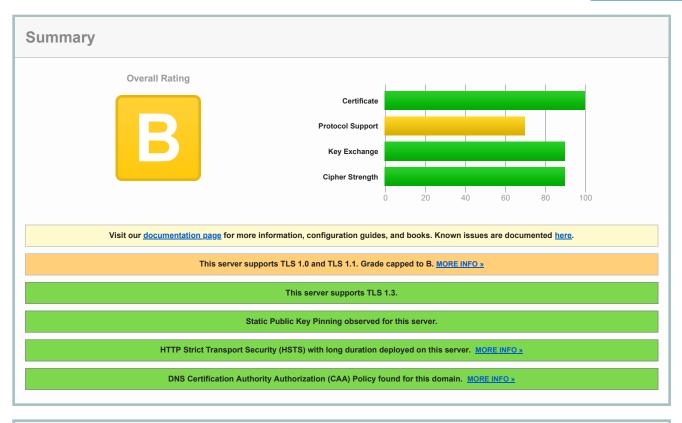
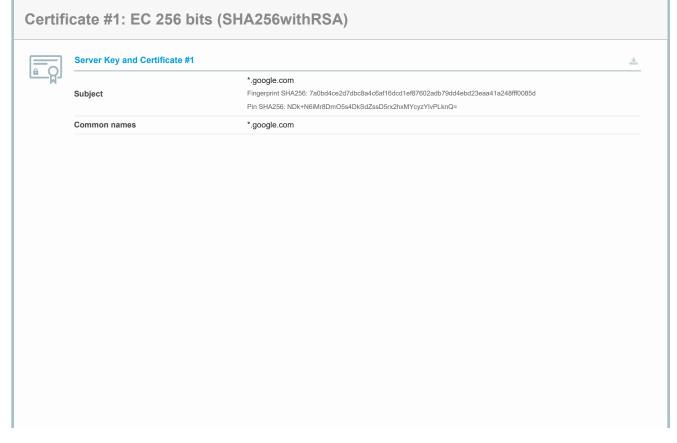
You are here: <u>Home > Projects > SSL Server Test > youtube.com</u> > 172.217.5.110

SSL Report: youtube.com (172.217.5.110)

Assessed on: Fri, 22 Oct 2021 08:40:50 UTC | HIDDEN | Clear cache

Scan Another »





Server Key and Certificate #1	*
Alternative names	*.google.com *.appengine.google.com *.bdn.dev *.cloud.google.con *.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 *.googleadapis.com *.googleapis.cn *.googleapis-cn.com *.gstatic.cn *.gstatic-cn.com *.gstaticcnapps.cn googlecnapps.cn *.googlecnapps.cn googleapps-cn.com *.googleapps-cn.com gkecnapps.cn *.gkecnapps.cn googledownloads.cn *.googledownloads.cn recaptcha.net.cn *.recaptcha.net.cn widevine.cn *.widevine.cn ampproject.org.cn *.ampproject.org.cn ampproject.net.cn *.ampproject.net.cn google-analytics-cn.com *.google-analytics-cn.com googleapis-cn.com *.googleadservices-cn.com googlevads-cn.com *.googlevads-cn.com googleapis-cn.com *.googleapis-cn.com googleoptimize-cn.com *.googleoptimize-cn.com *.googleoptimize-cn.com *.googleoptimize-cn.com *.googleoptimize-cn.com *.googleoptimize-cn.com *.googletraveladservices-cn.com *.googletraveladservices-cn.com *.googletraveladservices-cn.com *.googletagservices-cn.com *.googletagservices-cn.com *.googletagservices-cn.com *.googletagservices-cn.com *.googletagservices-cn.com *.googletagservices-cn.com *.googlesyndication-cn.com *.safeframe.googlesyndication-cn.com app-measurement-cn.com *.googlesyndication-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 *.google-analytics.com *.gvt2.com *.gcp.gvt2.com *.gcp.gvt2.com *.gcp.gvt2.com *.gcp.gvt2.com *.gcp.gvt2.com *.gcp.gvt2.com *.gcp.gvt2.com *.gcp.gvt2.com *.google-analytics.com *.google-an
Serial Number	69ccc85dd5cb16340a0000000ff605c
Valid from	Mon, 13 Sep 2021 01:38:37 UTC
Valid until	Sat, 20 Nov 2021 01:38:36 UTC (expires in 28 days, 6 hours)
Key	EC 256 bits
Weak key (Debian)	No
Issuer	GTS CA 1C3 AIA: http://pki.goog/repo/certs/gts1c3.der
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	Yes (certificate)
OCSP Must Staple	No
Revocation information	CRL, OCSP CRL: http://crls.pki.goog/gts1c3/QOvJ0N1sT2A.crl OCSP: http://ocsp.pki.goog/gts1c3
Revocation status	Good (not revoked)
DNS CAA	Yes policy host: youtube.com issue: pki.goog flags:0



Trusted

Additional Certificates (if supplied)

Certificates provided

Chain issues

Valid until

Yes

3 (6344 bytes)

None

Mozilla Apple Android Java Windows

#2	
	GTS CA 1C3
Subject	Fingerprint SHA256: 23ecb03eec17338c4e33a6b48a41dc3cda12281bbc3ff813c0589d6cc2387522
	Pin SHA256: zCTnfLwLKbS9S2sbp+uFz4KZOocFvXxkV06Ce9O5M2w=
Valid until	Thu, 30 Sep 2027 00:00:42 UTC (expires in 5 years and 11 months)
Key	RSA 2048 bits (e 65537)
Issuer	GTS Root R1
Signature algorithm	SHA256withRSA
#3	
	GTS Root R1
Subject	Fingerprint SHA256: 3ee0278df71fa3c125c4cd487f01d774694e6fc57e0cd94c24efd769133918e5
	Pin SHA256: hxqRIPTu1bMS/0DITB1SSu0vd4u/8l8TjPgfaAp63Gc=

Fri, 28 Jan 2028 00:00:42 UTC (expires in 6 years and 3 months)

Additional Certificates (if supplied)		*
Key	RSA 4096 bits (e 65537)	
Issuer	GlobalSign Root CA	
Signature algorithm	SHA256withRSA	



Certification Paths



Click here to expand

		bits (SHA256withRSA)
-0	Server Key and Certificate #1	
-⊠-	Subject	*.google.com Fingerprint SHA256: 6ccf591f9caaf92f908281e251a50c5141f0c77419d6111f5a20971d04f480f1 Pin SHA256: lq7VE6ETJCjzw4QPmPZ7yNiwWT7efKoov+NyB+T90zg=
	Common names	*.google.com
	Alternative names	*.google.com *.appengine.google.com *.bdn.dev *.cloud.google.co.m *.crowdsource.google.com *.datacompute.google.com *.google.com *.google.co.in *.google.co.in *.google.co.jp *.google.co.uk *.google.com. *.google.com.uk *.google.pl
	Serial Number	00dce95b7a66d3c17f0a00000000ff6045
	Valid from	Mon, 13 Sep 2021 01:37:29 UTC
	Valid until	Sat, 20 Nov 2021 01:37:28 UTC (expires in 28 days, 6 hours)
	Key	RSA 2048 bits (e 65537)
	Weak key (Debian)	No
	Issuer	GTS CA 1C3 AIA: http://pki.goog/repo/certs/gts1c3.der
	Signature algorithm	SHA256withRSA
	Extended Validation	No
	Certificate Transparency	Yes (certificate)
	OCSP Must Staple	No
	Revocation information	CRL, OCSP CRL: http://crls.pki.goog/gts1c3/fVJxbV-Ktmk.crl OCSP: http://ccsp.pki.goog/gts1c3
	Revocation status	Good (not revoked)
	DNC CAA	Yes policy host: youtube.com
	DNS CAA	issue: pki.goog flags:0



Additional Certificates (if supplied)

Certificates provided	3 (6548 bytes)
Chain issues	None

#2

GTS CA 1C3

Fingerprint SHA256: 23ecb03eec17338c4e33a6b48a41dc3cda12281bbc3ff813c0589d6cc2387522 Subject Pin SHA256: zCTnfLwLKbS9S2sbp+uFz4KZOocFvXxkV06Ce9O5M2w=

Valid until Thu, 30 Sep 2027 00:00:42 UTC (expires in 5 years and 11 months)

