The Second Hurdle for Email Encryption is the Exchange of Public Keys

(April 06, 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. How to pass this hurdle will be discussed in detail in the next blog post.

The second hurdle is the exchange of public keys. If both the sender and receiver have passed the first hurdle and they have the email certificates, they must send a digitally signed email to each other to realize the public key exchange. Only the public key is exchanged, then the sender can use the receiver's public key to send encrypted email to the receiver. This article will talk about how to pass this hurdle. As for the third hurdle, it is the private key management, and this hurdle will be discussed in detail in a later blog post.

Regarding the three hurdles of email encryption, why does the author talk about the second hurdle first? Because public key exchange is the most critical and cumbersome step in S/MIME email encryption, if without this step, even if everyone has an email certificate, email encryption cannot be achieved. It is precisely because of this cumbersome key exchange mechanism that email encryption cannot be widely used. The problem of public key exchange must be thoroughly solved to realize automatic email encryption and to popularize email encryption applications.

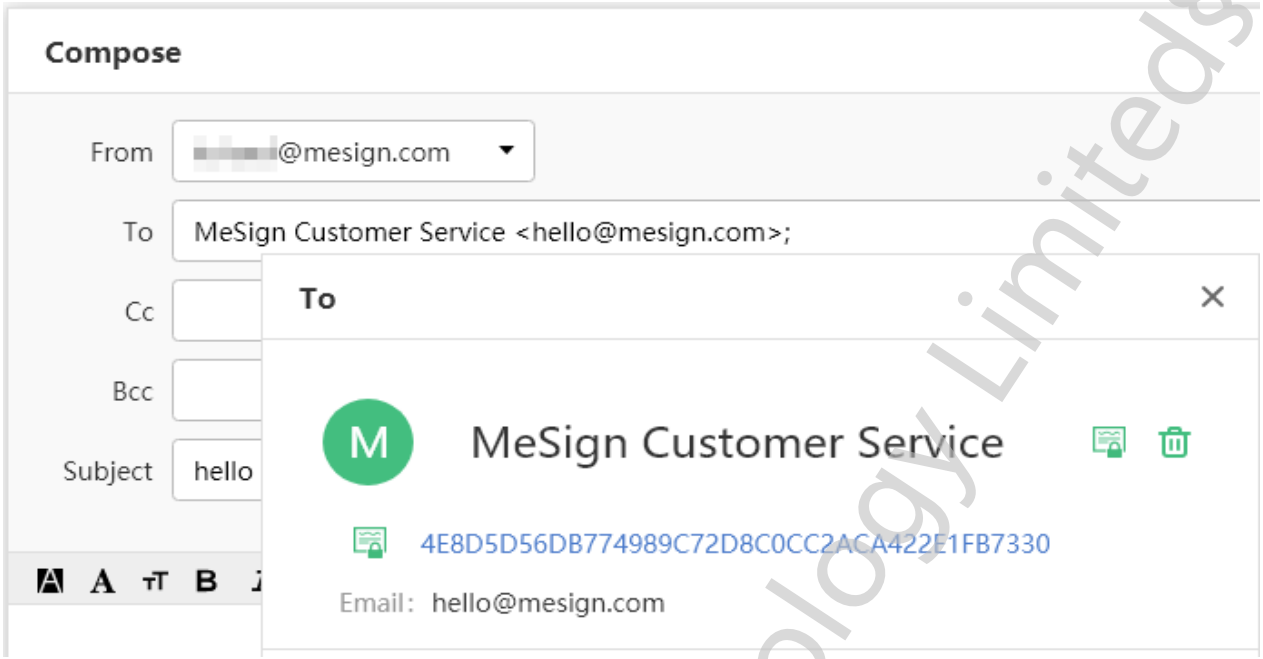
So, how to past the second hurdle of email encryption? Let's tell a true story first. The author once recommended the MeSign App to an attendee sitting next to me at an international conference (let’s call him Jason). I asked him to use MeSign App to send encrypted emails to the gentleman who was giving a speech (let’s call him Andy), because his email address was published on the speaker's PPT presentation. Jason said that I haven't exchanged public keys

with the speaker Andy, how can I send encrypted emails to him? I told Jason that using MeSign App to send encrypted emails does not need to exchange public keys in advance. He suspiciously used MeSign App to send an encrypted email to the speaker and prompted that the sending was successful. After returning to the audience seat, the speaker also replied to the encrypted email, which was sent using Outlook. This made Jason very curious and asked me how the MeSign App did it. I told him about our solution. He is now a fan of MeSign App. This article will share with you how we did it.

