SSL Report: hk.guger.ml (149.129.104.107)
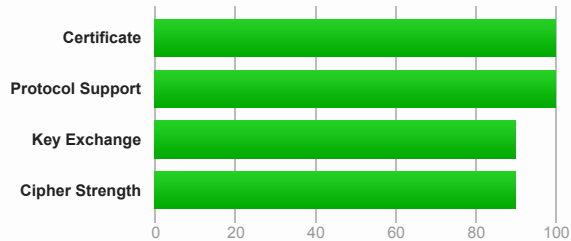
Assessed on: Thu, 14 Feb 2019 01:24:22 UTC | Hide | Clear cache

Scan Another »

Summary

Overall Rating

A+

	0	20	40	60	80	100
Certificate						
Protocol Support						
Key Exchange						
Cipher Strength						

Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

Renegotiation test has been disabled temporarily due to an Apache httpd 2.4.37 bug. **MORE INFO »**

Experimental: This server supports TLS 1.3 (RFC 8446).

HTTP Strict Transport Security (HSTS) with long duration deployed on this server. **MORE INFO »**

DNS Certification Authority Authorization (CAA) Policy found for this domain. **MORE INFO »**

Certificate #1: RSA 2048 bits (SHA256withRSA)

Server Key and Certificate #1

Subject	hk.guger.ml Fingerprint SHA256: fb7fa6250a60e30e2792e67efc9023ee5d48e2342f3f7baf9252bcf5961770e2 Pin SHA256: srFhCYxORRaEI3n6eJQ1omgnhSyqkD6xZ2viBKzTBhk=
Common names	hk.guger.ml
Alternative names	hk.guger.ml
Serial Number	03b559e469899318b96439ee8065c8b9da82
Valid from	Sat, 19 Jan 2019 13:48:51 UTC
Valid until	Fri, 19 Apr 2019 13:48:51 UTC (expires in 2 months and 5 days)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	Let's Encrypt Authority X3 AIA: http://cert.int-x3.letsencrypt.org/
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	Yes (certificate)
OCSP Must Staple	No
Revocation information	OCSP OCSP: http://ocsp.int-x3.letsencrypt.org
Revocation status	Good (not revoked)
DNS CAA	Yes policy host: hk.guger.ml issue: letsencrypt.org flags:0
Trusted	Yes Mozilla Apple Android Java Windows

Additional Certificates (if supplied)

Additional Certificates (if supplied)

Certificates provided	2 (2538 bytes)
Chain issues	None

#2

Subject	Let's Encrypt Authority X3
	Fingerprint SHA256: 25847d668eb4f04fdd40b12b6b0740c567da7d024308eb6c2c96fe41d9de218d
	Pin SHA256: YLh1dUR9y6Kja30RrAn7JKnbQG/uEtLMkBgFF2Fuihg=
Valid until	Wed, 17 Mar 2021 16:40:46 UTC (expires in 2 years and 1 month)
Key	RSA 2048 bits (e 65537)
Issuer	DST Root CA X3
Signature algorithm	SHA256withRSA

Certification Paths

Click here to expand

Configuration

Protocols

TLS 1.3	Yes
TLS 1.2	Yes
TLS 1.1	No
TLS 1.0	No
SSL 3	No
SSL 2	No

For TLS 1.3 tests, we only support RFC 8446.

Cipher Suites

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 (server has no preference)

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ECDH x25519 (eq. 3072 bits RSA) FS		128
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) ECDH x25519 (eq. 3072 bits RSA) FS		128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ECDH x25519 (eq. 3072 bits RSA) FS		256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) ECDH x25519 (eq. 3072 bits RSA) FS		256
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8) ECDH x25519 (eq. 3072 bits RSA) FS		256

