Website	https://echo360.com/pointsolutions-login/	https://utk.instructure.com/	https://myutk.utk.edu/	https://www.amazon.com/	https://www.youtube.com/
Subject	echo360.com	cluster95.canvas-user-content.com	*.utk.edu	www.amazon.com	*.google.com
Common Name	echo360.com	cluster95.canvas-user-content.com	*.utk.edu	www.amazon.com	*.google.com
Alternative Names	echo360.com	cluster95.canvas-user-content.com *.instructure.com instructure.com canvaslms.com *.canvaslms.com *.cluster95.canvas-user-content.com	*.utk.edu	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 buckeye-retail-website.amazon.com huddles.amazon.com p-nt-www-amazon-com-kalias.amazon.com p-yo-www-amazon-com-kalias.amazon.com p-y3-www-amazon-com-kalias.amazon.com yellowpages.amazon.com www.m.amazon.com www.cdn.amazon.com test-www.amazon.com mp3recs.amazon.com konrad-test.amazon.com shop.business.amazon.com	*.google.com *.appengine.google.com *.bdn.dev *.origin-test.bdn.dev *.cloud.google.com *.crowdsource.google.com *.datacompute.google.com *.google.ca *.google.cl *.google.co.in *.google.co.jp *.google.co.uk *.google.com.ar *.google.com.au *.google.com.br *.google.com.co *.google.com.mx *.google.com.tr *.google.com.vn *.google.de *.google.es *.google.fr *.google.hu *.google.it *.google.nl *.google.pl *.google.pt *.googleapis.cn *.googlevideo.com *.gstatic.cn *.gstatic-cn.com googlecnapps.cn *.googlecnapps.cn googleapps-cn.com *.googleapps-cn.com gkecnapps.cn *.gkecnapps.cn googledownloads.cn *.googledownloads.cn recaptcha.net.cn *.recaptcha.net.cn recaptcha-cn.net *.recaptcha-cn.net widevine.cn *.widevine.cn ampproject.org.cn *.ampproject.org.cn ampproject.net.cn *.ampproject.net.cn google-analytics-cn.com *.google-analytics-cn.com googleadservices-cn.com *.googleadservices-cn.com googlevads-cn.com *.googlevads-cn.com googleapis-cn.com *.googleapis-cn.com googleoptimize-cn.com *.googleoptimize-cn.com doubleclick-cn.net *.doubleclick-cn.net *.fls.doubleclick-cn.net *.g.doubleclick-cn.net doubleclick.cn *.doubleclick.cn *.fls.doubleclick.cn *.g.doubleclick.cn dartsearch-cn.net *.dartsearch-cn.net googletraveladservices-cn.com *.googletraveladservices-cn.com googletagservices-cn.com *.googletagservices-cn.com googletagmanager-cn.com *.googletagmanager-cn.com googlesyndication-cn.com *.googlesyndication-cn.com *.safeframe.googlesyndication-cn.com app-measurement-cn.com *.app-measurement-cn.com gvt1-cn.com *.gvt1-cn.com gvt2-cn.com *.gvt2-cn.com 2mdn-cn.net *.2mdn-cn.net googleflights-cn.net *.googleflights-cn.net admob-cn.com *.admob-cn.com *.gemini.cloud.google.com googlesandbox-cn.com *.googlesandbox-cn.com *.safenup.googlesandbox-cn.com *.gstatic.com *.metric.gstatic.com *.gvt1.com *.gcpcdn.gvt1.com *.gvt2.com *.gcp.gvt2.com *.url.google.com *.youtube-nocookie.com *.ytimg.com ai.android