Report

Jackson Mowry

March 29, 2025

Contents

1 Part 1 – Investigating Web PKI Certificates

1.1 google.com

1. What is the subject of the leaf certificate?
   - *.google.com
2. What is the issuer of the leaf certificate?
   - WR2, `http://i.pki.goog/wr2.crt`
3. What is its validity period?
   - 10 Mar 2025 - 2 Jun 2025
4. What type of public key is it using?

   - EC 256 Bits

5. What algorithm was used to sign the certificate?
   - SHA256withRSA

1.2 amazon.com

1. What is the subject of the leaf certificate?
   - *.peg.a2z.com
2. What is the issuer of the leaf certificate?
   - DigiCert Global CA G2
3. What is its validity period?
   - 26 Aug 2024 - 27 Jul 2025
4. What type of public key is it using?
   - RSA 2048 Bits
5. What algorithm was used to sign the certificate?
   - SHA256withRSA

1.3 utk.edu

1. What is the subject of the leaf certificate?
   - utk.edu
2. What is the issuer of the leaf certificate?
   - R10
3. What is its validity period?
   - 5 Mar 2025 - 3 Jun 2025
4. What type of public key is it using?
   - RSA 2048 Bits
5. What algorithm was used to sign the certificate?
   - SHA256withRSA

1.4 dhs.gov

1. What is the subject of the leaf certificate?
   - www.dhs.gov
2. What is the issuer of the leaf certificate?
   - GeoTrust RSA CA 2018
3. What is its validity period?
   - 29 Jan 2025 - 16 Dec 2025
4. What type of public key is it using?
   - RSA 2048 Bits
5. What algorithm was used to sign the certificate?
   - SHA256withRSA

1.5 self-signed.badssl.com

1. What is the subject of the leaf certificate?
   - *.badssl.com
2. What is the issuer of the leaf certificate?
   - *.badssl.com (Self-signed)
3. What is its validity period?
   - 25 Mar 2025 - 25 Mar 2027
4. What type of public key is it using?
   - RSA 2048 Bits
5. What algorithm was used to sign the certificate?
   - SHA256withRSA
6. Problematic Field?
   - Issue, to fix this you would need to get a certificate signed by a trusted CA, not signed by the subject itself.

1.6 untrusted-root.badssl.com

1. What is the subject of the leaf certificate?
   - *.badssl.com
2. What is the issuer of the leaf certificate?
   - BadSSL Untrusted Root Certificate Authority
3. What is its validity period?
   - 25 Mar 2025 - 25 Mar 2027
4. What type of public key is it using?
   - RSA 2048 Bits
5. What algorithm was used to sign the certificate?
   - SHA256withRSA
6. Problematic Field?
   - Issuer, this issue is not in our browsers trust store. We would need to get our certificate request signed by a commonly trusted CA.

1.7 wrong.host.badssl.com

1. What is the subject of the leaf certificate?
   - badssl-fallback-unknown-subdomain-or-no-sni
2. What is the issuer of the leaf certificate?
   - BadSSL Intermediate Certificate Authority
3. What is its validity period?
   - 8 Aug 2016 - 8 Aug 2018
4. What type of public key is it using?
   - RSA 2048 Bits
5. What algorithm was used to sign the certificate?

- SHA256withRSA

6. Problematic Field?

    - Subject, this does not match the actual domain of the site. We would need to get a certificate that is explicitly bound to the domain.
    - Additionally the certificate is also expired, therefore we would need to get a new certificate.

1.8 expired.badssl.com

1. What is the subject of the leaf certificate?

    - *.badssl.com

2. What is the issuer of the leaf certificate?

    - COMODO RSA Domain Validation Secure Server CA

3. What is its validity period?

    - 9 Apr 2015 - 12 Apr 2015

4. What type of public key is it using?

    - RSA 2048 Bits

5. What algorithm was used to sign the certificate?

    - SHA256withRSA

6. Problematic Field?

    - Valid until, this certificate expired almost 10 years ago. To fix this we would need to get another certificate.

