

You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > maxgremez.com

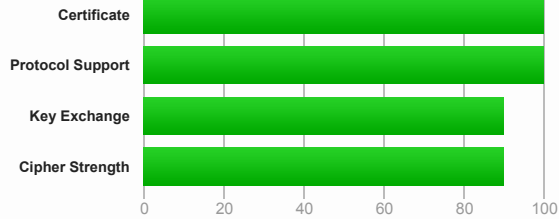
# SSL Report: maxgremez.com (109.234.161.166)

Assessed on: Mon, 14 Feb 2022 09:05:56 UTC | **HIDDEN** | [Clear cache](#)

[Scan Another »](#)

## Summary

Overall Rating



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 »](#)

## Certificate #1: RSA 2048 bits (SHA256withRSA)



### Server Key and Certificate #1



<b>Subject</b>	maxgremez.com Fingerprint SHA256: cc1b6b72d227fa62d39ac1896a7e645bb0f3c2ba7e97e7877e763bf9d7c2b823 Pin SHA256: we4kFnDJf52y8mz67qnY4jFSXQNntdM6DfAf5w07ry0=
<b>Common names</b>	maxgremez.com
<b>Alternative names</b>	cpanel.maxgremez.com cpcalendars.maxgremez.com cpcontacts.maxgremez.com mail.maxgremez.com maxgremez.com webdisk.maxgremez.com webmail.maxgremez.com www.maxgremez.com
<b>Serial Number</b>	0372b98b5c914acf1bb3de2c85041662ef3d
<b>Valid from</b>	Mon, 24 Jan 2022 15:17:02 UTC
<b>Valid until</b>	Sun, 24 Apr 2022 15:17:01 UTC (expires in 2 months and 10 days)
<b>Key</b>	RSA 2048 bits (e 65537)
<b>Weak key (Debian)</b>	No
<b>Issuer</b>	R3 AIA: <a href="http://r3.i.lencr.org/">http://r3.i.lencr.org/</a>
<b>Signature algorithm</b>	SHA256withRSA
<b>Extended Validation</b>	No
<b>Certificate Transparency</b>	Yes (certificate)
<b>OCSP Must Staple</b>	No
<b>Revocation information</b>	OCSP OCSP: <a href="http://r3.o.lencr.org">http://r3.o.lencr.org</a>
<b>Revocation status</b>	Good (not revoked)
<b>DNS CAA</b>	No ( <a href="#">more info</a> )
<b>Trusted</b>	Yes Mozilla Apple Android Java Windows



### Additional Certificates (if supplied)



Certificates provided 2 (2786 bytes)

Chain issuer Certificates (if supplied)

None



#2

<b>Subject</b>	R3 Fingerprint SHA256: 67add1166b020ae61b8f5fc96813c04c2aa589960796865572a3c7e737613dfd Pin SHA256: jQJTbIh0grw0/1TKHSumWb+Fs0Ggogr621gT3PvPKG0=
<b>Valid until</b>	Mon, 15 Sep 2025 16:00:00 UTC (expires in 3 years and 7 months)
<b>Key</b>	RSA 2048 bits (e 65537)
<b>Issuer</b>	ISRG Root X1
<b>Signature algorithm</b>	SHA256withRSA



Certification Paths



[Click here to expand](#)

Certificate #2: RSA 2048 bits (SHA256withRSA) No SNI



[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

(\*) Experimental: Server negotiated using No-SNI



Cipher Suites

<b># TLS 1.3 (server has no preference)</b>			
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
<b># TLS 1.2 (server has no preference)</b>			
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e)	DH 4096 bits FS		128
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	ECDH secp521r1 (eq. 15360 bits RSA) FS		128
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f)	DH 4096 bits FS		256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	ECDH secp521r1 (eq. 15360 bits RSA) FS		256
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xc0ca8)	ECDH secp521r1 (eq. 15360 bits RSA) FS		256



