

HomeProjectsQualys Free TrialContact

You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > smart-lighting.me


SSL Report: smart-lighting.me (20.234.143.169)

Assessed on: Sat, 21 Jan 2023 08:35:00 UTC | [Hide](#) | [Clear cache](#)

[Scan Another »](#)

Summary

Overall Rating



Certificate

Protocol Support

Key Exchange

Cipher Strength

0

20

40

60

80

100

100

100

90


90

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

This server supports TLS 1.3.

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

Certificate #1: EC 256 bits (SHA256withRSA)



Server Key and Certificate #1

Subject

Common names

Alternative names

Serial Number

Valid from

Valid until

Key

Weak key (Debian)

Issuer

Signature algorithm

Extended Validation

Certificate Transparency

OCSP Must Staple

Revocation information

Revocation status

DNS CAA

Trusted

*.smart-lighting.me

Fingerprint SHA256: 0688ade45304596b4fba319444053ef216018009700059c062f6e12dd4c309d

Pin SHA256: EqENIRIjxHEL+IT9Zo5BIVXRTPDoZG8QywiV4e0RIY=

*.smart-lighting.me

*.smart-lighting.me smart-lighting.me

036cbe160b99bf3b804f8eb1dd40391d3f58

Wed, 18 Jan 2023 14:35:45 UTC

Tue, 18 Apr 2023 14:35:44 UTC (expires in 2 months and 28 days)

EC 256 bits

No

R3

AIA: <http://r3.i.lencr.org/>

SHA256withRSA

No

Yes (certificate)

No

OCSP


[OCSP: http://r3.o.lencr.org](http://r3.o.lencr.org)

Good (not revoked)

No (more info)

Yes

Mozilla Apple Android Java Windows



Additional Certificates (if supplied)

Certificates provided

Chain issues

3 (3830 bytes)

None

#2

https://www.ssllabs.com/ssltest/analyze.html?d=smart-lighting.me



1/3

Additional Certificates (if supplied)

Subject	R3
	Fingerprint SHA256: 67add1166b020ae61b8f5fc96813c04c2aa589960796865572a3c7e737613dfd
	Pin SHA256: jQJTbIh0grw0/1TkHSumWb+Fs0Ggogr621gT3PvPKG0=
Valid until	Mon, 15 Sep 2025 16:00:00 UTC (expires in 2 years and 7 months)
Key	RSA 2048 bits (e 65537)
Issuer	ISRG Root X1
Signature algorithm	SHA256withRSA

#3

Subject	ISRG Root X1
	Fingerprint SHA256: 6d99fb265eb1c5b3744765fcbc648f3cd8e1bffa4dc4c2f99b9d47cf7ff1c24f
	Pin SHA256: C5+lpZ7tcVwmwQIMcRtPbsQtWLABXhQzejna0wHFr8M=
Valid until	Mon, 30 Sep 2024 18:14:03 UTC (expires in 1 year and 8 months)
Key	RSA 4096 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		No
TLS 1.1		No
TLS 1.0		No
SSL 3		No
SSL 2		No



# TLS 1.3 (suites in server-preferred order)			
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_AES_128_GCM_SHA256 (0x1301)	ECDH x25519 (eq. 3072 bits RSA)	FS	128




Handshake Simulation			
Android 8.1	-	TLS 1.3	TLS_AES_256_GCM_SHA384 ECDH x25519 FS
Android 9.0	-	TLS 1.3	TLS_AES_256_GCM_SHA384 ECDH x25519 FS
Chrome 69 / Win 7 R	-	Server sent fatal alert: protocol_version	
Chrome 70 / Win 10	-	TLS 1.3	TLS_AES_256_GCM_SHA384 ECDH x25519 FS
Chrome 80 / Win 10 R	-	TLS 1.3	TLS_AES_256_GCM_SHA384 ECDH x25519 FS
Firefox 62 / Win 7 R	-	Server sent fatal alert: protocol_version	
Firefox 73 / Win 10 R	-	TLS 1.3	TLS_AES_256_GCM_SHA384 ECDH x25519 FS
Java 11.0.3	-	TLS 1.3	TLS_AES_256_GCM_SHA384 ECDH secp256r1 FS
Java 12.0.1	-	TLS 1.3	TLS_AES_256_GCM_SHA384 ECDH secp256r1 FS
OpenSSL 1.1.0k R	-	Server sent fatal alert: protocol_version	
OpenSSL 1.1.1c R	-	TLS 1.3	TLS_AES_256_GCM_SHA384 ECDH x25519 FS
Safari 12.1.2 / MacOS 10.14.6 Beta R	-	TLS 1.3	TLS_AES_256_GCM_SHA384 ECDH x25519 FS
Safari 12.1.1 / iOS 12.3.1 R	-	TLS 1.3	TLS_AES_256_GCM_SHA384 ECDH x25519 FS
# Not simulated clients (Protocol mismatch)			

Handshake Simulation

[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	Unable to perform this test due to an internal error.
	(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
	INTERNAL ERROR: connect timed out
ROBOT (vulnerability)	No (more info)
Forward Secrecy	Yes (with most browsers) ROBUST (more info)
ALPN	Yes http/1.1
Session resumption (tickets)	No
OCSP stapling	No
Strict Transport Security (HSTS)	Yes
	max-age=63072000; 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)	Unknown
Supported Named Groups	x25519, secp256r1, secp384r1, secp521r1, ffdhe2048, ffdhe3072 (server preferred order)
SSL 2 handshake compatibility	No
0-RTT enabled	Test failed



HTTP Requests	
1	https://smart-lighting.me/ (HTTP/1.1 200 OK)



Miscellaneous	
Test date	Sat, 21 Jan 2023 08:34:01 UTC
Test duration	59.504 seconds
HTTP status code	200
HTTP server signature	-
Server hostname	-