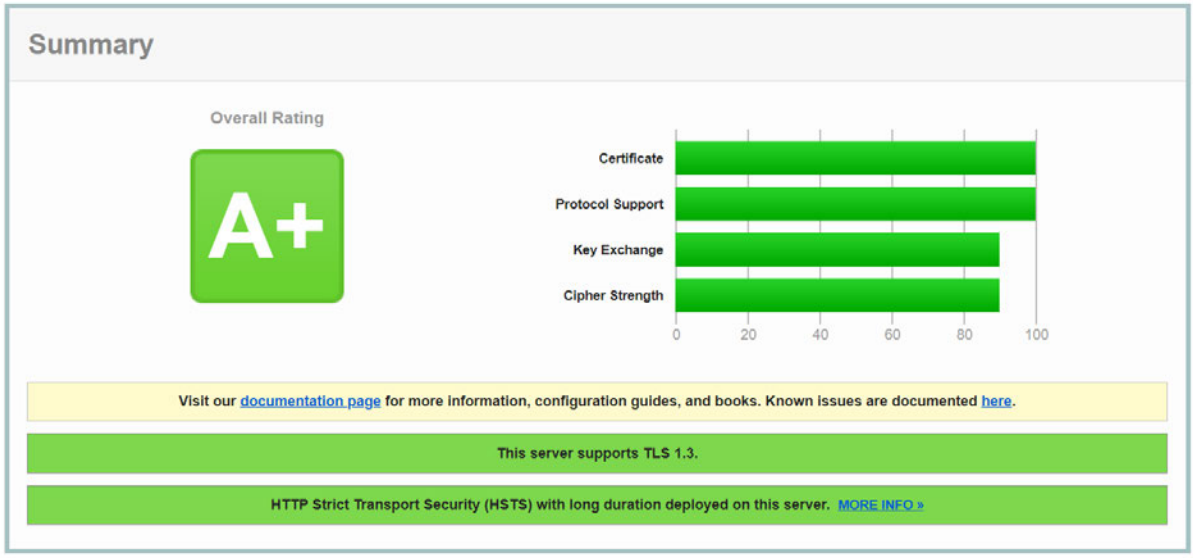
Qualys. SSL Labs

Consultant Indépendant – Qualys SSL Labs (api.[redacted])



Certificate #1: EC 256 bits (SHA256withRSA)

Server Key and Certificate #1

Subject	api.[redacted] Fingerprint SHA256: 068cb885b0c39baa3828c737beee83e856984a2da8f3e65517c866261db331ab Pin SHA256: TWtUlvs[redacted]
Common names	api.[redacted]
Alternative names	api.[redacted]
Serial Number	0419424[redacted]
Valid from	Tue, 09 Jan 2024 20:41:11 UTC
Valid until	Mon, 08 Apr 2024 20:41:10 UTC (expires in 2 months and 23 days)
Key	EC 256 bits

Qualys. SSL Labs

Server Key and Certificate #1

Weak key (Debian)	No
Issuer	R3 AIA: http://r3.i.lencr.org/
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	**Yes (certificate)**
OCSP Must Staple	No
Revocation information	OCSP OCSP: http://r3.o.lencr.org
Revocation status	Good (not revoked)
DNS CAA	No (more info)
Trusted	**Yes** **Mozilla Apple Android Java Windows**

Additional Certificates (if supplied)

Certificates provided	3 (3756 bytes)
Chain issues	None

Qualys. SSL Labs

Additional Certificates (if supplied)

#2	
Subject	R3 Fingerprint SHA256: 67add1166b020ae61b8f5fc96813c04c2aa589960796865572a3c7e737613dfd Pin SHA256: jQJTbIh0g[redacted]
Valid until	Mon, 15 Sep 2025 16:00:00 UTC (expires in 1 year and 7 months)
Key	RSA 2048 bits (e 65537)
Issuer	ISRG Root X1
Signature algorithm	SHA256withRSA

#3	
Subject	ISRG Root X1 Fingerprint SHA256: 6d99fb265eb1c5b3744765fcbc648f3cd8e1bffafdc4c2f99b9d47cf7ff1c24f Pin SHA256: C5+lpZ7tcVw[redacted]
Valid until	Mon, 30 Sep 2024 18:14:03 UTC (expires in 8 months and 13 days)
Key	RSA 4096 bits (e 65537)
Issuer	DST Root CA X3
Signature algorithm	SHA256withRSA

Protocols

TLS 1.3	Yes

Qualys. SSL Labs

Protocols

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_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

 # TLS 1.2 (suites in server-preferred order)

TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c) ECDH x25519 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca9) ECDH x25519 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_ECDSA_WITH_AES_256_CCM_8 (0xc0af) ECDH x25519 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_ECDSA_WITH_AES_256_CCM (0xc0ad) ECDH x25519 (eq. 3072 bits RSA) FS	256

Qualys. SSL Labs

Cipher Suites

TLS_ECDHE_ECDSA_WITH_ARIA_256_GCM_SHA384 (0xc05d) ECDH x25519 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b) ECDH x25519 (eq. 3072 bits RSA) FS	128
TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8 (0xc0ae) ECDH x25519 (eq. 3072 bits RSA) FS	128
TLS_ECDHE_ECDSA_WITH_AES_128_CCM (0xc0ac) ECDH x25519 (eq. 3072 bits RSA) FS	128
TLS_ECDHE_ECDSA_WITH_ARIA_128_GCM_SHA256 (0xc05c) ECDH x25519 (eq. 3072 bits RSA) FS	128
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc024) ECDH x25519 (eq. 3072 bits RSA) FS **WEAK**	256
TLS_ECDHE_ECDSA_WITH_CAMELLIA_256_CBC_SHA384 (0xc073) ECDH x25519 (eq. 3072 bits RSA) FS **WEAK**	256
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023) ECDH x25519 (eq. 3072 bits RSA) FS **WEAK**	128
TLS_ECDHE_ECDSA_WITH_CAMELLIA_128_CBC_SHA256 (0xc072) ECDH x25519 (eq. 3072 bits RSA) FS **WEAK**	128
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a) ECDH x25519 (eq. 3072 bits RSA) FS **WEAK**	256
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009) ECDH x25519 (eq. 3072 bits RSA) FS **WEAK**	128

Protocol Details

Secure Renegotiation	**Supported**

Qualys. SSL Labs

Protocol Details

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) TLS 1.2 : 0xc023
GOLDENDOODLE	No (more info) TLS 1.2 : 0xc023
OpenSSL 0-Length	No (more info) TLS 1.2 : 0xc023
Sleeping POODLE	No (more info) TLS 1.2 : 0xc023
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)

Qualys. SSL Labs

Protocol Details

Forward Secrecy	**Yes (with most browsers) ROBUST** (more info)
ALPN	Yes http/1.1
NPN	Yes http/1.1
Session resumption (caching)	**No (IDs assigned but not accepted)**
Session resumption (tickets)	Yes
OCSP stapling	No
Strict Transport Security (HSTS)	**Yes** max-age=31556926; includeSubDomains
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

Qualys. SSL Labs

Protocol Details

DH public server param (Ys) reuse	No, DHE suites not supported
ECDH public server param reuse	No
Supported Named Groups	x25519, secp256r1 (server preferred order)
SSL 2 handshake compatibility	No
0-RTT enabled	No

HTTP Requests

1 https://api.[redacted] (HTTP/1.1 200 OK)