Understanding S/MIME Email Encryption (Part I)

There are many email encryption solutions on the market. ZoTrus adopts a technical route based on the S/MIME standard. This article explains how S/MIME technology implements email encryption and digital signatures to help users understand the charm of S/MIME and correctly choose email encryption solutions. And this article explains how ZoTrus solves the difficulties in the implementation of S/MIME technology, so that users can SMILE when they see S/MIME.

1. History of S/MIME

To explain what S/MIME is, we must first explain what MIME is, just like to explain what HTTPS is, we must first explain what HTTP is. The **S** in these two most used Internet protocols stands is the first letter of Secure, HTTP is the plaintext Hypertext Transfer Protocol, and HTTPS is the Hypertext Transfer Protocol Secure.

MIME is the abbreviation of Multipurpose Internet Mail Extensions, an Internet standard that extends the email format, allowing emails that only support English ASCII characters to send text in character sets other than ASCII, and to send various formats of files such as audio, video, images, and applications as attachments. Emails with MIME format are transmitted using standard protocols such as Simple Mail Transfer Protocol (SMTP), Post Office Protocol (POP), and Internet Mail Access Protocol (IMAP). Although the MIME format is mainly designed for SMTP, its content type is also used in other communication protocols, such as the HTTP protocol. The web server inserts a MIME header field at the beginning of any web transmission, and the client uses the content type or media type header to select the appropriate application for the indicated data type.

S/MIME is the abbreviation of Secure/Multipurpose Internet Mail Extensions, which is to send and receive emails securely, and use cryptographic technology to implement digital signature and encryption of email. The first version of S/MIME was developed by many security vendors in 1995, but no standard was formed. In 1998, S/MIME V2 was released and submitted to IETF to form RFC

2311 and RFC 2312 standards, the former established the standard for messages, and the latter established the standard for certificate handling. These two RFC standards jointly provide a framework based on Internet standards, and all relevant parties can follow this framework to provide interoperable message security solutions, making S/MIME V2 the email security standard. In 1999, IETF proposed S/MIME V3 - RFC 2632 (Certificate Handing), RFC 2633 (Message Specification) and RFC 2634 (Enhanced Security Services), which enhanced the S/MIME function based on V2. In 2004, S/MIME V3.1 was released - RFC 3851 (Message Specification), which is an upgraded version of RFC 2633. In 2010, S/MIME 3.2 was released - RFC 5751 (Message Specification), which is an upgraded version of RFC 3851. In 2019, S/MIME V4.0 was released - RFC 8551 (Message Specification), which is an upgraded version of RFC 5751. This is the latest version. These standards are based on the Cryptographic Message Syntax (CMS, RFC 5652), which is roughly the same as PKCS #7. One of the enhanced features of S/MIME V3 is " triple-wrapping". Triple-wrapped S/MIME emails are signed, encrypted, and signed again, which can ensure the integrity of the encrypted email body data. The S/MIME V4 version mainly adds support for the ECC algorithm.

2. S/MIME Digital Signature

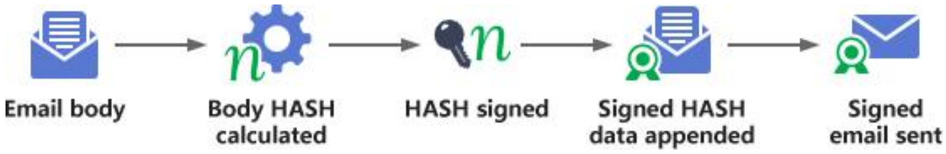
The first feature of S/MIME is digital signature. As the name implies, digital signatures are the digital counterpart of traditional handwritten signatures on paper documents. Like handwritten signatures, email S/MIME digital signatures provide the following security capabilities:

- **Authentication**: Digital signatures are used **to** validate an identity, answer the question "who are you?" and prove the uniqueness of an entity. Since there is no authentication in plaintext SMTP emails, it is impossible to know who really sent the email. Authentication in digital signatures solves this problem, and it assures the recipient that the email was indeed sent by the claimed sender.

