Andrew Rochford

AIST 4720

03/24/24

Lab 5

1. ID 4 certificate authorities currently operating on the Web who sell certificates signed by their CA. Give links for each and a brief description of their service offerings.
   1. Let’s encrypt
      1. <https://letsencrypt.org>
         1. They offer 2048-bit encryption with free certificates that are instantly available but only offer DV, SAN, and UC certificates that are compatible with most major browsers and devices but not all of them
   2. Comodo
      1. <https://ssl.comodoca.com>
         1. Offers great encryption options and offers premium SSL certificates with warranties. They also offer DV, wildcard, and EV certificates
   3. Digicert
      1. <https://www.digicert.com/campaign/trust-lifecycle-manager?mkwid=_pcrid__pdv_c_pmt__pkw__slid__product__pgrid__ptaid_&gad_source=1&gclid=Cj0KCQjw-_mvBhDwARIsAA-Q0Q6_w_iiSX2X6g3W3obrrdezfSwqPyHs4JEQ9VIq2ZlVA4NnDC-TrhIaAnDAEALw_wcB>
         1. Also offers a wide range of encryption options and offers five types of certificates; SSL plus, EV, multi-domain, and wildcard plus. They work with all major browsers and mobile devices
   4. GeoTrust
      1. <https://www.geotrust.com>
         1. Globally recognized as a TLS/SSL certificate seller and powered by digicert. Offers encryption and hands on support for businesses and private consumers
2. Who is the CA? What is the URL for the CA's website?
   1. GlobalSign
   2. https://support.globalsign.com/ca-certificates/root-certificates/globalsign-root-certificates
3. What signature hash was used? Link to the standard for this hash on the web (hint: it's published by NIST).
   1. SHA256
   2. https://datatracker.ietf.org/doc/html/rfc6234
4. What version of TLS is used? Link to the request for comment (RFC) document that

established it. (hint: RFCs are published by the Internet Engineering Task Force)

1. 1.2
2. https://datatracker.ietf.org/doc/html/rfc5246
3. What other versions of TLS exist? Would they be OK to be used for this certificate?
   1. 1.0 and 1.1
   2. In my opinion they wouldn’t be okay to be used for this certificate purely based on the fact that they are no longer considered secure
4. What does ECDHE\_RSA mean?
   1. It’s an algorithm used in cryptography so parties are able to communicate safely without exchanging keys
5. What does "with X25519" mean? Link to the RFC used to describe it.
   1. It’s an algorithm in cryptography used for key exchange and is used by most major web browsers
   2. https://datatracker.ietf.org/doc/html/rfc7748
6. What does AES\_128\_GCM mean? Link to the standard published by NIST.
   1. Type of encryption (128-bit) used to protect a user’s data as a block cipher.
   2. <https://www.rfc-editor.org/rfc/rfc3826.html>
7. There is no certificate
8. No hash
9. It’s the same type of encryption but it’s based off 256 bits rather than 128

A screenshot of a computer

Description automatically generated