GTS Root R1

RSA 2048 bits (e 65537) Key

Signature algorithm SHA256withRSA

Issuer

GTS Root R1

Fingerprint SHA256: 3ee0278df71fa3c125c4cd487f01d774694e6fc57e0cd94c24efd769133918e5 Subject Pin SHA256: hxqRIPTu1bMS/0DITB1SSu0vd4u/8l8TjPgfaAp63Gc=

Valid until Fri, 28 Jan 2028 00:00:42 UTC (expires in 6 years and 3 months)

Key RSA 4096 bits (e 65537)

GlobalSign Root CA Issuer

SHA256withRSA Signature algorithm

Certification Paths

+

No

Click here to expand

Configuration



TLS 1.3	Yes
TLS 1.2	Yes
TLS 1.1	Yes
TLS 1.0	Yes
SSL 3	No



Cipher Suites

SSL 2

#TLS 1.3 (server has no preference)	
TLS_AES_128_GCM_SHA256 (0x1301) ECDH x25519 (eq. 3072 bits RSA) FS	128
TLS_AES_256_GCM_SHA384 (0x1302) ECDH x25519 (eq. 3072 bits RSA) FS	256
TLS_CHACHA20_POLY1305_SHA256 (0x1303) ECDH x25519 (eq. 3072 bits RSA) FS	256
# TLS 1.2 (suites in server-preferred order)	
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b) ECDH x25519 (eq. 3072 bits RSA) FS	128
TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca9) ECDH x25519 (eq. 3072 bits RSA) FS	256 ^P
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c) ECDH x25519 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009) ECDH x25519 (eq. 3072 bits RSA) FS WEAK	128
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a) ECDH x25519 (eq. 3072 bits RSA) FS WEAK	256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) ECDH x25519 (eq. 3072 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8) ECDH x25519 (eq. 3072 bits RSA) FS	256 ^P

Cipher Suites

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) ECDH x25519 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ECDH x25519 (eq. 3072 bits RSA) FS WEAK	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ECDH x25519 (eq. 3072 bits RSA) FS WEAK	256
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c) WEAK	128
TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d) WEAK	256
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) WEAK	128
TLS_RSA_WITH_AES_256_CBC_SHA (0x35) WEAK	256
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa) WEAK	112
# TLS 1.1 (suites in server-preferred order)	+
# TLS 1.0 (suites in server-preferred order)	+

(P) This server prefers ChaCha20 suites with clients that don't have AES-NI (e.g., Android devices)



