PGP and S/MIME

November 30, 2023

Gage Moore

Email Exploration

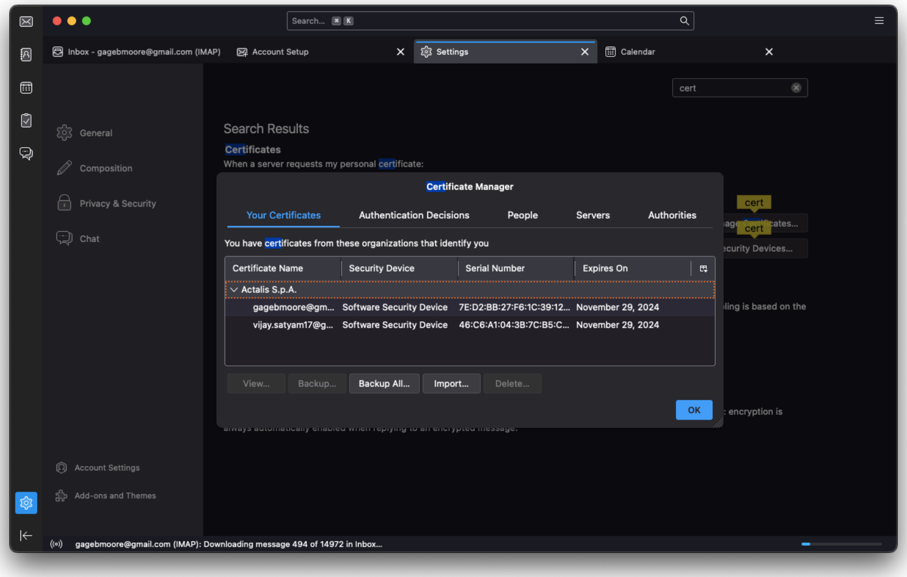
I exchanged emails with **REDACTED**. We learned a great deal about the importance of PGP and S/MIME and had fun whilst learning.

Part 1 - S/MIME

S/Mime is a widely used cryptographic protocol designed for digitally signing and encrypting email messages. It uses asymmetric cryptography to protect users' emails from unwanted third-party access and involves digital signatures in order to verify the sender's identity.

The first step is to get an S/MIME certificate. This was the hardest part of the lab for me and generated a lot of frusteration. I was able to download a certificate from the Italian company *Actalis*. The certificate download page was frighteningly sketchy and resulted in 500-level errors until it correctly provided an S/MIME certificate after about 20 minutes of trying.

With an S/MIME certificate in hand, (and Vijay having accomplished the same thing), we then exchanged certificates so that both could be added to our email client, Thunderbird. We exchanged certificates via email and PGP, which is described in the next section. By adding the certificates for our respective emails, Thunderbird would be equipped to sign and encrypt emails sent between both me and Vijay. A screenshot of these certificates being added in Thunderbird is shown below:



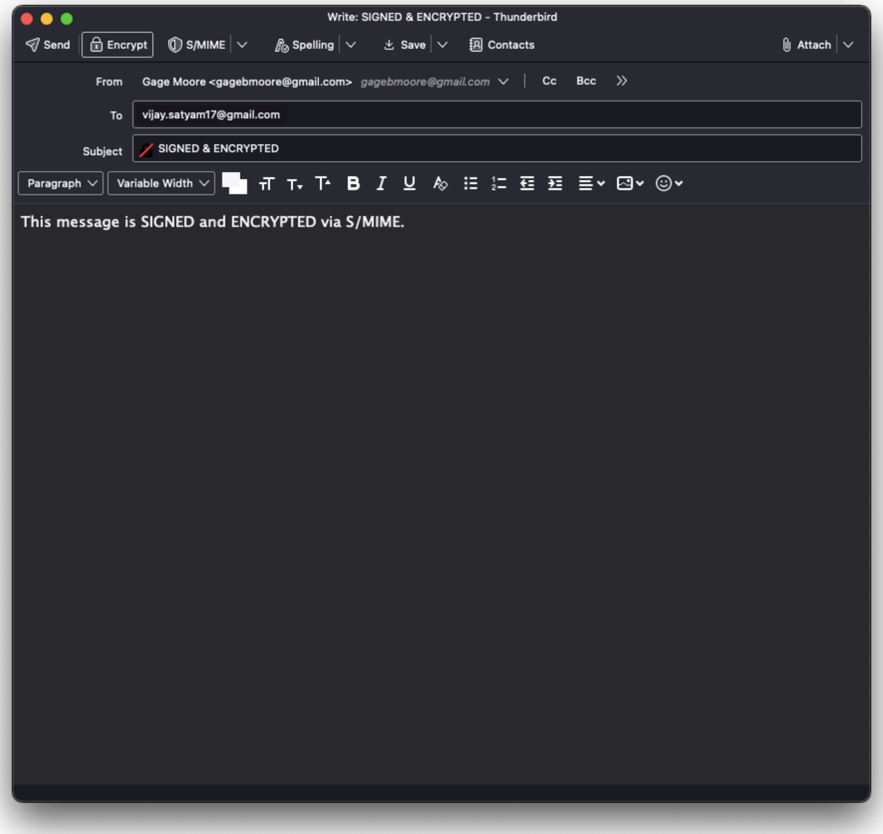
When a server requests my personal certificate:

You have certificates from these organizations that identify you

Certificate Name	Security Device	Serial Number	Expires On
Actalis S.p.A.			
gagebmoore@gm...	Software Security Device	7E:D2:BB:27:F6:1C:39:12...	November 29, 2024
vijay.satyam17@g...	Software Security Device	46:C6:A1:04:3B:7C:B5:C...	November 29, 2024

gagebmoore@gmail.com (IMAP): Downloading message 494 of 14972 in Inbox...