android.com *.android.com *.flash.android.com g.cn *.g.cn g.co *.g.co goo.gl www.goo.gl google-analytics.com *.google-analytics.com google.com googlecommerce.com *.googlecommerce.com ggpht.cn *.ggpht.cn urchin.com *.urchin.com youtu.be youtube.com *.youtube.com music.youtube.com *.music.youtube.com youtubeeducation.com *.youtubeeducation.com youtubekids.com *.youtubekids.com yt.be *.yt.be android.clients.google.com *.android.google.cn *.chrome.google.cn *.developers.google.cn *.aistudio.google.com
Validity Period	Valid from: Thu, 11 Sep 2025 21:41:05 UTC Valid until: Wed, 10 Dec 2025 21:41:04 UTC	Valid from Mon, 02 Jun 2025 00:00:00 UTC Valid until Wed, 01 Jul 2026 23:59:59 UTC	Valid fromTue, 19 Nov 2024 00:00:00 UTC Valid untilSat, 20 Dec 2025 23:59:59 UTC	Valid fromFri, 24 Oct 2025 00:00:00 UTC Valid untilTue, 20 Oct 2026 23:59:59 UTC	Valid fromWed, 01 Oct 2025 14:32:25 UTC Valid untilWed, 24 Dec 2025 14:32:24 UTC
Cryptographic Key Type	RSA 2048 bits (e 65537)	RSA 2048 bits (e 65537)	RSA 2048 bits (e 65537)	RSA 2048 bits (e 65537)	EC 256 bits
Certificate Chain	1 Sent by server echo360.com Fingerprint SHA256: bd93bfbb9e387e78b752947aff75a6c231b7a79c3c6069f9046c8ae86763fe6b Pin SHA256: /9Lva6KgloEKbpEtp6zlV/PYKendOgnZ1m58IMkCrCo= RSA 2048 bits (e 65537) / SHA256withRSA 2 Sent by server R12 Fingerprint SHA256: 131fce7784016899a5a00203a9efc80f18ebbd75580717edc1553580930836ec Pin SHA256: kZwN96eHtZftBWrOZUsd6cA4es80n3NzSk/XtYz2EqQ= RSA 2048 bits (e 65537) / SHA256withRSA 3 In trust store ISRG Root X1 Self-signed Fingerprint SHA256: 96bcec06264976f37460779acf28c5a7cfe8a3c0aae11a8ffcee05c0bddf08c6 Pin SHA256: C5+lpZ7tcVwmwQIMcRtPbsQtWLABXhQzejna0wHFr8M= RSA 4096 bits (e 65537) / SHA256withRSA	1 Sent by server cluster95.canvas-user-content.com Fingerprint SHA256: 695481c07bcb546070d31b2923b0464c67565c954ca9403d5d2f435b231feb02 Pin SHA256: 6k+M8oSbeZ6FyRqHjRXtPmJM5gmDXmyc30orApl6KW4= RSA 2048 bits (e 65537) / SHA256withRSA 2 Sent by server Amazon RSA 2048 M03 Fingerprint SHA256: bf8a69027bcc8d2d42a6e6d25bdd4873f6a34b8f90edf07e86c5d6916da0b933 Pin SHA256: vxRon/El5Kul4vx5ey1DgmsYmRY0nDd5Cg4GfJ8S+bg= RSA 2048 bits (e 65537) / SHA256withRSA 3 In trust store Amazon Root CA 1 Self-signed Fingerprint SHA256: 8ecde6884f3d87b1125ba31ac3fcb13d7016de7f57cc904fe1cb97c6ae98196e Pin SHA256: ++MBgDH5WGvL9Bcn5Be30cRcL0f5O+NyoXuWtQdX1aI= RSA 2048 bits (e 65537) / SHA256withRSA	1Sent by server*.utk.edu Fingerprint SHA256: e5f5c9497d7855680c0c53c99039e5062f3822d5eb640678bb7b92d9a18a1891 Pin SHA256: xxe58PgdFUTqUinmzZCR2d355Dza4mdbatE6TWF7lac= RSA 2048 bits (e 65537) / SHA384withRSA 2Sent by serverInCommon RSA Server CA 2 Fingerprint SHA256: 87e01cc4dd0c9d92a3dbd49092ff13f9cd387445cdc57e5b984e1b7721b5b029 Pin SHA256: nIUvrOVzCyKOqY+U4sofEeIMk94Dt/WuMgaesi8NITk= RSA 