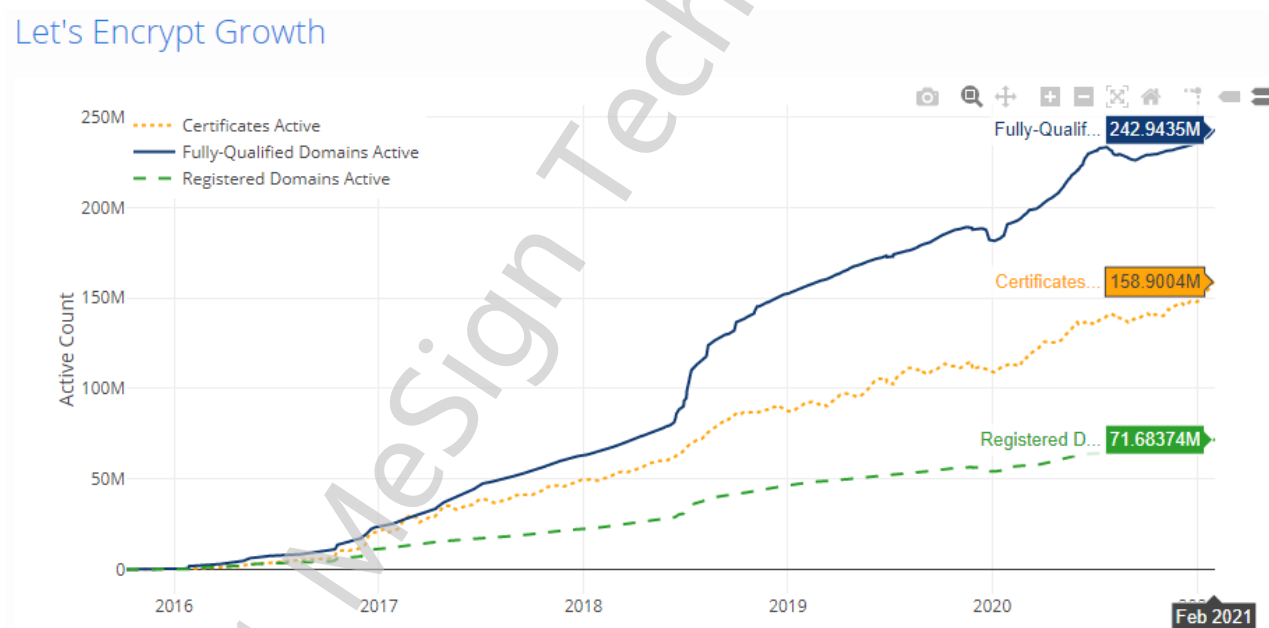


What Can We Learn from the Success of Let's Encrypt?

(Feb 22, 2021)

Let's Encrypt is no stranger to most readers. According to statistics on its official website, the number of active SSL certificates is 158.90 million, and the maximum number of SSL certificates issued per day is 2.09 million. 242.94 million active websites are using its SSL certificates. And according to third party statistics, Let's Encrypt global market share in SSL certificate exceeds 65%, this result only took 5 years. What can we learn from its great success? Everyone may have their own answers. I would like to share my views with you here for your reference.

