QUALYS® SSL LABS

Home | Projects | Qualys.com | Contact

You are here: Home > Projects > SSL Server Test > ebanking.unionbankph.com > 203.82.36.182

SSL Report: ebanking.unionbankph.com (203.82.36.182)

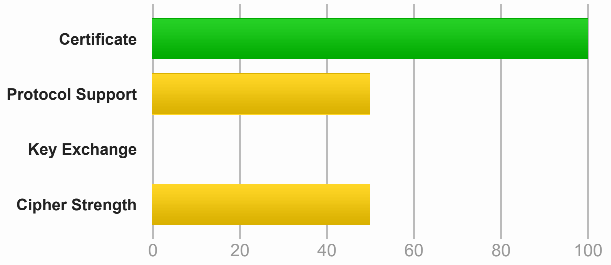
Assessed on: Fri, 27 Nov 2015 17:19:40 UTC | Clear cache

Scan Another »

Summary

Overall Rating

F



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

This server supports 512-bit export suites and might be vulnerable to the FREAK attack. Grade set to F. MORE INFO »

This server uses SSL 3, which is obsolete and insecure. Grade capped to B. MORE INFO »

Certificate has a weak signature and expires after 2015. Upgrade to SHA2 to avoid browser warnings. MORE INFO »

The server supports only older protocols, but not the current best TLS 1.2. Grade capped to C. MORE INFO »

This server accepts RC4 cipher, but only with older protocol versions. Grade capped to B. MORE INFO »

The server does not support Forward Secrecy with the reference browsers. MORE INFO »

Authentication

Server Key and Certificate #1

Subject	ebanking.unionbankph.com Fingerprint SHA1: 5fabdf19e8efaf4bee9e28f078ff21fa7a035e08 Pin SHA256: LHWQ4GnREQxTs8kGWk8RkEsl47IznlvsfCc+fklsQ2o=
Common names	ebanking.unionbankph.com
Alternative names	ebanking.unionbankph.com
Prefix handling	Not required for subdomains
Valid from	Tue, 23 Jun 2015 10:16:05 UTC
Valid until	Tue, 26 Jul 2016 12:21:02 UTC (expires in 7 months and 28 days)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	GlobalSign Extended Validation CA - G2
Signature algorithm	SHA1withRSA **WEAK**
Extended Validation	Yes
Certificate Transparency	Yes (certificate)
Revocation information	CRL, OCSP
Revocation status	Good (not revoked)
Trusted	Yes

Additional Certificates (if supplied)

Certificates provided	3 (4188 bytes)
Chain issues	None

#2

Subject	GlobalSign Extended Validation CA - G2 Fingerprint SHA1: 06456b2c4c26f37c95266793bbedff61e6373dc2 Pin SHA256: SG/sBoMJc9IgJ8+dGgIHyTLvz7wyVBio7lMoDanPuRk=
Valid until	Wed, 13 Apr 2022 10:00:00 UTC (expires in 6 years and 4 months)
Key	RSA 2048 bits (e 65537)
Issuer	GlobalSign
Signature algorithm	SHA1withRSA **WEAK**

#3

Subject	GlobalSign Fingerprint SHA1: 9563f9a74ea68df514c9053d6af8cee72bd6cb88 Pin SHA256: iie1VXtL7HzAMF+/PVPR9xzT80kQxdZeJ+zduCB3uj0=
Valid until	Fri, 28 Jan 2028 12:00:00 UTC (expires in 12 years and 2 months)
Key	RSA 2048 bits (e 65537)
Issuer	GlobalSign Root CA
Signature algorithm	SHA1withRSA **WEAK**

Certification Paths

Path #1: Trusted

1	Sent by server	ebanking.unionbankph.com Fingerprint SHA1: 5fabdf19e8efaf4bee9e28f078ff21fa7a035e08 Pin SHA256: LHWQ4GnREQxTs8kGWk8RkEsl47IznlvsfCc+fklsQ2o= RSA 2048 bits (e 65537) / SHA1withRSA **WEAK SIGNATURE**
2	Sent by server	GlobalSign Extended Validation CA - G2 Fingerprint SHA1: 06456b2c4c26f37c95266793bbedff61e6373dc2 Pin SHA256: SG/sBoMJc9IgJ8+dGgIHyTLvz7wyVBio7lMoDanPuRk= RSA 2048 bits (e 65537) / SHA1withRSA **WEAK SIGNATURE**
3	In trust store	GlobalSign Self-signed Fingerprint SHA1: 75e0abb6138512271c04f85fddde38e4b7242efe Pin SHA256: iie1VXtL7HzAMF+/PVPR9xzT80kQxdZeJ+zduCB3uj0= RSA 2048 bits (e 65537) / SHA1withRSA Weak or insecure signature, but no impact on root certificate

