Interpretation of the U.S. Federal Zero Trust Strategy (Part 3): Email Security

On September 7, 2021, the U.S. Office of Management and Budget (OMB) released a draft of the Federal Zero Trust Strategy and solicited comments online to support Presidential Executive Order No. 14028, Improving the Nation's Cybersecurity, to guide federal government agencies to migrate their security architecture to be based on zero trust principles.

It states the following about encrypting email traffic:

> **3. Encrypting email traffic**
>
> It remains challenging today to easily and reliably encrypt an email all the way between any sender and any recipient. Unlike HTTP and DNS, there is not today a clear path forward for guaranteeing that Federal emails are encrypted in transit, particularly for emails with external parties.[12]
>
> **CISA will evaluate the viability of MTA-STS as a government-wide solution for encrypted email and make recommendations to OMB to inform future government-wide actions.**

Since it was a public comment, the author sent my opinions to the public comment email, clearly pointing out that the TLS email encryption solution (MTA-STS) is not the best solution, and the best solution should be end-to-end encryption. After the deadline for comments, the author received a thank you letter. Although it was a courtesy reply, I still felt their determination to implement zero trust security for email.

RE: [EXTERNAL] RE: Public comment on the Federal Zero Trust Strategy from ZoTrus

MO MBX OMB OFCIO <MBX.O @OMB.eop.gov> 2021/9/23 (THU) 0:56
to @zotrus.com'
cc MBX O

Hello,

We just wanted to acknowledge receipt, and to thank you for your comments, which we will consider before finalizing OMB's federal zero trust strategy. We really appreciate you taking the time to send us your feedback, and your interest in helping strengthen federal cybersecurity.

Let’s take a look at the official version released on January 26, 2022. The MTA-STS content has been removed. It can also be understood that the official version has listened to the author’s advice that TLS encryption is not a good solution, so it no longer mentions this solution. Instead, it says in the fourth paragraph of “Encrypting email traffic”: CISA will evaluate the viability of current open standards as Government-wide solutions for encrypted email in transit and make recommendations to OMB to inform future Government-wide actions. As part of its evaluation, CISA should partner with FedRAMP to convene and consult with cloud service providers and other participants in the email ecosystem.

To give readers a comprehensive understanding of the difficulty of email encryption, you can take a look at the requirements of the UK government website:

How to secure email

You must:

- encrypt and authenticate email in transit by supporting Transport Layer Security (TLS) and Domain-based Message Authentication, Reporting and Conformance (DMARC) as a minimum
- use extra encryption if your data needs more protection
- make sure the recipient protects the data you send to them
- make email security invisible to end users as far as practically possible

From the last requirement of not changing users' email usage habits, it is not difficult to understand why the UK government website's email security requirements have changed from the previous requirement to use S/MIME encryption (as shown in the figure below) to the current use of TLS email encryption, because the S/MIME encryption solutions currently on the market are very inefficient and provide poor user experience.

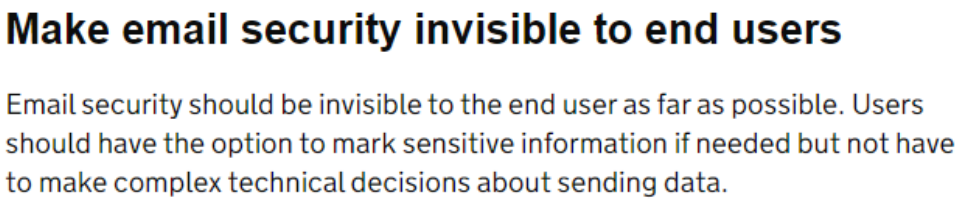
Transfer sensitive information

You should only use message-based encryption like PGP or S/MIME occasionally for transfer of sensitive information as it’s inefficient and provides a poor user experience.

For the sake of user experience, the US government and the UK government have chosen TLS email transmission encryption that does not affect the user experience, including the use of MTA-STS. However, TLS email encryption can only guarantee the transmission encryption between the user and their own email server. If the recipient's email server does not use TLS encryption, only the sender

channel encryption is used at the email sending end, but the transmission between the email servers and the receiving end are not encrypted. This is why TLS encryption is required to be mandatory (STS).

The UK government website also has a special paragraph emphasizing user experience - Make email security invisible to end users and try not to force end users to adopt very complex technical measures for email security.



So, what kind of email encryption solution do users really need? What kind of encryption solution can make end users invisible? The author has been thinking about and practicing this difficult problem for many years. The first paragraph of "Encrypting Email Traffic" in the U.S. Federal Zero Trust Strategy said: "It remains challenging today to easily and reliably encrypt an email all the way between any sender and any recipient. Unlike HTTP and DNS, there is not today a clear path forward for guaranteeing that Federal emails are encrypted in transit, particularly for emails with external parties. "It is indeed true that finding a suitable email encryption solution is very challenging.

The second paragraph said: However, email remains a critical method of communication and authentication in the operation of everyday life in the Federal Government. Since emails to, from, and within the Federal Government are sent and received by a tremendous diversity of clients and service providers, any solution will necessarily be based on open standards.