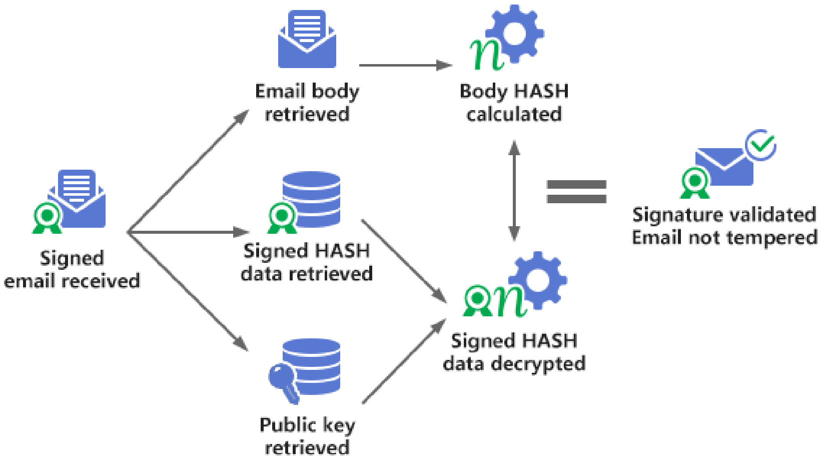
- **Nonrepudiation**: The uniqueness of a digital signature prevents the signer from denying the signature. This feature is called nonrepudiation, and the authentication provided by digital signatures provides a means of enforcing nonrepudiation, which is increasingly recognized as legally binding in some areas, similar to the nonrepudiation of handwritten signatures on paper, solving the problem that plain text SMTP email sending cannot provide nonrepudiation.

- **Data integrity**: Another security guarantee provided by digital signatures is data integrity. With data integrity, when the recipient of a digitally signed email verifies the digital signature, the recipient can be confident that the received email has not been tampered with during transmission. Because after the digital signature, any tampering with the message during transmission will invalidate the digital signature. In this way, digital signatures provide guarantees that paper handwritten signatures cannot provide, because paper handwritten signatures may be tampered with undetected after signing.

The figure below shows the flow chart of sending S/MIME digitally signed emails. The email client software uses the SHA-2 algorithm to calculate the HASH value of the email body, then signs the HASH value with the sender's private key and then appends this HASH value to the email body as a digital signature. After adding the email header, the digitally signed email can be sent.



The following figure shows the verification flow chart of S/MIME digital signature. After the recipient receives the signed email, he/she obtains the email body, signed HASH data and sender's signature certificate (public key) respectively, and uses the sender's public key to decrypt the signed HASH data to obtain the email body HASH value, and then calculates the HASH value of the email body, and compares whether the two HASH values are the same. If they are the same, the signature is valid, indicating that the email has not been tampered with, and the email client will display the signer's identity information.


Email body retrieved
Body HASH calculated
Signed email received
Signed HASH data retrieved
Signature validated Email not tempered
Signed HASH data decrypted
Public key retrieved

This is the signing and verification process of the S/MIME digital signature. Users need an S/MIME email certificate to complete the digital signature of email, and the email client must also support the S/MIME standard to verify the digital signature.

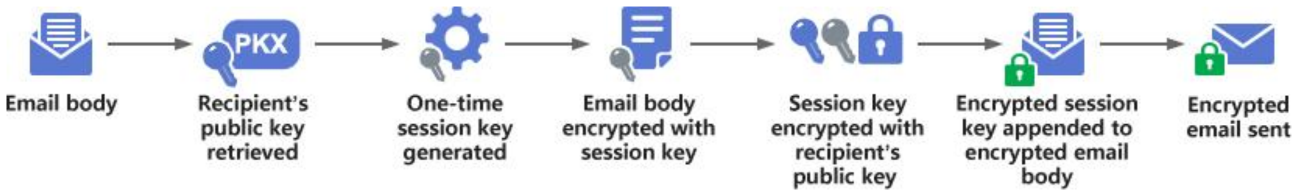
Although S/MIME digital signatures provide data integrity, they do not guarantee confidentiality. Digitally signed only emails are sent in plain text and can be read by others. Even Base64-encoded opaque signatures can only provide a certain degree of obfuscation, but it is still plain text. In order to ensure the confidentiality of email content, S/MIME encryption must be used.

