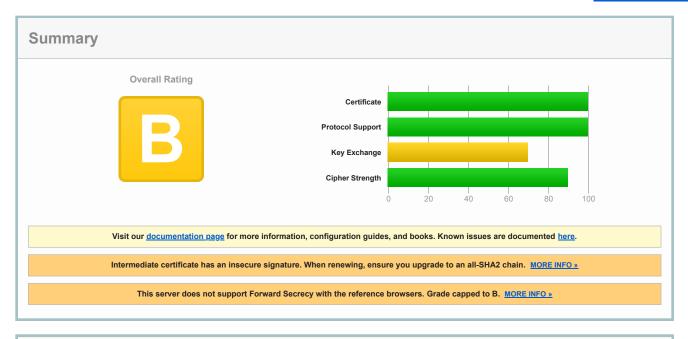


You are here: <u>Home</u> > <u>Projects</u> > <u>SSL Server Test</u> > mastercard.com

SSL Report: mastercard.com (216.119.209.64)

Assessed on: Fri, 22 Oct 2021 19:15:31 UTC | Hide | Clear cache

Scan Another »



Certificate #1: RSA 2048 bits (SHA256withRSA)



Subject	mastercard.com Fingerprint SHA256: dd8d2c274ec98c7c669c2246d5c69d46ce4260c55b2806e635458a0f1fd86879	
Jubject	Pin SHA256: bOw89rdff5kH6e0etfWn30uUMLD6MSN7M3ffhVh2ztw=	
Common names	mastercard.com	
Alternative names	mastercard.com	
Serial Number	07bc5d755ecbd799e9d8dee42896f18b	
/alid from	Fri, 04 Jun 2021 17:46:28 UTC	
/alid until	Sat, 04 Jun 2022 17:46:28 UTC (expires in 7 months and 12 days)	
Key	RSA 2048 bits (e 65537)	
Weak key (Debian)	No	
ssuer	Entrust Certification Authority - L1K AIA: http://aia.entrust.net//1lk-chain256.cer	
Signature algorithm	SHA256withRSA	
Extended Validation	No	
Certificate Transparency	Yes (certificate)	
OCSP Must Staple	No	
Revocation information	CRL, OCSP CRL: http://crl.entrust.net/level1k.crl OCSP: http://ocsp.entrust.net	
Revocation status	Good (not revoked)	
ONS CAA	No (more info)	
Frusted	Yes Mozilla Apple Android Java Windows	



Certificates provided	6 (7852 bytes)	
hain issues	Incorrect order, Extra certs, Contains anchor	
2		
	Entrust.net Certification Authority (2048) In trust store	
Subject	Fingerprint SHA256: 6dc47172e01cbcb0bf62580d895fe2b8ac9ad4f873801e0c10b9c837d21eb177	
	Pin SHA256: HqPF5D7WbC2imDpCpKebHpBnhs6fG1hiFBmgBGOofTg=	
/alid until	Tue, 24 Jul 2029 14:15:12 UTC (expires in 7 years and 9 months)	
Key	RSA 2048 bits (e 65537)	
ssuer	Entrust.net Certification Authority (2048) Self-signed	
Signature algorithm	SHA1withRSA Weak, but no impact on root certificate	
‡ 3		
	Entrust Certification Authority - L1C	
Subject	Fingerprint SHA256: 0ee4daf71a85d842d23f4910fd4c909b7271861931f1d5feac868225f52700e2	
	Pin SHA256: VFv5NemtodoRftw8KsvFb8AoCWwOJL6b0JS+Ui0bQ94=	
/alid until	Fri, 12 Nov 2021 02:51:17 UTC (expires in 20 days, 7 hours)	
Кеу	RSA 2048 bits (e 65537)	
ssuer	Entrust.net Certification Authority (2048)	
Signature algorithm	SHA1withRSA INSECURE	
#4		
	Entrust Certification Authority - L1K	
Subject	Fingerprint SHA256: f5c2f23c6518f9d19b6f39beaea4fbae10031ba9dc985ce1563a520da0ad4116	
	Pin SHA256: 980lonqp3wkYtN9SZVgMzuWQzJta1nfxNPwTem1X0uc=	
/alid until	Wed, 23 Oct 2024 07:33:22 UTC (expires in 3 years)	
Кеу	RSA 2048 bits (e 65537)	
ssuer	Entrust Root Certification Authority - G2	
Signature algorithm	SHA256withRSA	
#5		
	Entrust Root Certification Authority - G2	
Subject	Fingerprint SHA256: 6b143c2005d5539cc22eab5f772db2a9fe87467feffa07fcf0a9f7d28274ca7a	
	Pin SHA256: du6FkDdMcVQ3u8prumAo6t3i3G27uMP2EOhR8R0at/U=	
/alid until	Mon, 23 Sep 2024 01:31:53 UTC (expires in 2 years and 11 months)	
Key	RSA 2048 bits (e 65537)	
ssuer	Entrust Root Certification Authority	
Signature algorithm	SHA256withRSA	
#6		
No. let 4	Entrust Certification Authority - L1K	
Subject	Fingerprint SHA256: 3b0cc20384ad7f24eb438f2b80c63ebe003f7f215b8877e418ebb0484028db57 Pin SHA256: 980lonqp3wkYtN9SZVgMzuWQzJta1nfxNPwTem1X0uc=	
falid metil		
/alid until	Tue, 27 Aug 2024 08:34:47 UTC (expires in 2 years and 10 months)	
Key	RSA 2048 bits (e 65537)	
ssuer	Entrust Root Certification Authority - G2	



