SSL Report: peahi.be (65.8.158.121)

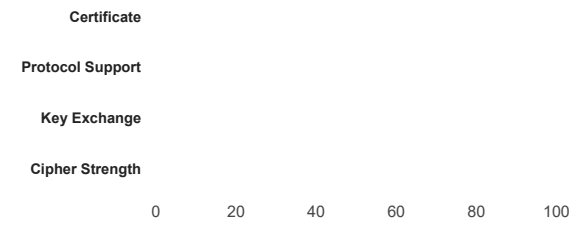
Assessed on: Sat, 11 Dec 2021 14:34:05 UTC | Clear cache

Scan Another »

Summary

Overall Rating

A+



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

This site works only in browsers with SNI support.

This server supports TLS 1.3.

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	peahi.be Fingerprint SHA256: 108b36d2b5ac7bf6639c4124a4b737b454f4932539cfacf9b2a80007ccd6e558 Pin SHA256: QEut/o6li05x/nBFklhGVU17En5GJ/cwlKyacrpLMvY=
Common names	peahi.be
Alternative names	peahi.be *.peahi.be
Serial Number	0476b2d9aaa07d537723e060a7662ec0
Valid from	Wed, 10 Nov 2021 00:00:00 UTC
Valid until	Fri, 09 Dec 2022 23:59:59 UTC (expires in 11 months and 28 days)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	Amazon AIA: http://crt.sca1b.amazontrust.com/sca1b.crt
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	Yes (certificate)
OCSP Must Staple	No
Revocation information	CRL, OCSP CRL: http://crl.sca1b.amazontrust.com/sca1b-1.crl OCSP: http://ocsp.sca1b.amazontrust.com
Revocation status	Good (not revoked)
DNS CAA	Yes policy host: peahi.be issue: amazon.com flags:0
Trusted	Yes Mozilla Apple Android Java Windows

Additional Certificates (if supplied)

Certificates provided	4 (4915 bytes)
Chain issues	None

#2

Subject	Amazon Fingerprint SHA256: f55f9ffcb83c73453261601c7e044db15a0f034b93c05830f28635ef889cf670 Pin SHA256: JSMzqOOrtyOT1kmau6zKhgT676hGgczD5VMdRMyJZFA=
Valid until	Sun, 19 Oct 2025 00:00:00 UTC (expires in 3 years and 10 months)
Key	RSA 2048 bits (e 65537)
Issuer	Amazon Root CA 1
Signature algorithm	SHA256withRSA

#3

Subject	Amazon Root CA 1 Fingerprint SHA256: 87dcd4dc74640a322cd205552506d1be64f12596258096544986b4850bc72706 Pin SHA256: ++MBgDH5WGvL9Bcn5Be30cRcL0f5O+NyoXuWtQdX1aI=
Valid until	Thu, 31 Dec 2037 01:00:00 UTC (expires in 16 years)
Key	RSA 2048 bits (e 65537)
Issuer	Starfield Services Root Certificate Authority - G2
Signature algorithm	SHA256withRSA

#4

Subject	Starfield Services Root Certificate Authority - G2 Fingerprint SHA256: 28689b30e4c306aab53b027b29e36ad6dd1dcf4b953994482ca84bdc1ecac996 Pin SHA256: KwccWaCgrnaw6tsrrSO61FgLacNgG2MMLq8GE6+oP5I=
Valid until	Wed, 28 Jun 2034 17:39:16 UTC (expires in 12 years and 6 months)
Key	RSA 2048 bits (e 65537)
Issuer	Starfield Technologies, Inc. / Starfield Class 2 Certification Authority
Signature algorithm	SHA256withRSA

Certification Paths

Mozilla Apple Android Java Windows

Mozilla Apple Android Java Windows

Path #1: Trusted

1	Sent by server	peahi.be Fingerprint SHA256: 108b36d2b5ac7bf6639c4124a4b737b454f4932539cfacf9b2a80007ccd6e558 Pin SHA256: QEut/o6li05x/nBFklhGVU17En5GJ/cwIKyacrpLMvY= RSA 2048 bits (e 65537) / SHA256withRSA
2	Sent by server	Amazon Fingerprint SHA256: f55f9ffcb83c73453261601c7e044db15a0f034b93c05830f28635ef889cf670 Pin SHA256: JSMzqOOrtyOT1kmau6zKhgT676hGgczD5VMdRMyJZFA= 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