Let's Encrypt Growth



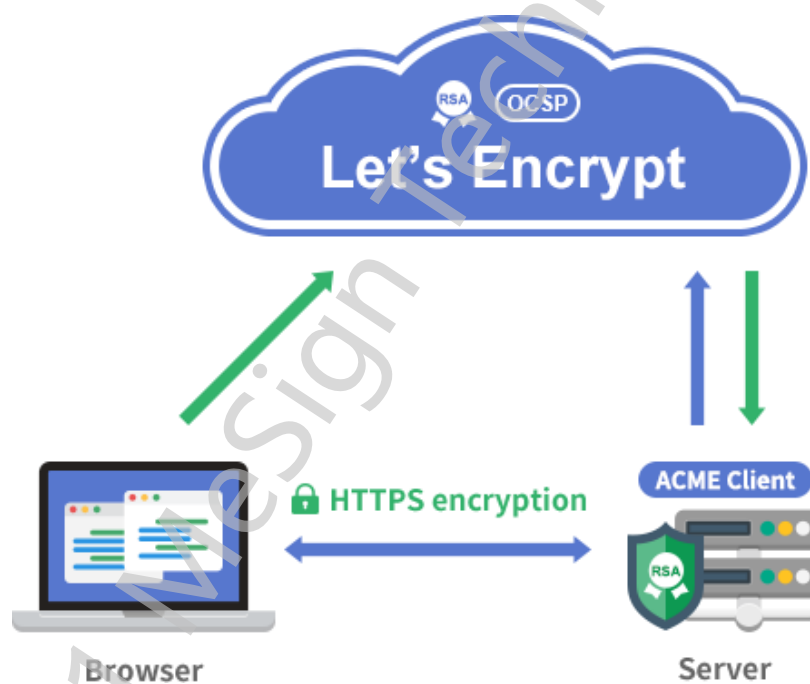
In order to answer this question, it is necessary to learn a little about SSL certificate knowledge so that users who have not experienced SSL certificate application and deployment can refer to it. If you understand these, you can skip to the next paragraph. SSL certificate is used for website https transmission encryption because Web pages used the HTTP protocol that was transmitted in cleartext when they were invented and used. The information transmission from the browser to the server is also transmitted in cleartext just like the current email transmission. It is easy to leak all confidential information such as login username and password submitted

by the user from the browser, especially when the Internet is used for online payment. Once the payment information is illegally tampered with and stolen during transmission, it is a big problem, the result is transferring \$1,000 to John may be tampered with and transferred to Jason. Therefore, Netscape, the originator of the browser, invented the SSL protocol and deployed an SSL certificate on the server. The browser supports the use of certificate public keys to encrypt http traffic and realize https transmission encryption. This “S” is the meaning of Secure. Simply put, to realize the transmission encryption from the Web client to the server, the user must apply for an SSL certificate from a CA. Of course, it used to be charged, and the high-end brand SSL certificate was charged as high as \$1,200/year in 2000. If you think about the salary income of 20 years ago, you know what this means, which means that SSL certificates cannot be widely used. Not only is the cost high, but it may take a week from applying for a certificate to getting the certificate. After getting the certificate, it is very laborious to deploy and use on the Web servers, to realize https encrypted transmission and protect the data security of Web traffic.

If you have read my blog ["What you need is bread instead of flour or wheat when hungry"](#), you may remember my product innovation point of view: Let us return to the origin of user needs to analyze user needs and provide users the required products directly instead of the intermediate products. In terms of https website transmission encryption, what users need is to realize the transmission encryption from the browser to the server, not the SSL certificate. At present, CAs all over the world are selling SSL certificates. They did not recognize the real needs of users. However, the browser manufacturer Mozilla (Firefox) realized that the real needs of users is Web transmission encryption and takes the leads in cooperating with other organization to launch the Let's Encrypt project. It is not so much a CA project as a software project, because Let's Encrypt does not provide users to apply for SSL certificates on their websites like other CA and give the certificates to users so that users can deploy the certificate in the web server but provide user a software that develop it on the web server. Starting this software can automatically configure the required SSL certificate for the user's website, thereby automatically implementing https encryption.

What users need is Web transmission encryption, not an SSL certificate. Therefore, Let's

