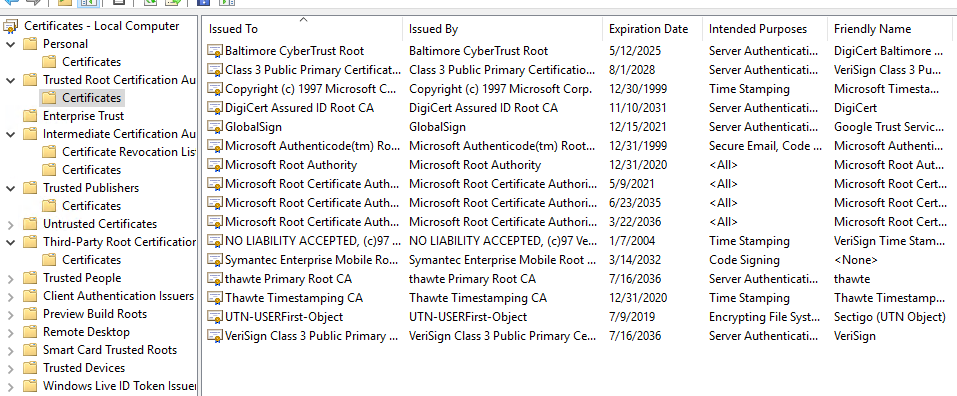
**CIS 313 – Cryptography – Digital Certificates Exercise**

**Name: James Chad Ballay**

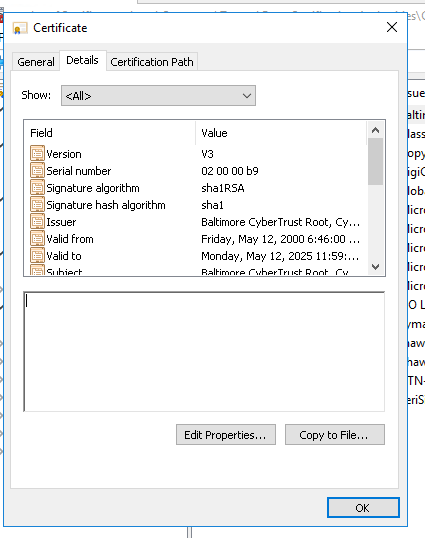
***System Certificates Overview***

Spun up a Windows Server 2016 in Gcloud. Standard issue VM.

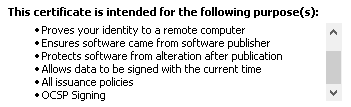


***OS Certificates***

**Baltimore CyberTrust Root**

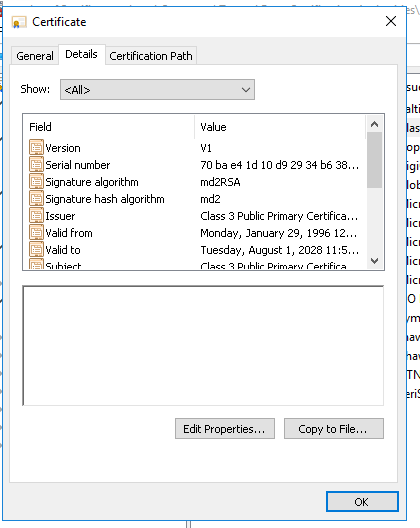


Algorithm is using SHA-1 RSA. I am surprised that it is good for 25 years.

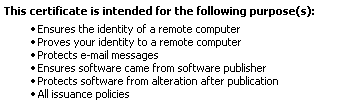


The write up about the history of Baltimore Cybertrust reads like a veritable who’s who of tech/communication companies. Verizon, PWC, GTE <https://en.wikipedia.org/wiki/CyberTrust> I trust theis cert only because Microsoft decided to trust them. I may not be smart enough but they probably employee enough smart people to verify them.

**Verisign Class 3 Public Primary Certificate**

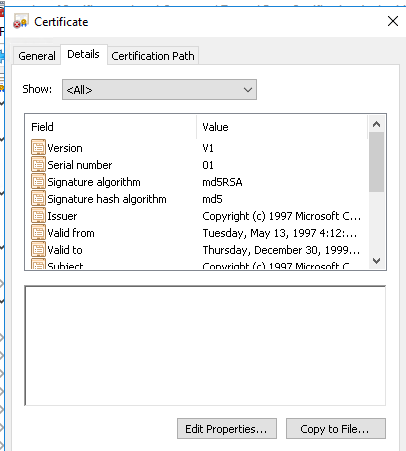


Algorithm is md2RSA. Again I’m surprised at how long this cert is good for. The cert has been around long enough that it’s old enough to drink.



Verisign probably is one of the key players in CA business so if they are comprimised then we’ve got big issues. <https://en.wikipedia.org/wiki/Verisign> Again, I don’t know enough to critque their inclusion but if they were trusted with the .gov, .edu, etc... TLD’s they probably are doing many things correctly.