Path #2: Trusted

1	Sent by server	peahi.be Fingerprint SHA256: 108b36d2b5ac7bf6639c4124a4b737b454f4932539cfacf9b2a80007ccd6e558 Pin SHA256: QEut/o6li05x/nBFklhGVU17En5GJ/cwIKyacrpLMvY= RSA 2048 bits (e 65537) / SHA256withRSA
2	Sent by server	Amazon Fingerprint SHA256: f55f9ffcb83c73453261601c7e044db15a0f034b93c05830f28635ef889cf670 Pin SHA256: JSMzqOOrtyOT1kmau6zKhgT676hGgczD5VMdRMyJZFA= RSA 2048 bits (e 65537) / SHA256withRSA
3	Sent by server	Amazon Root CA 1 Fingerprint SHA256: 87dcd4dc74640a322cd205552506d1be64f12596258096544986b4850bc72706 Pin SHA256: ++MBgDH5WGvL9Bcn5Be30cRcL0f5O+NyoXuWtQdX1aI= RSA 2048 bits (e 65537) / SHA256withRSA
4	In trust store	Starfield Services Root Certificate Authority - G2 Self-signed Fingerprint SHA256: 568d6905a2c88708a4b3025190edcfedb1974a606a13c6e5290fcb2ae63edab5 Pin SHA256: KwccWaCgrnaw6tsrrSO61FgLacNgG2MMLq8GE6+oP5I= RSA 2048 bits (e 65537) / SHA256withRSA

Path #3: Trusted

1	Sent by server	peahi.be Fingerprint SHA256: 108b36d2b5ac7bf6639c4124a4b737b454f4932539cfacf9b2a80007ccd6e558 Pin SHA256: QEut/o6li05x/nBFklhGVU17En5GJ/cwIKyacrpLMvY= RSA 2048 bits (e 65537) / SHA256withRSA
2	Sent by server	Amazon Fingerprint SHA256: f55f9ffcb83c73453261601c7e044db15a0f034b93c05830f28635ef889cf670 Pin SHA256: JSMzqOOrtyOT1kmau6zKhgT676hGgczD5VMdRMyJZFA= RSA 2048 bits (e 65537) / SHA256withRSA
3	Sent by server	Amazon Root CA 1 Fingerprint SHA256: 87dcd4dc74640a322cd205552506d1be64f12596258096544986b4850bc72706 Pin SHA256: ++MBgDH5WGvL9Bcn5Be30cRcL0f5O+NyoXuWtQdX1aI= RSA 2048 bits (e 65537) / SHA256withRSA
4	Sent by server	Starfield Services Root Certificate Authority - G2 Fingerprint SHA256: 28689b30e4c306aab53b027b29e36ad6dd1dcf4b953994482ca84bdc1ecac996 Pin SHA256: KwccWaCgrnaw6tsrrSO61FgLacNgG2MMLq8GE6+oP5I= RSA 2048 bits (e 65537) / SHA256withRSA
5	In trust store	Starfield Technologies, Inc. / Starfield Class 2 Certification Authority Self-signed Fingerprint SHA256: 1465fa205397b876faa6f0a9958e5590e40fcc7faa4fb7c2c8677521fb5fb658 Pin SHA256: FfFKxFycfaIz00eRZOgTf+Ne4POK6FgYPwhBDqgqxLQ= RSA 2048 bits (e 3) / SHA1withRSA Weak or insecure signature, but no impact on root certificate

Configuration

Protocols

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

Cipher Suites

TLS 1.3 (suites in server-preferred order)

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_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	ECDH x25519 (eq. 3072 bits RSA) FS	128
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_128_GCM_SHA256 ECDH secp256r1 FS
Android 5.0.0	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Android 6.0	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Android 7.0	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS
Android 8.0	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS
Android 8.1	-	TLS 1.3	TLS_AES_128_GCM_SHA256 ECDH x25519 FS
Android 9.0	-	TLS 1.3	TLS_AES_128_GCM_SHA256 ECDH x25519 FS
BingPreview Jan 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Chrome 49 / XP SP3	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Chrome 69 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2 > h2	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
Chrome 80 / Win 10 R	-	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 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Firefox 49 / XP SP3	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Firefox 62 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_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	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS
IE 11 / Win 7 R	Protocol or cipher suite mismatch		
IE 11 / Win 8.1 R	Protocol or cipher suite mismatch		
IE 11 / Win Phone 8.1 R	Protocol or cipher suite mismatch		
IE 11 / Win Phone 8.1 Update R	Protocol or cipher suite mismatch		
IE 11 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Edge 15 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS
Edge 16 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS
Edge 18 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS
Edge 13 / Win Phone 10 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Java 8u161	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Java 11.0.3	-	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 1.0.1l R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_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	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS
OpenSSL 1.1.1c R	-	TLS 1.3	TLS_AES_128_GCM_SHA256 ECDH x25519 FS
Safari 6 / iOS 6.0.1	Protocol or cipher suite mismatch		
Safari 7 / iOS 7.1 R	Protocol or cipher suite mismatch		
Safari 7 / OS X 10.9 R	Protocol or cipher suite mismatch		
Safari 8 / iOS 8.4 R	Protocol or cipher suite mismatch		
Safari 8 / OS X 10.10 R	Protocol or cipher suite mismatch		
Safari 9 / iOS 9 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Safari 9 / OS X 10.11 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Safari 10 / iOS 10 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS

Handshake Simulation

Safari 10 / OS X 10.12 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Safari 12.1.2 / MacOS 10.14.6 Beta R	-	TLS 1.3	TLS_AES_128_GCM_SHA256 ECDH x25519 FS
Safari 12.1.1 / iOS 12.3.1 R	-	TLS 1.3	TLS_AES_128_GCM_SHA256 ECDH x25519 FS
Apple ATS 9 / iOS 9 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Yahoo Slurp Jan 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
YandexBot Jan 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS

Not simulated clients (Protocol mismatch)

Android 2.3.7 No SNI [2]	Protocol mismatch (not simulated)
Android 4.0.4	Protocol mismatch (not simulated)
Android 4.1.1	Protocol mismatch (not simulated)
Android 4.2.2	Protocol mismatch (not simulated)
Android 4.3	Protocol mismatch (not simulated)
Baidu Jan 2015	Protocol mismatch (not simulated)
IE 6 / XP No FS [1] No SNI [2]	Protocol mismatch (not simulated)
IE 7 / Vista	Protocol mismatch (not simulated)
IE 8 / XP No FS [1] No SNI [2]	Protocol mismatch (not simulated)
IE 8-10 / Win 7 R	Protocol mismatch (not simulated)
IE 10 / Win Phone 8.0	Protocol mismatch (not simulated)
Java 6u45 No SNI [2]	Protocol mismatch (not simulated)
Java 7u25	Protocol mismatch (not simulated)
OpenSSL 0.9.8y	Protocol mismatch (not simulated)
Safari 5.1.9 / OS X 10.6.8	Protocol mismatch (not simulated)
Safari 6.0.4 / OS X 10.8.4 R	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) 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
Secure Renegotiation	**Supported**
Secure Client-Initiated Renegotiation	No
Insecure Client-Initiated Renegotiation	No
BEAST attack	Mitigated server-side (more info)
POODLE (SSLv3)	No, SSL 3 not supported (more info)
POODLE (TLS)	No (more info)
Zombie POODLE	No (more info)
GOLDENDOODLE	No (more info)
OpenSSL 0-Length	No (more info)
Sleeping POODLE	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)

Protocol Details

ALPN	Yes h2 http/1.1
NPN	No
Session resumption (caching)	**No (IDs assigned but not accepted)**
Session resumption (tickets)	Yes
OCSP stapling	No
Strict Transport Security (HSTS)	**Yes** max-age=31536000; includeSubDomains; preload
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 (server preferred order)
SSL 2 handshake compatibility	No
0-RTT enabled	No

HTTP Requests

1 **https://peahi.be/** (HTTP/1.1 200 OK)

1	**Content-Type**	text/html; charset=utf-8
	Content-Length	6552
	Connection	close
	Vary	Accept-Encoding
	Date	Sat, 11 Dec 2021 14:30:11 GMT
	Server	Microsoft-IIS/10.0
	Strict-Transport-Security	max-age=31536000; includeSubDomains; preload
	Vary	Origin
	X-Cache	Miss from cloudfront
	Via	1.1 649e92b251b584632a2d3462342d816a.cloudfront.net (CloudFront)
	X-Amz-Cf-Pop	SFO53-C1
	X-Amz-Cf-Id	VUlER47KRebQMRm7UZ2-5LcppLU92GTFV4dvR803r8FFPtoMqRpvkw==

Miscellaneous

Test date	Sat, 11 Dec 2021 14:30:04 UTC
Test duration	60.275 seconds
HTTP status code	200
HTTP server signature	Microsoft-IIS/10.0
Server hostname	server-65-8-158-121.sfo53.r.cloudfront.net

SSL Report v2.1.8