Path #2: Trusted

1	Sent by server	ebanking.unionbankph.com Fingerprint SHA1: 5fabdf19e8efaf4bee9e28f078ff21fa7a035e08 Pin SHA256: LHWQ4GnREQxTs8kGWk8RkEsl47IznlvsfCc+fklsQ2o= RSA 2048 bits (e 65537) / SHA1withRSA **WEAK SIGNATURE**
2	Sent by server	GlobalSign Extended Validation CA - G2 Fingerprint SHA1: 06456b2c4c26f37c95266793bbedff61e6373dc2 Pin SHA256: SG/sBoMJc9IgJ8+dGgIHyTLvz7wyVBio7lMoDanPuRk= RSA 2048 bits (e 65537) / SHA1withRSA **WEAK SIGNATURE**
3	Sent by server	GlobalSign Fingerprint SHA1: 9563f9a74ea68df514c9053d6af8cee72bd6cb88 Pin SHA256: iie1VXtL7HzAMF+/PVPR9xzT80kQxdZeJ+zduCB3uj0= RSA 2048 bits (e 65537) / SHA1withRSA **WEAK SIGNATURE**
4	In trust store	GlobalSign Root CA Self-signed Fingerprint SHA1: b1bc968bd4f49d622aa89a81f2150152a41d829c Pin SHA256: K87oWBWM9UZfyddvDfoxL+8lpNyoUB2ptGtn0fv6G2Q= RSA 2048 bits (e 65537) / SHA1withRSA

Weak or insecure signature, but no impact on root certificate

Configuration

Protocols

TLS 1.2	No
TLS 1.1	No
TLS 1.0	Yes
SSL 3 **INSECURE**	Yes
SSL 2	No

Cipher Suites (SSL 3+ suites in server-preferred order; deprecated and SSL 2 suites at the end)

TLS_RSA_WITH_RC4_128_MD5 (0x4) **INSECURE**	128
TLS_RSA_WITH_RC4_128_SHA (0x5) **INSECURE**	128
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa)	112
TLS_RSA_WITH_DES_CBC_SHA (0x9) **WEAK**	56
TLS_RSA_EXPORT1024_WITH_RC4_56_SHA (0x64) **INSECURE**	56
TLS_RSA_EXPORT1024_WITH_DES_CBC_SHA (0x62) **WEAK**	56
TLS_RSA_EXPORT_WITH_RC4_40_MD5 (0x3) **INSECURE**	40
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5 (0x6) **INSECURE**	40

Handshake Simulation

Android 2.3.7 No SNI [2]	TLS 1.0	TLS_RSA_WITH_RC4_128_MD5 (0x4) No FS RC4	128
Android 4.0.4	TLS 1.0	TLS_RSA_WITH_RC4_128_MD5 (0x4) No FS RC4	128
Android 4.1.1	TLS 1.0	TLS_RSA_WITH_RC4_128_MD5 (0x4) No FS RC4	128
Android 4.2.2	TLS 1.0	TLS_RSA_WITH_RC4_128_MD5 (0x4) No FS RC4	128
Android 4.3	TLS 1.0	TLS_RSA_WITH_RC4_128_MD5 (0x4) No FS RC4	128
Android 4.4.2	TLS 1.0	TLS_RSA_WITH_RC4_128_MD5 (0x4) No FS RC4	128
Android 5.0.0	TLS 1.0	TLS_RSA_WITH_RC4_128_MD5 (0x4) No FS RC4	128
Baidu Jan 2015	TLS 1.0	TLS_RSA_WITH_RC4_128_MD5 (0x4) No FS RC4	128
BingPreview Jan 2015	TLS 1.0	TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa) No FS	112
Chrome 45 / OS X R	TLS 1.0	TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa) No FS	112
Firefox 31.3.0 ESR / Win 7	TLS 1.0	TLS_RSA_WITH_RC4_128_MD5 (0x4) No FS RC4	128
Firefox 41 / OS X R	TLS 1.0	TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa) No FS	112
Googlebot Feb 2015	TLS 1.0	TLS_RSA_WITH_RC4_128_MD5 (0x4) No FS RC4	128
IE 6 / XP No FS [1] No SNI [2]	SSL 3	TLS_RSA_WITH_RC4_128_MD5 (0x4) No FS RC4	128
IE 7 / Vista	TLS 1.0	TLS_RSA_WITH_RC4_128_MD5 (0x4) No FS RC4	128
IE 8 / XP No FS [1] No SNI [2]	TLS 1.0	TLS_RSA_WITH_RC4_128_MD5 (0x4) No FS RC4	128
IE 8-10 / Win 7 R	TLS 1.0	TLS_RSA_WITH_RC4_128_MD5 (0x4) No FS RC4	128
IE 11 / Win 7 R	TLS 1.0	TLS_RSA_WITH_RC4_128_MD5 (0x4) No FS RC4	128
IE 11 / Win 8.1 R	TLS 1.0	TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa) No FS	112
IE 10 / Win Phone 8.0	TLS 1.0	TLS_RSA_WITH_RC4_128_MD5 (0x4) No FS RC4	128
IE 11 / Win Phone 8.1 R	TLS 1.0	TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa) No FS	112
IE 11 / Win Phone 8.1 Update R	TLS 1.0	TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa) No FS	112
IE 11 / Win 10 R	TLS 1.0	TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa) No FS	112
Edge / Win 10 R	TLS 1.0	TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa) No FS	112
Java 6u45 No SNI [2]	TLS 1.0	TLS_RSA_WITH_RC4_128_MD5 (0x4) No FS RC4	128
Java 7u25	TLS 1.0	TLS_RSA_WITH_RC4_128_MD5 (0x4) No FS RC4	128
Java 8u31	TLS 1.0	TLS_RSA_WITH_RC4_128_MD5 (0x4) No FS RC4	128