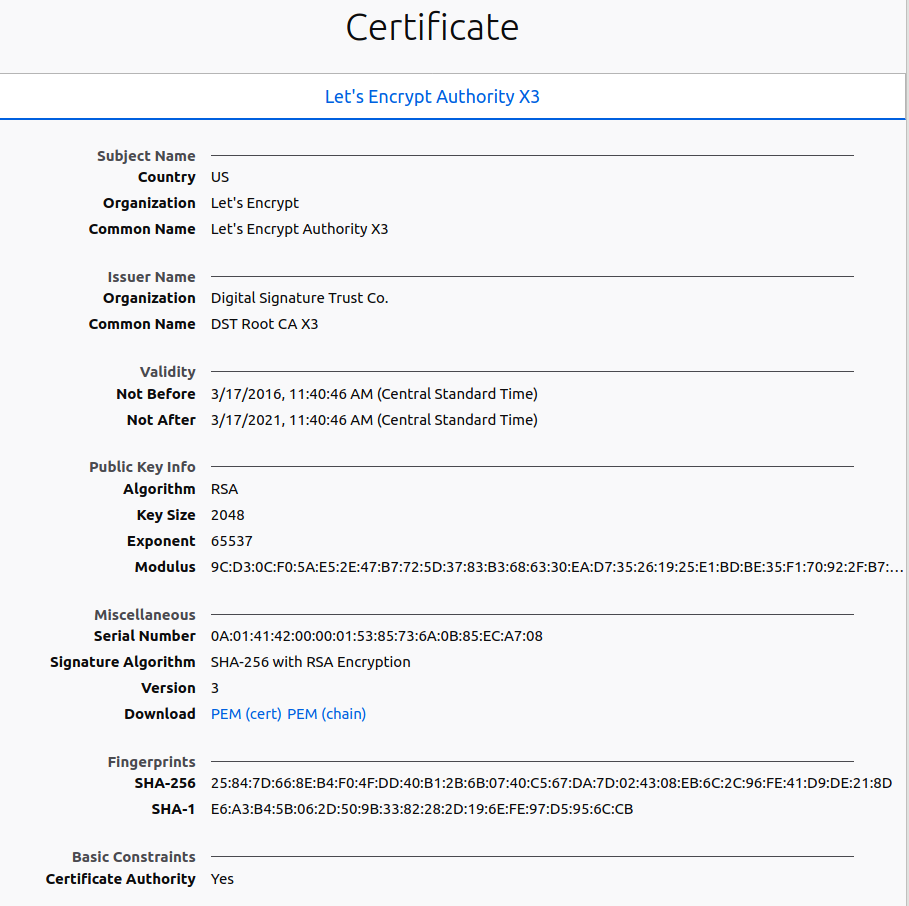
**Microsoft Timestamp Root**



Algorithm is md5RSA. Reason I selected this was because it caught my eye. It was only valid for a little over two years and expired in 1999. Digging into it, Microsoft recommends keeping it around as part of legacy system requirements. All the more reason to upgrade off of XP and Server2003. (<https://support.microsoft.com/en-au/help/293781/trusted-root-certificates-that-are-required-by-windows-server-2008-r2>) Similarly, to the statement that no one has ever been fired for buying IBM, I would say err on the side of caution and be ok with them being there. Microsoft recommended them for a reason to be kept.

