Ciphire Mail
Technical Introduction

Abstract

Ciphire Mail is cryptographic software providing email encryption and digital signatures. The Ciphire Mail client resides on the user's computer between the email client and the email server, intercepting, encrypting, decrypting, signing, and authenticating email communication. During normal operation, all operations are performed in the background, making it very easy to use even for non-technical users.

Ciphire Mail provides automated secure public-key exchange using an automated fingerprinting system. It uses cryptographic hash values to identify and validate certificates, thus enabling clients to detect malicious modification of certificates. This data is automatically circulated among clients, making it impossible to execute fraud without alerting users.

The Ciphire system is a novel concept for making public-key cryptography usable for email communication. It is the first transparent email encryption system that allows everyone to secure their communications without a steep learning curve.

Overview

Ciphire Mail is cryptographic software providing email encryption and digital signatures. The Ciphire Mail client resides on the user's computer between the email client (mail user agent, MUA) and the email server (mail transfer agent, MTA), intercepting, encrypting, decrypting, signing, and authenticating email communication. During normal operation, all operations are performed in the background. This makes Ciphire Mail very similar to a transparent proxy. Apart from per-user installations, Ciphire Mail may also be deployed on mail servers as a gateway solution. A combination of per-user and per-server installations is possible, as well.

Public-key exchange and key agreement are automated and handled via certificates available through a central certificate directory. These services are operated by Ciphire Labs and do not require any local server installations, additional hardware, or additional software.

Ciphire Mail uses only well-known standard cryptographic algorithms including RSA, AES, Twofish, or SHA for its cryptographic operations. It uses 2048-bit keys for asymmetric algorithms and 256-bit keys for symmetric algorithms.

Installation and Integration

Ciphire Mail Client

The Ciphire Mail client consists of three parts: the core client, a graphical configuration interface, and mail connector modules (redirector). Supported email protocols include SMTP, POP3, and IMAP4. The STARTTLS and direct SSL/TLS variants of these protocols are supported as well.

For the proprietary email systems Microsoft Exchange and Lotus Notes separate connector modules are available that directly integrate with the Outlook and Notes client as a plug-in and automatically handle communication between Ciphire Mail and the email application.

Ciphire Mail Gateway

The Ciphire Mail client can be run in "server mode" providing a gateway solution. When used in this mode, Ciphire Mail allows creation of single keys as well as creation of server certificates. By default, lookups are performed to find the certificate corresponding to the exact email address of the recipient. If no certificate is found for this email address, the lookup will automatically fall back to the domain name level.

Ciphire Certificates

Ciphire certificates use ASN.1 format. This makes them similar to X.509 certificates, with the following exceptions and improvements:

- User controls certificate creation, renewal, and revocation
- Certificate can contain multiple keys (default: RSA, DSA, and ElGamal)
- Certificate links keys to an email address or a fully-qualified domain name (no other

information about the user's identity is included)

- Certificate contains multiple issuer signatures (Ciphire CA)
- Certificate contains multiple self-signatures from the private key owner.
- Certificate chaining (security property for renewed certificates)
- Automatic certificate verification via fingerprint lists (see below)
- The client always creates the public-private key pairs; the user's private key never leaves his computer.

Certification

Certification is an automated process invoked by a Ciphire Mail client when the user creates a certificate for a specific email address (or fully-qualified domain name). To verify the existence of the given address and to verify that the owner of the address owns the private keys corresponding to the public key, the Ciphire CA uses a mail-based challenge/response mechanism.

Certificates are revoked by issuing a matching revocation certificate. The revocation has to be authorized by the certificate owner. Renewal of a certificate involves the revocation of the old and creation of a new certificate. A certificate can be renewed at any time.

If all criteria for a particular certification request have been met, the Ciphire CA issues the certificate (or revocation certificate) and publishes it in the Ciphire Certificate Directory (CCD). The CA ensures that only one active certificate can be available for a specific address at any time.

Ciphire Certificate Directory

The CCD contains all certificates issued by the Ciphire CA, including active and revoked certificates. CCD servers are part of a central infrastructure operated by Ciphire Labs. The infrastructure provides redundant services and is distributed over multiple data centers in different locations.

Every client can download certificates from the CCD by looking them up by their email address or their unique serial ID. Lookups by email address always retrieve the current active certificate, provided one is available for the given address. The CCD uses multiple caching proxy servers as a front-end service that is being accessed by Ciphire Mail clients. If a larger number of local clients are to be served, a local Ciphire proxy can be installed to minimize bandwidth consumption and to increase lookup performance.

All certificate lookups are fully automated and performed by the Ciphire Mail client whenever a certificate and its associated public keys are required to process a certain email message.

Trusted Certification and Directory Services

In many public-key cryptography solutions the user is required to blindly trust a third-party, like a classical certification authority (CA), that the issued certificate is still valid and has not been tampered with. Other systems, like PGP-based systems, require the user to perform manual verifications of an owner's identity and integrity of a public key to find out if it is valid or not.

