The First Hurdle for Email Encryption is Certificate Application

（April 12, 2021）

There are three hurdles in email encryption. The first hurdle is to apply for an email certificate. This is easy to understand. Without an email certificate, email encryption cannot be achieved. This is the foundation and basic condition. The second hurdle is the public key exchange. How to pass this hurdle has been clearly explained in the blog post "The second hurdle of email encryption is the exchange of public keys", which is to realize automatic public key exchange through the cloud public key database. The third hurdle is key management. This has been made clear in the blog post "The third hurdle of email encryption is key management", which is to solve the problem through cloud key management service.

Today, let's talk about the first hurdle for email encryption. In 1995, RSA and other companies proposed the V1 version of the S/MIME protocol (Secure/Multipurpose Internet Mail Extensions), which is a solution to the email security problem with digital signature and encryption technology. In 1998 and 1999, V2/V3 version were successively introduced and submit IETF to form a series of RFC standards. Since then, email certificate has been used for email encryption and digital signature. Users must apply for email certificates from CA and configure it for use in email clients. This process has gone through 21 years, basically without any innovation, the only change in recent years is, with the withdrawal of IE browser from the market, the key pair and certificate signing request generated by the user on the computer have been changed to directly give the user a .pfx (.p12) format certificate by the CA, because of other browsers does not support the operation process of generating a key pair on user's computer.

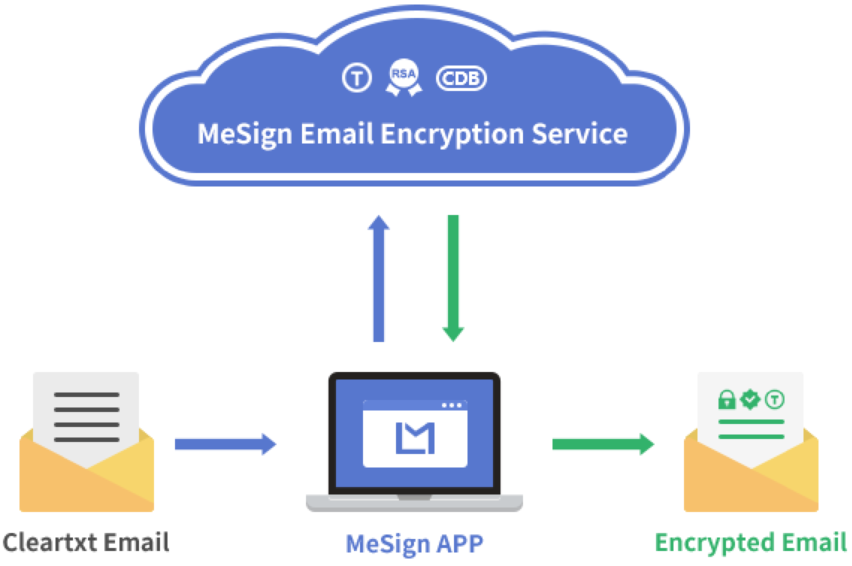
Let's go back to the origin of email encryption requirements and reflect on the cumbersome email certificate application process. What we need is to protect confidential email information through email encryption, not email certificate. Email certificate is only a tool for email encryption, not the product that users ultimately need, this statement may sound unacceptable to friends in the CA industry, but think about why S/MIME email encryption technology is still not popularized in 21 years later, and everyone knows that cleartext emails are not secure, but why not use S/MIME email encryption technology to protect email security?

The first hurdle-"applying for a certificate" blocks users out of the door! Not to mention the many hurdles after getting the email certificate. To send encrypted emails, you must exchange the public key with the recipient in advance. After the certificate expires, you need to apply for a new certificate again. You also need to keep the expired email certificate for decrypting previously encrypted emails and so on. All these tedious processes of email encryption start from applying for email certificates, it can be said to be a never-ending nightmare. Life is not easy, who would like to hurt himself for email encryption! This is the fundamental reason why the S/MIME email encryption standard has been born for 21 years, but it has not been widely used.

However, mankind must progress, and email must be encrypted. What should we do? MeSign Technology has completely solved the two problems of public key exchange and private key management, and we also have completely solved the problem of applying for an email certificate. Since the user needs email encryption, not the email certificate, so we put the email certificate application process in the background, which is automatically completed by our email client software - MeSign App. The user only needs to set up the email account, log in to his mailbox, then the email certificate will be configured automatically, then user can send encrypted email immediately. In other words, our email encryption solution does not require users to apply for email certificates, which means that they have passed the first hurdle of email encryption without feeling.