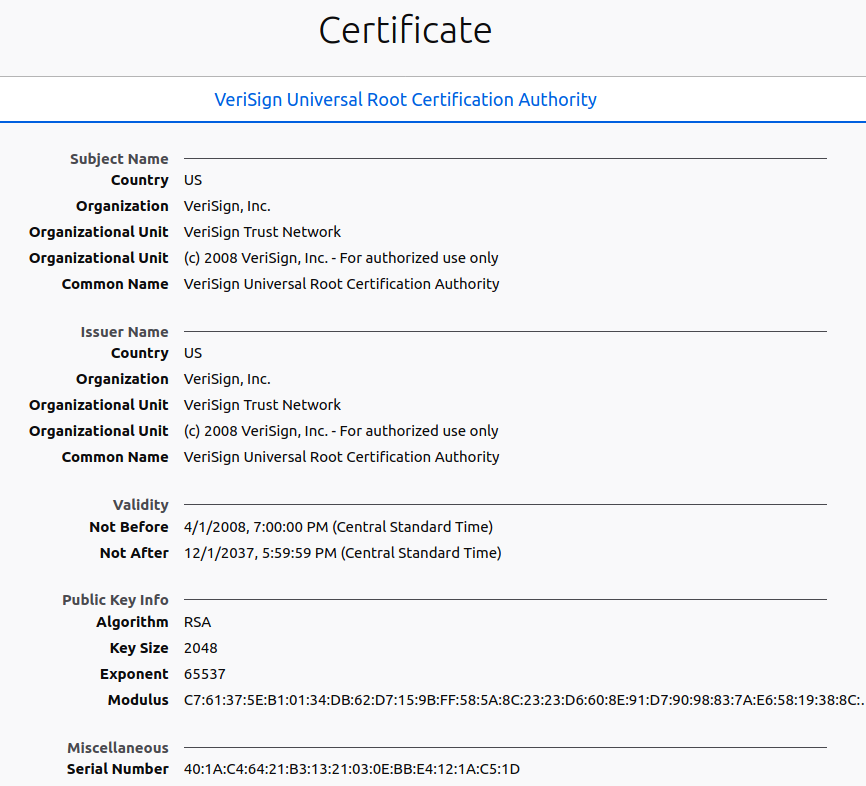
***Web Browser Certificates***

**Let’s Encrypt Authority X3**



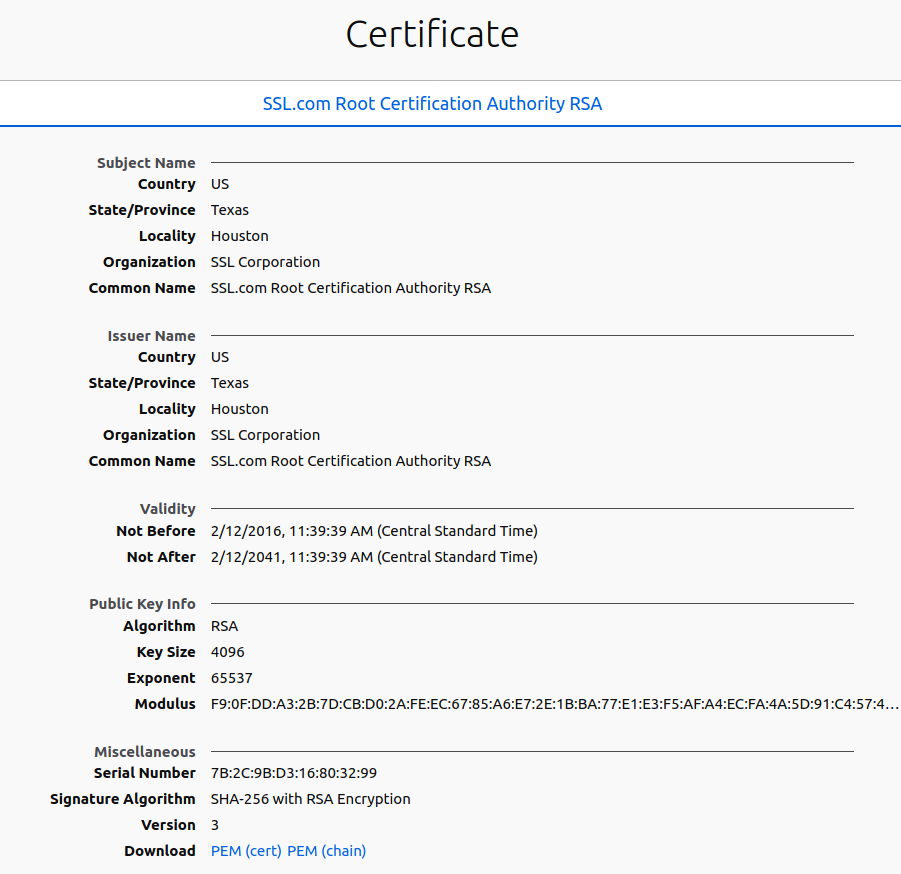
Rsa with a 2048 key size. Signature is SHA-256. Can be used for Digital Signature, Certificate Signing, & CRL Signing. Good for 5 years only. I trust them mainly due to the stated goals of the project and having the EFF stamp of approval.

**VeriSign Universal Root CA**



Rsa with 2048 key size. Signature is SHA-256. This one differs from Let’s Encrypt on the duration. It’s valid all the way until 2037. It also differs on what it can be used for. No digital signage, only Certificate Signing and CRL Signing. Without not a bit of shame, the trust I extend to this is mainly due to the name brand recognition. I honestly don’t know if they really are the bee’s knees but people I trust to be smart are trusting of them. Firefox has had several lines in the sand about privacy so I feel their goals would align with my own. If A == B and B == C then A == C....

**SSL.com Root CA**



Rsa with 4096 key size. Signature is SHA-256. What caught my eye was the larger key size as well as the expiration date being out to 2041. The cert has an active lifespan of 35 years. That seems like an odd numbered time frame. As for trusting them.... I chose this one since it seemed like a generically named cert and I was curious about the providence of it. After a bit of googling, I cam across a few webhost forums that absolutely trashed this company. From deceptive practices to just all around poor service. Admittedly nothing of this was around the actual security of their products but it certainly makes me wonder around the quality they exercise in all aspects of their business.