SSL Report: webinar.ujd.edu.pl (212.87.235.39)

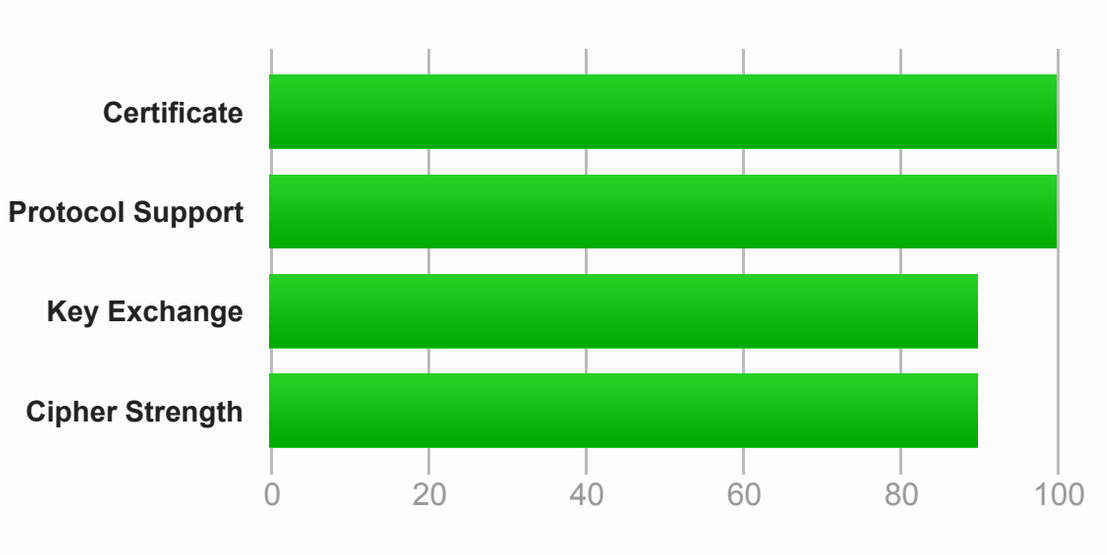
Assessed on: Mon, 17 Jan 2022 14:30:39 UTC | Hide | Clear cache

Scan Another »

Summary

Overall Rating

A



Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

This server supports TLS 1.3.

Certificate #1: RSA 4096 bits (SHA256withRSA)

Server Key and Certificate #1

Subject	*.ujd.edu.pl Fingerprint SHA256: f041f10cb8e9df56cea64547461d64cc3050d59b367967a13641fa2c11c0b25d Pin SHA256: x0to4zO9A1hSKFxs6Zr0dG0+kHqZhELP2//JSW8Mb1E=
Common names	*.ujd.edu.pl
Alternative names	*.ujd.edu.pl ujd.edu.pl
Serial Number	111f16b3f013da6d224b362764944836
Valid from	Tue, 09 Jun 2020 22:00:00 UTC
Valid until	Thu, 09 Jun 2022 22:00:00 UTC (expires in 4 months and 23 days)
Key	RSA 4096 bits (e 65537)
Weak key (Debian)	No
Issuer	Certum Organization Validation CA SHA2 AIA: http://repository.certum.pl/ovcasha2.cer
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	Yes (certificate)
OCSP Must Staple	No
Revocation information	CRL, OCSP CRL: http://crl.certum.pl/ovcasha2.crl OCSP: http://ovcasha2.ocsp-certum.com
Revocation status	Good (not revoked)
DNS CAA	No (more info)
Trusted	Yes Mozilla Apple Android Java Windows

Additional Certificates (if supplied)

Certificates provided	4 (5274 bytes)
Chain issues	Contains anchor

#2

Subject	Certum Organization Validation CA SHA2 Fingerprint SHA256: fd02362244f31266caff005818d1004ec4eb08fb239aafaaafff47497d6005d6 Pin SHA256: 51GveKNrpJjtGpXY5QDx03s3YTQwaQic6dWBqo3zX6s=
Valid until	Wed, 09 Jun 2027 10:46:39 UTC (expires in 5 years and 4 months)
Key	RSA 2048 bits (e 65537)
Issuer	Certum Trusted Network CA
Signature algorithm	SHA256withRSA

#3

Subject	Certum Trusted Network CA Fingerprint SHA256: 949424dc2ccaab5e9e80d66e0e3f7deeb3201c607d4315ef4c6f2d93a917279d Pin SHA256: qiYwp7YXsE0KKUureoyqpQFubb5gSDeoOoVxn6tmfrU=
Valid until	Thu, 10 Jun 2027 10:46:39 UTC (expires in 5 years and 4 months)
Key	RSA 2048 bits (e 65537)
Issuer	Certum CA
Signature algorithm	SHA256withRSA

