

You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > [bakalari.gybon.cz](#) > 195.113.185.163

SSL Report: [bakalari.gybon.cz](#) (195.113.185.163)

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 supports TLS 1.0 and TLS 1.1. Grade capped to B. [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	*.gybon.cz Fingerprint SHA256: 67c918879e70c938d67ac6f4770be969b4e3e7e9f7a41fed818fd5003b01f19d Pin SHA256: cPgHO4zI4DsecWUK2M5UK277trwb6QDwm/k9R34E/NM=
Common names	*.gybon.cz
Alternative names	*.gybon.cz gybon.cz
Serial Number	071b4b61e73c13e045906c68eb56d19f
Valid from	Thu, 11 Jan 2024 00:00:00 UTC
Valid until	Mon, 10 Feb 2025 23:59:59 UTC (expires in 11 months and 24 days)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	RapidSSL TLS RSA CA G1 AIA: http://cacerts.rapidssl.com/RapidSSLTLRSACAG1.crt
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	Yes (certificate)
OCSP Must Staple	No
Revocation information	CRL, OCSP CRL: http://cdp.rapidssl.com/RapidSSLTLRSACAG1.crl OCSP: http://status.rapidssl.com
Revocation status	Good (not revoked)
DNS CAA	Yes policy host: gybon.cz issue: digicert.com flags:0
Trusted	Yes Mozilla Apple Android Java Windows



Additional Certificates (if supplied)

Certificates provided	2 (2778 bytes)
Chain issues	None
#2	
Subject	RapidSSL TLS RSA CA G1 Fingerprint SHA256: 4422e963ee53cd58cc9f85cd40bf5f5fec0095fdf1a154535661c1c06bcadc69b Pin SHA256: E3iYcwe9CiqATmKtpMLW5V+pzlk+ZoDmpXSJIJGmTo=
Valid until	Tue, 02 Nov 2027 12:24:33 UTC (expires in 3 years and 8 months)

Handshake Simulation

Chrome 70 / Win 10	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp384r1 FS
Chrome 80 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp384r1 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_256_GCM_SHA384	ECDH secp384r1 FS
Firefox 62 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp384r1 FS
Firefox 73 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp384r1 FS
Googlebot Feb 2018	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp384r1 FS
IE 7 / Vista	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp384r1 FS
IE 8 / XP No FS ¹ No SNI ²	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_3DES_EDE_CBC_SHA	
IE 8-10 / Win 7 R	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp384r1 FS
IE 11 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	DH 2048 FS
IE 11 / Win 8.1 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	DH 2048 FS
IE 10 / Win Phone 8.0	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp384r1 FS
IE 11 / Win Phone 8.1 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	ECDH secp256r1 FS
IE 11 / Win Phone 8.1 Update R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	DH 2048 FS
IE 11 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp384r1 FS
Edge 15 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp384r1 FS
Edge 16 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp384r1 FS
Edge 18 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp384r1 FS
Edge 13 / Win Phone 10 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp384r1 FS
Java 6u45 No SNI ²	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA	No FS
Java 7u25	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp256r1 FS
Java 8u161	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp384r1 FS
Java 11.0.3	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp384r1 FS
Java 12.0.1	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp384r1 FS
OpenSSL 0.9.8y	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA	No FS
OpenSSL 1.0.1l R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp384r1 FS
OpenSSL 1.0.2s R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp384r1 FS
OpenSSL 1.1.0k R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp384r1 FS
OpenSSL 1.1.1c R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp384r1 FS
Safari 5.1.9 / OS X 10.6.8	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp384r1 FS
Safari 6 / iOS 6.0.1	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp384r1 FS
Safari 6.0.4 / OS X 10.8.4 R	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp384r1 FS
Safari 7 / iOS 7.1 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp384r1 FS
Safari 7 / OS X 10.9 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp384r1 FS
Safari 8 / iOS 8.4 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp384r1 FS
Safari 8 / OS X 10.10 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp384r1 FS
Safari 9 / iOS 9 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp384r1 FS
Safari 9 / OS X 10.11 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp384r1 FS
Safari 10 / iOS 10 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp384r1 FS
Safari 10 / OS X 10.12 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp384r1 FS
Safari 12.1.2 / MacOS 10.14.6 Beta R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp384r1 FS
Safari 12.1.1 / iOS 12.3.1 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp384r1 FS
Apple ATS 9 / iOS 9 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp384r1 FS
Yahoo Slurp Jan 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp384r1 FS
YandexBot Jan 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp384r1 FS

Not simulated clients (Protocol mismatch)

[IE 6 / XP](#) No FS¹ No SNI² 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

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

Protocol Details

	INTERNAL ERROR: test.drownattack.com INTERNAL ERROR: test.drownattack.com
Secure Renegotiation	Supported
Secure Client-Initiated Renegotiation	No
Insecure Client-Initiated Renegotiation	No
BEAST attack	Not mitigated server-side (more info) TLS 1.0: 0xc014
POODLE (SSLv3)	No, SSL 3 not supported (more info)
POODLE (TLS)	No (more info)
Zombie POODLE	No (more info) TLS 1.2 : 0xc027
GOLDENDOODLE	No (more info) TLS 1.2 : 0xc027
OpenSSL 0-Length	No (more info) TLS 1.2 : 0xc027
Sleeping POODLE	No (more info) TLS 1.2 : 0xc027
Downgrade attack prevention	No, TLS_FALLBACK_SCSV not 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	With modern browsers (more info)
ALPN	Yes h2 http/1.1
NPN	No
Session resumption (caching)	No (IDs assigned but not accepted)
Session resumption (tickets)	No
OCSP stapling	Yes
Strict Transport Security (HSTS)	No
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
DH public server param (Ys) reuse	No
ECDH public server param reuse	Yes
Supported Named Groups	secp384r1, x25519, secp256r1 (server preferred order)
SSL 2 handshake compatibility	Yes



HTTP Requests



1 https://bakalari.gybon.cz/ (HTTP/1.1 200 OK)



Miscellaneous

Test date	Sat, 17 Feb 2024 16:37:57 UTC
Test duration	152.85 seconds
HTTP status code	200
HTTP server signature	Microsoft-IIS/10.0
Server hostname	bakalari.gybon.cz

Copyright © 2009-2024 [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.