Once we had these S/MIME certificates properly imported within our email clients, we then exchanged emails. I was able to send an email, (both encrypted and digitally signed via S/MIME), as shown in the screenshot below.



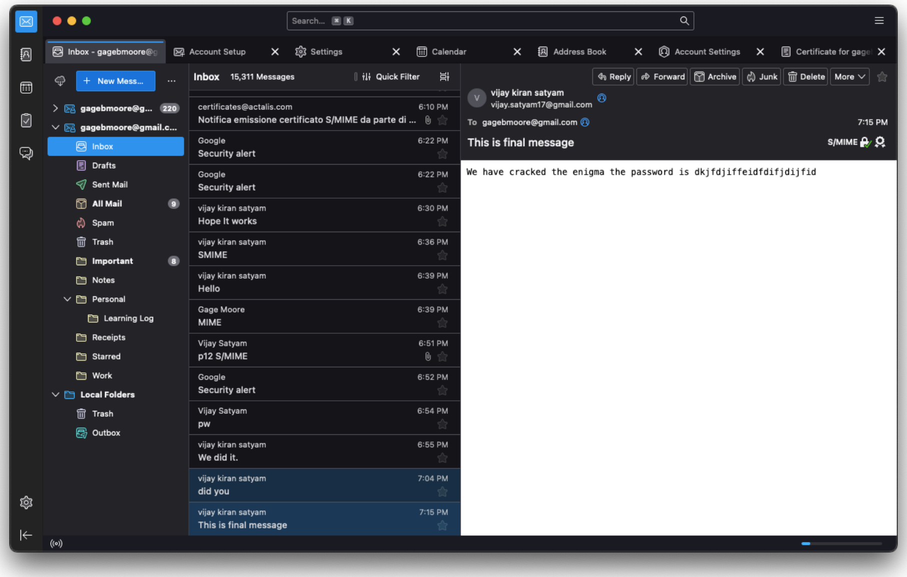
From Gage Moore <gagebmoore@gmail.com> gagebmoore@gmail.com

To vijay.satyam17@gmail.com

Subject SIGNED & ENCRYPTED

This message is SIGNED and ENCRYPTED via S/MIME.

Vijay did the same thing, and upon receiving his email I was pleased to find that it was verified, (on account of being digitally signed), and encrypted, (which Thunderbird automatically decrypted for me). A screenshot of the received email is shown below:



Inbox 15,311 Messages

certificates@actalis.com Notifica emissione certificato S/MIME da parte di ...	6:10 PM
Google Security alert	6:22 PM
Google Security alert	6:22 PM
vijay kiran satyam Hope It works	6:30 PM
vijay kiran satyam SMIME	6:36 PM
vijay kiran satyam Hello	6:39 PM
Gage Moore MIME	6:39 PM
Vijay Satyam p12 S/MIME	6:51 PM
Google Security alert	6:52 PM
Vijay Satyam pw	6:54 PM
vijay kiran satyam We did it.	6:55 PM
vijay kiran satyam did you	7:04 PM
vijay kiran satyam This is final message	7:15 PM

vijay kiran satyam
vijay.satyam17@gmail.com

To gagebmoore@gmail.com 7:15 PM

This is final message S/MIME

```
We have cracked the enigma the password is dkjfdjiffeidfdifjdijfid
```

S/MIME SUS Score

Each question is given a score of 1-5.

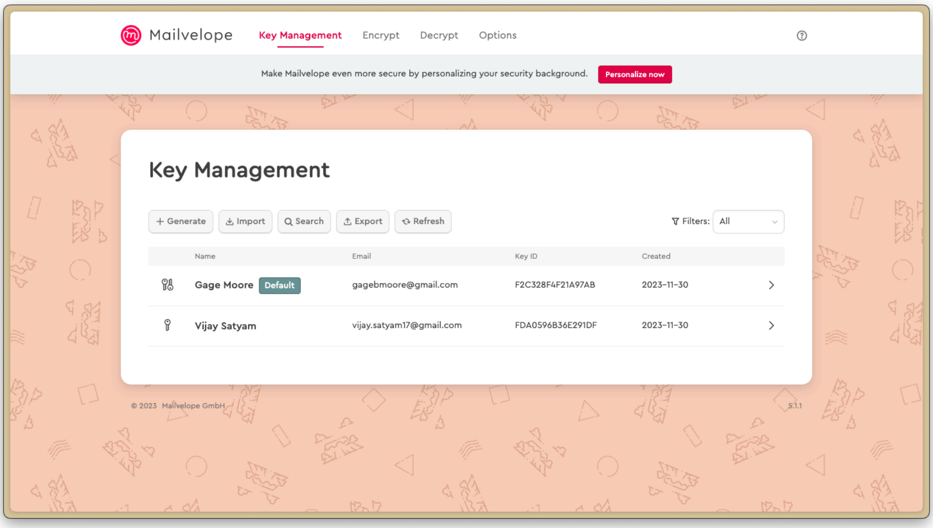
I think that I would like to use this system frequently: 2
I found the system unnecessarily complex: 3
I thought the system was easy to use: 2
I think that I would need the support of a technical person to be able to use this system: 2
I found the various functions in this system were well integrated: 2
I thought there was too much inconsistency in this system: 1
I would imagine that most people would learn to use this system very quickly: 1 **I found the system very cumbersome to use:** 3 **I felt very confident using the system:** 2 **I needed to learn a lot of things before I could get going with this system:** 5