3. S/MIME Encryption

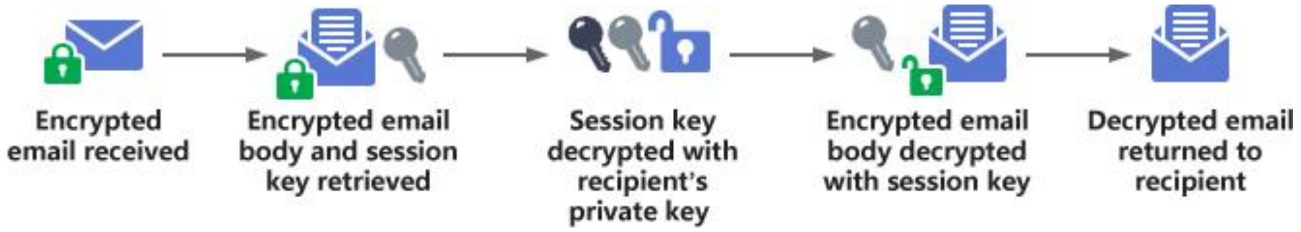
S/MIME encryption is designed to solve the security problem of SMTP plain text transmission of emails. Anyone may illegally obtain the email content and illegally tamper with the email content during the email transmission process and can also view the plain text email on the email server, especially now that all emails are in the cloud. These problems are solved by S/MIME encryption technology. Encryption is a way of transforming information so that the information cannot be read or understood before it is restored to a readable and understandable form. Email S/MIME encryption provides the following security capabilities:

- **Confidentiality**: Email S/MIME encryption is used to protect email content. Only the intended recipient can view the content, and the content remains confidential and cannot be decrypted by anyone else who may receive or view the message. S/MIME encryption provides confidentiality during message transmission and storage.
- **Data integrity**: Like digital signatures, email encryption also provides data integrity guarantees, which ensures its integrity because it cannot be decrypted.

The following figure shows the flow chart of S/MIME encrypted email. The email client software must first obtain the recipient's public key, then generate a one-time symmetric session key, and use the session key to encrypt the email body. It then encrypts the session key with the recipient's public key and includes the encrypted session key in the encrypted email body. Together with the email header and other information, the encrypted email can be sent.


Email body
PKX
Recipient's public key retrieved
One-time session key generated
Email body encrypted with session key
Session key encrypted with recipient's public key
Encrypted session key appended to encrypted email body
Encrypted email sent

The following figure shows the flow chart of S/MIME decryption email. After the recipient receives the encrypted email, he/she obtains the encrypted email body and the encrypted session key respectively, decrypts the encrypted session key with the recipient's private key, and then uses the decrypted session key to decrypt the encrypted email body. In this way, the recipient can view the decrypted email content.


Encrypted email received
Encrypted email body and session key retrieved
Session key decrypted with recipient's private key
Encrypted email body decrypted with session key
Decrypted email returned to recipient

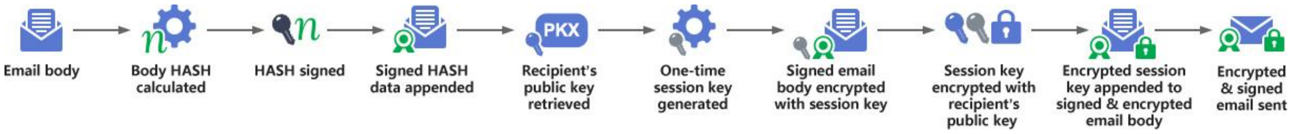
This is the encryption and decryption process of S/MIME. The sender must obtain the public key of the recipient through certain channels. Usually, the sender and the receiver send a digitally signed email to complete the public key exchange. The recipient must have the private key of the S/MIME certificate to complete the decryption of the email.

