

You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > pleiades.stoa.org

## SSL Report: pleiades.stoa.org (66.35.62.82)

Assessed on: Fri, 23 Sep 2016 18:41:34 UTC | [Hide](#) | [Clear cache](#)

[Scan Another »](#)

### Summary

Overall Rating

# B

Certificate

Protocol Support

Key Exchange

Cipher Strength

0    20    40    60    80    100

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

This server's certificate chain is incomplete. Grade capped to B.

### Authentication



#### Server Key and Certificate #1

<b>Subject</b>	pleiades.stoa.org Fingerprint SHA1: 9243fa3fc687c031f61cb54508b414627e5d07fd Pin SHA256: 58GzMVY6KcH6ApDpVuNUTWp2qJzWQ5P12b1Xiq/icz8=
<b>Common names</b>	pleiades.stoa.org
<b>Alternative names</b>	pleiades.stoa.org
<b>Valid from</b>	Fri, 23 Sep 2016 03:44:00 UTC
<b>Valid until</b>	Thu, 22 Dec 2016 03:44:00 UTC (expires in 2 months and 28 days)
<b>Key</b>	RSA 4096 bits (e 65537)
<b>Weak key (Debian)</b>	No
<b>Issuer</b>	Let's Encrypt Authority X3 AIA: http://cert.int-x3.letsencrypt.org/
<b>Signature algorithm</b>	SHA256withRSA
<b>Extended Validation</b>	No
<b>Certificate Transparency</b>	No
<b>OCSP Must Staple</b>	No
<b>Revocation information</b>	OCSP OCSP: http://ocsp.int-x3.letsencrypt.org/
<b>Revocation status</b>	Good (not revoked)
<b>Trusted</b>	<b>Yes</b>



#### Additional Certificates (if supplied)

<b>Certificates provided</b>	1 (1546 bytes)
<b>Chain issues</b>	<b>Incomplete</b>



#### Certification Paths

**Exportable Certificates** (suites in server-preferred order; deprecated and SSL 2 suites at the end)

**Path #1: Trusted**

1	Sent by server	<p>pleiades.stoa.org</p> <p>Fingerprint SHA1: 9243fa3fc687c031f61cb54508b414627e5d07fd</p> <p>Pin SHA256: 58GzMVY6KcH6ApDpVuNUTWp2qJzWQ5Pt2b1Xiq/icz8=</p> <p>RSA 4096 bits (e 65537) / SHA256withRSA</p>
2	Extra download	<p>Let's Encrypt Authority X3</p> <p>Fingerprint SHA1: e6a3b45b062d509b3382282d196efe97d5956ccb</p> <p>Pin SHA256: YLh1dUR9y6Kja30RrAn7JKnbQG/uEILMkBgFF2Fuihg=</p> <p>RSA 2048 bits (e 65537) / SHA256withRSA</p>
3	In trust store	<p>DST Root CA X3 Self-signed</p> <p>Fingerprint SHA1: dac9024f54d8f6df94935fb1732638ca6ad77c13</p> <p>Pin SHA256: Vjs8r4z+80wjNcr1YKepWQboSIRi63WsWXhIMN+eWys=</p> <p>RSA 2048 bits (e 65537) / SHA1withRSA</p> <p>Weak or insecure signature, but no impact on root certificate</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_GCM_SHA384 (0xc030)	ECDH secp256r1 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)	ECDH secp256r1 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	ECDH secp256r1 (eq. 3072 bits RSA) FS	256
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f)	DH 4096 bits FS	256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x6b)	DH 4096 bits FS	256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39)	DH 4096 bits FS	256



**Handshake Simulation**

<a href="#">Android 2.3.7</a>	No SNI <sup>2</sup>	Server sent fatal alert: handshake_failure		
<a href="#">Android 4.0.4</a>	RSA 4096 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1 FS
<a href="#">Android 4.1.1</a>	RSA 4096 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1 FS
<a href="#">Android 4.2.2</a>	RSA 4096 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1 FS
<a href="#">Android 4.3</a>	RSA 4096 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1 FS
<a href="#">Android 4.4.2</a>	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
<a href="#">Android 5.0.0</a>	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1 FS
<a href="#">Android 6.0</a>	RSA 4096 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1 FS
<a href="#">Baidu Jan 2015</a>	RSA 4096 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1 FS
<a href="#">BingPreview Jan 2015</a>	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
<a href="#">Chrome 51 / Win 7</a> R	RSA 4096 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
<a href="#">Firefox 31.3.0 ESR / Win 7</a>	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1 FS
<a href="#">Firefox 46 / Win 7</a> R	RSA 4096 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1 FS
<a href="#">Firefox 47 / Win 7</a> R	RSA 4096 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1 FS
<a href="#">Googlebot Feb 2015</a>	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1 FS
<a href="#">IE 6 / XP</a>	No FS <sup>1</sup> No SNI <sup>2</sup>	Server closed connection		
<a href="#">IE 7 / Vista</a>	RSA 4096 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1 FS
<a href="#">IE 8 / XP</a>	No FS <sup>1</sup> No SNI <sup>2</sup>	Server sent fatal alert: handshake_failure		