What is the standard for email encryption? Of course, there is only the S/MIME international standard, which is the RFC 2311 standard that was established in 1998. At present, all commonly used email client software supports this standard, and all globally trusted CAs are issuing email certificates based on this standard. The S/MIME Certificate Working Group of the International Organization - CA/Browser Forum officially released the "Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates" on January 01, 2023. This is the world's first international standard for regulating the issuance of email certificates by global CAs. Of course, it also clearly affirms the international status of the S/MIME technical standard. Email encryption is based on

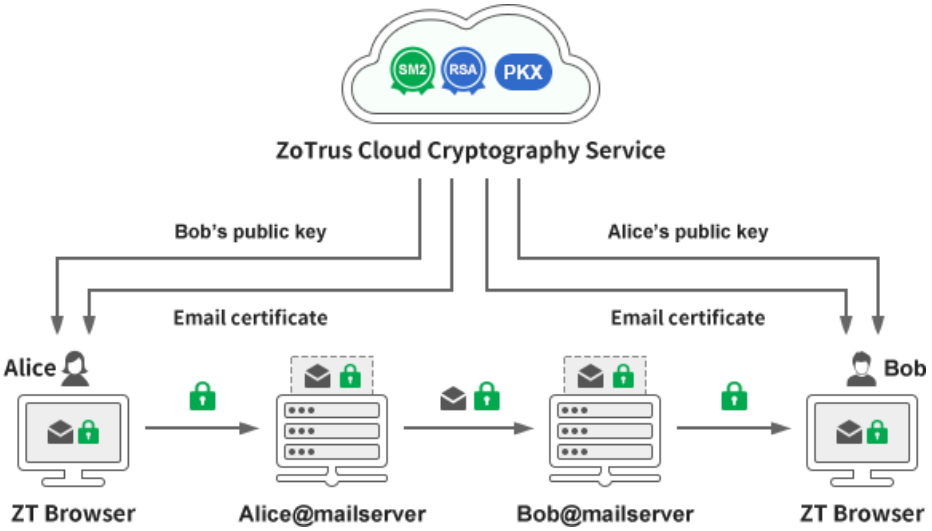
S/MIME standard.

However, why has this encryption scheme based on the S/MIME standard technology not been widely used 26 years after the birth of the S/MIME standard? It is because the user experience mentioned on the British government website is too poor. It is very difficult to use. Users not only have to go to the trouble to apply for an email certificate from the CA, but also must exchange public keys with the recipient to achieve mutual encryption. And they must manage the encryption key. Once the key is lost or the key protection password is forgotten, the encrypted email will never be decrypted. The author has deeply experienced this pain and regretted not encrypting it at the beginning.

Since it is so painful to use email certificates to implement email encryption, is there a painless solution? Email, as the second largest traffic on the Internet, carries a large amount of confidential information exchange and a large amount of personal privacy information and commercial confidential information stored in the cloud. This confidential information is all transmitted and stored in plain text, which is not secure. Through efforts, the global industry has gradually turned the largest traffic on the Internet, HTTP traffic, into HTTPS encrypted traffic, effectively ensuring the transmission security of the main information traffic on the global Internet. Although TLS/SSL certificates can also ensure the security of email transmission, the email transmission process is different from HTTPS encryption. The email system is a distributed and decentralized system that connects the world. It requires both the sender and receiver of emails, or even multiple parties, to take unified actions to fully implement email transmission encryption. Even if everyone has implemented TLS transmission encryption, the email content is still stored in plain text in the cloud email server, which is still not secure.

How to do? The innovative solution of ZoTrus Technology is a Client-Cloud integration solution. The client is ZT Browser, a high-performance browser based on the Google Chromium with a built-in email client. After the user logs into the mailbox using the ZT Browser, ZT Browser will automatically connect to the ZoTrus Cloud Cryptographic Service System to automatically complete the S/MIME certificate application, email control validation, email certificate issuance and configuration for the user. And when using ZT Browser to send encrypted emails, it will automatically connect to the Public Key Exchange (PKX) Service provided by ZoTrus Cloud Cryptography Service System, automatically obtain the recipient's public key certificate, and send encrypted emails without exchanging public keys

with the recipient in advance. The client-cloud integration completely solves the various technical problems encountered in email encryption, allowing users to send encrypted emails as easily as sending plain text emails, achieving end-to-end email encryption. The email content is also stored in ciphertext on the mail server, perfectly realizing the security of the entire life cycle of emails.



ZoTrus Email Encryption Automation Solution perfectly solves the technical problems of email encryption in the US Federal Zero Trust Strategy, and it solves the UK government's user insensitivity requirements for email security, and this innovative solution will definitely be recognized by worldwide users. ZoTrus Technology is willing to work together with global email users to make the second largest traffic on the Internet realize end-to-end full encryption, ensure the security of emails in transit and in the cloud, and let great emails continue to provide more secure communication services for mankind.

Richard Wang

October 14, 2024
In Shenzhen, China

Follow ZT Browser at X (Twitter) for more info. The author has published 72 articles in English (more than 90K words) and 183 articles in Chinese (more than 524K characters in total).