Certification Paths

<u>+</u>

Click here to expand

Certificate #2: RSA 2048 bits (SHA256withRSA)





Subject	mastercard.com Fingerprint SHA256: 070fac5f61d6fa4e17b4af9acdf3a22668a700a415246b23ba3bcc825e4be31f Pin SHA256: ZGCz0Lm51vIPSf0bnBeneE57WFpnFWvMovxtHm4F1BM=
Common names	mastercard.com
Alternative names	mastercard.com
Serial Number	6d91903c953c17ed022a5d4be09f9d75
Valid from	Tue, 04 May 2021 08:36:36 UTC
Valid until	Wed, 04 May 2022 08:36:35 UTC (expires in 6 months and 11 days)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	Entrust Certification Authority - L1K AIA: http://aia.entrust.net/l1k-chain256.cer
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	Yes (certificate)
OCSP Must Staple	No
Revocation information	CRL, OCSP CRL: http://crl.entrust.net/level1k.crl OCSP: http://ocsp.entrust.net
Revocation status	Good (not revoked)
DNS CAA	No (more info)
Trusted	Yes Mozilla Apple Android Java Windows

E Q

Additional Certificates (if supplied)

Certificates provided	5 (6651 bytes)
Chain issues	Incorrect order, Extra certs, Contains anchor

#2

Subject	Entrust.net Certification Authority (2048) In trust store Fingerprint SHA256: 6dc47172e01cbcb0bf62580d895fe2b8ac9ad4f873801e0c10b9c837d21eb177 Pin SHA256: HqPF5D7WbC2imDpCpKebHpBnhs6fG1hiFBmgBGOofTg=
Valid until	Tue, 24 Jul 2029 14:15:12 UTC (expires in 7 years and 9 months)
Key	RSA 2048 bits (e 65537)
Issuer	Entrust.net Certification Authority (2048) Self-signed
Signature algorithm	SHA1withRSA Weak, but no impact on root certificate

#3

	Entrust Certification Authority - L1C
Subject	Fingerprint SHA256: 0ee4daf71a85d842d23f4910fd4c909b7271861931f1d5feac868225f52700e2
	Pin SHA256: VFv5NemtodoRftw8KsvFb8AoCWwOJL6bOJS+Ui0bQ94=
Valid until	Fri, 12 Nov 2021 02:51:17 UTC (expires in 20 days, 7 hours)
Key	RSA 2048 bits (e 65537)
Issuer	Entrust.net Certification Authority (2048)
Signature algorithm	SHA1withRSA INSECURE

#4

Entrust Certification Authority - L1K
Fingerprint SHA256: f5c2f23c6518f9d19b6f39beaea4fbae10031ba9dc985ce1563a520da0ad4116
Pin SHA256: 980Ionqp3wkYtN9SZVgMzuWQzJta1nfxNPwTem1X0uc=
Wed, 23 Oct 2024 07:33:22 UTC (expires in 3 years)
RSA 2048 bits (e 65537)
Entrust Root Certification Authority - G2
SHA256withRSA