Handshake Simulation

Android 4.4.2	RSA 2048 (SHA256)	TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Android 5.0.0	RSA 2048 (SHA256)	TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS
Android 6.0	RSA 2048 (SHA256)	TLS 1.2 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Android 7.0	RSA 2048 (SHA256)	TLS 1.2 TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 ECDH x25519 FS
BingPreview Jan 2015	RSA 2048 (SHA256)	TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Chrome 49 / XP SP3	RSA 2048 (SHA256)	TLS 1.2 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Chrome 69 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS
Chrome 70 / Win 10	-	TLS 1.3 TLS_AES_128_GCM_SHA256 ECDH x25519 FS
Firefox 31.3.0 ESR / Win 7	RSA 2048 (SHA256)	TLS 1.2 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Firefox 47 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Firefox 49 / XP SP3	RSA 2048 (SHA256)	TLS 1.2 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Firefox 62 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS
Googlebot Feb 2018	RSA 2048 (SHA256)	TLS 1.2 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS

Handshake Simulation

Client		Cert	Protocol & Cipher	Key Exchange	FS
IE 11 / Win 7	R	RSA 2048 (SHA256)	TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1	FS
IE 11 / Win 8.1	R	RSA 2048 (SHA256)	TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1	FS
IE 11 / Win Phone 8.1	R	RSA 2048 (SHA256)	TLS 1.2 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp256r1	FS
IE 11 / Win Phone 8.1 Update	R	RSA 2048 (SHA256)	TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1	FS
IE 11 / Win 10	R	RSA 2048 (SHA256)	TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
Edge 15 / Win 10	R	RSA 2048 (SHA256)	TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH x25519	FS
Edge 13 / Win Phone 10	R	RSA 2048 (SHA256)	TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
Java 8u161		RSA 2048 (SHA256)	TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1	FS
OpenSSL 1.0.1l	R	RSA 2048 (SHA256)	TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
OpenSSL 1.0.2e	R	RSA 2048 (SHA256)	TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
Safari 6 / iOS 6.0.1		RSA 2048 (SHA256)	TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1	FS
Safari 7 / iOS 7.1	R	RSA 2048 (SHA256)	TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1	FS
Safari 7 / OS X 10.9	R	RSA 2048 (SHA256)	TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1	FS
Safari 8 / iOS 8.4	R	RSA 2048 (SHA256)	TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1	FS
Safari 8 / OS X 10.10	R	RSA 2048 (SHA256)	TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1	FS
Safari 9 / iOS 9	R	RSA 2048 (SHA256)	TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
Safari 9 / OS X 10.11	R	RSA 2048 (SHA256)	TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
Safari 10 / iOS 10	R	RSA 2048 (SHA256)	TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
Safari 10 / OS X 10.12	R	RSA 2048 (SHA256)	TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
Apple ATS 9 / iOS 9	R	RSA 2048 (SHA256)	TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
Yahoo Slurp Jan 2015		RSA 2048 (SHA256)	TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
YandexBot Jan 2015		RSA 2048 (SHA256)	TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS

 # Not simulated clients (Protocol mismatch) ✚

Click here to expand

(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).

(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 complete
BEAST attack	Mitigated server-side (more info)
POODLE (SSLv3)	No, SSL 3 not supported (more info)
POODLE (TLS)	No (more info)
Downgrade attack prevention	Yes, TLS_FALLBACK_SCSV supported (more info)
SSL/TLS compression	No
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	Yes (with most browsers) ROBUST (more info)
ALPN	No
NPN	No
Session resumption (caching)	No (IDs empty)
Session resumption (tickets)	Yes
OCSP stapling	No
Strict Transport Security (HSTS)	Yes max-age=31536000; includeSubDomains; preload

Protocol Details

HSTS Preloading	Not in: Chrome Edge Firefox IE
Public Key Pinning (HPKP)	No ([more info](#))
Public Key Pinning Report-Only	No
Public Key Pinning (Static)	No ([more info](#))
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
ECDH public server param reuse	No
Supported Named Groups	x25519, secp256r1, secp384r1, secp521r1 (server preferred order)
SSL 2 handshake compatibility	No

HTTP Requests ⊞

1 **https://hk.guger.ml/** (HTTP/1.1 200 OK)

Miscellaneous

Test date	Thu, 14 Feb 2019 01:23:26 UTC
Test duration	56.162 seconds
HTTP status code	200
HTTP server signature	nginx/1.14.2
Server hostname	-

SSL Report v1.32.16