MeSign Technology's solution is to innovatively build a global public key database. MeSign App, as an email client software, automatically collects the public key used by the user to communicate with other recipients, and automatically synchronizes it to the cloud global public key database, so that the user does not need to exchange the public key with the recipient in advance while writing email to anyone, MeSign App can automatically obtain the recipient's public key from the cloud public key database. Only in this way can the user does not need to exchange the public key with the recipient in advance, the "cloud" and "client" work together to realize automatic email encryption.

Going back to the above story, because I have sent encrypted emails to the speaker Andy before, that is to say, I exchanged public keys with the speaker. Although he uses Outlook and the email certificate issued by his own CA, but MeSign App has automatically synchronized his public key to the public key database when I use MeSign App to send encrypted email to him. Therefore, when Jason uses MeSign App to write an email to the speaker, MeSign App will automatically connect to the cloud public key database and automatically retrieve the speaker's public key, so that an encrypted email can be automatically sent without having to exchange public keys with the speaker in advance.

Seeing is believing. As shown in the figure below, when you enter the MeSign customer service email address in the recipient field, then double-click the email address and the recipient's encrypting certificate information will pop up, which means that the recipient's public key has been successfully retrieved, then you can click "Send" to send an encrypted email to the recipient.



Of course, it is not enough to just collect the public keys used by MeSign App users. After all, there are very few users who have public keys. Therefore, MeSign Technology has built a cloud cryptographic infrastructure, providing cloud CA service and cloud key management services for users, so MeSign App can automatically get the free email certificates for users, and automatically configure the use of email certificates to realize automatic email encryption and digital signature. In this way, the public key of any user who uses MeSign App as the email client does not need to be collected, and it can be directly written into the public key database when MeSign CA issues the email certificate to the user.

Now, I believe that readers can understand why MeSign Technology can realize automatic email encryption, because we have built a public key database, and MeSign App automatically connects to the public key database to retrieve the recipient's public key. But at present, a large number of emails automatically sent by all kinds of management information systems are all cleartext emails. For example, banks have sent users a large number of important credit card bills, account statements and other important emails containing user confidential information, but they are all cleartext emails. And there are also many e-government systems that have sent a large number of notification emails to citizens, which are all cleartext emails. This is a big security hazard.

How to ensure the security of these emails containing confidential information that are automatically sent by the system? Of course, encrypted emails should be sent to users. But how to send? MeSign Technology has proposed a feasible solution, which is to open the public key database for free to let the business management system call MeSign Public Key API when sending business emails to users, and get the recipient's public key for free, then the business system can send encrypted emails to users automatically.

The reason why MeSign Technology is willing to open its public key database to users around the world for free, including government agencies, public service institutions, financial institutions, enterprises and other email client developers, is because MeSign Technology has a dream of realizing "Email Encryption Only", we hope to work with all email stakeholders to promote the popular application of automatic email encryption, jointly protect the security of email information of users around the world, work together to improve global Internet security for a better Internet and a better world.

Finally, leave a question for the reader: if someone has neither an email certificate issued by any CA, nor does he/she use MeSign App (there is no email certificate automatically issued by MeSign CA), that is to say, he/she does not have any email certificate at all. So, if you use MeSign App to send an encrypted email to him/her, how does MeSign App get this person's public key?

The answer to this question is the technical secrets of MeSign Technology (patent pending), MeSign Technology's global original solution, this is the confidence that we dare to call our public key database as "global public key database". The author can say without exaggeration that if you want to send an encrypted email to any email address, MeSign App can get its public key for you! Welcome to download MeSign App for free and enjoy a completely free automatic email encryption service!

---------- END ----------

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.