2 Part 2 – Using an Email PKI Certificate

1. The name of the student with which you (attempted to) exchanged secure email.

    - Peter (MACk Address) Hansen

2. What was the process for creating a certificate?

- We first tried to create our own self-signed certificates follwing this online guide, `https://community.lansweeper.com/t5/quick-tech-solutions/how-to-sign-an-email-with-a-self-signed-s-mime-certificate/ba-p/62255`. That ended up being a dead-end as we could not find an easy way to trust self-signed certificates in Thunderbird. After that we found an online service named Actalis which was very frustrating to use. In the end we don't think we were doing anything wrong, their service just suddenly emailed us the necessary information around 3 hours after we originally requested it. From there it was as simple as downloading our .p12 file and unlocking it with the password provided to us.

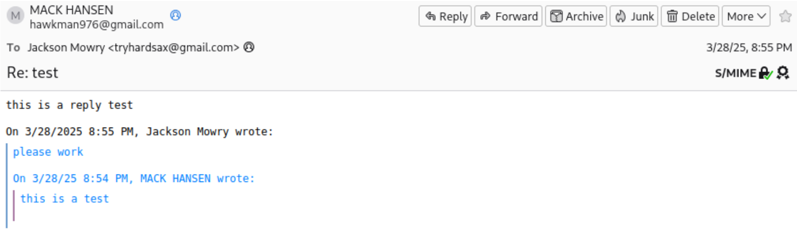
3. What was the process for getting that certificate signed?

   - Once we requested a certificate from Actalis we realized that they would generated the CSR for you, meaning the generation and signing was all handled on their end. This basically involved waiting around 3 hours for the request to be processed.

4. What was the process for sharing a key between you and your partner?

   - The process of sharing the key was not immediately obvious and we first tried to manually import each other's .p12 key into Thunderbird. We then realized this process was probably incorrect as it involved having to also share the associated password just to import it. Additionally, Thunderbird was not allowing us to import the .p12 file through the associated screen. Eventually we read online that you can first send a digitally signed email, which will automatically distribute your public key to the recipient. This then allowed the recipient to respond with an encrypted email, then finally the original sender is allowed to send an encrypted message back. This is fairly nice as only 1 message has to be sent unencrypted before encrypted communication can begin.

5. Include a screenshot of the signed and encrypted email you send and the email you received.



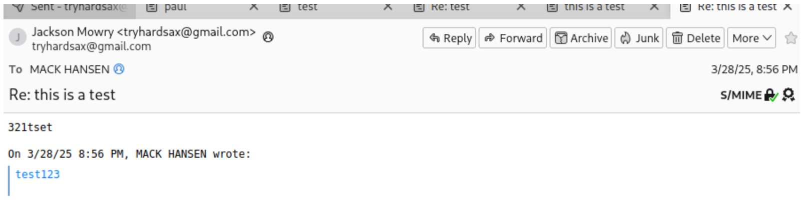
MACK HANSEN
hawkman976@gmail.com

To Jackson Mowry <tryhardsax@gmail.com>

3/28/25, 8:55 PM

Re: test

```
this is a reply test

On 3/28/2025 8:55 PM, Jackson Mowry wrote:
> please work
>
> On 3/28/25 8:54 PM, MACK HANSEN wrote:
>> this is a test
```



