Qualys. SSL Labs

SSL Report: e-postbank.bg (195.242.126.250)

Assessed on: Mon, 16 Oct 2017 07:14:11 UTC | Hide | Clear cache

Scan Another »

Summary

Overall Rating

A-

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.

The server does not support Forward Secrecy with the reference browsers. Grade reduced to A-. MORE INFO »

Certificate #1: RSA 2048 bits (SHA256withRSA)

Server Key and Certificate #1

Subject	e-postbank.bg Fingerprint SHA256: 8ff423eaac76951a0c9e291f8403836a2d513f178adb95245cfc184fedb869bf Pin SHA256: Exnm+lvC5BiN94vF9MEawTzPUsxiVXXubiwD3w8JokA=
Common names	e-postbank.bg
Alternative names	e-postbank.bg www.e-postbank.bg
Serial Number	5c740132291f1b6198bfa3f89ce4e75d
Valid from	Wed, 12 Apr 2017 00:00:00 UTC
Valid until	Mon, 11 Jun 2018 23:59:59 UTC (expires in 7 months and 26 days)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	GeoTrust EV SSL CA - G4 AIA: http://gm.symcb.com/gm.crt
Signature algorithm	SHA256withRSA
Extended Validation	Yes
Certificate Transparency	Yes (certificate)
OCSP Must Staple	No
Revocation information	CRL, OCSP CRL: http://gm.symcb.com/gm.crl OCSP: http://gm.symcd.com
Revocation status	Good (not revoked)
DNS CAA	No (more info)
Trusted	Yes

Additional Certificates (if supplied)

Certificates provided	2 (2764 bytes)
Chain issues	None

#2

Subject	GeoTrust EV SSL CA - G4 Fingerprint SHA256: 95b09d02122fa8ae6235780f6ea6503e767ac021a0874fe831ce803a50ea8fd7 Pin SHA256: owrR9U9FWDWtrFF+myoRlu75JwU4sJwzvhCNLZoY37g=
Valid until	Mon, 30 Oct 2023 23:59:59 UTC (expires in 6 years)
Key	RSA 2048 bits (e 65537)
Issuer	GeoTrust Primary Certification Authority
Signature algorithm	SHA256withRSA

Certification Paths

Path #1: Trusted

1	Sent by server	e-postbank.bg Fingerprint SHA256: 8ff423eaac76951a0c9e291f8403836a2d513f178adb95245cfc184fedb869bf Pin SHA256: Exnm+lvC5BiN94vF9MEawTzPUsxiVXXubiwD3w8JokA= RSA 2048 bits (e 65537) / SHA256withRSA
2	Sent by server	GeoTrust EV SSL CA - G4 Fingerprint SHA256: 95b09d02122fa8ae6235780f6ea6503e767ac021a0874fe831ce803a50ea8fd7 Pin SHA256: owrR9U9FWDWtrFF+myoRlu75JwU4sJwzvhCNLZoY37g= RSA 2048 bits (e 65537) / SHA256withRSA
3	In trust store	GeoTrust Primary Certification Authority Self-signed Fingerprint SHA256: 37d51006c512eaab626421f1ec8c92013fc5f82ae98ee533eb4619b8deb4d06c Pin SHA256: SQVGZlOrQXi+kqxcvWWE96HhfydlLVqFr4lQTql5qqo= RSA 2048 bits (e 65537) / SHA1withRSA Weak or insecure signature, but no impact on root certificate

Configuration

Protocols

TLS 1.3	No
TLS 1.2	Yes
TLS 1.1	Yes
TLS 1.0	Yes
SSL 3	No
SSL 2	No

For TLS 1.3 tests, we currently support draft version 18.

Cipher Suites

 # TLS 1.2 (suites in server-preferred order)

TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	128
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)	256
TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c)	128
TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d)	256
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa) **WEAK**	112

 # TLS 1.1 (suites in server-preferred order)

TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	128
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)	256
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa) **WEAK**	112

 # TLS 1.0 (suites in server-preferred order)

TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	128
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)	256
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa) **WEAK**	112