Handshake Simulation

### Android 4.0.4 RSA 2648 (SHA266) TLS 1.0 TLS ECOHE_RSA_WITH_AES_128_CBC_SHA_ECOH sequ2561 FS ### Android 4.1.1 RSA 2048 (SHA266) TLS 1.0 TLS_ECOHE_ECOSA_WITH_AES_128_CBC_SHA_ECOH sequ2561 FS ### Android 4.2.2 EC 266 (SHA266) TLS 1.0 TLS_ECOHE_ECOSA_WITH_AES_128_CBC_SHA_ECOH sequ2561 FS ### Android 4.3.3 EC 266 (SHA266) TLS 1.0 TLS_ECOHE_ECOSA_WITH_AES_128_CBC_SHA_ECOH sequ2561 FS ### Android 4.3.2 EC 266 (SHA266) TLS 1.2 TLS_ECOHE_ECOSA_WITH_AES_128_CBC_SHA_ECOH sequ2561 FS ### Android 4.1.2 EC 266 (SHA266) TLS 1.2 TLS_ECOHE_ECOSA_WITH_AES_128_CBC_SHA_ECOH sequ2561 FS ### Android 5.0.0 EC 266 (SHA266) TLS 1.2 TLS_ECOHE_ECOSA_WITH_AES_128_CBC_SHA266 ECOH sequ2561 FS ### Android 5.0.0 EC 266 (SHA266) TLS 1.2 TLS_ECOHE_ECOSA_WITH_AES_128_CBC_SHA266 ECOH sequ2561 FS ### Android 5.0.0 EC 266 (SHA266) TLS 1.2 TLS_ECOHE_ECOSA_WITH_AES_128_CBC_SHA266 ECOH sequ2561 FS ### Android 5.0.0 EC 266 (SHA266) TLS 1.2 TLS_ECOHE_ECOSA_WITH_AES_128_CBC_SHA266 ECOH sequ2561 FS ### Android 5.0.0 EC 266 (SHA266) TLS 1.2 TLS_ECOHE_ECOSA_WITH_CHACHA20_POLY130S_SHA266 ECOH sequ2561 FS ### Android 5.0 EC 266 (SHA266) TLS 1.2 TLS_ECOHE_ECOSA_WITH_CHACHA20_POLY130S_SHA266 ECOH sequ2561 FS ### Android 5.0 EC 266 (SHA266) TLS 1.3 TLS_ECOHE_ECOSA_WITH_CHACHA20_POLY130S_SHA266 ECOH sequ2561 FS ### Android 5.0 EC 266 (SHA266) TLS 1.2 TLS_ECOHE_ECOSA_WITH_AES_128_CBC_SHA_ECOH sequ2561 FS ### BingPreview Jan 2015 RS 2048 (SHA266) TLS 1.2 TLS_ECOHE_ECOSA_WITH_AES_128_CBC_SHA_ECOH sequ2561 FS ### ECOHE 60 (AV ST	Hariasilake Olihalation			
Android 4.1.1 R9A 2048 (9HA259) TLS 1.0 TLS ECDHE_RSA_WITH_AES_128_CEC_SHA_ECDH_sequ2561 FS Android 4.2.2 EC 266 (9HA269) TLS 1.0 TLS_ECDHE_ECDSA_WITH_AES_128_CEC_SHA_ECDH_sequ2561 FS Android 4.3 EC 266 (9HA269) TLS 1.0 TLS_ECDHE_ECDSA_WITH_AES_128_CEC_SHA_ECDH_sequ2561 FS Android 4.2.2 EC 266 (9HA269) TLS 1.2 TLS_ECDHE_ECDSA_WITH_AES_128_CEC_SHA_ECDH_sequ2561 FS Android 4.0 EC 266 (9HA269) TLS 1.2 TLS_ECDHE_ECDSA_WITH_AES_128_CEC_SHA_ECDH_sequ2561 FS Android 5.0.0 EC 266 (9HA269) TLS 1.2 TLS_ECDHE_ECDSA_WITH_AES_128_CEC_SHA268 ECDH_sequ2561 FS Android 5.0 EC 266 (9HA269) TLS 1.2 > http://li> Android 5.0 EC 266 (9HA269) TLS 1.2 > http://li> Android 5.0 EC 266 (9HA269) TLS 1.2 > http://li> Android 5.0 EC 266 (9HA269) TLS 1.2 > http://li> Android 5.0 EC 266 (9HA269) TLS 1.2 > http://li> Android 5.0 EC 266 (9HA269) TLS 1.3 > TLS_CHACHA20_POLY1305_SHA266 ECDH_sep361 FS Android 8.0 EC 266 (9HA269) TLS 1.3 TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA266 ECDH_s25519 FS Android 9.0 - TLS 1.3 TLS_CHACHA20_POLY1305_SHA266 ECDH_sep361 FS Baildu Jan 2015 EC 266 (9HA269) TLS 1.2 > httls_ECDHE_ECDSA_WITH_AES_128_CEC_SHA_ECDH_sep361 FS Baildu Jan 2015 EC 266 (9HA269) TLS 1.2 > httls_ECDHE_ECDSA_WITH_AES_128_CEC_SHA_ECDH_sep361 FS Chrome_467_XFS_ESS_ RSA_264 (9HA269) TLS 1.2 > httls_ECDHE_ECDSA_WITH_AES_128_CEC_SHA_ECDH_sep361 FS Chrome_667_WINT_T EC 266 (9HA269) TLS 1.2 > httls_ECDHE_ECDSA_WITH_AES_128_CEC_SHA266 ECDH_sep361 FS Chrome_67_WINT_T EC 266 (9HA269) TLS 1.2 > httls_ECDHE_ECDSA_WITH_AES_128_CEC_SHA266 ECDH_sep361 FS Chrome_67_WINT_T EC 266 (9HA269) TLS 1.2 > httls_ECDHE_ECDSA_WITH_AES_128_CEC_SHA266 ECDH_sep361 FS TLS_ECHE_ECDSA_WITH_AES_128_CEC_SHA266 ECDH_sep361 FS TLS_ECHE_ECDSA_WITH_AES_128_CECM_SHA266 ECDH_sep361 FS TLS_ECHE_ECDSA_WITH_AES_128	Android 2.3.7 No SNI ²	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA No FS
### PANDOID 14.2.2 EC 286 (SHA256) TLS 1.0 TLS ECDHE_ECDSA_WITH_AES_128_CBC_SHA ECDH secq25611 FS Android 4.3 EC 286 (SHA256) TLS 1.0 TLS ECDHE_ECDSA_WITH_AES_128_CBC_SHA ECDH secq25611 FS Android 4.3.2 EC 286 (SHA256) TLS 1.2 TLS ECDHE_ECDSA_WITH_AES_128_CBC_SHA ECDH secq25611 FS Android 5.0.0 EC 286 (SHA256) TLS 1.2 TLS ECDHE_ECDSA_WITH_AES_128_CBC_SHA ECDH secq25611 FS Android 5.0.0 EC 286 (SHA256) TLS 1.2 > INLS 1.2 TLS ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 ECDH secq25611 FS Android 5.0.0 EC 286 (SHA256) TLS 1.2 > INLS ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 ECDH secq25611 FS Android 5.0 EC 286 (SHA256) TLS 1.2 > INLS ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 ECDH secq25611 FS Android 5.0 EC 286 (SHA256) TLS 1.3 TLS ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 ECDH secq25611 FS Android 5.0 TLS 1.3 TLS ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 ECDH secq25611 FS Android 5.0 TLS 1.3 TLS ECDHE_ECDSA_WITH_AES_128_CBC_SHA ECDH secq25611 FS Baldu Jan 2015 EC 286 (SHA256) TLS 1.2 > INLS ECDHE_ECDSA_WITH_AES_128_CBC_SHA ECDH secq25611 FS Baldu Jan 2015 EC 286 (SHA256) TLS 1.2 > INLS ECDHE_ECDSA_WITH_AES_128_CBC_SHA ECDH secq25611 FS BangPireview_Lan 2015 EC 286 (SHA256) TLS 1.2 > INLS ECDHE_ECDSA_WITH_AES_128_CBC_SHA ECDH secq25611 FS Chrome 59 I.Wm 7, R EC 286 (SHA256) TLS 1.2 > INLS ECDHE_ECDSA_WITH_AES_128_CBC_SHA ECDH secq25611 FS Chrome 50 I.Wm 1.0 TLS 1.3 TLS ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 ECDH secq25611 FS Chrome 50 I.Wm 1.0 TLS 1.3 TLS ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 ECDH secq25611 FS Chrome 50 I.Wm 1.0 TLS 1.3 TLS ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 ECDH secq25611 FS Chrome 50 I.Wm 1.0 TLS 1.3 TLS ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 ECDH secq25611 FS TLS 1.2 > INLS ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 ECDH secq25611 FS TLS ECDHE_ECDSA_WITH_AES	Android 4.0.4	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
### Pandroid 1.3	Android 4.1.1	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
Android 4.4.2 EC.256 (SHA256) TLS 1.2 TLS_ECOHE_ECOSA_WITH_AES_128_GOM_SHA256 ECOH-seep25611 FS Android 5.0.0 EC.256 (SHA256) TLS 1.2 TLS_ECOHE_ECOSA_WITH_AES_128_GOM_SHA256 ECOH-seep25611 FS Android 5.0.0 EC.256 (SHA256) TLS 1.2 Ntbp1/.1 TLS_ECOHE_ECOSA_WITH_AES_128_GOM_SHA256 ECOH-seep25611 FS Android 5.0.0 EC.256 (SHA256) TLS 1.2 > http1/.1 TLS_ECOHE_ECOSA_WITH_AES_128_GOM_SHA256 ECOH-seep25611 FS Android 5.0 EC.256 (SHA256) TLS 1.2 > http://li> Android 5.0 EC.256 (SHA256) TLS 1.2 > http://li> Android 5.1 . TLS 1.2 > http://li> Android 5.1 . TLS 1.2 > http://li> Android 5.1 . TLS 1.3 TLS_CHACHA20_POLY130S_SHA256 ECOH-x25519 FS Android 5.1 . TLS 1.3 TLS_CHACHA20_POLY130S_SHA256 ECOH-x25519 FS Android 5.0 . TLS 1.3 TLS_CHACHA20_POLY130S_SHA256 ECOH-x25519 FS EingPreview_lan_2015 EC.256 (SHA256) TLS 1.0 TLS_ECOHE_ECOSA_WITH_AES_128_GOM_SHA256 ECOH-x25519 FS EingPreview_lan_2015 RSA 2046 (SHA256) TLS 1.2 TLS_ECOHE_ECOSA_WITH_AES_128_GOM_SHA256 ECOH-seep25611 FS Chrome 49 / XP SP3 RSA 2046 (SHA256) TLS 1.2 TLS_ECOHE_ECOSA_WITH_AES_128_GOM_SHA256 ECOH-seep2561 FS Chrome 50 / Win 1.0 . TLS 1.3 TLS_ECOHE_ECOSA_WITH_AES_128_GOM_SHA256 ECOH-seep2561 FS Chrome 50 / Win 1.0 . TLS 1.3 TLS_ECOHE_ECOSA_WITH_AES_128_GOM_SHA256 ECOH-seep2561 FS Chrome 50 / Win 1.0 R . TLS 1.3 TLS_AES_128_GOM_SHA256 ECOH-seep2561 FS Eindox 31 3.0 ESS / Win 7. EC.256 (SHA256) TLS 1.2 > http://li> Eindox 47 / Win 7. R EC.256 (SHA256) TLS 1.2 > http://li> Eindox 47 / Win 7. R EC.256 (SHA256) TLS 1.2 > http://li> Eindox 47 / Win 7. R EC.256 (SHA256) TLS 1.2 > http://li> Eindox 47 / Win 7. R EC.256 (SHA256) TLS 1.2 > http://li> Eindox 47 / Win 7. R EC.256 (SHA256) TLS 1.2 TLS_ECOHE_ECOSA_WITH_AES_128_GOM_SHA256 ECOH-seep25611 FS Eindox 47 / Win 1.0 R . TLS 1.3 TLS_ECOHE_ECOSA_WITH_AES_128_GOM_SHA256 ECOH-seep25611 FS Eindox 47 / Win 1.0 R EC.256 (SHA256) TLS 1.0 TLS 1.2 SCOHE_ECOSA_WITH_AES_128_GOM_SHA256 ECOH-seep25611 FS Eindox 47 / Win 1.0 R EC.256 (SHA256) TLS 1.0 TLS_ECOHE_ECOSA_WITH_AES_128_GOM_SHA256 ECOH-seep25611 FS Eindox 47 / Win 1.0 R	Android 4.2.2	EC 256 (SHA256)	TLS 1.0	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
Android 5.0.0 EC 256 (BHA256) TLS 1.2 TLS ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH seep256r1 FS Android 6.0 EC 256 (BHA256) TLS 1.2 > http/1.1 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH seep256r1 FS Android 8.0 EC 256 (BHA256) TLS 1.2 > htz TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 ECDH x25519 FS Android 8.0 EC 256 (BHA256) TLS 1.2 > hz TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 ECDH x25519 FS Android 8.1 - TLS 1.3 TLS_CHACHA20_POLY1305_SHA256 ECDH x25519 FS Android 9.0 - TLS 1.3 TLS_CHACHA20_POLY1305_SHA256 ECDH x25519 FS Baidu Jan 2015 EC 256 (BHA256) TLS 1.0 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH seep256r1 FS Baidu Jan 2015 RSA 2046 (SHA256) TLS 1.2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH seep256r1 FS Chrome 49 1/X SP23 RSA 2046 (SHA256) TLS 1.2 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS Chrome 69 1/Win 7 R EC 256 (SHA256) TLS 1.2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS Chrome 70 1/Win 10 - TLS 1.3 TLS_AES_128_GCM_SHA256 ECDH x25519 FS Chrome 80 1/Win 7 R EC 256 (SHA256) TLS 1.2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS Chrome 80 1/Win 7 R EC 256 (SHA256) TLS 1.2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS Eirefox 47 1/Win 7 R EC 256 (SHA256) TLS 1.2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS Eirefox 47 1/Win 7 R EC 256 (SHA256) TLS 1.2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS Eirefox 49 1/X SP23 EC 256 (SHA256) TLS 1.2 > hz TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS Eirefox 49 1/X SP23 EC 256 (SHA256) TLS 1.2 > hz TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS Eirefox 49 1/X SP23 EC 256 (SHA256) TLS 1.2 > hz TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS Eirefox 49 1/X SP23 EC 256 (SHA256) TLS 1.2 > hz TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS EIREFOX 49 1/X SP23 EC 256 (SHA256) TLS 1.2 > hz TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS EIREFOX 49 1/X SP23 EC 256 (SHA256) TLS 1.0 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS EIREFOX 49 1/X SP23 EC 256 (SHA	Android 4.3	EC 256 (SHA256)	TLS 1.0	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