OpenSSL 0.9.8y	TLS 1.0	TLS_RSA_WITH_RC4_128_MD5 (0x4) No FS RC4	128
OpenSSL 1.0.1l R	TLS 1.0	TLS_RSA_WITH_RC4_128_MD5 (0x4) No FS RC4	128
OpenSSL 1.0.2 R	Protocol or cipher suite mismatch		Fail[3]
Safari 5.1.9 / OS X 10.6.8	TLS 1.0	TLS_RSA_WITH_RC4_128_MD5 (0x4) No FS RC4	128
Safari 6 / iOS 6.0.1 R	TLS 1.0	TLS_RSA_WITH_RC4_128_MD5 (0x4) No FS RC4	128
Safari 6.0.4 / OS X 10.8.4 R	TLS 1.0	TLS_RSA_WITH_RC4_128_MD5 (0x4) No FS RC4	128
Safari 7 / iOS 7.1 R	TLS 1.0	TLS_RSA_WITH_RC4_128_MD5 (0x4) No FS RC4	128
Safari 7 / OS X 10.9 R	TLS 1.0	TLS_RSA_WITH_RC4_128_MD5 (0x4) No FS RC4	128
Safari 8 / iOS 8.4 R	TLS 1.0	TLS_RSA_WITH_RC4_128_MD5 (0x4) No FS RC4	128
Safari 8 / OS X 10.10 R	TLS 1.0	TLS_RSA_WITH_RC4_128_MD5 (0x4) No FS RC4	128
Safari 9 / iOS 9 R	TLS 1.0	TLS_RSA_WITH_RC4_128_MD5 (0x4) No FS RC4	128
Safari 9 / OS X 10.11 R	TLS 1.0	TLS_RSA_WITH_RC4_128_MD5 (0x4) No FS RC4	128
Apple ATS 9 / iOS 9 R	Protocol or cipher suite mismatch		Fail[3]
Yahoo Slurp Jan 2015	TLS 1.0	TLS_RSA_WITH_RC4_128_SHA (0x5) No FS RC4	128
YandexBot Jan 2015	TLS 1.0	TLS_RSA_WITH_RC4_128_MD5 (0x4) No FS RC4	128

(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 tend to 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

Secure Renegotiation	**Supported**
Secure Client-Initiated Renegotiation	No
Insecure Client-Initiated Renegotiation	No
BEAST attack	Mitigated server-side (more info) SSL 3: 0x4, TLS 1.0: 0x4
POODLE (SSLv3)	No, mitigated (more info) SSL 3: 0x4
POODLE (TLS)	No (more info)
Downgrade attack prevention	**No, TLS_FALLBACK_SCSV not supported** (more info)
SSL/TLS compression	No
RC4	**Yes INSECURE** (more info)
Heartbeat (extension)	No
Heartbleed (vulnerability)	No (more info)
OpenSSL CCS vuln. (CVE-2014-0224)	No (more info)
Forward Secrecy	**No WEAK** (more info)
Next Protocol Negotiation (NPN)	No
Session resumption (caching)	Yes
Session resumption (tickets)	No
OCSP stapling	No
Strict Transport Security (HSTS)	No
HSTS Preloading	**Not in: Chrome Edge Firefox IE Tor** ebanking.unionbankph.com
Public Key Pinning (HPKP)	No
Public Key Pinning Report-Only	No
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
SSL 2 handshake compatibility	Yes

Miscellaneous

Test date	Fri, 27 Nov 2015 17:15:38 UTC
Test duration	122.871 seconds
HTTP status code	200
HTTP server signature	Microsoft-IIS/6.0
Server hostname	-

SSL Report v1.20.28

Terms and Conditions