the public key from the certifier / certificate owner
2. Automatically attach the public key to the signed data

The validity of a certificate is usually shown automatically. Revoked certificates can be queried at the certifier.

Unlike PGP, S/MIME exclusively uses a hierarchical certification structure with X.509 protocol, i.e. the pairs of keys needed for asymmetric encryption are electronically signed by a CA after having checked and confirmed the owner's identity.

[5] **See whitepaper Cryptography – iQ.Suite Crypt Pro Basics**

The identity check is possible at different levels:

- Checking the existence of the email address
- Checking the key owner’s identity with the help of the postal address
- Checking the key owner’s identity with the help of documents
- Checking the key owner’s identity with the help of a notary or other public person

In today’s email environments, S/MIME has a few weak points:

- As specified by the IETF, S/MIME-signed data is sent in two parts, i.e. the data separately from the signature. Both parts are interpreted as two parts of a "multi-part/signed" MIME-formatted email. The advantage is that MIME-capable email clients will recognize that a digital signature has been attached to the mail. But if the encryption protocol is not supported by the client, the latter may ignore the signature and only show the message.
- The drawback is that some gateways treat these multi-part message types as “non-transparent". The gateways check whether the next node supports MIME or 8bit and if not, they transform the data into an appropriate format, usually making the signature invalid in the process.

4.3 Differences between S/MIME and PGP

- Creating certificates
  - □ PGP uses the so-called Web of Trust, a "network of mutual trust". The validity of a person's public key is accepted even when the corresponding key has not been verified. In the Web of Trust, the users mutually sign their keys after having verified and confirmed their authenticity. Each user thus fully controls whom he trusts and to what extent. The user may choose between several levels of trust. To make sure that the Web of Trust cannot be circumvented, it is crucial to have an authority that all users trust. Whenever requested to do so, this authority is able to confirm that a key really belongs to the person it claims to belong to. Such an authority could be a Trust Center or Certification Authority.
  - □ S/MIME has a strict hierarchy of X.509 certificates (see Public-Key Infrastructures). **Note:** Under Windows XP, the trustworthiness of a CA is a question taken care of by Microsoft. Certificates are automatically considered trustworthy if the issuing CA is deemed trustworthy by Microsoft.
- Revoking certificates
  - □ PGP is able to create a key revocation certificate, which allows to inform other users that the corresponding public key is no longer valid. This does not mean the key can no longer be used. Signed documents can still be verified with the key. PGP stores revoked keys on the same key server. The revocation is attached to the key as separate signature.
  - □ S/MIME uses the CRL (see Public-Key Infrastructures). To be informed, users have to periodically download the lists from dedicated CRL servers.

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.