Android 6.0 EC 256 (BHA256) TLS 1.2 > http://li>	Android 4.4.2	EC 256 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Android 7.0 EC 256 (8HA256) TLS 1.2 > h2 TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256_ECDH x25519_FS Android 8.0 EC 256 (8HA256) TLS 1.2 > h2 TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256_ECDH x25519_FS Android 8.1 - TLS 1.3 TLS_CHACHA20_POLY1305_SHA256_ECDH x25519_FS Android 8.1 - TLS 1.3 TLS_CHACHA20_POLY1305_SHA256_ECDH x25519_FS Baidu_Jan 2015 Baidu_Jan 2015 Baidu_Jan 2015 BRA 2048 (8HA256) TLS 1.2 TLS_ECDHE_ECDSA_WITH_AES_128_GCBC_SHA_ECDH xscq25611_FS BindPreview_Jan 2015 BRA 2048 (8HA256) TLS 1.2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_ECDH xscq25611_FS Chrome 49 / XP_SP2 BRA 2048 (8HA256) TLS 1.2 > h2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_ECDH xscq25611_FS Chrome 69 / Win 7 R EC 256 (8HA256) TLS 1.2 > h2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_ECDH xscq25611_FS Chrome 80 / Win 10 R - TLS 1.3 TLS_AES_128_GCM_SHA256_ECDH xscq25611_FS Erefox 31 .30 ESR/ Win 7 EC 256 (8HA256) TLS 1.2 > h2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_ECDH xscq25611_FS Erefox 31 .30 ESR/ Win 7 EC 256 (8HA256) TLS 1.2 > h2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_ECDH xscq25611_FS Erefox 31 .30 ESR/ Win 7 Erefox 31 .30 ESR/ Win 7 EC 256 (8HA256) TLS 1.2 > h2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_ECDH xscq25611_FS Erefox 40 / XP_SP3 EC 256 (8HA256) TLS 1.2 > h2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_ECDH xscq25611_FS Erefox 62 / Win 7 R EC 256 (8HA256) TLS 1.2 > h2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_ECDH xscq25611_FS Erefox 73 / Win 10 R - TLS 1.3 TLS_AES_128_GCM_SHA256_ECDH xscq25611_FS Erefox 73 / Win 10 R - TLS 1.3 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_ECDH xscq25611_FS ERE XP_NoFS1_No SN12 RSA_2048 (8HA256) TLS 1.0 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_ECDH xscq25611_FS ERE XP_NoFS1_No SN12 RSA_2048 (8HA256) TLS 1.0 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_ECDH xscq25611_FS ERE XP_NoFS1_No SN12 RSA_2048 (8HA256) TLS 1.0 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_ECDH xscq25611_FS ERE XP_NoFS1_No SN12 RSA_2048 (8HA256) TLS 1.0 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_ECDH xscq25611_FS ERE XP_NOFS1_NO SN12 RSA_2048 (8HA25	Android 5.0.0	EC 256 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
### Page 18	Android 6.0	EC 256 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Android 8.1 - TLS 1.3 TLS_CHACHA20_POLY130S_SHA256 ECDH x25519 FS Android 9.0 - TLS 1.3 TLS_CHACHA20_POLY130S_SHA256 ECDH x25519 FS Baidu_lan 2015	Android 7.0	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 ECDH x25519 FS
Android 9.0 - TLS 1.3 TLS_CHACHA20_POLY1305_SHA256_ECDH x25519_FS Baldu Jan 2015 EC 256 (SHA256) TLS 1.0 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_ECDH secp256r1_FS BingPreview Jan 2015 R5A 2048 (SHA256) TLS 1.2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_ECDH secp256r1_FS Chrome 49 / XP_SP3 R5A 2048 (SHA256) TLS 1.2 > h2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_ECDH secp256r1_FS Chrome 69 / Win 7_R EC 256 (SHA256) TLS 1.2 > h2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_ECDH x25519_FS Chrome 69 / Win 10 - TLS 1.3 TLS_AES_128_GCM_SHA256_ECDH x25519_FS Chrome 70 / Win 10 - TLS 1.3 TLS_AES_128_GCM_SHA256_ECDH x25519_FS Chrome 80 / Win 10 R - TLS 1.3 TLS_AES_128_GCM_SHA256_ECDH x25519_FS Eirefox 31.3.0 ESR / Win 7 EC 256 (SHA256) TLS 1.2 > h2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_ECDH secp256r1_FS Eirefox 47 / Win 7 R EC 256 (SHA256) TLS 1.2 > h2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_ECDH secp256r1_FS Eirefox 49 / XP_SP3 EC 256 (SHA256) TLS 1.2 > h2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_ECDH secp256r1_FS Eirefox 62 / Win 7 R EC 256 (SHA256) TLS 1.2 > h2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_ECDH x25519_FS Eirefox 73 / Win 10 R - TLS 1.3 TLS_AES_128_GCM_SHA256_ECDH x25519_FS Eirefox 73 / Win 10 R - TLS 1.3 TLS_AES_128_GCM_SHA256_ECDH x25519_FS EE 7 / Vista EC 256 (SHA256) TLS 1.0 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_ECDH x25519_FS EE 8 / XP_NoFS1_NOSN2 RSA_2048 (SHA256) TLS 1.0 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_ECDH x25519_FS EE 11 / Win 7 R EC 256 (SHA256) TLS 1.0 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_ECDH x25519_FS EE 11 / Win 7 R EC 256 (SHA256) TLS 1.0 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_ECDH x25519_FS EE 11 / Win 7 R EC 256 (SHA256) TLS 1.0 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_ECDH x25519_FS EE 11 / Win 7 R EC 256 (SHA256) TLS 1.0 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_ECDH x25519_FS EE 11 / Win 7 R EC 256 (SHA256) TLS 1.0 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_ECDH x25519_FS EE 11 / Win Phone 8.1 R EC 256 (SHA256) TLS 1.2 > http://lll TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_ECDH x25519_FS EE	Android 8.0	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 ECDH x25519 FS
Baidu Jan 2015 EC 256 (SHA256) TLS 1.0 TLS ECDHE_ECDSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS	Android 8.1	-	TLS 1.3	TLS_CHACHA20_POLY1305_SHA256 ECDH x25519 FS
BingPreview_Jan 2015 R3A 2048 (SHA256) TLS 1.2 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS	Android 9.0	-	TLS 1.3	TLS_CHACHA20_POLY1305_SHA256 ECDH x25519 FS
Chrome 49 / XP SP3 RSA 2048 (SHA256) TLS 1.2 > h2 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH seep256r1 FS Chrome 69 / Win 7 R EC 256 (SHA256) TLS 1.2 > h2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS Chrome 70 / Win 10 - TLS 1.3 TLS_AES_128_GCM_SHA256 ECDH x25519 FS Chrome 80 / Win 10 R - TLS 1.3 TLS_AES_128_GCM_SHA256 ECDH x25519 FS Chrome 80 / Win 10 R - TLS 1.3 TLS_AES_128_GCM_SHA256 ECDH x25519 FS Chrome 80 / Win 70 R - TLS 1.3 TLS_AES_128_GCM_SHA256 ECDH x25519 FS Eirefox 47 / Win 7 R EC 256 (SHA256) TLS 1.2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH seep256r1 FS Eirefox 49 / XP SP3 EC 256 (SHA256) TLS 1.2 > h2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH seep256r1 FS Eirefox 49 / XP SP3 EC 256 (SHA256) TLS 1.2 > h2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH seep256r1 FS Eirefox 62 / Win 7 R EC 256 (SHA256) TLS 1.2 > h2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS Eirefox 73 / Win 10 R - TLS 1.3 TLS_AES_128_GCM_SHA256 ECDH x25519 FS Eirefox 73 / Win 10 R - TLS 1.3 TLS_AES_128_GCM_SHA256 ECDH x25519 FS Eirefox 73 / Win 10 R - TLS 1.3 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS Eirefox 73 / Win 10 R - TLS 1.3 TLS_AES_128_GCM_SHA256 ECDH x25519 FS Eirefox 73 / Win 10 R - TLS 1.3 TLS_AES_128_GCM_SHA256 ECDH x25519 FS Eirefox 73 / Win 10 R - TLS 1.3 TLS_AES_128_GCM_SHA256 ECDH x25519 FS Eirefox 73 / Win 10 R - TLS 1.3 TLS_AES_128_GCM_SHA256 ECDH x25519 FS Eirefox 74 / Win 75 R - TLS 1.3 TLS_AES_128_GCM_SHA256 ECDH x25519 FS Eirefox 75 / Win 77 R EC 256 (SHA256) TLS 1.0 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH seep256r1 FS EIL 1 / Win 7 R EC 256 (SHA256) TLS 1.0 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH seep256r1 FS EIL 1 / Win 8.1 R EC 256 (SHA256) TLS 1.2 > http/1.1 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH seep256r1 FS EIL 1 / Win Phone 8.1 R EC 256 (SHA256) TLS 1.2 > http/1.1 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH seep256r1 FS EIL 1 / Win 10 R EC 256 (SHA256) TLS 1.2 > http/1.1 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH seep256r1 FS EIL 1 / Win 10 R EC 256	Baidu Jan 2015	EC 256 (SHA256)	TLS 1.0	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
Chrome 69 / Win 7 R	BingPreview Jan 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Chrome 70 / Win 10	Chrome 49 / XP SP3	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Chrome 80 / Win 10 R - TLS 1.3 TLS_AES_128_GCM_SHA256 ECDH x25519 FS Firefox 31.3.0 ESR / Win 7 EC 256 (SHA256) TLS 1.2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS Firefox 49 / XP SP3 EC 256 (SHA256) TLS 1.2 > h2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS Firefox 49 / XP SP3 EC 256 (SHA256) TLS 1.2 > h2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS Firefox 62 / Win 7 R EC 256 (SHA256) TLS 1.2 > h2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS Firefox 73 / Win 10 R - TLS 1.3 TLS_AES_128_GCM_SHA256 ECDH x25519 FS Googlebot Feb 2018 EC 256 (SHA256) TLS 1.2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS IE 7 / Vista EC 256 (SHA256) TLS 1.0 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS IE 8 / XP No FS No SNI 2 RSA 2048 (SHA256) TLS 1.0 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS IE 8 / XP No FS No SNI 2 RSA 2048 (SHA256) TLS 1.0 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS IE 11 / Win 7 R EC 256 (SHA256) TLS 1.0 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS IE 11 / Win 7 R EC 256 (SHA256) TLS 1.2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS IE 11 / Win 8.1 R EC 256 (SHA256) TLS 1.2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS IE 11 / Win Phone 8.0 EC 256 (SHA256) TLS 1.0 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS IE 11 / Win Phone 8.1 R EC 256 (SHA256) TLS 1.2 > http/1.1 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS IE 11 / Win Phone 8.1 R EC 256 (SHA256) TLS 1.2 > http/1.1 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS IE 11 / Win Phone 8.1 R EC 256 (SHA256) TLS 1.2 > http/1.1 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS IE 11 / Win 10 R EC 256 (SHA256) TLS 1.2 > http/1.1 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS IE 11 / Win 10 R EC 256 (SHA256) TLS 1.2 > http/1.1 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS IE 11 / Win 10 R EC 256 (SHA256) TLS 1.2 > http/1.2 > http/1.1 TLS_ECDHE_ECDSA_WITH_AES_128_G	Chrome 69 / Win 7 R	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS
Firefox 31.3.0 ESR / Win 7	Chrome 70 / Win 10	-	TLS 1.3	TLS_AES_128_GCM_SHA256 ECDH x25519 FS
TLS 1.2 > h2	Chrome 80 / Win 10 R	-	TLS 1.3	TLS_AES_128_GCM_SHA256 ECDH x25519 FS
Firefox 49 / XP SP3	Firefox 31.3.0 ESR / Win 7	EC 256 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
TLS 1.2 > h2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS	Firefox 47 / Win 7 R	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
TLS 1.3 TLS_AES_128_GCM_SHA256 ECDH x25519 FS	Firefox 49 / XP SP3	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Cooglebot Feb 2018 EC 256 (SHA256) TLS 1.2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS E7 / Vista	Firefox 62 / Win 7 R	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS
E 7 / Vista	Firefox 73 / Win 10 R	-	TLS 1.3	TLS_AES_128_GCM_SHA256 ECDH x25519 FS
RSA 2048 (SHA256) TLS 1.0 TLS_RSA_WITH_3DES_EDE_CBC_SHA RSA 2048 (SHA256) TLS 1.0 TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS RE 11 / Win 7 R EC 256 (SHA256) TLS 1.2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS RE 11 / Win 8.1 R EC 256 (SHA256) TLS 1.2 > http/1.1 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS RE 10 / Win Phone 8.0 EC 256 (SHA256) TLS 1.0 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS RE 11 / Win Phone 8.1 R EC 256 (SHA256) TLS 1.2 > http/1.1 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS RE 11 / Win Phone 8.1 Update R EC 256 (SHA256) TLS 1.2 > http/1.1 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS RE 11 / Win 10 R EC 256 (SHA256) TLS 1.2 > h2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS RE 11 / Win 10 R EC 256 (SHA256) TLS 1.2 > h2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS RE 11 / Win 10 R EC 256 (SHA256) TLS 1.2 > h2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS RE 11 / Win 10 R EC 256 (SHA256) TLS 1.2 > h2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS RE 11 / Win 10 R EC 256 (SHA256) TLS 1.2 > h2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS RE 11 / Win 10 R EC 256 (SHA256) TLS 1.2 > h2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS RE 11 / Win 10 R EC 256 (SHA256) TLS 1.2 > h2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS RE 11 / Win 10 R EC 256 (SHA256) TLS 1.2 > h2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS RE 11 / Win 10 R EC 256 (SHA256) TLS 1.2 > h2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS RE 11 / Win 10 R EC 256 (SHA256) TLS 1.2 > h2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS RE 11 / Win 10 R EC 256 (SHA256) TLS 1.2 > h2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS	Googlebot Feb 2018	EC 256 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS
E 8-10 / Win 7 R EC 256 (SHA256) TLS 1.0 TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS E 11 / Win 7 R EC 256 (SHA256) TLS 1.2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS E 11 / Win 8.1 R EC 256 (SHA256) TLS 1.2 > http/1.1 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS E 10 / Win Phone 8.0 EC 256 (SHA256) TLS 1.0 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS E 11 / Win Phone 8.1 R EC 256 (SHA256) TLS 1.2 > http/1.1 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS E 11 / Win Phone 8.1 Update R EC 256 (SHA256) TLS 1.2 > http/1.1 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS E 11 / Win 10 R EC 256 (SHA256) TLS 1.2 > h2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS E 11 / Win 10 R EC 256 (SHA256) TLS 1.2 > h2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS E 11 / Win 10 R EC 256 (SHA256) TLS 1.2 > h2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS E 11 / Win 10 R EC 256 (SHA256) TLS 1.2 > h2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS E 11 / Win 10 R EC 256 (SHA256) TLS 1.2 > h2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS E 11 / Win 10 R EC 256 (SHA256) TLS 1.2 > h2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS E 11 / Win 10 R EC 256 (SHA256) TLS 1.2 > h2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS E 11 / Win 10 R EC 256 (SHA256) TLS 1.2 > h2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS E 11 / Win 10 R EC 256 (SHA256) TLS 1.2 > h2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS E 11 / Win 10 R EC 256 (SHA256) TLS 1.2 > h2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS E 11 / Win 10 R EC 256 (SHA256) TLS 1.2 > h2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA25	IE 7 / Vista	EC 256 (SHA256)	TLS 1.0	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
IE 11 / Win 7 R EC 256 (SHA256) TLS 1.2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS IE 11 / Win 8.1 R EC 256 (SHA256) TLS 1.2 > http/1.1 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS IE 10 / Win Phone 8.0 EC 256 (SHA256) TLS 1.0 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS IE 11 / Win Phone 8.1 R EC 256 (SHA256) TLS 1.2 > http/1.1 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS IE 11 / Win Phone 8.1 Update R EC 256 (SHA256) TLS 1.2 > http/1.1 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS IE 11 / Win 10 R EC 256 (SHA256) TLS 1.2 > h2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS Edge 15 / Win 10 R EC 256 (SHA256) TLS 1.2 > h2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS Edge 18 / Win 10 R EC 256 (SHA256) TLS 1.2 > h2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS Edge 18 / Win 10 R EC 256 (SHA256) TLS 1.2 > h2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS <td>IE 8 / XP No FS 1 No SNI 2</td> <td>RSA 2048 (SHA256)</td> <td>TLS 1.0</td> <td>TLS_RSA_WITH_3DES_EDE_CBC_SHA</td>	IE 8 / XP No FS 1 No SNI 2	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_3DES_EDE_CBC_SHA
E 11 / Win 8.1 R EC 256 (SHA256) TLS 1.2 > http/1.1 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS EE 10 / Win Phone 8.0 EC 256 (SHA256) TLS 1.0 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS EE 11 / Win Phone 8.1 R EC 256 (SHA256) TLS 1.2 > http/1.1 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS EE 11 / Win Phone 8.1 Update R EC 256 (SHA256) TLS 1.2 > http/1.1 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS EE 11 / Win 10 R EC 256 (SHA256) TLS 1.2 > h2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS Edge 15 / Win 10 R EC 256 (SHA256) TLS 1.2 > h2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS Edge 16 / Win 10 R EC 256 (SHA256) TLS 1.2 > h2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS Edge 18 / Win 10 R EC 256 (SHA256) TLS 1.2 > h2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS Edge 18 / Win 10 R EC 256 (SHA256) TLS 1.2 > h2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS Edge 18 / Win 10 R EC 256 (SHA256) TLS 1.2 > h2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS	I <u>E 8-10 / Win 7</u> R	EC 256 (SHA256)	TLS 1.0	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
IE 10 / Win Phone 8.0 EC 256 (SHA256) TLS 1.0 TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS IE 11 / Win Phone 8.1 R EC 256 (SHA256) TLS 1.2 > http/1.1 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS IE 11 / Win Phone 8.1 Update R EC 256 (SHA256) TLS 1.2 > http/1.1 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS IE 11 / Win 10 R EC 256 (SHA256) TLS 1.2 > h2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS Edge 15 / Win 10 R EC 256 (SHA256) TLS 1.2 > h2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS Edge 16 / Win 10 R EC 256 (SHA256) TLS 1.2 > h2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS Edge 18 / Win 10 R EC 256 (SHA256) TLS 1.2 > h2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS	I <u>E 11 / Win 7</u> R	EC 256 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
E 11 / Win Phone 8.1 R EC 256 (SHA256) TLS 1.2 > http/1.1 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS E 11 / Win Phone 8.1 Update R EC 256 (SHA256) TLS 1.2 > http/1.1 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS E 11 / Win 10 R EC 256 (SHA256) TLS 1.2 > h2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS E 15 / Win 10 R EC 256 (SHA256) TLS 1.2 > h2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS E 16 / Win 10 R EC 256 (SHA256) TLS 1.2 > h2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS E 18 / Win 10 R EC 256 (SHA256) TLS 1.2 > h2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS E 18 / Win 10 R EC 256 (SHA256) TLS 1.2 > h2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS E 18 / Win 10 R EC 256 (SHA256) TLS 1.2 > h2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS E 18 / Win 10 R EC 256 (SHA256) TLS 1.2 > h2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS E 18 / Win 10 R EC 256 (SHA256) TLS 1.2 > h2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS E 18 / Win 10 R EC 256 (SHA256) TLS 1.2 > h2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS E 18 / Win 10 R EC 256 (SHA256) TLS 1.2 > h2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS E 18 / Win 10 R EC 256 (SHA256) TLS 1.2 > h2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS E 18 / Win 10 R EC 256 (SHA256) TLS 1.2 > h2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS E 18 / Win 10 R EC 256 (SHA256) TLS 1.2 > h2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS E 18 / Win 10 R EC 256 (SHA256) TLS 1.2 > h2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS E 18 / Win 10 R EC 256 (SHA256) TLS 1.2 > h2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS E 18 / Win 10 R EC 256 (SHA256) TLS 1.2 > h2 TLS_ECDHE_ECD	IE 11 / Win 8.1 R	EC 256 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
IE 11 / Win Phone 8.1 Update R EC 256 (SHA256) TLS 1.2 > http/1.1 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS IE 11 / Win 10 R EC 256 (SHA256) TLS 1.2 > h2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS Edge 15 / Win 10 R EC 256 (SHA256) TLS 1.2 > h2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS Edge 16 / Win 10 R EC 256 (SHA256) TLS 1.2 > h2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS Edge 18 / Win 10 R EC 256 (SHA256) TLS 1.2 > h2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS Edge 18 / Win 10 R EC 256 (SHA256) TLS 1.2 > h2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS Edge 18 / Win 10 R EC 256 (SHA256) TLS 1.2 > h2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS Edge 18 / Win 10 R EC 256 (SHA256) TLS 1.2 > h2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS Edge 18 / Win 10 R EC 256 (SHA256) TLS 1.2 > h2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS Edge 18 / Win 10 R EC 256 (SHA256) TLS 1.2 > h2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS Edge 18 / Win 10 R EC 256 (SHA256) TLS 1.2 > h2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS Edge 18 / Win 10 R EC 256 (SHA256) TLS 1.2 > h2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS Edge 18 / Win 10 R EC 256 (SHA256) TLS 1.2 > h2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS Edge 18 / Win 10 R EC 256 (SHA256) TLS 1.2 > h2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS Edge 18 / Win 10 R EC 256 (SHA256) TLS 1.2 > h2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS Edge 18 / Win 10 R EC 256 (SHA256) TLS 1.2 > h2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS Edge 18 / Win 10 R EC 256 (SHA256) TLS 1.2 > h2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 TLS 1.	IE 10 / Win Phone 8.0	EC 256 (SHA256)	TLS 1.0	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
EE 11 / Win 10 R EC 256 (SHA256) TLS 1.2 > h2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS Edge 15 / Win 10 R EC 256 (SHA256) TLS 1.2 > h2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS Edge 16 / Win 10 R EC 256 (SHA256) TLS 1.2 > h2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS Edge 18 / Win 10 R EC 256 (SHA256) TLS 1.2 > h2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS	IE 11 / Win Phone 8.1 R	EC 256 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Edge 15 / Win 10 R EC 256 (SHA256) TLS 1.2 > h2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS Edge 16 / Win 10 R EC 256 (SHA256) TLS 1.2 > h2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS Edge 18 / Win 10 R EC 256 (SHA256) TLS 1.2 > h2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS	IE 11 / Win Phone 8.1 Update R	EC 256 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Edge 16 / Win 10 R EC 256 (SHA256) TLS 1.2 > h2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS Edge 18 / Win 10 R EC 256 (SHA256) TLS 1.2 > h2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS	IE 11 / Win 10 R	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Edge 18 / Win 10 R EC 256 (SHA256) TLS 1.2 > h2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS	Edge 15 / Win 10 R	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS
	Edge 16 / Win 10 R	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS
Edge 13 / Win Phone 10 R EC 256 (SHA256) TLS 1.2 > h2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS	Edge 18 / Win 10 R	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS
	Edge 13 / Win Phone 10 R	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS

Har	de	hal	10	Simu	lati	Or

Java 6u45 No SNI ²	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA No FS
Java 7u25	EC 256 (SHA256)	TLS 1.0	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
<u>Java 8u161</u>	EC 256 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
<u>Java 11.0.3</u>	-	TLS 1.3	TLS_AES_128_GCM_SHA256 ECDH secp256r1 FS
Java 12.0.1	-	TLS 1.3	TLS_AES_128_GCM_SHA256 ECDH secp256r1 FS
OpenSSL 0.9.8y	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA No FS
OpenSSL 1.0.1I R	EC 256 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
OpenSSL 1.0.2s R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
OpenSSL 1.1.0k R	EC 256 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 ECDH x25519 FS
OpenSSL 1.1.1c R	-	TLS 1.3	TLS_AES_256_GCM_SHA384 ECDH x25519 FS
Safari 5.1.9 / OS X 10.6.8	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
Safari 6 / iOS 6.0.1	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
Safari 6.0.4 / OS X 10.8.4 R	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
Safari 7 / iOS 7.1 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
<u>Safari 7 / OS X 10.9</u> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
Safari 8 / iOS 8.4 R	EC 256 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
Safari 8 / OS X 10.10 R	EC 256 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
Safari 9 / iOS 9 R	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
<u>Safari 9 / OS X 10.11</u> R	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Safari 10 / iOS 10 R	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Safari 10 / OS X 10.12 R	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
<u>Safari 12.1.2 / MacOS 10.14.6</u> <u>Beta</u> R	-	TLS 1.3	TLS_CHACHA20_POLY1305_SHA256 ECDH x25519 FS
<u>Safari 12.1.1 / iOS 12.3.1</u> R	-	TLS 1.3	TLS_CHACHA20_POLY1305_SHA256 ECDH x25519 FS
Apple ATS 9 / iOS 9 R	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Yahoo Slurp Jan 2015	EC 256 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
YandexBot Jan 2015	EC 256 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS