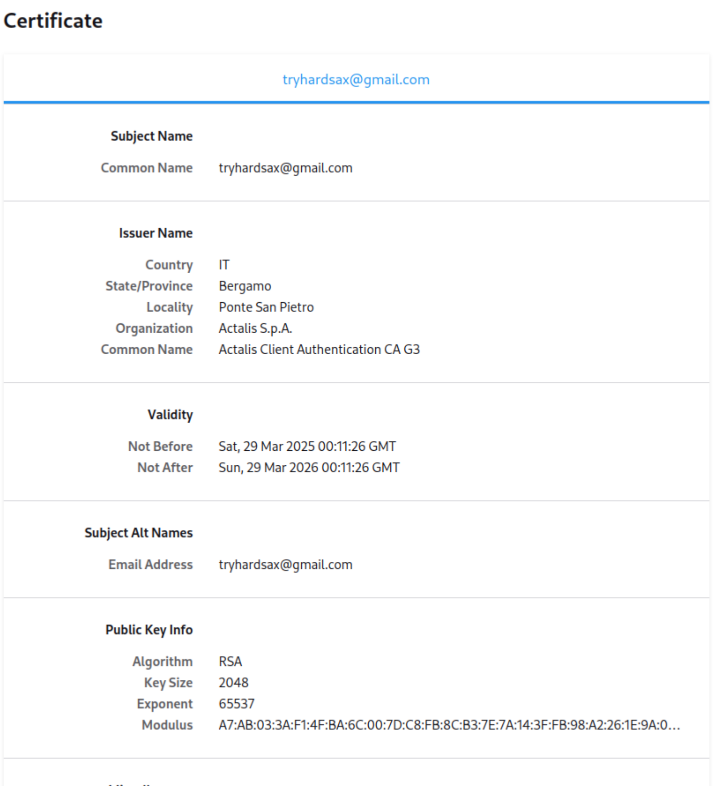
Jackson Mowry <tryhardsax@gmail.com>
tryhardsax@gmail.com

To MACK HANSEN

3/28/25, 8:56 PM

Re: this is a test

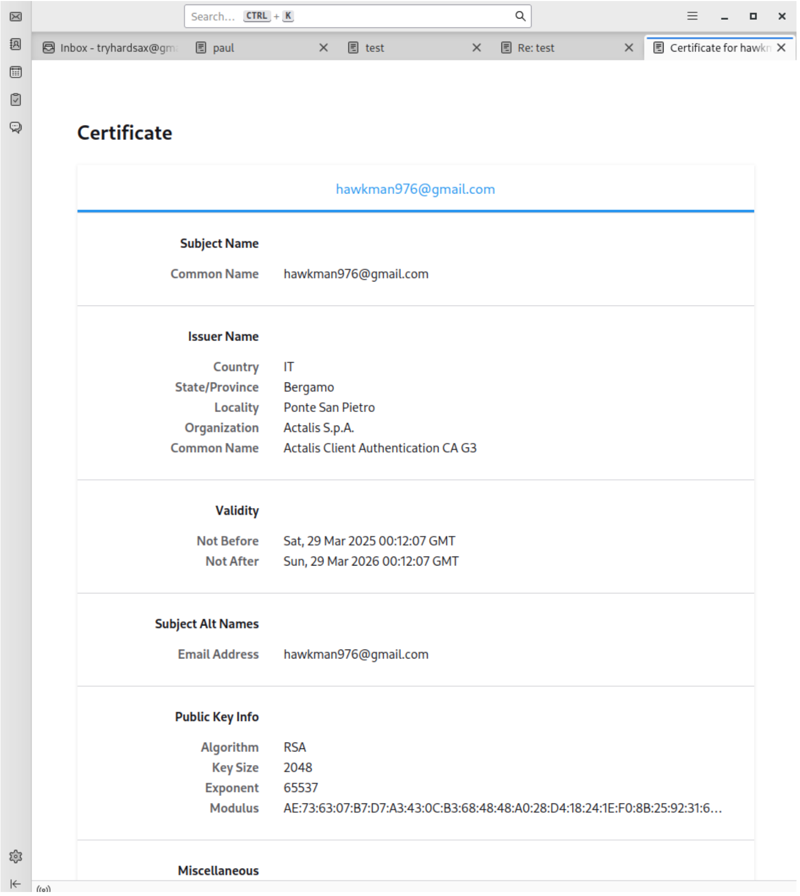
```
321tset

On 3/28/25 8:56 PM, MACK HANSEN wrote:
> test123
```



