Trinity Bissahoyo
COSC 483
Dr. Ruoti
October 25, 2025

TLS Project

1. Netflix

Subject	www.netflix.com
Common/ Alternative Names	www.netflix.com, account.netflix.com, ca.netflix.com, netflix.ca, netflix.com, signup.netflix.com, www.netflix.ca, www1.netflix.com, www2.netflix.com, www3.netflix.com, develop-stage.netflix.com, release-stage.netflix.com, www.netflix.com, tv.netflix.com, embed.develop-stage.netflix.com, embed.release-stage.netflix.co
Validity Period	Fri, 13 Dec 2024 - Tue, 13 Jan 2026
Cryptographic Key	RSA 2048 bits (e 65537)
Certificate Chain	Issuer: DigiCert Secure Site ECC CA-1 AIA: http://cacerts.digicert.com/DigiCertSecureSiteECCCA-1.crt
Authentication Algorithm	SHA256withRSA
Symmetric Key (Algorithm, Size, Mode)	AES_128_GCM
Hashing Algorithm	SHA256
Cryptographic Guarantees	Confidentiality, integrity, authentication
Other Properties	1. Support secure renegotiation 2. Has strict transport security 3. Supported TLS 1.0 and 1.1

2. Roblox

Subject	roblox.com
Common/ Alternative Names	roblox.com, *.roblox.com
Validity Period	Mon, 02 Jun 2025 - Tue, 02 Jun 2026
Cryptographic Key	RSA 2048 bits (e 65537)
Certificate Chain	Issuer: Sectigo Public Server Authentication CA OV R36 AIA: http://crt.sectigo.com/SectigoPublicServerAuthenticationCAOVR36.crt
Authentication Algorithm	SHA384withRSA
Symmetric Key (Algorithm, Size, Mode)	AES_128_GCM
Hashing Algorithm	SHA384
Cryptographic Guarantees	Confidentiality, integrity, authentication, forward secrecy
Other Properties	1. Has secure renegotiation 2. Has strict transport security 3. OSCP stapling

3. Star Stables

Subject	*.starstable.com

Common/ Alternative Names	*.starstable.com, prod.starstable.com, *.prod.starstable.com, starstable.com
Validity Period	Mon, 08 Sep 2026 - Wed, 07 Oct 2026
Cryptographic Key	RSA 2048 bits (e 65537)
Certificate Chain	Issuer: Amazon RSA 2048 M03 AIA: AIA: http://crt.r2m03.amazontrust.com/r2m03.cer
Authentication Algorithm	SHA256withRSA
Symmetric Key (Algorithm, Size, Mode)	AES_128_GCM
Hashing Algorithm	SHA256
Cryptographic Guarantees	Confidentiality, integrity, authentication, forward secrecy
Other Properties	1. Has secure renegotiation 2. Has strict transport security 3. Downgrade attack prevention

4. Shien

Subject	shien.com
Common/ Alternative Names	shien.com, *.shien.com, shien.com
Validity Period	Tue, 02 Sep 2025 03:26:01 UTC - Mon, 01 Dec 2025 03:26:00 UTC
Cryptographic Key	RSA 2048 (e 65537)
Certificate Chain	Issuer: R13 AIA: http://r13.i.lencr.org/
Authentication Algorithm	SHA256withRSA
Symmetric Key (Algorithm, Size, Mode)	AES_128_GCM
Hashing Algorithm	SHA256
Cryptographic Guarantees	Confidentiality, integrity, authentication
Other Properties	1. Supports secure renegotiation 2. Has forward secrecy with some browsers 3. Has downgrade attack prevention

5. Amazon

Subject	*.peg.a2z.com
Common/ Alternative Names	*.peg.a2z.com, amazon.co.uk uedata.amazon.co.uk www.amazon.co.uk origin-www.amazon.co.uk *.peg.a2z.com amazon.com amzn.com uedata.amazon.com us.amazon.com www.amazon.com www.amzn.com corporate.amazon.com buybox.amazon.com iphone.amazon.com yp.amazon.com home.amazon.com origin-www.amazon.com origin2-www.amazon.com buckeye-retail-website.amazon.com huddles.amazon.com amazon.de www.amazon.de origin-www.amazon.de amazon.co.jp amazon.jp www.amazon.jp www.amazon.co.jp origin-www.amazon.co.jp *.aa.peg.a2z.com *.ab.peg.a2z.com *.ac.peg.a2z.com origin-www.amazon.com.au www.amazon.com.au *.bz.peg.a2z.com amazon.com.au origin2-www.amazon.co.jp edgeflow.aero.4d5ad1d2b-frontier.amazon.co.jp edgeflow.aero.04f01a85e-frontier.amazon.com.au edgeflow.aero.47cf2c8c9-frontier.amazon.com edgeflow.aero.abe2c2f23-frontier.amazon.de edgeflow.aero.bfbdc3ca1-frontier.amazon.co.uk edgeflow-dp.aero.4d5ad1d2b-frontier.amazon.co.jp edgeflow-dp.aero.04f01a85e-frontier.amazon.com.au edgeflow-dp.aero.47cf2c8c9-

	frontier.amazon.com edgeflow-dp.aero.bfbdc3ca1-frontier.amazon.co.uk edgeflow-dp.aero.abe2c2f23-frontier.amazon.de
Validity Period	Thu, 26 Jun 2025 - Fri, 19 Jun 2026
Cryptographic Key	RSA 2048 bits (e 65537
Certificate Chain	Issuer: DigiCert Global CA G2 AIA: http://cacerts.digicert.com/DigiCertGlobalCAG2.crt
Authentication Algorithm	SHA256withRSA
Symmetric Key (Algorithm, Size, Mode)	AES_128_GCM
Hashing Algorithm	SHA256
Cryptographic Guarantees	Confidentiality, integrity, authentication
Other Properties	1. Has OCSP stapling 2. Has SSL 2 handshake compatibility 3. Only forward secrecy with modern browsers