Not simulated clients (Protocol mismatch)



<u>IE 6 / XP</u> No FS ¹ No SNI ² Protocol mismatch (not simulated)

- (1) Clients that do not support Forward Secrecy (FS) are excluded when determining support for it.
- (2) No support for virtual SSL hosting (SNI). Connects to the default site if the server uses SNI.
- $(3) \ {\hbox{Only first connection attempt simulated. Browsers sometimes retry with a lower protocol version.}$
- (R) Denotes a reference browser or client, with which we expect better effective security.
- (All) We use defaults, but some platforms do not use their best protocols and features (e.g., Java 6 & 7, older IE).
- (All) Certificate trust is not checked in handshake simulation, we only perform TLS handshake.



Protocol Details

DROWN	No, server keys and hostname not seen elsewhere with SSLv2 (1) For a better understanding of this test, please read this longer explanation (2) Key usage data kindly provided by the Censys network search engine; original DROWN website here (3) Censys data is only indicative of possible key and certificate reuse; possibly out-of-date and not complet
Secure Renegotiation	Supported
Secure Client-Initiated Renegotiation	No
Insecure Client-Initiated Renegotiation	No
BEAST attack	Not mitigated server-side (more info) TLS 1.0: 0xc009
POODLE (SSLv3)	No, SSL 3 not supported (more info)
POODLE (TLS)	No (more info)
Zombie POODLE	No (<u>more info</u>) TLS 1.2 : 0xc009
GOLDENDOODLE	No (more info) TLS 1.2 : 0xc009
OpenSSL 0-Length	No (more info) TLS 1.2 : 0xc009
Sleeping POODLE	No (more info) TLS 1.2: 0xc009
Downgrade attack prevention	Yes, TLS_FALLBACK_SCSV supported (more info)
SSL/TLS compression	No