Although S/MIME encryption provides confidentiality guarantees, it does not verify the identity of the sender in any way. An encrypted email without a digital signature is just as easy to impersonate as a plaintext email without encryption, and email encryption does not provide nonrepudiation. Although email encryption also provides data integrity, encrypted emails can only show that the message has not been tampered with since it was sent, and do not provide identity information about who sent the email. In order to prove the trusted identity of the email sender, an S/MIME digital signature must be used at the same time.

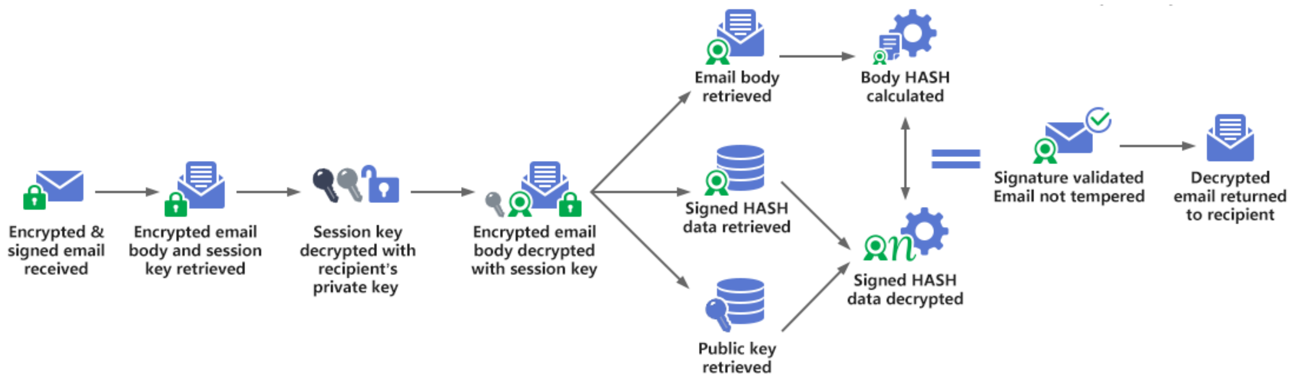
4. S/MIME digital signature and encryption

It is precisely because S/MIME digital signatures only solve the problems of the integrity of email content and the trusted identity of email sender, and S/MIME encryption only solves the confidentiality of email content. Therefore, in order to truly ensure email security, S/MIME digital signatures and encryption must be implemented at the same time. Only in this way can the four painful email security problems of confidentiality, integrity, nonrepudiation and authentication of emails be solved at the same time (**PAIN**, Privacy/Authentication/ Integrity /Nonrepudiation).

The following figure shows a flowchart for sending S/MIME digitally signed and encrypted email. The email client software calculates the HASH value of the email body, signs the HASH value with the sender's private key, and then attaches the HASH value to the email body as a digital signature. This completes the digital signature. Then, the recipient's public key is obtained to generate a one-time symmetric session key, and the signed email body is encrypted using the session key. The session key is then encrypted with the recipient's public key, and the encrypted session key is included in the signed and encrypted email body. Together with the email header and other information, the digitally signed and encrypted email can be sent.


Email body
Body HASH calculated
HASH signed
Signed HASH data appended
PKX
Recipient's public key retrieved
One-time session key generated
Signed email body encrypted with session key
Session key encrypted with recipient's public key
Encrypted session key appended to signed & encrypted email body
Encrypted & signed email sent

The following figure shows the flow chart of verifying S/MIME signed email and decrypting encrypted email. After the recipient receives the encrypted and digitally signed email, he/she obtains the encrypted email body and session key respectively and uses the recipient's private key to decrypt the encrypted session key and then uses the decrypted session key to decrypt the encrypted and signed email body, thus completing the decryption process. Then, the email body, the signed HASH data, and the sender's public key are obtained respectively, and the sender's public key is used to decrypt the HASH signature data to obtain the email body HASH value, and then the email body HASH value is calculated. The two HASH values are compared to see if they are the same. If they are the same, the signature is valid, indicating that the email has not been tampered with. In this way, the recipient can view the decrypted email content, and the email client will display the signer’s identity information.