Handshake Simulation

Android 2.3.7 No SNI 2	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA	No FS
Android 4.0.4	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA	No FS
Android 4.1.1	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA	No FS
Android 4.2.2	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA	No FS
Android 4.3	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA	No FS
Android 4.4.2	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_128_CBC_SHA	No FS
Android 5.0.0	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_128_CBC_SHA	No FS
Android 6.0	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_128_CBC_SHA	No FS
Android 7.0	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_128_CBC_SHA	No FS
Baidu Jan 2015	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA	No FS
BingPreview Jan 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_128_CBC_SHA	No FS
Chrome 49 / XP SP3	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_128_CBC_SHA	No FS
Chrome 57 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_128_CBC_SHA	No FS

Handshake Simulation

Firefox 31.3.0 ESR / Win 7	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_128_CBC_SHA No FS
Firefox 47 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_128_CBC_SHA No FS
Firefox 49 / XP SP3	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_128_CBC_SHA No FS
Firefox 53 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_128_CBC_SHA No FS
Googlebot Feb 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_128_CBC_SHA No FS
IE 7 / Vista	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA No 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_RSA_WITH_AES_128_CBC_SHA No FS
IE 11 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_128_CBC_SHA No FS
IE 11 / Win 8.1 R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_128_CBC_SHA No FS
IE 10 / Win Phone 8.0	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA No FS
IE 11 / Win Phone 8.1 R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_128_CBC_SHA No FS
IE 11 / Win Phone 8.1 Update R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_128_CBC_SHA No FS
IE 11 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_128_CBC_SHA No FS
Edge 13 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_128_CBC_SHA No FS
Edge 13 / Win Phone 10 R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_128_CBC_SHA No 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_RSA_WITH_AES_128_CBC_SHA No FS
Java 8u31	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_128_CBC_SHA No FS
OpenSSL 0.9.8y	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA No FS
OpenSSL 1.0.1l R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_128_CBC_SHA No FS
OpenSSL 1.0.2e R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_128_CBC_SHA No FS
Safari 5.1.9 / OS X 10.6.8	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA No FS
Safari 6 / iOS 6.0.1	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_128_CBC_SHA No FS
Safari 6.0.4 / OS X 10.8.4 R	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA No FS
Safari 7 / iOS 7.1 R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_128_CBC_SHA No FS
Safari 7 / OS X 10.9 R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_128_CBC_SHA No FS
Safari 8 / iOS 8.4 R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_128_CBC_SHA No FS
Safari 8 / OS X 10.10 R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_128_CBC_SHA No FS
Safari 9 / iOS 9 R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_128_CBC_SHA No FS
Safari 9 / OS X 10.11 R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_128_CBC_SHA No FS
Safari 10 / iOS 10 R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_128_CBC_SHA No FS
Safari 10 / OS X 10.12 R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_128_CBC_SHA No FS
Apple ATS 9 / iOS 9 R	Server closed connection		
Yahoo Slurp Jan 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_128_CBC_SHA No FS
YandexBot Jan 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_128_CBC_SHA No FS

Not simulated clients (Protocol mismatch)

IE 6 / XP No FS [1] No SNI [2] Protocol mismatch (not simulated)

(1) Certificate trust is not checked in handshake simulation, we only perform TLS handshake.

(2) Clients that do not support Forward Secrecy (FS) are excluded when determining support for it.

(3) No support for virtual SSL hosting (SNI). Connects to the default site if the server uses SNI.

(4) 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).

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	Not mitigated server-side (more info) TLS 1.0: 0x2f
POODLE (SSLv3)	No, SSL 3 not supported (more info)
POODLE (TLS)	No (more info)
Downgrade attack prevention	No, TLS_FALLBACK_SCSV not supported (more info)
SSL/TLS compression	No
RC4	No
Heartbeat (extension)	No

Protocol Details

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)
Forward Secrecy	**No WEAK** (more info)
ALPN	No
NPN	No
Session resumption (caching)	Yes
Session resumption (tickets)	No
OCSP stapling	**Invalid** Failed to validate response
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, DHE suites not supported
DH public server param (Ys) reuse	No, DHE suites not supported
ECDH public server param reuse	No, ECDHE suites not supported
Supported Named Groups	-
SSL 2 handshake compatibility	Yes

HTTP Requests

1 **https://e-postbank.bg/** (HTTP/1.1 200 OK)

Miscellaneous

Test date	Mon, 16 Oct 2017 07:12:30 UTC
Test duration	101.590 seconds
HTTP status code	200
HTTP server signature	Microsoft-IIS/7.5
Server hostname	www.e-postbank.bg

SSL Report v1.29.7