#5

Additional Certificates (if supplied)		<u>±</u>
Subject	Entrust Root Certification Authority - G2 Fingerprint SHA256: 6b143c2005d5639cc22eab5f772db2a9fe87467feffa07fcf0a9f7d28274ca7a Pin SHA256: du6FkDdMcVQ3u8prumAo6t3i3G27uMP2EOhR8R0at/U=	
Valid until	Mon, 23 Sep 2024 01:31:53 UTC (expires in 2 years and 11 months)	
Key	RSA 2048 bits (e 65537)	
Issuer	Entrust Root Certification Authority	
Signature algorithm	SHA256withRSA	



Certification Paths

+

Click here to expand

Configuration



Protocols





Cipher Suites

# TLS 1.2 (server has no preference)	
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa) WEAK	112
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (0xc012) ECDH sect571r1 (eq. 15360 bits RSA) FS WEAK	112
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) WEAK	128
TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33) DH 2048 bits FS WEAK	128
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (0x41) WEAK	128
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (0x45) DH 2048 bits FS WEAK	128
TLS_RSA_WITH_SEED_CBC_SHA (0x96) WEAK	128
TLS_DHE_RSA_WITH_SEED_CBC_SHA (0x9a) DH 2048 bits FS WEAK	128
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ECDH sect571r1 (eq. 15360 bits RSA) FS WEAK	128
TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c) WEAK	128
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x67) DH 2048 bits FS WEAK	128
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c) WEAK	128
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e) DH 2048 bits FS	128
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) ECDH sect571r1 (eq. 15360 bits RSA) FS WEAK	128
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) ECDH sect571r1 (eq. 15360 bits RSA) FS	128
TLS_RSA_WITH_IDEA_CBC_SHA (0x7) WEAK	128
TLS_RSA_WITH_AES_256_CBC_SHA (0x35) WEAK	256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) DH 2048 bits FS WEAK	256
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (0x84) WEAK	256
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0x88) DH 2048 bits FS WEAK	256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ECDH sect571r1 (eq. 15360 bits RSA) FS WEAK	256
TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d) WEAK	256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x6b) DH 2048 bits FS WEAK	256
TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d) WEAK	256
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f) DH 2048 bits FS	256



256256



Handshake Simulation

Handshake Simulation			
Android 4.4.2	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp521r1 FS
Android 5.0.0	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp521r1 FS
Android 6.0	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Android 7.0	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Android 8.0	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Android 8.1	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Android 9.0	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
BingPreview Jan 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH sect571r1 FS
Chrome 49 / XP SP3	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Chrome 69 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
<u>Chrome 70 / Win 10</u>	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Chrome 80 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 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 > http/1.1	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Firefox 49 / XP SP3	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Firefox 62 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Firefox 73 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Googlebot Feb 2018	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
<u>IE 11 / Win 7</u> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS
<u>IE 11 / Win 8.1</u> R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS
IE 11 / Win Phone 8.1 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_RSA_WITH_AES_128_CBC_SHA256 No FS
IE 11 / Win Phone 8.1 Update R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS
<u>IE 11 / Win 10</u> R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Edge 15 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Edge 16 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Edge 18 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Edge 13 / Win Phone 10 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
<u>Java 8u161</u>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS
Java 11.0.3	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
<u>Java 12.0.1</u>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
OpenSSL 1.0.1I R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH sect571r1 FS
OpenSSL 1.0.2s R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
OpenSSL 1.1.0k R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
OpenSSL 1.1.1c R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
<u>Safari 6 / iOS 6.0.1</u>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS
Safari 7 / iOS 7.1 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS
<u>Safari 7 / OS X 10.9</u> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS
Safari 8 / iOS 8.4 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS
<u>Safari 8 / OS X 10.10</u> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS
Safari 9 / iOS 9 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
<u>Safari 9 / OS X 10.11</u> R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Safari 10 / iOS 10 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Safari 10 / OS X 10.12 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
<u>Safari 12.1.2 / MacOS 10.14.6</u> <u>Beta</u> R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
<u>Safari 12.1.1 / iOS 12.3.1</u> R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Apple ATS 9 / iOS 9 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS

Handshake Simulation

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 sect571r1 FS

Not simulated clients (Protocol mismatch)



Click here to expand

- (1) Clients that do not support Forward Secrecy (FS) are excluded when determining support for it.
- $(2) \ No \ support \ for \ virtual \ SSL \ hosting \ (SNI). \ Connects \ to \ the \ default \ site \ if \ the \ server \ uses \ SNI.$
- $(3) \ {\hbox{Only first connection attempt simulated. Browsers sometimes retry with a lower protocol version.}$
- (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