Encrypted & signed email received
Encrypted email body and session key retrieved
Session key decrypted with recipient's private key
Encrypted email body decrypted with session key
Email body retrieved
Body HASH calculated
Signed HASH data retrieved
Public key retrieved
Signed HASH data decrypted
Signature validated Email not tempered
Decrypted email returned to recipient

There is no need to explain the implementation process of triple-wrapped S/MIME email encryption and digital signature here. Consistent with the basic principles above, it adds additional digital signature and verify it again to enhance the protection of the integrity of the encrypted email body data.

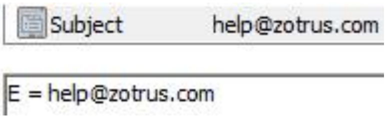
5. S/MIME certificate and S/MIME client

S/MIME email digital signature and encryption are inseparable from digital certificate, namely S/MIME certificate, or simply email certificate. Email certificate, like TLS/SSL certificate, must be issued by a third-party CA after completing mailbox control validation and certificate applicant identity validation. It must also have a certificate issuance management standard like TLS/SSL certificate, and it must also have a trust mechanism for email clients like TLS/SSL certificate for browsers. Only in this way can there be a complete PKI application ecosystem, and can the full life cycle security of emails be truly realized through cryptography protection.

(1) S/MIME Certificate

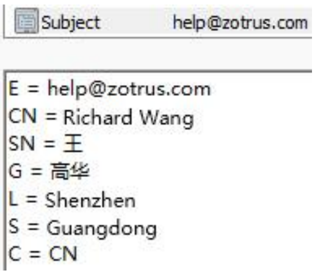
S/MIME certificate is standard X.509 V3 digital certificate, just like TLS/SSL certificate. Unlike TLS/SSL certificate that is bound to domain name, email certificate is bound to email address. Therefore, just as issuing SSL certificate requires verifying the control of the domain name, issuing email certificate requires verifying the email address. The verification method used is to send an email with a verification code to the email address for which the email certificate is applied. This verification process is the same as the admin email verification for SSL certificate. Only after verifying the user's control over the email address can the CA system issue an email certificate.

Like SSL certificates, email certificates are divided into four categories according to the strictness of identity validation: MV certificate, IV certificate, OV certificate, and SV certificate. The identity validation rules are similar to the four categories of SSL certificates: DV certificate, IV certificate, OV certificate, and EV certificate. However, the SV certificate is slightly different from EV certificate. This type of certificate is equivalent to an IV+OV certificate, which means that it validates both individual identity (IV) and organization identity (OV). The MV email certificate only validates the mailbox control, not the user's identity. The subject information of these four types of email certificates is shown in the figure below, which are MV/IV/OV/SV email certificates.



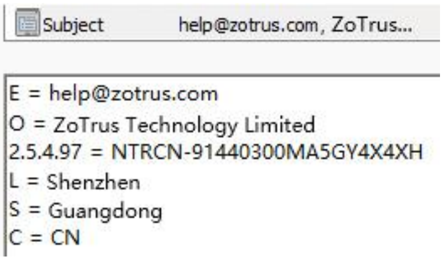
Subject help@zotrus.com

E = help@zotrus.com



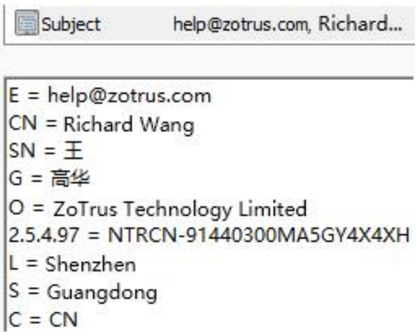
Subject help@zotrus.com

E = help@zotrus.com
CN = Richard Wang
SN = 王
G = 高华
L = Shenzhen
S = Guangdong
C = CN



Subject help@zotrus.com, ZoTrus...