SUS Score: 37.5.

Part 2 - PGP

PGP stands for "Pretty Good Privacy". It is an encryption program that can be used for encrypted and decrypting data. For the purpose of this lab, Vijay and I sent and received emails protected by end-to-end encryption using PGP. This was accomplished with the extension *Mailvelope*.

Within the extension, I was able to create a key pair that would be used for encryption. Like S/MIME, sending PGP-protected emails involves asymmetric encryption via a key pair. My key pair is included below, alongside Vijay's public key.

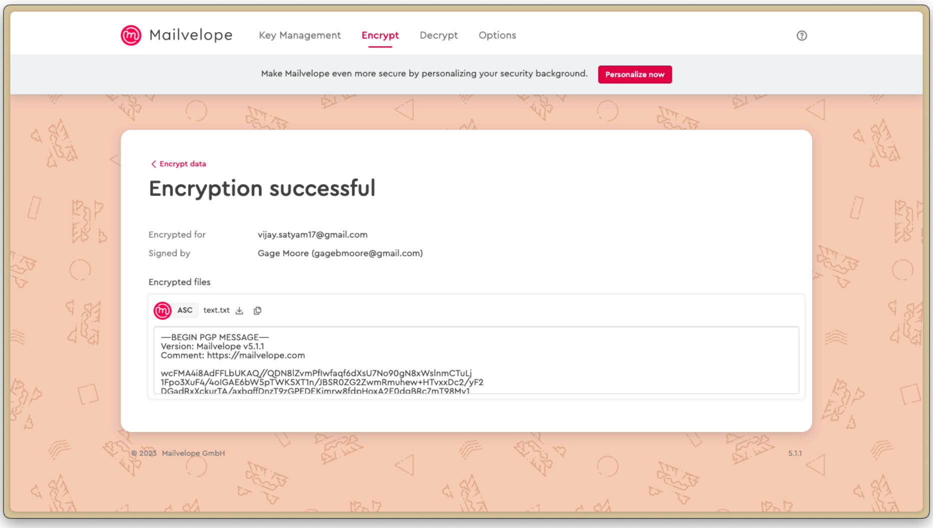


Make Mailvelope even more secure by personalizing your security background.

Key Management

Name	Email	Key ID	Created
Gage Moore Default	gagebmoore@gmail.com	F2C328F4F21A97AB	2023-11-30
Vijay Satyam	vijay.satyam17@gmail.com	FDA0596B36E291DF	2023-11-30

With my key pair generated, I successfully sent an encrypted email to Vijay, and received one from him as well.



Make Mailvelope even more secure by personalizing your security background.

Encryption successful

Encrypted for vijay.satyam17@gmail.com

Signed by Gage Moore (gagebmoore@gmail.com)

Encrypted files

text.txt

```
—BEGIN PGP MESSAGE—
Version: Mailvelope v5.1.1
Comment: https://mailvelope.com

wcFMA4i8AdFFLbUKAQ//QDN8lZvmPflwfaqf6dXsU7No90gN8xWslnmCTuLj
1Fpo3XuF4/4oIGAE6bW5pTWK5XT1n/JBSR0ZG2ZwmRmuhew+HTvxxDc2/yF2
DGadRxXckurTA/axbqffDnzT9zGPFDFKimrw8fdpHoxA2F0dqBRc7mT98Mv1
```

© 2023 Mailvelope GmbH 5.1.1

PGP SUS Score

Each question is given a score of 1-5.

I think that I would like to use this system frequently: 4
I found the system unnecessarily complex: 2
I thought the system was easy to use: 5
I think that I would need the support of a technical person to be able to use this system: 1
I found the various functions in this system were well integrated: 2
I thought there was too much inconsistency in this system: 1
I would imagine that most people would learn to use this system very quickly: 2 **I found the system very cumbersome to use:** 1 **I felt very confident using the system:** 4 **I needed to learn a lot of things before I could get going with this system:** 1

SUS Score: 77.5.

Quick Conculsion

Going forward, I will continue using encryption standards for my email, like the methods described above, because I feel that they improve my privacy while using email and are worth it in the daily activity that I am involved in with email.