#4

Subject	Certum CA Not in trust store Fingerprint SHA256: d8e0febc1db2e38d00940f37d27d41344d993e734b99d5656d9778d4d8143624 Pin SHA256: lzasOyXRbEWkVBipZFeBVkgKjMQ0VB3cXdWSMyKYaN4=
Valid until	Fri, 11 Jun 2027 10:46:39 UTC (expires in 5 years and 4 months)
Key	RSA 2048 bits (e 65537)
Issuer	Certum CA Self-signed
Signature algorithm	SHA1withRSA Weak, but no impact on root certificate

Certification Paths

Mozilla Apple Android Java Windows

Path #1: Trusted

1	Sent by server	*.ujd.edu.pl Fingerprint SHA256: f041f10cb8e9df56cea64547461d64cc3050d59b367967a13641fa2c11c0b25d Pin SHA256: x0to4zO9A1hSKFxs6Zr0dG0+kHqZhELP2//JSW8Mb1E= RSA 4096 bits (e 65537) / SHA256withRSA
2	Sent by server	Certum Organization Validation CA SHA2 Fingerprint SHA256: fd02362244f31266caff005818d1004ec4eb08fb239aafaaafff47497d6005d6 Pin SHA256: 51GveKNrpJjtGpXY5QDx03s3YTQwaQic6dWBqo3zX6s= RSA 2048 bits (e 65537) / SHA256withRSA
3	In trust store	Certum Trusted Network CA Self-signed Fingerprint SHA256: 5c58468d55f58e497e743982d2b50010b6d165374acf83a7d4a32db768c4408e Pin SHA256: qiYwp7YXsE0KKUureoyqpQFubb5gSDeoOoVxn6tmfrU= RSA 2048 bits (e 65537) / SHA1withRSA Weak or insecure signature, but no impact on root certificate

Path #2: Trusted

1	Sent by server	*.ujd.edu.pl Fingerprint SHA256: f041f10cb8e9df56cea64547461d64cc3050d59b367967a13641fa2c11c0b25d Pin SHA256: x0to4zO9A1hSKFxs6Zr0dG0+kHqZhELP2//JSW8Mb1E= RSA 4096 bits (e 65537) / SHA256withRSA
2	Sent by server	Certum Organization Validation CA SHA2 Fingerprint SHA256: fd02362244f31266caff005818d1004ec4eb08fb239aafaaafff47497d6005d6 Pin SHA256: 51GveKNrpJjtGpXY5QDx03s3YTQwaQic6dWBqo3zX6s= RSA 2048 bits (e 65537) / SHA256withRSA
3	Sent by server	Certum Trusted Network CA Fingerprint SHA256: 949424dc2ccaab5e9e80d66e0e3f7deeb3201c607d4315ef4c6f2d93a917279d Pin SHA256: qiYwp7YXsE0KKUureoyqpQFubb5gSDeoOoVxn6tmfrU= RSA 2048 bits (e 65537) / SHA256withRSA
4	Sent by server In trust store	Certum CA Self-signed Fingerprint SHA256: d8e0febc1db2e38d00940f37d27d41344d993e734b99d5656d9778d4d8143624 Pin SHA256: lzasOyXRbEWkVBipZFeBVkgKjMQ0VB3cXdWSMyKYaN4= RSA 2048 bits (e 65537) / SHA1withRSA Weak or insecure signature, but no impact on root certificate

