The Third Hurdle for Email Encryption is Key Management

(April 09, 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 explained in detail in the next blog post. The second hurdle is public key exchange. If both the sender and receiver have passed the first hurdle and both have an email certificate, they must first send a digitally signed email to realize the public key exchange. Only the public key is exchanged, the sender can use the receiver's public key to send an encrypted email to the receiver. How to pass this hurdle has been clearly explained in the blog post "The second hurdle for email encryption is the exchange of public key", which is to realize automatic public key exchange through the cloud public key database.

The third hurdle of email encryption is key management. Why is this a hurdle? Readers who familiar with email encryption must know that the current email encryption is that users apply for an email certificate from a CA, user manages the keys. It is necessary to manually import the certificate to email clients and devices, which is very cumbersome. And if the certificate expires, user needs to apply for a new email certificate, and in order to decrypt the previously encrypted email, user needs to keep the expired email certificate. The author started to use email certificate for encrypting emails 15 years ago, and now I can't find some previous email certificates for some reasons. As a result, even if the previous emails are still on the mail server, they cannot be decrypted because I cannot find the email certificate. This is the trouble of email encryption. Regarding an important email that cannot be decrypted, I even regret that it should not be encrypted at that time! This is a hurdle for email encryption - key management, we must find a way to pass it!

How to solve? The author thought of cloud services. Using Google to search for "cloud key

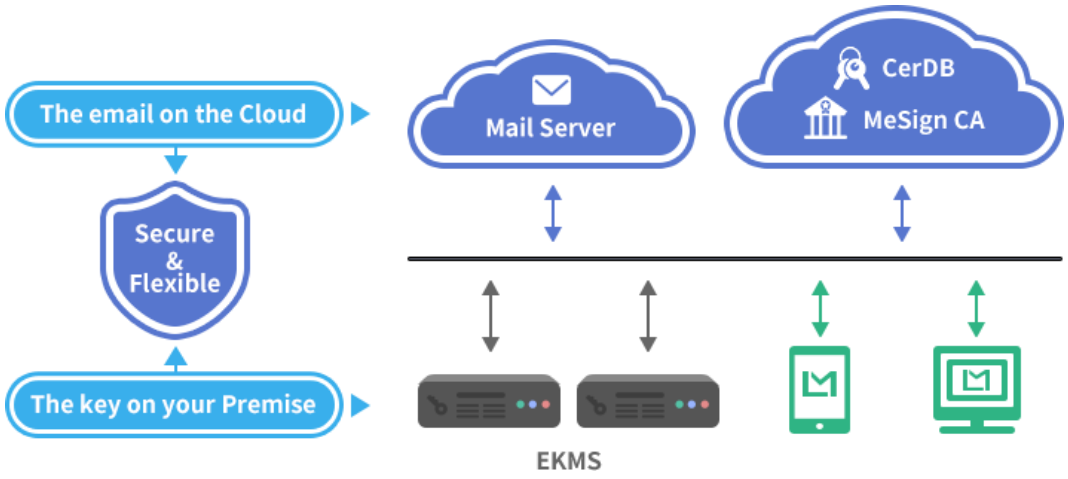
management", it can search for cloud key management services provided by cloud service providers. After investigating these cloud key management services, MeSign Technology decided to build its own cloud key management system, so that users can use our email client software - MeSign App to automatically obtain the encrypting key to decrypt the encrypted emails using any device anytime and anywhere, completely solving the dilemma when users manage the keys by themselves. Only in this way can the key management problem be solved, so that users do not need to laboriously configure the email certificate to be used in the email clients, do not need to laboriously manage the encrypting key, and do not need to worry about key loss that cannot decrypt the encrypted emails. And only in this way can it make encrypted emails as easy as normal cleartext emails and can truly popularize email encryption applications.

In other words, the realization of MeSign Technology's automatic email encryption is a successful application of cloud key management services. The integration of "cloud" and "client" allows users to easily pass the third hurdle of email encryption! The author firmly believes that the cloud key management service will definitely become a very important cloud service, because in order to protect the security of the data in cloud, the data needs to be encrypted and digitally signed, and these actions are inseparable from the cloud key management service.

A MeSign App user used a very vivid word to express his praise for MeSign solution - "**lifesaver**", which is explained by dictionary: “a thing that saves one from serious difficulty. For example: a microwave oven could be a lifesaver this Christmas.” It can be explained vividly as: This is simply saving lives. Because the other email encryption solutions on the market are difficult to use, it may not be possible to get it done, so this user said that MeSign App is saving lives!

For government agencies, financial institutions or large enterprises, if you want to control the encrypting keys by yourself and do not like to use cloud key management services, MeSign Technology also has solution. You can deploy the MeSign Enterprise Key Management System locally and manage the keys locally. In this way, MeSign App will automatically connect to

the local key management system to obtain the user's key, instead of connecting to MeSign cloud key management system, so as to satisfy the user's need to manage keys locally, to achieve a new mode of email security management of "emails in cloud" but "keys in hand".



In short, if you want to realize automatic email encryption, you must use a key management service. MeSign Technology provides free cloud key management services for MeSign App global users, with many advantages such as "obtain on demand, available at any time", "free use, universal encryption", "cloud-client integration, solving problem". For users who want to manage their keys by themselves, MeSign Technology also provides an enterprise key management system that can be quickly deployed locally, allowing users to manage keys locally, realizing "emails in cloud, keys in hand", so you can use the cloud email service with confidence.

---------- 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.