3072 bits (e 65537) / SHA384withRSA 3In trust storeUSERTrust RSA Certification Authority Self-signed Fingerprint SHA256: e793c9b02fd8aa13e21c31228accb08119643b749c898964b1746d46c3d4cbd2 Pin SHA256: x4QzPSC810K5/cMjb05Qm4k3Bw5zBn4lTdO/nEW/Td4= RSA 4096 bits (e 65537) / SHA384withRSA	1Sent by serverwww.amazon.com Fingerprint SHA256: c00c1e1930e03744e6f74ee86d8caa3ed2fd350fe3e8430539d7c39df75769e3 Pin SHA256: 9Ld5gTt0ktHUUaWQXdYC5L5X1vQLyB3MFjTN0S+4q2Y= RSA 2048 bits (e 65537) / SHA256withRSA 2Sent by serverDigiCert Global CA G2 Fingerprint SHA256: 8fac576439c9fd3ef153b51f9edd0d381b5df7b87559cebeca04297dd44a639b Pin SHA256: njN4rRG+22dNXAi+yb8e3UMypgzPUPHlv4+foULwl1g= RSA 2048 bits (e 65537) / SHA256withRSA 3In trust storeDigiCert Global Root G2 Self-signed Fingerprint SHA256: cb3ccbb76031e5e0138f8dd39a23f9de47ffc35e43c1144cea27d46a5ab1cb5f Pin SHA256: i7WTqTvh0OioIruIfFR4kMPnBqrS2rdiVPl/s2uC/CY= RSA 2048 bits (e 65537) / SHA256withRSA	1Sent by server*.google.com Fingerprint SHA256: d2927dd45d78bc69fc3273d816ef3a373a0e0c2d504ffe517ef7ea9356b98c1d Pin SHA256: nq2DWadg5ObO8jrElkHbTHRDKaPpnOUx5Qr5mduFUf0= EC 256 bits / SHA256withECDSA 2Sent by serverWE2 Fingerprint SHA256: 9c3f2fd11c57d7c649ad5a0932c0f0d29756f6a0a1c74c43e1e89a62d64cd320 Pin SHA256: vh78KSg1Ry4NaqGDV10w/cTb9VH3BQUZoCWNa93W/EY= EC 256 bits / SHA384withECDSA 3In trust storeGTS Root R4 Self-signed Fingerprint SHA256: 349dfa4058c5e263123b398ae795573c4e1313c83fe68f93556cd5e8031b3c7d Pin SHA256: mEflZT5enoR1FuXLgYYGqnVEoZvmf9c2bVBpiOjYQ0c= EC 384 bits / SHA384withECDSA
Authentication Algorithm	RSA	RSA	RSA	RSA	ECDSA
Sym Encryption Algorithm	AES_128_GCM	AES_128_GCM	AES_256_GCM	AES_128_GCM	AES_128_GCM
Hashing Algorithm	SHA256	SHA256	SHA384	SHA256	SHA256
Cryptographic Guarantees	Confidentiality, Integrity, and Forward Secrecy	Confidentiality, Integrity, and Forward Secrecy	Confidentiality, Integrity, and Forward Secrecy	Confidentiality, Integrity, and Forward Secrecy	Confidentiality, Integrity, and Forward Secrecy
Trusted	Yes Mozilla Apple Android Java Windows	Yes Mozilla Apple Android Java Windows	Yes Mozilla Apple Android Java Windows	Yes Mozilla Apple Android Java Windows	Yes Mozilla Apple Android Java Windows
Protocols	TLS 1.3 and TLS 1.2	TLS 1.3 and TLS 1.2	TLS 1.2	TLS 1.3, TLS 1.2, TLS 1.1, TLS 1.0	TLS 1.3, TLS 1.2, TLS 1.1, TLS 1.0
Issuer	R12 AIA: http://r12.i.lencr.org/	Amazon RSA 2048 M03 AIA: http://crt.r2m03.amazontrust.com/r2m03.cer	InCommon RSA Server CA 2 AIA: http://crt.sectigo.com/InCommonRSAServerCA2.crt	DigiCert Global CA G2 AIA: http://cacerts.digicert.com/DigiCertGlobalCAG2.crt	WE2 AIA: http://i.pki.goog/we2.crt
Rating	A	A+	A-	B	**B**

Website	https://www.dndbeyond.com/	https://github.com/	https://www.curseforge.com/	https://www.wikipedia.org/	https://www.walmart.com/