Handshake Simulation

<a href="#">Android 4.4.2</a>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp521r1 FS
<a href="#">Android 5.0.0</a>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp521r1 FS
<a href="#">Android 6.0</a>	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
<a href="#">Android 7.0</a>	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	ECDH x25519 FS
<a href="#">Android 8.0</a>	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	ECDH x25519 FS
<a href="#">Android 8.1</a>	-	TLS 1.3	TLS_CHACHA20_POLY1305_SHA256	ECDH x25519 FS
<a href="#">Android 9.0</a>	-	TLS 1.3	TLS_CHACHA20_POLY1305_SHA256	ECDH x25519 FS

Client	Cipher Suite	Protocol	Signature Algorithm	Key Exchange	Forward Secrecy
<a href="#">Handshake Simulation</a> <a href="#"> Bing Preview Jan 2015</a>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH	secp256r1 FS
<a href="#">Chrome 49 / XP SP3</a>	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH	secp256r1 FS
<a href="#">Chrome 69 / Win 7</a> R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH	x25519 FS
<a href="#">Chrome 70 / Win 10</a>	-	TLS 1.3	TLS_AES_128_GCM_SHA256	ECDH	x25519 FS
<a href="#">Chrome 80 / Win 10</a> R	-	TLS 1.3	TLS_AES_128_GCM_SHA256	ECDH	x25519 FS
<a href="#">Firefox 31.3.0 ESR / Win 7</a>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH	secp256r1 FS
<a href="#">Firefox 47 / Win 7</a> R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH	secp256r1 FS
<a href="#">Firefox 49 / XP SP3</a>	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH	secp256r1 FS
<a href="#">Firefox 62 / Win 7</a> R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH	x25519 FS
<a href="#">Firefox 73 / Win 10</a> R	-	TLS 1.3	TLS_AES_128_GCM_SHA256	ECDH	x25519 FS
<a href="#">Googlebot Feb 2018</a>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH	x25519 FS
<a href="#">IE 11 / Win 7</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	DH	4096 FS
<a href="#">IE 11 / Win 8.1</a> R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	DH	4096 FS
<a href="#">IE 11 / Win Phone 8.1</a> R	Server sent fatal alert: handshake_failure				
<a href="#">IE 11 / Win Phone 8.1 Update</a> R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	DH	4096 FS
<a href="#">IE 11 / Win 10</a> R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH	secp256r1 FS
<a href="#">Edge 15 / Win 10</a> R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH	x25519 FS
<a href="#">Edge 16 / Win 10</a> R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH	x25519 FS
<a href="#">Edge 18 / Win 10</a> R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH	x25519 FS
<a href="#">Edge 13 / Win Phone 10</a> R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH	secp256r1 FS
<a href="#">Java 8u161</a>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH	secp256r1 FS
<a href="#">Java 11.0.3</a>	-	TLS 1.3	TLS_AES_128_GCM_SHA256	ECDH	secp256r1 FS
<a href="#">Java 12.0.1</a>	-	TLS 1.3	TLS_AES_128_GCM_SHA256	ECDH	secp256r1 FS
<a href="#">OpenSSL 1.0.1l</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH	secp521r1 FS
<a href="#">OpenSSL 1.0.2s</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH	secp256r1 FS
<a href="#">OpenSSL 1.1.0k</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH	x25519 FS
<a href="#">OpenSSL 1.1.1c</a> R	-	TLS 1.3	TLS_AES_256_GCM_SHA384	ECDH	x25519 FS
<a href="#">Safari 6 / iOS 6.0.1</a>	Server sent fatal alert: handshake_failure				
<a href="#">Safari 7 / iOS 7.1</a> R	Server sent fatal alert: handshake_failure				
<a href="#">Safari 7 / OS X 10.9</a> R	Server sent fatal alert: handshake_failure				
<a href="#">Safari 8 / iOS 8.4</a> R	Server sent fatal alert: handshake_failure				
<a href="#">Safari 8 / OS X 10.10</a> R	Server sent fatal alert: handshake_failure				
<a href="#">Safari 9 / iOS 9</a> R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH	secp256r1 FS
<a href="#">Safari 9 / OS X 10.11</a> R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH	secp256r1 FS
<a href="#">Safari 10 / iOS 10</a> R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH	secp256r1 FS
<a href="#">Safari 10 / OS X 10.12</a> R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH	secp256r1 FS
<a href="#">Safari 12.1.2 / MacOS 10.14.6 Beta</a> R	-	TLS 1.3	TLS_CHACHA20_POLY1305_SHA256	ECDH	x25519 FS
<a href="#">Safari 12.1.1 / iOS 12.3.1</a> R	-	TLS 1.3	TLS_CHACHA20_POLY1305_SHA256	ECDH	x25519 FS
<a href="#">Apple ATS 9 / iOS 9</a> R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH	secp256r1 FS
<a href="#">Yahoo Slurp Jan 2015</a>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH	secp384r1 FS
<a href="#">YandexBot Jan 2015</a>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH	secp521r1 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

