

You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > www.edge.nhs.uk

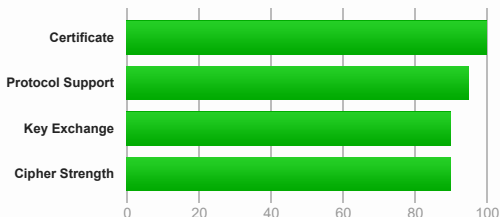
SSL Report: www.edge.nhs.uk (83.98.30.179)

Assessed on: Wed, 26 Oct 2016 13:40:00 UTC | [HIDDEN](#) | [Clear cache](#)

[Scan Another »](#)

Summary

Overall Rating



Visit our [documentation page](#) for more information, configuration guides, and books. Known issues are documented [here](#).

Authentication



Server Key and Certificate #1



Subject	*.edge.nhs.uk Fingerprint SHA1: 74c84e21aed3732bf29a68fe12922b32eea793ca Pin SHA256: MGkkR/OAKQOSJURVWvmHW0T/6KFicLRPHr1CeWrN/XA=
Common names	*.edge.nhs.uk
Alternative names	*.edge.nhs.uk edge.nhs.uk
Valid from	Thu, 16 Apr 2015 10:27:05 UTC
Valid until	Fri, 31 Mar 2017 13:00:02 UTC (expires in 5 months and 4 days)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	GlobalSign Organization Validation CA - SHA256 - G2 AIA: http://secure.globalsign.com/cacert/gsignorganizationvalsha2g2r1.crt
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	No
OCSP Must Staple	No
Revocation information	CRL, OCSP CRL: http://crl.globalsign.com/gsignorganizationvalsha2g2r1.crt OCSP: http://ocsp2.globalsign.com/gsignorganizationvalsha2g2r1.crt
Revocation status	Good (not revoked)
Trusted	Yes



Additional Certificates (if supplied)



Certificates provided	2 (2486 bytes)
Chain issues	None

#2

Subject	GlobalSign Organization Validation CA - SHA256 - G2 Fingerprint SHA1: 902ef2deeb3c5b13ea4c3d5193629309e231ae55 Pin SHA256: IQBnNBEiFuhj+8x6X8XLgh01V9lc5/V3IRQLNFFc7v4=
Valid until	Tue, 20 Feb 2024 10:00:00 UTC (expires in 7 years and 3 months)
Key	RSA 2048 bits (e 65537)
Issuer	GlobalSign Root CA
Signature algorithm	SHA256withRSA



Certification Paths

Path #1: Trusted

1	Sent by server	<p>*.edge.nhs.uk</p> <p>Fingerprint SHA1: 74c84e21aed3732bf29a68fe12922b32eea793ca</p> <p>Pin SHA256: MGkkR/OAKQOSIJRVVwmHW0T/6KFicLRPHr1CeWrN/XA=</p> <p>RSA 2048 bits (e 65537) / SHA256withRSA</p>
2	Sent by server	<p>GlobalSign Organization Validation CA - SHA256 - G2</p> <p>Fingerprint SHA1: 902ef2deeb3c5b13ea4c3d5193629309e231ae55</p> <p>Pin SHA256: IQBnNBEIFuhj+8x6X8XLgh01V9lc5/V3IRQLNFFc7v4=</p> <p>RSA 2048 bits (e 65537) / SHA256withRSA</p>
3	In trust store	<p>GlobalSign Root CA Self-signed</p> <p>Fingerprint SHA1: b1bc9e8bd4f49d622aa89a81f2150152a41d829c</p> <p>Pin SHA256: K87oWBWM9UZfyddvDfoXL+8lpNy0UB2ptGtn0fv6G2Q=</p> <p>RSA 2048 bits (e 65537) / SHA1withRSA</p> <p>Weak or insecure signature, but no impact on root certificate</p>

Path #2: Trusted

1	Sent by server	<p>*.edge.nhs.uk</p> <p>Fingerprint SHA1: 74c84e21aed3732bf29a68fe12922b32eea793ca</p> <p>Pin SHA256: MGkkR/OAKQOSIJRVVwmHW0T/6KFicLRPHr1CeWrN/XA=</p> <p>RSA 2048 bits (e 65537) / SHA256withRSA</p>
2	Extra download	<p>GlobalSign Organization Validation CA - SHA256 - G2</p> <p>Fingerprint SHA1: ef90b2b86f4756ebe7d36f3015d63523a0078e9</p> <p>Pin SHA256: IQBnNBEIFuhj+8x6X8XLgh01V9lc5/V3IRQLNFFc7v4=</p> <p>RSA 2048 bits (e 65537) / SHA256withRSA</p>
3	In trust store	<p>GlobalSign Self-signed</p> <p>Fingerprint SHA1: d69b561148f01c77c54578c10926df5b856976ad</p> <p>Pin SHA256: cGuxAXyFXFKWm61cF4HPWX8S0srS9j0aSqN0k4AP+4A=</p> <p>RSA 2048 bits (e 65537) / SHA256withRSA</p>