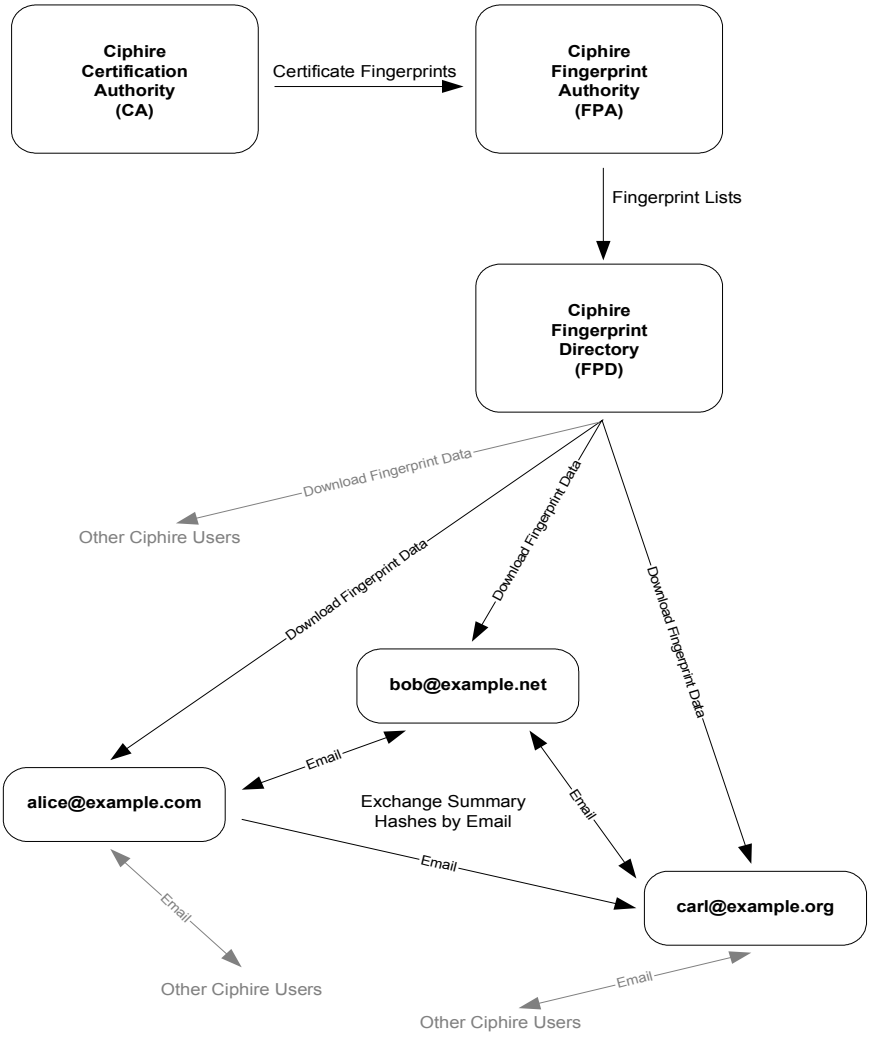
In the Ciphire system a user is not required to perform manual verifications and most importantly he is not required to blindly trust the Ciphire CA.

To achieve this, the Ciphire system uses, in addition to the usual CA certification, an automated fingerprinting system that provides the following:

- Verification, if a certificate for a particular user (email address) has been issued by the CA (non-repudiation of certificate issuance)
- Verification, that a certificate has not been modified after it has been issued by the CA (proof of certificate integrity)

This is achieved by the Ciphire Fingerprint System using hash-chaining techniques to create a trusted log of all certification actions the Ciphire CA has performed. In makes sure, that old entries in the log cannot be changed at a later time without invalidating newer entries.

These fingerprint data is made available to all Ciphire Mail clients and used by the clients to automatically authenticate certificates. To ensure that every client has the same fingerprint data as any other client, the most current log entry (summary hash) is exchanged with other clients. When the user sends a secure email message to another Ciphire user, the client automatically includes the summary hash in the email message. The receiving client extracts the hash and compares it with the corresponding hash in its local copy of the fingerprint data. If the hash values do not match, either the sending client or the receiving client has wrong fingerprint data.The Ciphire Mail client handles all this processing automatically.



Drawing 1: Flow of fingerprint data in the Ciphire System.

Secure Email Communication

When an email message is submitted by an MUA the redirector (mail connector module) intercepts the communication and looks up certificates for all recipient email addresses. If no certificate exists for a recipient, the client either sends the email unencrypted, rejects the email, or asks the user what to do, depending on the user's configuration.

If a certificate is available, the client automatically validates it by verifying the certificates in-built security properties (e.g., self-signature and issuer signature) and by verifying the certificate with the fingerprint system described above. When the certificate is validated, the email is encrypted and sent.

Similar steps are followed when performing decryption, creation and verification of digital signatures.

Requirements

Supported operating systems:

- Windows: XP and 2000
- Mac OS X: 10.3
- Linux: Kernel 2.4.0 or higher

Supported email applications:

- Email applications using standard SMTP for sending and POP3 or IMAP4 for receiving email (including SSL/TLS variants and STARTTLS support)
- Outlook with Microsoft Exchange (supported in future versions)
- Lotus Notes (supported in future versions)

Cryptographic Specifications

Algorithms used in Ciphire-specific cryptographic functions:

- Asymmetric algorithms: RSA, ElGamal, and DSA-2k (DSA-2k is a variation of the standard DSA/DSS algorithm supporting 2048-bit keys)
- Key agreement algorithms: (not required)
- Symmetric algorithms: AES, Twofish, and Serpent
- Operation modes and authentication algorithms: CBC-HMAC, CCM, and CTR
- Hash algorithms: SHA_d-256 and $Whirlpool_d$-512
- Pseudo-random number generation algorithms: Fortuna using Twofish in CTR mode
- Supported signing modes: SHA_d-256 with DSA-2k and $Whirlpool_d$-512 with RSA