Protocol Details	
RC4	No
Heartbeat (extension)	No
Heartbleed (vulnerability)	No (more info)
Ticketbleed (vulnerability)	No (more info)
OpenSSL CCS vuln. (CVE-2014-0224)	No (more info)
OpenSSL Padding Oracle vuln. (CVE-2016-2107)	No (more info)
ROBOT (vulnerability)	No (more info)
Forward Secrecy	With modern browsers (more info)
ALPN	Yes h2 http/1.1
NPN	Yes grpc-exp h2 http/1.1
Session resumption (caching)	Yes
Session resumption (tickets)	Yes
OCSP stapling	No
Strict Transport Security (HSTS)	Yes max-age=31536000; includeSubDomains; preload
HSTS Preloading	Chrome Edge Firefox IE
Public Key Pinning (HPKP)	No (more info)
3()	\
Public Key Pinning Report-Only	No
Public Key Pinning Report-Only Public Key Pinning (Static)	Yes includeSubDomains: true report-uri: http://clients3.google.com/cert_upload_json pin-sha256: IPMbDAjLVSGntGO3WP53X/zilCVndez5YJ2+vJvhJsA= pin-sha256: YZPgTZ+woNCCCIW3LH2CxQeLzB/1m42QcCTBSdgayjs= pin-sha256: YxPgTZ+woNCCCIW3LH2CxQeLzB/1m42QcCTBSdgayjs= pin-sha256: Vxfd95BwDesQo+NUYxVEEIlvkOlWY2SalKK1IPhzOx78= pin-sha256: Oxnt2YHvdHR3tJYmQIr0Paosp6t/nggsEGD4QJZ3Q0g= pin-sha256: mEfiZTSenoR1FuXLgYYGqnVEoZvmf9c2bVBpiOJYQ0c= pin-sha256: iie1VXtL7HzAMF+/PVPR9xzT80KxdZeJ+zduCB3uJ0= pin-sha256: hxrRCWbljB5FGRZv++qAms7uX69qFC45aBhVpeGclco= (Forbidden) pin-sha256: SG/sBoMJc9lgJ8+dGglHyTLvz7wyVBio7IMoDanPuRk= (Forbidden) pin-sha256: LvRiGEjRqfzurezaWuj8Wie2gyHMrW5Q06LspMnox7A= (Forbidden)
	Yes includeSubDomains: true report-uri: http://clients3.google.com/cert_upload_json pin-sha256: IPMbDAjLVSGntGO3WP53X/zilCVndez5YJ2+vJvhJsA= pin-sha256: YZPgTZ+woNCCCIW3LH2CxQeLzB/1m42QcCTBSdgayjs= pin-sha256: hxqRIPTu1bMS/0DITB1SSu0vd4w/8l8TjPgfaAp63Gc= pin-sha256: Vfd95BwDeSQo+NUYxVEEIlvkOIWY2SalKK1IPhzOx78= pin-sha256: QXnt2YHvdHR3tJYmQlr0Paosp6t/nggsEGD4QJZ3Q0g= pin-sha256: mEfiZT5enoR1FuXLgYYGqnVEoZvmf9c2bVBpiOjYQ0c= pin-sha256: iie1VXtL7HzAMF+/PVPR9xzT80kQxdZeJ+zduCB3ujO= pin-sha256: hxrRCWbljB5FGRZv++qAms7uX69qFC45aBhVpeGclco= (Forbidden) pin-sha256: SG/sBoMJc9lgJ8+dGgIHyTLvz7wyVBio7IMoDanPuRk= (Forbidden)
Public Key Pinning (Static)	Yes includeSubDomains: true report-uri: http://clients3.google.com/cert_upload_json pin-sha256: IPMbDAjLVSGntGO3WP53X/zilCVndez5YJ2+vJvhJsA= pin-sha256: YZPgTZ+woNCCCIW3LH2CxQeLzB/Im42QcCTBSdgayjs= pin-sha256: hxqRIPTu1bMS/0DITB1SSu0vd4w/8l8TjPgfaAp63Gc= pin-sha256: Vfd95BwDeSQo+NUYxVEEIIvk0/WY2SalKK1IPhzOx78= pin-sha256: Qxnt2YHvdHR3tJYmQIn0Paosp6VnggsEGD4QJZ3Q0g= pin-sha256: mEflZT5enoR1FuXLgYYGqnVEoZvmf9c2bVBpiOjYQ0c= pin-sha256: ie1vXtL7HzAMF+/PVPR9xZT80kQxdZeJ+zduCB3uj0= pin-sha256: kxrRCWbljB5FGRZv++qAms7uX69qFC45aBhVpeGclco= (Forbidden) pin-sha256: SG/sBoMJc9lgJ8+dGgIHyTLvz7wyVBio7IMoDanPuRk= (Forbidden) pin-sha256: LvRiGEjRqfzurezaWuj8Wie2gyHMrW5Q06LspMnox7A= (Forbidden)
Public Key Pinning (Static) Long handshake intolerance	Yes includeSubDomains: true report-uri: http://clients3.google.com/cert_upload_json pin-sha256: IPMbDAjLVSGntGO3WP53X/zilCVndez5YJ2+vJvhJsA= pin-sha256: YZPgTZ+woNCCCIW3LH2CxQeLzB/Im42QcCTBSdgayjs= pin-sha256: hxqRIPTu1bMS/0DITB1SSu0vd4w/8l8TjPgfaAp63Gc= pin-sha256: Vfd95BwDeSQo+NUYxVEEllvkOIWY2SalKK1IPhzOx78= pin-sha256: Qxnt2YHvdHR3tJYmQIr0Paosp6t/nggsEGD4QJZ3Q0g= pin-sha256: mEliZT5enoR1FuXLgYYQqnVEoZvmf9c2bVBpiOjYQ0c= pin-sha256: iie1VXtL7HzAMF+/FVPR9xzT80kQxdZeJ+zduCB3uj0= pin-sha256: hxrRCWbljB5FGRZv++qAms7uX69qFC45aBhVpeGcloc= (Forbidden) pin-sha256: SG/sBoMJc9lgJ8+dGgIHyTLvz7wyVBio7IMoDanPuRk= (Forbidden) pin-sha256: LvRiGEjRqfzurezaWuj8Wie2gyHMrW5Q06LspMnox7A= (Forbidden) No
Public Key Pinning (Static) Long handshake intolerance TLS extension intolerance	Yes includeSubDomains: true report-uri: http://clients3.google.com/cert_upload_json pin-sha256: IPMbDAjLVSGntGO3WP53X/zilCVndez5YJ2+vJvhJsA= pin-sha256: YZPgTZ+woNCCCIW3LH2CxQeLzB/1m42QcCTBSdgayjs= pin-sha256: hxqRIPTu1bMS/0DITB1SSu0vd4w/8l8TjPgfaAp63Gc= pin-sha256: Vfd95BwDesQo+NUYxVEEIlvkOIWY2SalKK1IPhzOx78= pin-sha256: Qxnt2YHvdHR3tJYmQIr0Paosp6t/nggsEGD4QJZ3Q0g= pin-sha256: mEflZT5enoR1FuXLgYYGqnVEoZvmf9c2bVBpiOjYQ0c= pin-sha256: ile1VXtL7HzAMF+/PVPR9xzT80kQxdZeJ+zduCB3uj0= pin-sha256: hxrRCWbjB5FGRZv++qAms7uX69qFC45aBhVpeGclco= (Forbidden) pin-sha256: SG/sBoMJc9lgJ8+dGgIHyTLvz7wyVBio7IMoDanPuRk= (Forbidden) pin-sha256: LvRiGEjRqfzurezaWuj8Wie2gyHMrW5Q06LspMnox7A= (Forbidden) No
Public Key Pinning (Static) Long handshake intolerance TLS extension intolerance TLS version intolerance	Yes includeSubDomains: true report-uri: http://clients3.google.com/cert_upload_json pin-sha256: IPMbbAjLVSGntGO3WP53X/zilCVndez5YJ2+vJvhJsA= pin-sha256: YZPgTZ+woNCCClW3LH2CxQeLzB/Im42QcCTBSdgayjs= pin-sha256: Vfd95BwDeSQo+NUYxVEEIlvk0lWY2SalKK1IPhzOx78= pin-sha256: Vfd95BwDeSQo+NUYxVEEIlvk0lWY2SalKK1IPhzOx78= pin-sha256: Qxnt2YHvdHR3tJYmQIn0Paosp6VnggsEGD4QJZ3Q0g= pin-sha256: mEflZT5enoR1FuXLgYYGqnVEoZvmf9c2bVBpiOjYQ0c= pin-sha256: ite1VXtL7HzAMF+/PVPR9xZT80kQxdZeJ+zduCB3uj0= pin-sha256: hxrRCWbljB5FGRZv++qAms7uX69qFC45aBhVpeGclco= (Forbidden) pin-sha256: SG/sBoMJc9lgJ8+dGgIHyTLvz7wyvBio7lMoDanPuRk= (Forbidden) pin-sha256: LvRiGEjRqfzurezaWuj8Wie2gyHMrW5Q06LspMnox7A= (Forbidden) No No
Public Key Pinning (Static) Long handshake intolerance TLS extension intolerance TLS version intolerance Incorrect SNI alerts	Yes includeSubDomains: true report-uri: http://clients3.google.com/cert_upload_json pin-sha256: IPMbbDAjLVSGntGO3WP53X/zilCVndez5YJ2+vJvhJsA= pin-sha256: YZPgTZ+woNCCCIW3LH2CxQeLzB/1m42QcCTBSdgayjs= pin-sha256: hxqRIPTu1bMS/0DITB1SSu0vd4w(8I8TjPgfaAp63Gc= pin-sha256: Vfd95BwDeSQo+NUYxVEElivkOIWY2SalKK1IPhzOx78= pin-sha256: Qxnt2YHvdHR3tJYmQIr0Paosp6t/nggsEGD4QJZ3Q0g= pin-sha256: mefitZT5enoR1FuXLgYYGqnVEoZvmf9c2bVBpiOJYQ0c= pin-sha256: iie1VXtL7HzAMF+/PVPR9xZT80kQxdz4z+zduCB3uj0= pin-sha256: hxrRCWbljB5FGRZv++qAms7uX69qFC45aBhVpeGclco= (Forbidden) pin-sha256: SG/sBoMJc9lgJ8+dGglHyTLvz7wyVBio7IMoDanPuRk= (Forbidden) pin-sha256: LvRiGEjRqfzurezaWuj8Wie2gyHMrW5Q06LspMnox7A= (Forbidden) No No
Public Key Pinning (Static) Long handshake intolerance TLS extension intolerance TLS version intolerance Incorrect SNI alerts Uses common DH primes	includeSubDomains: true report-uri: http://clients3.google.com/cert_upload_json pin-sha256: IPMbDAjLVSGntGO3WP53X/zilCVndez5YJ2+vJvhJsA= pin-sha256: YzPgTZ+woNCCCIW3LH2CxQeLzB/Ima2QcCTBSdgayjs= pin-sha256: hxqRIPTu1bMS/0DITB1SSu0vd4w/8l8TjPgfaAp63Gc= pin-sha256: Vfd95BwDeSQo+NUVxVEEllvkOIWV2SalKK1IPhzOx78= pin-sha256: OXnt2YHvdHR3tJYmQIr0Paosp6t/nggsEGD4QJZ3Q0g= pin-sha256: mEflZT5enoR1FuXLgYYQqnVEoZvmf9c2bVBpiOjYQ0c= pin-sha256: iie1VXtL7HzAMF+/PVPR9xZT80kQxdZeJ+zduCB3uj0= pin-sha256: hxrRCWbljB5FGRZv++qAms7uX69qFC45aBhVpeGclco= (Forbidden) pin-sha256: SG/sBoMJc9lgJ8+dGgIHyTLvz7wyVBio7IMoDanPuRk= (Forbidden) pin-sha256: LvRiGEjRqfzurezaWuj8Wie2gyHMrW5Q06LspMnox7A= (Forbidden) No No No No
Public Key Pinning (Static) Long handshake intolerance TLS extension intolerance TLS version intolerance Incorrect SNI alerts Uses common DH primes DH public server param (Ys) reuse	Yes includeSubDomains: true report-uri: http://clients3.google.com/cert_upload_json pin-sha256: IPMbbAjLVSGntGO3WP53X/zilCVndez5YJ2+vJvhJsA= pin-sha256: YZPgTZ+woNCCClW3LH2CxQeLzB/Im42QcCTBSdgayjs= pin-sha256: Vfd95BwDeSQo+NUYxVEEIlwk0lW2SalKK1IPhzOx78= pin-sha256: Vfd95BwDeSQo+NUYxVEEIlwk0lW2SalKK1IPhzOx78= pin-sha256: Qxnt2YHvdHR3tJYmQIn0Paosp6t/nggsEGD4QJZ3Q0g= pin-sha256: mEflZT5enoR1FuXLgYYGqnVEoZvmf9c2bVBpiOjYQ0c= pin-sha256: ite1VXtL7HzAMF+/PVPR9xZT80kQxdZeJ+zduCB3uj0= pin-sha256: hxrRCWbljB5FGRZv++qAms7uX69qFC45aBhVpeGcloc= (Forbidden) pin-sha256: SG/sBoMJc9lgJ8+dGgIHyTLvz7wyvBio7lMoDanPuRk= (Forbidden) pin-sha256: LvRiGEjRqfzurezaWuj8Wie2gyHMrW5Q06LspMnox7A= (Forbidden) No No No No DHE suites not supported No, DHE suites not supported



HTTP Requests

0-RTT enabled

SSL 2 handshake compatibility





Yes

No



Miscellaneous

Test date	Fri, 22 Oct 2021 08:37:23 UTC
Test duration	104.363 seconds
HTTP status code	301
HTTP forwarding	https://www.youtube.com
HTTP server signature	ESF
Server hostname	sfo03s07-in-f14.1e100.net

SSL Report v2.1.8

Copyright © 2009-2021 Qualys, Inc. All Rights Reserved.

Terms and Conditions

<u>Try Qualys for free!</u> Experience the award-winning <u>Qualys Cloud Platform</u> and the entire collection of <u>Qualys Cloud Apps</u>, including <u>certificate security</u> solutions.