6. Reddit

Subject	*.reddit.com
Common/ Alternative Names	*.reddit.com, reddit.com
Validity Period	Sat, 12 Jul 2025 - Wed, 07 Jan 2026
Cryptographic Key	RSA 2048 bits (e 65537)
Certificate Chain	Issuer: DigiCert Global G2 TLS RSA SHA256 2020 CA1 AIA: AIA: http://cacerts.digicert.com/DigiCertGlobalG2TLSRSASHA2562020CA1-1.crt
Authentication Algorithm	SHA256withRSA
Symmetric Key (Algorithm, Size, Mode)	AES_128_GCM
Hashing Algorithm	SHA256
Cryptographic Guarantees	Confidentiality, integrity, authentication forward secrecy
Other Properties	1. Has downgrade attack prevention 2. OSCP stapling 3. HSTS preloading

7. Weather

Subject	weather.com
Common/ Alternative Names	weather.com, weather.com *.cogads.weather.com *.dev.cogads.weather.com *.qa.cogads.weather.com *.w-x.co *.weather.com *.wsi.com *.wunderground.com *.wxug.com crazimals.com dev.theweathercompany.info stage.theweathercompany.info stg.crazimals.com theweathercompany.info w-x.co weatherunderground.com wsi.com wund.com wunderground.com wundermap.com wunderstation.com www.crazimals.com www.weather.com wxug.com
Validity Period	Fri, 14 Feb 2025 - Sat, 14 Feb 2026
Cryptographic Key	EC 256 bits
Certificate Chain	Issuer: DigiCert TLS Hybrid ECC SHA384 2020 CA1 AIA: http://cacerts.digicert.com/DigiCertTLSHybridECCSHA3842020CA1-1.crt

Authentication Algorithm	SHA384withECDSA
Symmetric Key (Algorithm, Size, Mode)	AES_256_GCM
Hashing Algorithm	SHA384
Cryptographic Guarantees	Confidentiality, integrity, authentication, forward secrecy
Other Properties	1. Has client-initiated renegotiation 2. OCSP stapling 3. Has strict transport security

8. Typing.com

Subject	keybr.com
Common/ Alternative Names	keybr.com, *.keybr.com
Validity Period	Thu, 18 Sep 2025 - Wed, 17 Dec 2025
Cryptographic Key	RSA 2048 bits (e 65537)
Certificate Chain	Issuer: WR1 AIA: http://i.pki.goog/wr1.crt
Authentication Algorithm	SHA256withRSA
Symmetric Key (Algorithm, Size, Mode)	AES_128_GCM
Hashing Algorithm	SHA256
Cryptographic Guarantees	Confidentiality, integrity, authentication, forward secrecy
Other Properties	1. Site only works in browsers with SNI support 2. Has downgrade attack prevention 3. OCSP stapling

9. Grubhub

Subject	*.grubhub.com
Common/ Alternative Names	*.grubhub.com, grubhub.com
Validity Period	Thu, 23 Oct 2025 - Tue, 24 Nov 2026
Cryptographic Key	RSA 2048 bits (e 65537)
Certificate Chain	Issuer: GlobalSign Atlas R3 DV TLS CA 2025 Q4 AIA: http://secure.globalsign.com/cacert/gsatlasr3dvtlsca2025q4.crt
Authentication Algorithm	SHA256withRSA
Symmetric Key (Algorithm, Size, Mode)	AES_128_GCM
Hashing Algorithm	SHA256
Cryptographic Guarantees	Confidentiality, integrity, authentication, forward secrecy
Other Properties	1. Has OCSP stapling 2. Has strict transport security 3. Has session resumption

10. Regal

Subject	regmovies.com
Common/ Alternative Names	regmovies.com, *.regmovies.com
Validity Period	Mon, 22 Sep 2025 - Sun, 21 Dec 2025

Cryptographic Key	EC 256 bits
Certificate Chain	Issuer: WE1 AIA: http://i.pki.goog/we1.crt
Authentication Algorithm	SHA256withECDSA
Symmetric Key (Algorithm, Size, Mode)	AES_128_GCM
Hashing Algorithm	SHA256
Cryptographic Guarantees	Confidentiality, integrity, authentication, forward secrecy
Other Properties	1. Has OCSP stapling 2. Has session resumption only for tickets 3. Has strict transport security

Summary

Some interesting differences among the websites is they had different length in their validity periods. The site also varied in whether they had DNS Certificate Authority Authorization and OCSP stapling. Another difference is the number of alternative names some of the sites have. I assume it is related to specific pages they have (e.g. sign up, payment center, etc) and platforms the websites can be viewed on. Lastly, the issuers among their certificates were different but I did see some use DigiCert. Most of the sites have forward secrecy but a few only had it for some browsers. They all, also prioritized the same symmetric key using the AES algorithm of 128 bits with mode GCM. Additionally, all but one of the sites used the same authentication and hashing algorithm of SHA 256 or 384 with 2048 RSA keys.

Questions

1. I find it interesting that sites I assume have more traffic have a lower score than sites I assume are less popular. Most of the lower grades were B's due to lacking forward secrecy. My question is, why might these sites lack forward secrecy, or have a lower grade when they have larger resources.
2. Why might a certificate have a validity period less than 5 months, that seems very short?

My report was reviewed by Kayla Stevenson.