## Protocol Details

<a href="#">IE 8-10 / Win 7</a> R	RSA 4096 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1	FS
<a href="#">IE 11 / Win 7</a> R	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1	FS
<a href="#">IE 11 / Win 8.1</a> R	RSA 4096 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1	FS
<a href="#">IE 10 / Win Phone 8.0</a>	RSA 4096 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1	FS
<a href="#">IE 11 / Win Phone 8.1</a> R	RSA 4096 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1	FS
<a href="#">IE 11 / Win Phone 8.1 Update</a> R	RSA 4096 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1	FS
<a href="#">IE 11 / Win 10</a> R	RSA 4096 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
<a href="#">Edge 13 / Win 10</a> R	RSA 4096 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
<a href="#">Edge 13 / Win Phone 10</a> R	RSA 4096 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
<a href="#">Java 6u45</a> No SNI <sup>2</sup>	Server sent fatal alert: handshake_failure				
<a href="#">Java 7u25</a>	Server sent fatal alert: handshake_failure				
<a href="#">Java 8u31</a>	Server sent fatal alert: handshake_failure				
<a href="#">OpenSSL 0.9.8y</a>	RSA 4096 (SHA256)	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA	DH 4096	FS
<a href="#">OpenSSL 1.0.1l</a> R	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
<a href="#">OpenSSL 1.0.2e</a> R	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
<a href="#">Safari 5.1.9 / OS X 10.6.8</a>	RSA 4096 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1	FS
<a href="#">Safari 6 / iOS 6.0.1</a> R	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1	FS
<a href="#">Safari 6.0.4 / OS X 10.8.4</a> R	RSA 4096 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1	FS
<a href="#">Safari 7 / iOS 7.1</a> R	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1	FS
<a href="#">Safari 7 / OS X 10.9</a> R	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1	FS
<a href="#">Safari 8 / iOS 8.4</a> R	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1	FS
<a href="#">Safari 8 / OS X 10.10</a> R	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1	FS
<a href="#">Safari 9 / iOS 9</a> R	RSA 4096 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
<a href="#">Safari 9 / OS X 10.11</a> R	RSA 4096 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
<a href="#">Apple ATS 9 / iOS 9</a> R	RSA 4096 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
<a href="#">Yahoo Slurp Jan 2015</a>	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
<a href="#">YandexBot Jan 2015</a>	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	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

DROWN (experimental)	No, server keys and hostname not seen elsewhere with SSLv2 (1) For a better understanding of this test, please read <a href="#">this longer explanation</a> (2) Key usage data kindly provided by the <a href="#">Censys</a> network search engine; original DROWN test <a href="#">here</a> (3) Censys data is only indicative of possible key and certificate reuse; possibly out-of-date and not complete
<b>Secure Renegotiation</b>	<b>Supported</b>
Secure Client-Initiated Renegotiation	No
Insecure Client-Initiated Renegotiation	No
BEAST attack	Not mitigated server-side ( <a href="#">more info</a> ) TLS 1.0: 0xc014
POODLE (SSLv3)	No, SSL 3 not supported ( <a href="#">more info</a> )
POODLE (TLS)	No ( <a href="#">more info</a> )
<b>Downgrade attack prevention</b>	<b>Yes, TLS_FALLBACK_SCSV supported (<a href="#">more info</a>)</b>
SSL/TLS compression	No
RC4	No
Heartbeat (extension)	Yes
Heartbleed (vulnerability)	No ( <a href="#">more info</a> )
OpenSSL CCS vuln. (CVE-2014-0224)	No ( <a href="#">more info</a> )
OpenSSL Padding Oracle vuln. (CVE-2016-2107)	No ( <a href="#">more info</a> )
<b>Forward Secrecy</b>	<b>Yes (with most browsers) ROBUST (<a href="#">more info</a>)</b>

### Miscellaneous

ALPN	Yes
NPN	No
Session resumption (caching)	Yes
Session resumption (tickets)	Yes
OCSF stapling	No
Strict Transport Security (HSTS)	No
HSTS Preloading	Not in: Chrome Edge Firefox IE Tor
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
DH public server param (Ys) reuse	No
SSL 2 handshake compatibility	Yes



### Miscellaneous

Test date	Fri, 23 Sep 2016 18:40:09 UTC
Test duration	84.673 seconds
HTTP status code	200
HTTP server signature	Apache/2.4.18 (Ubuntu)
Server hostname	isaw1.atlantides.org