Configuration

Protocols

TLS 1.3	Yes
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_RSA_WITH_AES_256_GCM_SHA384 (0xc030) ECDH x25519 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) ECDH x25519 (eq. 3072 bits RSA) FS	128
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f) DH 4096 bits FS	256
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e) DH 4096 bits FS	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) ECDH x25519 (eq. 3072 bits RSA) FS WEAK	256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ECDH x25519 (eq. 3072 bits RSA) FS WEAK	256
TLS_DHE_RSA_WITH_AES_256_CCM_8 (0xc0a3) DH 4096 bits FS	256
TLS_DHE_RSA_WITH_AES_256_CCM (0xc09f) DH 4096 bits FS	256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x6b) DH 4096 bits FS WEAK	256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) DH 4096 bits FS WEAK	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) ECDH x25519 (eq. 3072 bits RSA) FS WEAK	128
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ECDH x25519 (eq. 3072 bits RSA) FS WEAK	128
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x67) DH 4096 bits FS WEAK	128
TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33) DH 4096 bits FS WEAK	128
TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d) WEAK	256
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c) WEAK	128
TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d) WEAK	256
TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c) WEAK	128
TLS_RSA_WITH_AES_256_CBC_SHA (0x35) WEAK	256
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) WEAK	128
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8) ECDH x25519 (eq. 3072 bits RSA) FS	256
TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xccaa) DH 4096 bits FS	256
TLS_ECDHE_RSA_WITH_ARIA_256_GCM_SHA384 (0xc061) ECDH x25519 (eq. 3072 bits RSA) FS	256
TLS_DHE_RSA_WITH_ARIA_256_GCM_SHA384 (0xc053) DH 4096 bits FS	256
TLS_DHE_RSA_WITH_AES_128_CCM_8 (0xc0a2) DH 4096 bits FS	128
TLS_DHE_RSA_WITH_AES_128_CCM (0xc09e) DH 4096 bits FS	128
TLS_ECDHE_RSA_WITH_ARIA_128_GCM_SHA256 (0xc060) ECDH x25519 (eq. 3072 bits RSA) FS	128
TLS_DHE_RSA_WITH_ARIA_128_GCM_SHA256 (0xc052) DH 4096 bits FS	128
TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384 (0xc077) ECDH x25519 (eq. 3072 bits RSA) FS WEAK	256
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA256 (0xc4) DH 4096 bits FS WEAK	256
TLS_ECDHE_RSA_WITH_CAMELLIA_128_CBC_SHA256 (0xc076) ECDH x25519 (eq. 3072 bits RSA) FS WEAK	128
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA256 (0xbe) DH 4096 bits FS WEAK	128
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0x88) DH 4096 bits FS WEAK	256
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (0x45) DH 4096 bits FS WEAK	128
TLS_RSA_WITH_AES_256_CCM_8 (0xc0a1) WEAK	256
TLS_RSA_WITH_AES_256_CCM (0xc09d) WEAK	256
TLS_RSA_WITH_ARIA_256_GCM_SHA384 (0xc051) WEAK	256
TLS_RSA_WITH_AES_128_CCM_8 (0xc0a0) WEAK	128
TLS_RSA_WITH_AES_128_CCM (0xc09c) WEAK	128
TLS_RSA_WITH_ARIA_128_GCM_SHA256 (0xc050) WEAK	128
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256 (0xc0) WEAK	256
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256 (0xba) WEAK	128
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (0x84) WEAK	256
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (0x41) WEAK	128

Handshake Simulation

Android 4.4.2	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Android 5.0.0	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Android 6.0	RSA 4096 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Android 7.0	RSA 4096 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH x25519 FS
Android 8.0	RSA 4096 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH x25519 FS
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
BingPreview Jan 2015	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Chrome 49 / XP SP3	RSA 4096 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Chrome 69 / Win 7 R	RSA 4096 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH x25519 FS
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 31.3.0 ESR / Win 7	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Firefox 47 / Win 7 R	RSA 4096 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Firefox 49 / XP SP3	RSA 4096 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Firefox 62 / Win 7 R	RSA 4096 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH x25519 FS
Firefox 73 / Win 10 R	-	TLS 1.3	TLS_AES_256_GCM_SHA384 ECDH x25519 FS
Googlebot Feb 2018	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH x25519 FS
IE 11 / Win 7 R	RSA 4096 (SHA256)	TLS 1.2	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 DH 4096 FS
IE 11 / Win 8.1 R	RSA 4096 (SHA256)	TLS 1.2 > http/1.1	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 DH 4096 FS
IE 11 / Win Phone 8.1 R	RSA 4096 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS
IE 11 / Win Phone 8.1 Update R	RSA 4096 (SHA256)	TLS 1.2 > http/1.1	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 DH 4096 FS
IE 11 / Win 10 R	RSA 4096 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Edge 15 / Win 10 R	RSA 4096 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH x25519 FS
Edge 16 / Win 10 R	RSA 4096 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH x25519 FS
Edge 18 / Win 10 R	RSA 4096 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH x25519 FS
Edge 13 / Win Phone 10 R	RSA 4096 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Java 8u161	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 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 1.0.1l R	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
OpenSSL 1.0.2s R	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
OpenSSL 1.1.0k R	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH x25519 FS
OpenSSL 1.1.1c R	-	TLS 1.3	TLS_AES_256_GCM_SHA384 ECDH x25519 FS
Safari 6 / iOS 6.0.1	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS
Safari 7 / iOS 7.1 R	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS
Safari 7 / OS X 10.9 R	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS
Safari 8 / iOS 8.4 R	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS
Safari 8 / OS X 10.10 R	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS
Safari 9 / iOS 9 R	RSA 4096 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Safari 9 / OS X 10.11 R	RSA 4096 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Safari 10 / iOS 10 R	RSA 4096 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Safari 10 / OS X 10.12 R	RSA 4096 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 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
Apple ATS 9 / iOS 9 R	RSA 4096 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Yahoo Slurp Jan 2015	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
YandexBot Jan 2015	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS

 # Not simulated clients (Protocol mismatch)

Android 2.3.7 No SNI [2]	Protocol mismatch (not simulated)
Android 4.0.4	Protocol mismatch (not simulated)
Android 4.1.1	Protocol mismatch (not simulated)
Android 4.2.2	Protocol mismatch (not simulated)
Android 4.3	Protocol mismatch (not simulated)
Baidu Jan 2015	Protocol mismatch (not simulated)
IE 6 / XP No FS [1] No SNI [2]	Protocol mismatch (not simulated)
IE 7 / Vista	Protocol mismatch (not simulated)
IE 8 / XP No FS [1] No SNI [2]	Protocol mismatch (not simulated)
IE 8-10 / Win 7 R	Protocol mismatch (not simulated)
IE 10 / Win Phone 8.0	Protocol mismatch (not simulated)
Java 6u45 No SNI [2]	Protocol mismatch (not simulated)
Java 7u25	Protocol mismatch (not simulated)
OpenSSL 0.9.8y	Protocol mismatch (not simulated)
Safari 5.1.9 / OS X 10.6.8	Protocol mismatch (not simulated)
Safari 6.0.4 / OS X 10.8.4 R	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	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
Secure Renegotiation	Supported
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 : 0xc014
GOLDENDOODLE	No (more info) TLS 1.2 : 0xc014
OpenSSL 0-Length	No (more info) TLS 1.2 : 0xc014
Sleeping POODLE	No (more info) TLS 1.2 : 0xc014
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)
Forward Secrecy	Yes (with most browsers) ROBUST (more info)
ALPN	Yes h2 http/1.1
NPN	Yes h2 http/1.1
Session resumption (caching)	Yes
Session resumption (tickets)	No
OCSP stapling	No
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	No
Supported Named Groups	x25519, secp256r1, x448, secp521r1, secp384r1 (server preferred order)
SSL 2 handshake compatibility	Yes
0-RTT enabled	No

HTTP Requests

1 https://webinar.ujd.edu.pl/ (HTTP/1.1 307 Temporary Redirect)

1	Server	nginx
	Date	Mon, 17 Jan 2022 14:28:10 GMT
	Content-Type	text/html
	Content-Length	180
	Location	https://webinar.ujd.edu.pl/b
	Connection	close

2 https://webinar.ujd.edu.pl/b (HTTP/1.1 200 OK)

2	Server	nginx
	Date	Mon, 17 Jan 2022 14:28:11 GMT
	Content-Type	text/html; charset=utf-8
	Transfer-Encoding	chunked
	Connection	close
	X-Frame-Options	SAMEORIGIN
	X-XSS-Protection	1; mode=block
	X-Content-Type-Options	nosniff
	X-Download-Options	noopen
	X-Permitted-Cross-Domain-Policies	none
	Referrer-Policy	strict-origin-when-cross-origin
	ETag	W/"4ca7b4ed844c0d6f5cb01f36578be29e"
	Cache-Control	max-age=0, private, must-revalidate
	Set-Cookie	_greenlight-2_3_session=3o1vggLxcd03etfYrZpsgDLI4b0yAdjlco6ihL%2B%2F2RL1Zu97f-X3BmDjy6zPUq7lHJYtGhN5slwJz6q0DdzFkXwtInFxa57mAShbC5gC69lvbKxPU3O8Bt0BH-hD18BV1mNSyx7vcZ1cqpGLWmZ78%3D--OHCDzkuajtpJdBjW--SQV15rXY4tug%2Ffc-c8Vcg0w%3D%3D; path=/; HttpOnly
	X-Request-Id	e2478d99-d70e-4084-8931-e9b3282ba7ac
	X-Runtime	0.036419

Miscellaneous

Test date	Mon, 17 Jan 2022 14:27:59 UTC
Test duration	160.272 seconds
HTTP status code	200
HTTP server signature	nginx
Server hostname	-

SSL Report v2.1.10