Valid until	Tue Feb 18 22:59:26 UTC 2020 (expires in 5 years and 9 months)
Key	RSA 2048 bits
Issuer	GeoTrust Global CA
Signature algorithm	SHA1withRSA

Certification Paths

Path #1: Trusted

1	Sent by server	www.nsa.gov SHA1: ac40f58487a796c69efc7d62f513f523a1cdd9c6 RSA 2048 bits / SHA1withRSA
2	Sent by server	GeoTrust SSL CA SHA1: 780a06f6e9b4061cad0c6502710606eb535f1c26 RSA 2048 bits / SHA1withRSA
3	In trust store	GeoTrust Global CA SHA1: de28f4a4ffe5b92fa3c503d1a349a7f9962a8212 RSA 2048 bits / SHA1withRSA

Configuration

Protocols

TLS 1.2	Yes
TLS 1.1	Yes
TLS 1.0	Yes
SSL 3	Yes
SSL 2	No

Cipher Suites (sorted by strength; the server has no preference)

TLS_RSA_EXPORT_WITH_RC4_40_MD5 (0x3) **WEAK**	40
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5 (0x6) **WEAK**	40
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA (0x8) **WEAK**	40
TLS_RSA_WITH_DES_CBC_SHA (0x9) **WEAK**	56
TLS_RSA_WITH_RC4_128_MD5 (0x4)	128
TLS_RSA_WITH_RC4_128_SHA (0x5)	128
TLS_RSA_WITH_IDEA_CBC_SHA (0x7)	128
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	128
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa)	112
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)	256

Handshake Simulation

Android 2.3.7 No SNI [2]	TLS 1.0	TLS_RSA_WITH_RC4_128_MD5 (0x4) No FS RC4	128
Android 4.0.4	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA (0x35) No FS	256
Android 4.1.1	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA (0x35) No FS	256
Android 4.2.2	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA (0x35) No FS	256
Android 4.3	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA (0x35) No FS	256
Android 4.4.2	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA (0x35) No FS	256
BingBot Dec 2013 No SNI [2]	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) No FS	128
BingPreview Dec 2013	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA (0x35) No FS	256
Chrome 33 / Win 7 R	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA (0x35) No FS	256
Firefox 24.2.0 ESR / Win 7	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA (0x35) No FS	256