E = help@zotrus.com
O = ZoTrus Technology Limited
2.5.4.97 = NTRCN-91440300MA5GY4X4XH
L = Shenzhen
S = Guangdong
C = CN



Subject help@zotrus.com, Richard...

E = help@zotrus.com
CN = Richard Wang
SN = 王
G = 高华
O = ZoTrus Technology Limited
2.5.4.97 = NTRCN-91440300MA5GY4X4XH
L = Shenzhen
S = Guangdong
C = CN

Like SSL certificates, email certificates also have international standards for certificate issuance and management - "Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates" developed by the CA/Browser Forum, which is used to regulate the issuance of S/MIME certificates by globally trusted CAs. It also regulates how S/MIME clients verify email certificates. With this standard, S/MIME technology has a complete industry standard, including S/MIME protocol standards and S/MIME certificate standards. This is a open ecosystem that has not been achieved by any other email encryption technology, allowing CAs and email client developers to achieve compatible and mutual recognition of email encryption and decryption based on industry standards.

(2) S/MIME Client

To achieve email encryption, of course, it is inseparable from the support of the email client. Now that the S/MIME standard has been established, all email clients only need to support email encryption and decryption in accordance with the S/MIME standard, implement email digital signatures and verify signatures. These clients are collectively referred to as S/MIME Clients. Currently, email clients that support the S/MIME standard include Microsoft Outlook, Mozilla Thunderbird, Apple Mail, Huawei Mail, etc. The best one is Outlook. Once the S/MIME certificate is installed in the Windows Certificate Store, Outlook can automatically configure and use it to automatically decrypt the encrypted emails. The best S/MIME client APP is Apple Mail, which requires manual installation and configuration of S/MIME certificate, but the configuration process is relatively complicated.

It is precisely because users need to apply for an S/MIME certificate from the CA before configuring it in the email client, although these two different industries both follow the S/MIME standard, they operate independently and do not cooperate well to achieve seamless integration, resulting in a very excellent email encryption technology that cannot be popularized and applied.

6. The S/MIME standard is the only universal standard for email encryption

The first four parts clearly explain the working principle of the S/MIME standard. Email digital signature and encryption complement each other and provide a comprehensive solution to the security issues of SMTP email. The fifth part briefly explains S/MIME certificates and S/MIME clients, which are important components of the S/MIME technology ecosystem. Digital certificates, email digital signatures and encryption are the core functions of S/MIME. The PKI public key mechanism makes S/MIME digital signatures and email encryption feasible, and digital certificates make it possible to use digital signatures and encryption through public and private key pairs.

The S/MIME standard implements true end-to-end encryption. The email is encrypted when it is generated in the email client, sent from the user end to the mail server in ciphertext, stored in the mail server in ciphertext, and sent to the recipient in ciphertext. The TLS email encryption on the market can actually only ensure that the transmission process of the email from the user end to the mail server is achieved through the encryption of the email transmission channel in a manner similar to HTTPS encryption, but it does not encrypt the email itself. Strictly speaking, it does not belong to email encryption technology. However, after IMAP and SMTP support TLS encryption, they can effectively ensure the security of email accounts and ensure that the username and password are transmitted to the mail server through an encrypted channel to complete the login verification. This is also very important for email security. Therefore, almost all email service providers have provided TLS encryption for IMAP and SMTP by default.

Except for the S/MIME email encryption solution based on international standards, other email encryption solutions are implemented using private protocols. They lack wide versatility and compatibility with multiple developers. And due to their closed nature, it is impossible to know whether they are truly secure (even if they are open source). Once used, users are locked to one service provider. The author does not think these solutions are good solutions. Therefore, ZoTrus Technology insists on following the S/MIME standard technology route.

To be continued ......

Richard Wang

Feb. 17, 2025
In Shenzhen, China

Follow ZT Browser at X (Twitter) for more info.
The author has published 85 articles in English (more than 111K words) and 202 articles in Chinese (more than 591K characters in total).