Certificate

tryhardsax@gmail.com

Subject Name	
Common Name	tryhardsax@gmail.com
Issuer Name	
Country	IT
State/Province	Bergamo
Locality	Ponte San Pietro
Organization	Actalis S.p.A.
Common Name	Actalis Client Authentication CA G3
Validity	
Not Before	Sat, 29 Mar 2025 00:11:26 GMT
Not After	Sun, 29 Mar 2026 00:11:26 GMT
Subject Alt Names	
Email Address	tryhardsax@gmail.com
Public Key Info	
Algorithm	RSA
Key Size	2048
Exponent	65537
Modulus	A7:AB:03:3A:F1:4F:BA:6C:00:7D:C8:FB:8C:B3:7E:7A:14:3F:FB:98:A2:26:1E:9A:0…



Certificate

hawkman976@gmail.com

Subject Name

Common Name hawkman976@gmail.com

Issuer Name

Country IT
State/Province Bergamo
Locality Ponte San Pietro
Organization Actalis S.p.A.
Common Name Actalis Client Authentication CA G3

Validity

Not Before Sat, 29 Mar 2025 00:12:07 GMT
Not After Sun, 29 Mar 2026 00:12:07 GMT

Subject Alt Names

Email Address hawkman976@gmail.com

Public Key Info

Algorithm RSA
Key Size 2048
Exponent 65537
Modulus AE:73:63:07:B7:D7:A3:43:0C:B3:68:48:48:A0:28:D4:18:24:1E:F0:8B:25:92:31:6...

Miscellaneous

(a) Identify where in the images you were able to verify the signature.

- The small 'ribon' icon has a pop-out menu that shows both encryption and digital signatures were used the messaged, sadly I cannot both open the menu and take a screenshot, but hopefully you get the idea. This is present on both my sent and received message.

(b) Identify where in the image you were able to confirm that encryption was used.

- Encryption was found in the 'ribon' menu I mentioned before, additionally within that menu you can see the actual certificate used by the send, which I have included summary screenshots for both me and my partner.

6. Explain which parts of the process were difficult to understand or ex-

ecute.

- The only real difficult part was finding information about the topic. Once we learned what to do the actual process was painless. For us the overall hardest part was just sitting around waiting for the certificate. During this time we were trying various different methods to obtain another certificate, which ultimately came up short. Lastly, it was not clear to us that our partner's certificate would be automatically imported after sending a digitally-signed email, before we would be allowed to encrypt an email.

7. Rate your experience using the System Usability Scale . Give your answer for each question and compute your overall score.

   (a) I think that I would like to use this system frequently.

   - 5. I would, just because I highly value confidentially and integrity.

   (b) I found the system unnecessarily complex.

   - 4. Yes, there were certainly parts that could have been made much more obvious to users.

   (c) I thought the system was easy to use.

   - 4. Once we got through the setup the actual using of the system was easy.

   (d) I think that I would need the support of a technical person to be able to use this system.

   - 1. No, I think this would work fairly easily going forward.

   (e) I found the various functions in this system were well integrated.

   - 3. If we're including the processing of getting the certificate then I could say no, otherwise yes.

   (f) I thought there was too much inconsistency in this system.

   - 1. The system felt very consistent.

   (g) I would imagine that most people would learn to use this system very quickly.

   - 1. Most users would have no hope of using this system.

   (h) I found the system very cumbersome to use.

   - 1. Now that I understand it I think it works fairly well.

   (i) I felt very confident using the system.

- 5. Now that I understand the system I would agree.

(j) I needed to learn a lot of things before I could get going with this system.

- 4. This is true, the concept of certificates on a person-by-person level is new to me.

8. Total Score

   - 67.5, which is just below a C.

9. Now that you know about secure email technology, will you continue using it in the future? Why or why not?

   - I think that the biggest problem in my social circle would be adoption. If the process was similar to PGP email encryption I think I would have a much higher chance at success.