SUBJECT / COMMON NAME	VALIDITY PERIOD	KEY TYPE	CERT CHAIN	AUTH ALGO	SYMETRIC ENCRYPTION	HASHING ALGO	CRYPTO GARUNTEES	OTHER PROPERTIES	ALTERNATE NAMES
www.minecraft.net	05/06/25 - 05/01/26	EC 256 bits	Two Certs, No issues. Azure ECC TLS Issuing CA 07 → DigiCert Global Root G3	SHA384 with ECDSA	Prefers AES 256 or 128 GCM, but also supports ChaCha20 and AES 256/128 CBC	SHA384 or 256	Confidentiality, Integrity, Forward Secrecy	Does not support below TLS 1.2, Not Vulnerable to known attacks, Does not support Session resumption (caching)	N/A
store.steampowered.com	08/15/25 - 08/18/26	EC 256 bits	Two Certs, No Issues. DigiCert EV RSA CA G2 → DigiCert Global Root G2	SHA384 with ECDSA	Prefers AES 256 or 128 GCM, but also supports ChaCha20	SHA384 or 256	Confidentiality, Integrity, Forward Secrecy	Does not support weak TLS suites, Displays handshake failures on Safari 8 and older, HSTS is marked as "Too Short"	checkout.steampowered.com
www.firsthorizon.com	05/19/25 - 05/18/26	EC 256 bits	Two Certs, No Issues. DigiCert Global G3 TLS ECC SHA384 2020 CA1 → DigiCert Global Root G3	SHA384 with ECDSA	Prefers AES 256 or 128 GCM, but also supports ChaCha20	SHA384 or 256	Confidentiality, Integrity, Forward Secrecy	A+ Ranking, No DNS CAA, TLS 1.2 Suites are slightly more strict comparatively	www.Capitalbank-firsttennessee.com, www.capitalbank-us.com, www.firsttennessee.com, www.ftb.com
5e.tools	09/27/25 - 12/26/25	RSA 2048 bits	Three Certs, No Issues. WR1 → GTS Root R1	SHA256 with RSA	Prefers AES 256 or 128 GCM, but also supports ChaCha20 and AES 256/128 CBC	SHA384 or 256 Preferred, but also supports SHA1	Confidentiality, Integrity, Forward Secrecy	A+ Ranking, Compatible with a lot of weak TLS 1.2 Suites, Very short validity period	N/A
www.youtube.com	10/01/25 - 12/24/25	EC 256 bits	Three Certs, No Issues. WE2 → GTS Root R4	SHA384 with ECDSA	Prefers AES 256 or 128 GCM, but also supports ChaCha20 and AES 256/128 CBC	SHA384 or 256 Preferred, but also supports SHA1	Confidentiality, Integrity, Forward Secrecy (With modern browsers)	Supports TLS 1.0 and 1.1, Very short validity period, Not vulnerable to known attacks	A lot, mostly referring to google.com and other google services
www.twitch.tv	05/07/25 - 06/08/26	RSA 2048 bits	Two Certs, No Issues. GlobalSign Atlas R3 DV TLS CA 2025 Q2 → GlobalSign	SHA256 with RSA	Prefers AES 256 or 128 GCM, but also supports ChaCha20 and AES 256/128 CBC	SHA384 or 256 Preferred, but also supports SHA1	Confidentiality, Integrity, Forward Secrecy	A+ Ranking, Some weak TLS 1.2 Suites supported, No DNS CAA	N/A
amazon.com	06/26/25 - 06/19/26	RSA 2048 bits	Three Certs, No Issues. DigiCert Global CA G2 → DigiCert Global Root G2	SHA256 with RSA	Prefers AES 256 or 128 GCM, but also supports AES256/128 CBC	SHA384 or 256 Preferred, but also supports SHA1	Confidentiality, Integrity, Forward Secrecy (with modern browsers)	Supports TLS 1.0 and 1.1, Supports a lot of weak TLS 1.2 Suites, No DNS CAA	Like YouTube, amazon.com has a lot of alternate names referring to other amazon services and locations.
myutk.utk.edu	11/19/24 - 12/20/25	RSA 2048 bits	Four Certs, One Issue: Contain Anchor. InCommon RSA Server CA 2 → USERTrust RSA Certification Authority	SHA384 with RSA	Prefers AES 256 or 128 GCM, but accepts a wide variety	Prefers SHA384 or 256	Confidentiality, Integrity, Forward Secrecy	Only supports TLS 1.1, Doesn't have HSTS, No DNS CAA	N/A
reddit.com	07/12/25 - 01/07/26	RSA 2048 bits	Two Certs, No Issues. DigiCert Global G2 TLS RSA SHA256 2020 CA1 → DigiCert Global Root G2	SHA256 with RSA	AES 256 or 128 GCM, but also accepts AES 128 and 256 CBC	SHA256 or 128	Confidentiality, Integrity, Forward Secrecy	A+ Ranking, Doesn't support below TLS 1.2, Supports HSTS	N/A
forum.paradoxplaza.com	09/25/25 - 10/27/26	RSA 2048 bits	Two Certs, No Issues. GlobalSign Atlas R3 DV TLS CA 2025 Q3 → GlobalSign	SHA256 with RSA	AES 256 or 128 GCM, but also accepts AES 128 and 256 CBC	SHA256 and 384 preferred, but supports SHA1	Confidentiality, Integrity, Forward Secrecy	Doesn't support TLS 1.3, No DNS CAA, No HSTS	N/A

Aaron Sparks - TLS Project

Question 2:

I think it is interesting that almost every site I checked with SSLLabs had a ranking of A or better. The only exceptions to this were YouTube and Amazon, which held a B ranking. Overall, almost every site used AES256 GCM and SHA256 as their preferred symmetric encryption and hashing algorithm, although it was intriguing to see SHA1 being used sometimes as well. Most sites used TLS 1.2 and 1.3, with only a few allowing 1.1 and under. Key types were also mostly consistent, with most of the sites using RSA 2048. I also thought it was interesting that even the most niche site I chose (5e.tools) had an A+ ranking on SSLLabs. It seems that a lot of these configurations are standardized, which makes it all the more interesting to me when a site still supports a configuration with something like SHA1.

Question 3:

Why do sites like YouTube and Amazon have such an extensive backlist of supported protocols (like TLS 1.0 and 1.1)? I understand it is probably to allow as much compatibility as possible with older devices, but what would drive Twitch (a YouTube rival owned by Amazon) to be more selective in allowed protocols? I also wonder about how HSTS and DNS CAA works, as it was one thing that seemed to be different between all of the sites. Some had DNS CAA, while others did not. Most had HSTS, but some were marked as being “Too Short”. I would like to know how much these features affect security.

Reviewed by Cayden Hernandez.