Subject	dndbeyond.com	github.com	curseforge.com	*.wikipedia.org	www.walmart.com
Common Name	dndbeyond.com	github.com	curseforge.com	*.wikipedia.org	www.walmart.com
Alternative Names	dndbeyond.com *.avrae.io *.dndbeyond.com avrae.io danddbeyond.com ddb.ac dndhero.com dragonbeyond.com dungeonbeyond.com tabletophero.com *.danddbeyond.com *.ddb.ac *.dndhero.com *.dragonbeyond.com *.dungeonbeyond.com *.tabletophero.com *.dndadventures.com dndadventures.com *.dev.playspace.dndbeyond.com *.prod.playspace.dndbeyond.com	github.com www.github.com	curseforge.com *.curseforge.com	*.m.mediawiki.org *.m.wikibooks.org *.m.wikidata.org *.m.wikimedia.org *.m.wikinews.org *.m.wikipedia.org *.m.wikiquote.org *.m.wikisource.org *.m.wikiversity.org *.m.wikivoyage.org *.m.wiktionary.org *.mediawiki.org *.planet.wikimedia.org *.wikibooks.org *.wikidata.org *.wikifunctions.org *.wikimedia.org *.wikimediafoundation.org *.wikinews.org *.wikipedia.org *.wikiquote.org *.wikisource.org *.wikiversity.org *.wikivoyage.org *.wiktionary.org *.wmfusercontent.org mediawiki.org w.wiki wikibooks.org wikidata.org wikifunctions.org wikimedia.org wikimediafoundation.org wikinews.org wikipedia.org wikiquote.org wikisource.org wikiversity.org wikivoyage.org wiktionary.org wmfusercontent.org	www.walmart.com beta.walmart.com grocery.walmart.com walmart.pharmacy walmartspecialty.pharmacy www.wal-mart.com walmart.com
Validity Period	Valid fromMon, 24 Feb 2025 16:34:21 UTC Valid untilSat, 28 Mar 2026 16:34:20 UTC	Valid fromMon, 10 Mar 2025 00:00:00 UTC Valid untilTue, 10 Mar 2026 23:59:59 UTC	Valid fromTue, 16 Sep 2025 14:36:52 UTC Valid untilMon, 15 Dec 2025 13:15:55 UTC	Valid fromThu, 09 Oct 2025 23:02:03 UTC Valid untilWed, 07 Jan 2026 23:02:02 UTC	Valid fromMon, 24 Feb 2025 17:02:01 UTC Valid untilSat, 28 Mar 2026 17:02:00 UTC
Cryptographic Key Type	RSA 2048 bits (e 65537)	RSA 4096 bits (e 65537)	RSA 2048 bits (e 65537)	EC 256 bits	EC 256 bits
Certificate Chain	1Sent by serverdndbeyond.com Fingerprint SHA256: 1174d11b67cf0ab958fda48ecc0560377f3b0e9539113c375a00ae24b2dccb5f Pin SHA256: xVvotlqF0lvBMgAkU+PUyNAHFC/3W23SAgbV9B/bavw= RSA 2048 bits (e 65537) / SHA256withRSA 2Sent by serverGlobalSign Atlas R3 DV TLS CA 2025 Q1 Fingerprint SHA256: 0bb2a52840f1de1040118276872a63f0986e42b15d3a1d7779f1f7757c992adc Pin SHA256: Qf3aXTojf9mFnBEx/Wp5Be0znuULC7BvBKWN6271010= RSA 2048 bits (e 65537) / SHA256withRSA 3In trust storeGlobalSign Self-signed Fingerprint SHA256: cbb522d7b7f127ad6a0113865bdf1cd4102e7d0759af635a7cf4720dc963c53b Pin SHA256: cGuxAXyFXFkWm61cF4HPWX8S0srS9j0aSqN0k4AP+4A= RSA 2048 bits (e 65537) / SHA256withRSA	1Sent by servergithub.com Fingerprint SHA256: 6157d9d5f6066c0085aa9e487f3ae7c94a6778b8f76ddca9c8539e730386f45f Pin SHA256: 1jXwPJjk3SAhvkPxGFQ0VP8KMMN1FEFUNBOz2uaHHGk= RSA 4096 bits (e 65537) / SHA256withRSA 2Sent by serverSectigo RSA Domain Validation Secure Server CA Fingerprint SHA256: 7fa4ff68ec04a99d7528d5085f94907f4d1dd1c5381bacdc832ed5c960214676 Pin SHA256: 4a6cPehI7OG6cuDZka5NDZ7FR8a60d3auda+sKfg4Ng= RSA 2048 bits (e 65537) / SHA384withRSA 3In trust storeUSERTrust RSA Certification Authority Self-signed Fingerprint SHA256: e793c9b02fd8aa13e21c31228accb08119643b749c898964b1746d46c3d4cbd2 Pin SHA256: x4QzPSC810K5/cMjb05Qm4k3Bw5zBn4lTdO/nEW/Td4= RSA 4096 bits (e 65537) / SHA384withRSA	1Sent by servercurseforge.com Fingerprint SHA256: 96d10431b1e686ed122ecb453f7e1276d9c5d118c6323f1d7deec7fa3758ede3 Pin SHA256: sRle5BXqtSCbKupI+XHfQoE4Sq3eprpabn1OG5ZenIc= RSA 2048 bits (e 65537) / SHA256withRSA 2Sent by serverWR1 Fingerprint SHA256: b10b6f00e609509e8700f6d34687a2bfce38ea05a8fdf1cdc40c3a2a0d0d0e45 Pin SHA256: yDu9og255NN5GEf+Bwa9rTrqFQ0EydZ0r1FCh9TdAW4= RSA 2048 bits (e 65537) / SHA256withRSA 3In trust storeGTS Root R1 Self-signed Fingerprint SHA256: d947432abde7b7fa90fc2e6b59101b1280e0e1c7e4e40fa3c6887fff57a7f4cf Pin SHA256: hxqRlPTu1bMS/0DITB1SSu0vd4u/8l8TjPgfaAp63Gc= RSA 4096 bits (e 65537) / SHA384withRSA	1Sent by server*.wikipedia.org Fingerprint SHA256: d8bbc0caa993c7bacae3113364695ababfce129495f3e02839e5b8ac8dda1b78 Pin SHA256: tuIFdyeqbDKwc6C0D9KfXhjRr6bHP+43OSIK3eMNyyw= EC 256 bits / SHA384withECDSA 2Sent by serverE7 Fingerprint SHA256: aeb1fd7410e83bc96f5da3c6a7c2c1bb836d1fa5cb86e708515890e428a8770b Pin SHA256: y7xVm0TVJNahMr2sZydE2jQH8SquXV9yLF9seROHHHU= EC 384 bits / SHA256withRSA 3In trust storeISRG Root X1 Self-signed Fingerprint SHA256: 96bcec06264976f37460779acf28c5a7cfe8a3c0aae11a8ffcee05c0bddf08c6 Pin SHA256: C5+lpZ7tcVwmwQIMcRtPbsQtWLABXhQzejna0wHFr8M= RSA 4096 bits (e 65537) / SHA256withRSA	1Sent by serverwww.walmart.com Fingerprint SHA256: 82aab6004cc09df51278f9bd5022bfc62e33cf4e0ccab05fddfc995a2a391017 Pin SHA256: HPX0QIfVQ5dFE+U+aMO9tGIAKm6ecJJXInACPhxiXE4= EC 256 bits / SHA384withECDSA 2Sent by serverGlobalSign ECC OV SSL CA 2018 Fingerprint SHA256: 87c71553445eb3c33c3e0710711b99e9c7773f04d91ac38a9f4c082ee24101ea Pin SHA256: KJpedoXG+Rd6IJnYeOJjxUjlaDEDI8K1vCBBgzeJkC4= EC 384 bits / SHA384withECDSA 3Sent by server In trust storeGlobalSign Self-signed Fingerprint SHA256: 179fbc148a3dd00fd24ea13458cc43bfa7f59c8182d783a513f6ebec100c8924 Pin SHA256: fg6tdrtoGdwvVFEahDVPboswe53YIFjqbABPAdndpd8= EC 384 bits / SHA384withECDSA
Authentication Algorithm	RSA	RSA	RSA	ECDSA	ECDSA
Sym Encryption Algorithm	AES_128_GCM	AES_128_GCM	AES_128_GCM	AES_128_GCM	AES_256_GCM
Hashing Algorithm	SHA256	SHA256	SHA256	SHA384	SHA384
Cryptographic Guarantees	Confidentiality, Integrity, and Forward Secrecy	Confidentiality, Integrity, and Forward Secrecy	Confidentiality, Integrity, and Forward Secrecy	Confidentiality, Integrity, and Forward Secrecy	Confidentiality, Integrity, and Forward Secrecy
