SSL Report: online.bdo.com.ph (203.177.92.11)

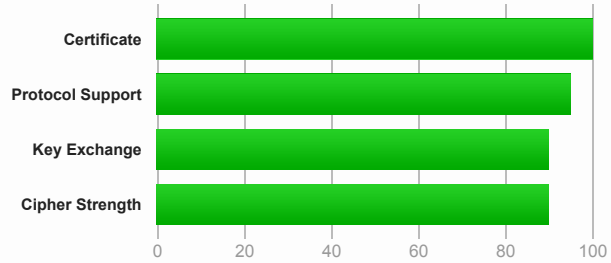
Assessed on: Fri, 27 Nov 2015 17:07:08 UTC | Clear cache

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_FALLBACK_SCSV to prevent protocol downgrade attacks.

Authentication

Server Key and Certificate #1

Subject	online.bdo.com.ph Fingerprint SHA1: 79d7d971116fd9cc45139953898cefa407b76aa6 Pin SHA256: w3eQEYi3Rhz7iZpHBrF9dy5EiZWo08CeEKPpo8d9mt4=
Common names	online.bdo.com.ph
Alternative names	online.bdo.com.ph
Prefix handling	Not required for subdomains
Valid from	Mon, 14 Sep 2015 00:00:00 UTC
Valid until	Thu, 14 Sep 2017 23:59:59 UTC (expires in 1 year and 9 months)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	Symantec Class 3 EV SSL CA - G3
Signature algorithm	SHA256withRSA
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 (4369 bytes)
Chain issues	Contains anchor

#2

Subject	Symantec Class 3 EV SSL CA - G3 Fingerprint SHA1: e3fc0ad84f2f5a83ed6f86f567f8b14b40dcbf12 Pin SHA256: gMxWOrX4PMQesK9qFNbYBxjBfjUvlkn/vN1n+L9lE5E=

Valid until	Mon, 30 Oct 2023 23:59:59 UTC (expires in 7 years and 11 months)
Key	RSA 2048 bits (e 65537)
Issuer	VeriSign Class 3 Public Primary Certification Authority - G5
Signature algorithm	SHA256withRSA

#3

Subject	VeriSign Class 3 Public Primary Certification Authority - G5 In trust store Fingerprint SHA1: 4eb6d578499b1ccf5f581ead56be3d9b6744a5e5 Pin SHA256: JbQbUG5JMJUoI6brnx0x3vZF6jilxsapbXGVfjhN8Fg=
Valid until	Wed, 16 Jul 2036 23:59:59 UTC (expires in 20 years and 7 months)
Key	RSA 2048 bits (e 65537)
Issuer	VeriSign Class 3 Public Primary Certification Authority - G5 Self-signed
Signature algorithm	SHA1withRSA Weak, but no impact on root certificate

Certification Paths

Path #1: Trusted

1	Sent by server	online.bdo.com.ph Fingerprint SHA1: 79d7d971116fd9cc45139953898cefa407b76aa6 Pin SHA256: w3eQEYi3Rhz7iZpHBrF9dy5EiZWo08CeEKPpo8d9mt4= RSA 2048 bits (e 65537) / SHA256withRSA
2	Sent by server	Symantec Class 3 EV SSL CA - G3 Fingerprint SHA1: e3fc0ad84f2f5a83ed6f86f567f8b14b40dcbf12 Pin SHA256: gMxWOrX4PMQesK9qFNbYBxjBfjUvlkn/vN1n+L9lE5E= RSA 2048 bits (e 65537) / SHA256withRSA
3	Sent by server In trust store	VeriSign Class 3 Public Primary Certification Authority - G5 Self-signed Fingerprint SHA1: 4eb6d578499b1ccf5f581ead56be3d9b6744a5e5 Pin SHA256: JbQbUG5JMJUoI6brnx0x3vZF6jilxsapbXGVfjhN8Fg= RSA 2048 bits (e 65537) / SHA1withRSA Weak or insecure signature, but no impact on root certificate

Configuration

Protocols

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

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

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ECDH 224 bits (eq. 2048 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ECDH 224 bits (eq. 2048 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (0xc012) ECDH 224 bits (eq. 2048 bits RSA) FS	112
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c)	128
TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c)	128
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)	256
TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d)	256

Handshake Simulation

Android 2.3.7 No SNI [2]	Protocol or cipher suite mismatch		Fail[3]
Android 4.0.4	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) FS	128
Android 4.1.1	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) FS	128

Android 4.2.2	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) FS	128
Android 4.3	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) FS	128
Android 4.4.2	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) FS	128
Android 5.0.0	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) FS	128
Baidu Jan 2015	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) FS	128
BingPreview Jan 2015	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) FS	128
Chrome 45 / OS X R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) FS	128
Firefox 31.3.0 ESR / Win 7	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) FS	128
Firefox 41 / OS X R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) FS	128
Googlebot Feb 2015	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) FS	128
IE 6 / XP No FS [1] No SNI [2]	Protocol or cipher suite mismatch		Fail[3]
IE 7 / Vista	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) FS	128
IE 8 / XP No FS [1] No SNI [2]	Protocol or cipher suite mismatch		Fail[3]
IE 8-10 / Win 7 R	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) FS	128
IE 11 / Win 7 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) FS	128
IE 11 / Win 8.1 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) FS	128
IE 10 / Win Phone 8.0	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) FS	128
IE 11 / Win Phone 8.1 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) FS	128
IE 11 / Win Phone 8.1 Update R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) FS	128
IE 11 / Win 10 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) FS	128
Edge / Win 10 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) FS	128
Java 6u45 No SNI [2]	Protocol or cipher suite mismatch		Fail[3]
Java 7u25	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) FS	128
Java 8u31	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) FS	128
OpenSSL 0.9.8y	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA (0x35) No FS	256
OpenSSL 1.0.1l R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) FS	128
OpenSSL 1.0.2 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) FS	128
Safari 5.1.9 / OS X 10.6.8	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) FS	128
Safari 6 / iOS 6.0.1 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) FS	128
Safari 6.0.4 / OS X 10.8.4 R	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) FS	128
Safari 7 / iOS 7.1 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) FS	128
Safari 7 / OS X 10.9 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) FS	128
Safari 8 / iOS 8.4 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) FS	128
Safari 8 / OS X 10.10 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) FS	128
Safari 9 / iOS 9 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) FS	128
Safari 9 / OS X 10.11 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) FS	128
Apple ATS 9 / iOS 9 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) FS	128
Yahoo Slurp Jan 2015	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) FS	128
YandexBot Jan 2015	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) FS	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	**Supported** **DoS DANGER** (more info)
Insecure Client-Initiated Renegotiation	No
BEAST attack	Not mitigated server-side (more info) TLS 1.0: 0xc013
POODLE (SSLv3)	No, SSL 3 not supported (more info)
POODLE (TLS)	No (more info)

Downgrade attack prevention	**Yes, TLS_FALLBACK_SCSV supported** (more info)
SSL/TLS compression	No
RC4	No
Heartbeat (extension)	No
Heartbleed (vulnerability)	No (more info)
OpenSSL CCS vuln. (CVE-2014-0224)	No (more info)
Forward Secrecy	With modern browsers (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** online.bdo.com.ph
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 17:02:22 UTC
Test duration	145.324 seconds
HTTP status code	200
HTTP server signature	Oracle-iPlanet-Web-Server/7.0
Server hostname	-

SSL Report v1.20.28