So, how does MeSign Technology realize automatic configuration of email certificates for MeSign App users? Of course, the cloud CA service is required first, which is one of the important components of the MeSign cloud cryptographic infrastructure, the second is the cloud key management service, and the third is the cloud public key database. Then, we must have email client software to connect to the cloud cryptography service to get the email certificates for users automatically. This is why MeSign Technology must develop an email client software, because currently there is no email client software on the market that can automatically apply for email certificates for users.

Users only need to download and install MeSign App, set up their own email account, MeSign App will automatically connect to the cloud CA system and cloud key management system to obtain the encrypting certificate and signing certificate bound to the user's email address, and automatically configure it for email encryption and decryption, and post the user's public key to the cloud public key database, so that other MeSign App users can automatically obtain their public keys and send encrypted email to the user automatically. For users using MeSign App as the email client software does not need to apply for an email certificate from CA at all! All are done automatically by MeSign App together with MeSign cloud cryptographic infrastructure, the first hurdle of email encryption has passed so easily!



Now it may conclude this article. But I still like to share some technical details with readers. At present, the email certificates issued to users by CAs in the world are all single certificate (including both encryption and digital signature usages). The advantage of this solution is that users only need to manage one certificate. However, if the cloud cryptography service is used to solve the problem of email encryption, the single certificate will be a problem, because encryption only requires the encryption usage, not the signature usage. According to the principle of minimization, only the encrypting key needs to be hosted in the cloud key management system.

(C) 2021 MeSign Technology Limited

Therefore, MeSign Technology splits the traditional single email certificate into two certificates (one signing certificate and one encrypting certificate). The encrypting key is generated in the cloud and securely stored in the cloud. After passing the email control validation, the encrypting key and certificate can be automatically obtained from the cloud by MeSign App for decrypting the encrypted email automatically, so that users do not need to spend time and effort to apply for email certificate and import email certificate into email clients to realize automatic email encryption and decryption. Since the signing certificate contains the user's identity information, the user's signing behavior has legal effect. Therefore, MeSign Technology designs the signing key is generated on user’s local device, and securely stored on the local device. This is why MeSign App users see that the serial number of signing certificate on different devices is different.

MeSign Technology splits the traditional email certificate into two certificates and adopts different key management methods according to the two different usages of signature and encryption, which perfectly solves the ease of use of the S/MIME email encryption service. At the same time, it inherits the non-counterfeiting, non-forgery and non-repudiation characteristics of S/MIME email signature, making S/MIME technology truly achieve zero threshold for use. Users don’t need to care about how the certificate come and where the certificate is, just write email as usual, and click “Send” to send encrypted email automatically and decrypt the encrypted email automatically.

Finally, let me share a little bit more with you. The topic of this blog post is to apply for an email certificate. MeSign App not only supports the automatic application and configuration of email certificate issued by MeSign Cloud CA that the email certificates are completely free, but also supports automatic application and configuration of email certificates issued by other CAs. The Starter Edition service automatically configures the email certificates issued by the world-renowned CA - Sectigo, which we call Vp Email Certificate, this is a charged service. Why do we need to configure this certificate automatically? Because this certificate is a publicly trusted email certificate, the signed email with this certificate is trusted by commonly used email client software, such as Outlook, Thunderbird, and Apple Mail. That is to say, the free configured email certificate is only trusted by MeSign, but the charged Vp Email

Certificate is publicly trusted by all email clients. MeSign App not only supports the automation of email certificate issued by MeSign CA, but also supports the automation of email certificate issued by other CAs. MeSign Technology adopts the same S/MIME technology supported by other email clients to realize the mutual encryption and decryption of email encryption and digital signature.

Well, to summarize, there are three hurdles in email encryption. MeSign Technology has built a cloud cryptography infrastructure and developed an email client software - MeSign App. The “cloud” and the “client” work together closely, and innovatively and perfectly help users smoothly and easily passing the three hurdles, users can use MeSign App to send encrypted emails and decrypt encrypted emails as easily as cleartext emails. Only in this way can email encryption be widely used, and email can securely benefit human life and work.

--- END ---

Richard Wang

Digitally signed by Richard Wang
ceo@mesign.com

Want to contact me to discuss this topic? Please use MeSign App (👤 - ⛶) to scan the QR code and send me an encrypted email, I will reply to your encrypted email ASAP.