**Protocol Details****Secure Renegotiation****Supported**

Secure Client-Initiated Renegotiation	No
Insecure Client-Initiated Renegotiation	No
BEAST attack	Mitigated server-side ( <a href="#">more info</a> )
POODLE (SSLv3)	No, SSL 3 not supported ( <a href="#">more info</a> )
POODLE (TLS)	No ( <a href="#">more info</a> )
Zombie POODLE	No ( <a href="#">more info</a> )
GOLDENDOODLE	No ( <a href="#">more info</a> )
OpenSSL 0-Length	No ( <a href="#">more info</a> )
Sleeping POODLE	No ( <a href="#">more info</a> )
<b>Downgrade attack prevention</b>	<b>Yes, TLS_FALLBACK_SCSV supported</b> ( <a href="#">more info</a> )
SSL/TLS compression	No
RC4	No
Heartbeat (extension)	No
Heartbleed (vulnerability)	No ( <a href="#">more info</a> )
Ticketbleed (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> )
ROBOT (vulnerability)	No ( <a href="#">more info</a> )
<b>Forward Secrecy</b>	<b>Yes (with most browsers) ROBUST</b> ( <a href="#">more info</a> )
ALPN	Yes h2 http/1.1
NPN	Yes h2 http/1.1
Session resumption (caching)	Yes
Session resumption (tickets)	Yes
<b>OCSP stapling</b>	<b>Yes</b>
<b>Strict Transport Security (HSTS)</b>	<b>Yes</b> max-age=31536000; includeSubDomains; preload
HSTS Preloading	Not in: Chrome Edge Firefox IE
Public Key Pinning (HPKP)	No ( <a href="#">more info</a> )
Public Key Pinning Report-Only	No
Public Key Pinning (Static)	No ( <a href="#">more info</a> )
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
ECDH public server param reuse	No
Supported Named Groups	secp256r1, secp384r1, secp521r1, x25519, x448 (Server has no preference)
SSL 2 handshake compatibility	Yes
0-RTT enabled	Yes

**HTTP Requests**1 <https://maxgremez.com/> (HTTP/1.1 200 OK)**Miscellaneous**

Test date	Mon, 14 Feb 2022 09:04:41 UTC
Test duration	75.335 seconds
HTTP status code	200
HTTP server signature	o2switch-PowerBoost-v3
Server hostname	diego.o2switch.net

SSL Report v2.1.10

Copyright © 2009-2022 [Qualys, Inc.](#) All Rights Reserved.

[Terms and Conditions](#)

[Try Qualys for free!](#) Experience the award-winning [Qualys Cloud Platform](#) and the entire collection of [Qualys Cloud Apps](#), including [certificate security](#) solutions.