Secure Renegotiation Supported Secure Client-Initiated Renegotiation No Insecure Client-Initiated Renegotiation No BEAST attack Miligated sever-side (more info) POODLE (SSLV3) No. SSL 3 not supported (more info) POODLE (TLS) No (more info) POODLE (SDLV3) No. (more info) SOURCE (SDLV3) No (more info) Statut S compression No No No RCA No RCA<	T TOLOCOT Details			
Secure Renegotiation Supported Secure Renegotiation No				
Secure Client-Initiated Renegotiation No Mispated Server-side (moze info) BEAST attack Mispated Server-side (moze info) POODLE (SLV3) No. SSL 3 not supported (moze info) POODLE (SLV3) No. (moze info) POODLE (TLS) No (moze info) TLS 1.2: 0x000x3 GOLDENDOODLE No (moze info) TLS 1.2: 0x000x3 GOLDENDOODLE No (moze info) TLS 1.2: 0x000x3 Steeping POODLE No (moze info) TLS 1.2: 0x000x3 Steeping POODLE No (moze info) TLS 1.2: 0x000x3 Steeping POODLE No (moze info) TLS 1.2: 0x000x3 SSL/TLS compression No (moze info) TLS 1.2: 0x000x3 SSL/TLS compression No (moze info) TLS 1.2: 0x000x3 SSL/TLS compression No (moze info) The Heartbeat (extension) Yes Heartbeat (extension) Yes Heartbeat (extension) No (moze info) The Heartbeat (extension) No (moze info) No (moze info) Session resumption (tickets) Yes (moze info) Session resumption (tickets) Yes (moze info) Session resumption (tickets) Yes (moze info) No (moze info) Public Key Pinning (HPKP) No (moze info) Public Key Pinning (HPKP) No (moze info) No (moze info) The Version intolerance No (moze info) The Version intolerance No (moze info) The Version intolerance No (moze info) Heartbeat (moze info) No (moze info) No (moze info) No (moze info) No (moze info) The Version intolerance No (moze info) No (moze info) No (moze info) No (moze info)	DROWN			
BEAST attack Miligated server-side (more info) POODLE (ISSLV3) No, SSL 3 not supported (more info) POODLE (ISSLV3) No (more info) POODLE (ISSLV3) No (more info) ILS 12 - 8-86989 Combie POODLE No (more info) ILS 12 - 8-86989 Combie POODLE No (more info) ILS 12 - 8-86989 CopenSSL 0-Length No (more info) ILS 12 - 8-86989 Steeping POODLE No (more info) ILS 12 - 8-86989 CopenSSL 0-Length No (more info) ILS 12 - 8-86989 Steeping POODLE No (more info) ILS 12 - 8-86989 CopenSSL Copensor No (more info) ILS 12 - 8-86989 Rear to the info ILS 12 - 8-86989 Rear to the in	Secure Renegotiation	Supported		
BEAST attack Mitigated server-side (more info) POODLE (SSLv3) No, SSL 3 not supported (more info) POODLE (TLS) No (more info) POODLE (No (more info) TLS 12: 0+00045 GOLLENDODLE No (more info) TLS 0+00045 GOLLEN	Secure Client-Initiated Renegotiation	No		
PODDLE (SSLV3) No. SSL 3 not supported (more info) PODDLE (TLS) No (more info) ROBIDE (PODDLE No (more info) TLS 12: 0-00003 ROBIDE PODDLE No (more info) TLS 12: 0-00003 ROBIDE ROBIDE ROBIDE NO (more info) ROBIDE	Insecure Client-Initiated Renegotiation	No		
PODDLE (TLS) No (more info) Zombie PODDLE No (more info) rt.S 1.2 : 0x0000.3 GOLDENDODLE No (more info) rt.S 1.2 : 0x0000.3 GOLDENDODLE No (more info) rt.S 1.2 : 0x0000.3 Sleeping POODLE No (more info) rt.S 1.2 : 0x0000.3 Downgrade attack prevention Unknown (requires support for at least two protocols, excl. SSL2) SSLTLS compression No RC4 No RC4 No RC4 No Heartbeed (extension) Yes Heartbeed (vulnerability) No (more info) Titcketbleed (vulnerability) No (more info) OpenSSL Padding Oracle vuln. No (more info) QOPENSL Padding Oracle vuln. No (more info) ROBOT (vulnerability) No (more info) ROBOT (vulnerability) No (more info) Forward Secrecy With some browsers (more info) ALPN Yes ntmpt.1 NPN No Session resumption (tacknies) No (IDS assigned but not accepted) Session resumption (titckets) Yes OCSP stapling No (more info)	BEAST attack	Mitigated server-side (more info)		