Configuration



Protocols

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



Cipher Suites (SSL 3+ suites in server-preferred order; deprecated and SSL 2 suites at the end)

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)	ECDH secp521r1 (eq. 15360 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)	ECDH secp521r1 (eq. 15360 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	ECDH secp521r1 (eq. 15360 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	ECDH secp521r1 (eq. 15360 bits RSA) FS	128
TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d)		256
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c)		128
TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d)		256
TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c)		128
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)		256
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)		128
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa)		112



Handshake Simulation

Android 2.3.7 No SNI ²	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA	No FS
Android 4.0.4	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp521r1 FS
Android 4.1.1	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp521r1 FS
Android 4.2.2	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp521r1 FS
Android 4.3	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp521r1 FS
Android 4.4.2	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	ECDH secp521r1 FS
Android 5.0.0	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp521r1 FS
Android 6.0	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp384r1 FS

Handshake Simulation

Android 7.0	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp384r1	FS
Baidu Jan 2015	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp521r1	FS
BingPreview Jan 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp521r1	FS
Chrome 49 / XP SP3	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp384r1	FS
Chrome 51 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp384r1	FS
Firefox 31.3.0 ESR / Win 7	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp521r1	FS
Firefox 47 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp521r1	FS
Firefox 49 / XP SP3	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp521r1	FS
Firefox 49 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp521r1	FS
Googlebot Feb 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp521r1	FS
IE 6 / XP No FS ¹ No SNI ²	Server closed connection				
IE 7 / Vista	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp521r1	FS
IE 8 / XP No FS ¹ No SNI ²	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_3DES_EDE_CBC_SHA		
IE 8-10 / Win 7 R	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp521r1	FS
IE 11 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp384r1	FS
IE 11 / Win 8.1 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp384r1	FS
IE 10 / Win Phone 8.0	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp384r1	FS
IE 11 / Win Phone 8.1 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	ECDH secp384r1	FS
IE 11 / Win Phone 8.1 Update R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp384r1	FS
IE 11 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp384r1	FS
Edge 13 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp384r1	FS
Edge 13 / Win Phone 10 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp384r1	FS
Java 6u45 No SNI ²	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA	No FS	
Java 7u25	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp521r1	FS
Java 8u31	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	ECDH secp521r1	FS
OpenSSL 0.9.8y	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA	No FS	
OpenSSL 1.0.1j R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp521r1	FS
OpenSSL 1.0.2e R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp521r1	FS
Safari 5.1.9 / OS X 10.6.8	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp521r1	FS
Safari 6 / iOS 6.0.1	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp521r1	FS
Safari 6.0.4 / OS X 10.8.4 R	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp521r1	FS
Safari 7 / iOS 7.1 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp521r1	FS
Safari 7 / OS X 10.9 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp521r1	FS
Safari 8 / iOS 8.4 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp521r1	FS
Safari 8 / OS X 10.10 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp521r1	FS
Safari 9 / iOS 9 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp521r1	FS
Safari 9 / OS X 10.11 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp521r1	FS
Safari 10 / iOS 10 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp521r1	FS
Safari 10 / OS X 10.12 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp521r1	FS
Apple ATS 9 / iOS 9 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp521r1	FS
Yahoo Slurp Jan 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp384r1	FS
YandexBot Jan 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp521r1	FS

(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) 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).



Protocol Details

	Check failed
	(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 test here
	(3) Censys data is only indicative of possible key and certificate reuse; possibly out-of-date and not complete
	ERROR: Connection refused
	ERROR: Connection refused
Secure Renegotiation	Supported
Secure Client-Initiated Renegotiation	No
Insecure Client-Initiated Renegotiation	No
BEAST attack	Not mitigated server-side (more info) TLS 1.0: 0xc014
POODLE (SSLv3)	No, SSL 3 not supported (more info)

Protocol Details

POODLE (TLS)	No (more info)
Downgrade attack prevention	No, TLS_FALLBACK_SCSV not supported (more info)
SSL/TLS compression	No
RC4	No
Heartbeat (extension)	No
Heartbleed (vulnerability)	No (more info)
OpenSSL CCS vuln. (CVE-2014-0224)	No (more info)
OpenSSL Padding Oracle vuln. (CVE-2016-2107)	No (more info)
Forward Secrecy	With modern browsers (more info)
ALPN	No
NPN	No
Session resumption (caching)	Yes
Session resumption (tickets)	No
OCSP stapling	No
Strict Transport Security (HSTS)	No
HSTS Preloading	Not in: Chrome Edge Firefox IE
Public Key Pinning (HPKP)	No
Public Key Pinning Report-Only	No
Long handshake intolerance	No
TLS extension intolerance	No
TLS version intolerance	No
Incorrect SNI alerts	No
Uses common DH primes	No, DHE suites not supported
DH public server param (Ys) reuse	No, DHE suites not supported
SSL 2 handshake compatibility	Yes

**Miscellaneous**

Test date	Wed, 26 Oct 2016 13:38:22 UTC
Test duration	98.181 seconds
HTTP status code	200
HTTP server signature	Microsoft-IIS/8.5
Server hostname	-

SSL Report v1.24.4