Trusted	Yes Mozilla Apple Android Java Windows	Yes Mozilla Apple Android Java Windows	Yes Mozilla Apple Android Java Windows	Yes Mozilla Apple Android Java Windows	Yes Mozilla Apple Android Java Windows
Protocols	TLS 1.3 and TLS 1.2	TLS 1.3 and TLS 1.2	TLS 1.3, TLS 1.2, TLS 1.1, TLS 1.0	TLS 1.3 and TLS 1.2	TLS 1.3 and TLS 1.2
Issuer	GlobalSign Atlas R3 DV TLS CA 2025 Q1 AIA: http://secure.globalsign.com/cacert/gsatlasr3dvtlsca2025q1.crt	Sectigo ECC Domain Validation Secure Server CA AIA: http://crt.sectigo.com/SectigoECCDomainValidationSecureServerCA.crt	WE1 AIA: http://i.pki.goog/we1.crt	E7 AIA: http://e7.i.lencr.org/	GlobalSign RSA OV SSL CA 2018 AIA: http://secure.globalsign.com/cacert/gsrsaovsslca2018.crt
Rating	A	A+	B	A+	A+

Reviewed By: Davis Akard

Textual Summary:

There were many intriguing findings regarding the results of all the tests. One of the most notable differences I observed was that every single website had a different issuer for its certificates. Another interesting difference I noticed was that although most websites used RSA, some used ECDSA for their authentication algorithms. One of the most common features I noticed was that all websites used AES with GCM for their symmetric encryption algorithms, along with all of the sites using SHA256 or SHA384 for their hashing algorithm. When it came to the cryptographic key type, most sites used RSA with 2048 or 4096 bits, while only a few used EC with 256 bits. Then, for the certificate chain, every single website had a 3-part chain where the site itself would start, then the issuer would go, and finally it would always finish off with a self-signed certificate. One major similarity I saw was that all sites were trusted by Mozilla, Apple, Android, Java, and Windows, with none of them ever being missing from the trusted section. A final difference I noticed was with the protocols; some sites had TLS 1.3 and TLS 1.2, with only one site having just TLS 1.2, which I believe is the reason it had an A- rating. Then, for some sites that had gone from TLS 1.3 to TLS 1.0, they would always get a B rating because it would cap them off there. Some sites also got an A+ rating, but I could not tell the difference between them and the A-rated sites. A final similarity I noticed is that every site provided all 3 of the cryptographic guarantees, as well as having a validity period of around a year.

Questions:

1. What affects whether a site gets an A rating or an A+ rating
2. Is it possible for a site to only be trusted by one of the given trusted companies/programs
3. Are websites using TLS 1.1 and TLS 1.0 really that much more unsafe than the ones using only TLS 1.3 and TLS 1.2
4. Are there websites that do not use AES with GCM