Zombie POODLE No (more info) TLS 12: exeesas GOLDENDOODLE No (more info) TLS 12: exeesas OpenSSL 0-Length No (more info) TLS 12: exeesas Steeping POODLE No (more info) TLS 12: exeesas Downgrade attack prevention Unknown (requires support for at least two protocols, excl. SSL2) SSLTLS compression No RC4 No Heartbeat (extension) Yes Heartbeat (extension) No (more info) Titcketbleed (vulnerability) No (more info) Titcketbleed (vulnerability) No (more info) OpenSSL Padding Oracle vuln. No (more info) CVE-2014-2024) No (more info) ROBOT (vulnerability) No (more info) ROBOT (vulnerability) No (more info) ROBOT (vulnerability) No (more info) ALPN Yes Intp/1.1 Session resumption (caching) No (more info) Session resumption (tickets) Yes Session resumption (tickets) Yes Session resumption (tickets) Yes Strict Transport Security (HSTS) No (more info) Publi	POODLE (SSLv3)	No, SSL 3 not supported (more info)		
SOLDENDODLE No (more info) TLS 1.2 : 0x000000 Sleeping POODLE No (more info) TLS 1.2 : 0x000000 SSLITLS compression No RC4 No Heartbeat (extension) Yes Heartblead (vulnerability) No (more info) OpenSSL C5 vuln. (CVE-2014-0224) No (more info) OpenSSL C5 vuln. (CVE-2014-0224) No (more info) OpenSSL C5 vuln. (CVE-2014-0224) No (more info) ROBOT (vulnerability) No (more info) ROBOT (vulnerability) No (more info) Session resumption (caching) No (IDS assigned but not accepted) Session resumption (tickets) Yes OCSP stapling No Strict Transport Security (HSTS) No HSTS Preloading HPKP) No (more info) Public Key Pinning (Report-Only No (more info) Long handshake intolerance No LTLS extension intolerance No Incorrect SNI alerts No LUses common DH primes No LUSES COMMON CARLES AND	POODLE (TLS)	No (more info)		
OpenSSL 0-Length No (more info) TLS 1.2 : 0x000000 Sileping POODLE No (more info) TLS 1.2 : 0x000000 SSLTLS compression No RC4 No Heartbleat (extension) Yes Heartbleat (extension) No (more info) TLKetbleed (vulnerability) No (more info) OpenSSL CS vuln. (CVE-2014-0224) No (more info) OpenSSL Padding Oracle vuln. (CVE-2014-0224) No (more info) OpenSSL Padding Oracle vuln. (CVE-2016-0224) No (more info) OpenSSL Padding Oracle vuln. (CVE-2016-0224) No (more info) OpenSSL Padding Oracle vuln. (CVE-2016-0224) No (more info) OpenSSL Secrecy With some browsers (more info) ALPN Yes Intp1.1 No Sassion resumption (caching) No (IDs assigned but not accepted) Session resumption (tickets) Yes 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 extension intolerance No Incorrect SNI alerts No	Zombie POODLE	No (more info) TLS 1.2: 0x000a		
Steping POODLE No (more info) TLS 1.2 : exeess a Downgrade attack prevention Unknown (requires support for at least two protocols, excl. SSL2) SSL/TLS compression No RC4 No Heartbeat (extension) Yes 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) ROBOT (vulnerability) No (more info) Forward Secrecy With some browsers (more info) ALPN Yes http://.1 NoN Session resumption (caching) No (IDs assigned but not accepted) Session resumption (tickets) Yes UCCSP stapling No (IDs assigned but not accepted) Strict Transport Security (HSTS) No HSTS Preloading Not in: Chrome Edge Firefox IE Public Key Pinning (HPKP) No (more info) Not in: Chrome Edge Firefox IE Public Key Pinning (Static) No (more info) Long handshake intolerance No No TLS extension intolerance No No Uses common DH primes No Uses common DH primes No No Increase common DH primes No No Increase common DH primes No No No No No No No No No N	GOLDENDOODLE	No (more info) TLS 1.2: 0x000a		
Downgrade attack prevention Unknown (requires support for at least two protocols, excl. SSL2) SSLTLS compression No RC4 No Heartbeat (extension) Yes Heartbedel (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) CVE-2016-2107) No (more info) ROBOT (vulnerability) No (more info) Forward Secrecy With some browsers (more info) ALPN Yes http:/.1 NNPN No (IDs assigned but not accepted) Session resumption (tacking) No (IDs assigned but not accepted) Session resumption (tickets) Yes Vestrict Transport Security (HSTS) No No (more info) No Public Key Pinning (HPKP) No (more info) Public Key Pinning (Static) No (more info) Long handshake intolerance No No No TLS extension intolerance No Lincorrect SNI alerts N	OpenSSL 0-Length	No (more info) TLS 1.2: 0x000a		