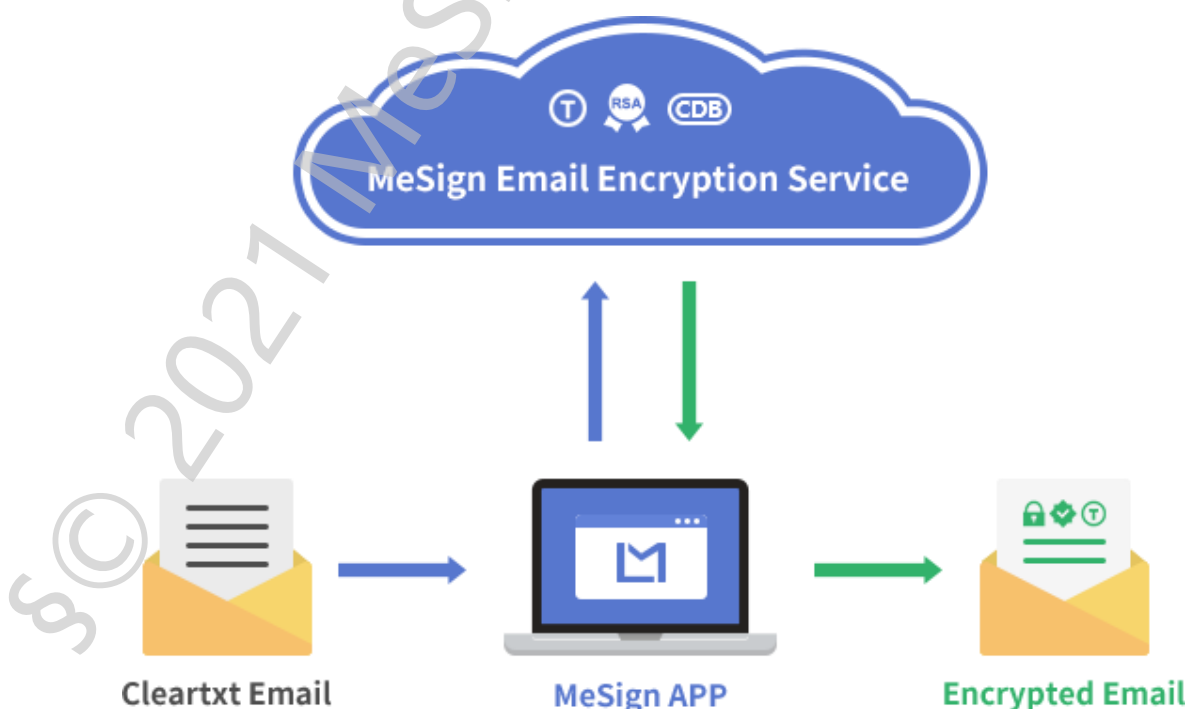
Encrypt does not give users an SSL certificate. Instead, it provides users with a software that can automatically apply SSL certificates and automatically deploy certificates to implement https encryption. Now, everyone should be able to understand the secrets and reasons why Let's Encrypt is so successful. Some users who know the CA market may say that the success of Let's Encrypt is because the certificate is free, which is certainly one of the factors, especially when new products are launched, free can attract users to try and use, but this is not an important one. The reason, the important reason is that its products really meet the real needs of users! I firmly believe that even if the Let's Encrypt service is no longer free, users are willing to pay, because they are used to the state that they only need to install a software and then do nothing, it is impossible to let these users go to the traditional CA to apply for SSL certificates and deploy the certificates in order to save money, these users will choose to pay to continue using Let's Encrypt service.



This is my analysis of why Let's Encrypt is successful. If you are already a user of MeSign App, or have read my blog ["What you need is bread instead of flour or wheat when hungry"](#), you will find that MeSign App also uses the same "routine"! In traditional email encryption services, users need to purchase and apply for an email certificate from CA. After receiving the certificate, they need to laboriously configure the certificate in the email client software that supports S/MIME email encryption and laboriously exchange public keys with the

recipient to achieve email encryption. The MeSign App integrates the functions such as automatic certificate application, automatic configuration and use of certificates, and automatic retrieval of public keys, allowing users to directly use MeSign App to achieve email encryption that no need to care about the email certificate. It is not difficult to explain why MeSign App so loved by worldwide users once it was launched, and now MeSign App users have covered 171 countries and regions. Our e-signature service - MeSignDoc is also the same idea, users don't need to care about the document signing certificate, do not need to upload the document to be signed to the e-signature platform, and directly use the MeSignDoc App to implement automatically document digital signature in user's computer.



Let's compare the similarities between the two solutions. Both have a cloud cryptography infrastructure for issuing certificates and other supporting services, and both give users a client software, and this client software is responsible for the tedious certificate application and certificate deployment, and what's the user gets is one time software installation for data encryption and digital signature service. As a practitioner who has been engaged in the CA business for 15 years, I have jumped out of the CA circle to re-understand the success of Let's Encrypt from the perspective of a software developer and have successfully applied this problem-solving idea to email encryption and document e-signature application.



I hope this article can be inspiring for CA practitioners and software developers. Of course, I also believe that this article can help MeSign users fully understand the advantages of our products and grow with us to realize the lofty ideals of "Email Encryption only" and "E-document Signature only" and work together to enhance the global Internet security for a better Internet and a better world.

----- 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.