SSLITLS compression No RC4 No Heartbeat (extension) Yes 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 some browsers (more info) ALPN Yes http/1.1 NPN No No Session resumption (tickets) Yes Session resumption (tickets) Yes Session resumption (tickets) Yes Session resumption (tickets) 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 (more info) Long handshake intolerance No Its extension intolerance No Incorrect SNI alerts No Uses common DH primes No	Sleeping POODLE	No (more info) TLS 1.2: 0x000a		
RC4 No Moderatheat (extension) Yes Heartbeat (extension) Yes Heartbleed (vulnerability) No (more info) OpenSSL CCS vuln. (CVE-2014-0224) No (more info) OpenSSL Padding Oracle vuln. (CVE-2016-2107) No (more info) OpenSSL Padding Oracle vuln. (CVE-2016-2107) No (more info) OpenSSL Padding Oracle vuln. (CVE-2016-2107) No (more info) ALPN Yes http/1.1 NPN No No (more info) No (IDs assigned but not accepted) Session resumption (tickets) Yes Session resumption (tickets) Yes 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 (Static) No (more info) Long handshake intolerance No TLS extension intolerance No Incorrect SNI alerts No Uses common DH primes No	Downgrade attack prevention	Unknown (requires support for at least two protocols, excl. SSL2)		
Heartbeat (extension) Yes Heartbead (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) ROBOT (vulnerability) No (more info) Forward Secrecy With some browsers (more info) ALPN Yes http:/.1 NPN No Session resumption (caching) No (IDs assigned but not accepted) Session resumption (tickets) Yes OCSP stapling No Strict Transport Security (HSTS) No HSTS Preloading Not in: Chrome Edge Firefox IE Public Key Pinning (HPKP) No (more info) No (more info) Public Key Pinning (Static) No (more info) No (more inf	SSL/TLS compression	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) ROBOT (vulnerability) No (more info) Forward Secrecy With some browsers (more info) ALPN Yes http:/.1 NPN No Session resumption (caching) No (IDs assigned but not accepted) Session resumption (tickets) Yes 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 (Static) No (more info) Long handshake intolerance No TLS extension intolerance No Incorrect SNI alerts No Uses common DH primes No Uses common DH primes No	RC4	No		
Ticketbleed (vulnerability) No (more info) OpenSSL CCS vuln. (CVE-2014-0224) No (more info) OpenSSL Padding Oracle vuln. (CVE-2016-2107) ROBOT (vulnerability) No (more info) Forward Secrecy With some browsers (more info) ALPN Yes http:/l.1 NPN No Session resumption (caching) No (IDs assigned but not accepted) Session resumption (tickets) Yes OCSP stapling No Strict Transport Security (HSTS) No HSTS Preloading Not in: Chrome Edge Firefox IE Public Key Pinning (HPKP) No (more info) No (more info) No (more info) No (more info) TLS extension intolerance No No No HOS AND	Heartbeat (extension)	Yes		
OpenSSL CCS vuln. (CVE-2014-0224) OpenSSL Padding Oracle vuln. (CVE-2016-2107) ROBOT (vulnerability) No (more info) Forward Secrecy With some browsers (more info) ALPN Yes http/1.1 NPN No Session resumption (caching) No (IDs assigned but not accepted) Session resumption (tickets) Yes OCSP stapling No Strict Transport Security (HSTS) No HSTS Preloading Not in: Chrome Edge Firefox IE Public Key Pinning (HPKP) No (more info) No (more info) No (more info) No (more info) No TLS extension intolerance No TLS extension intolerance No Incorrect SNI alerts No Uses common DH primes No Incorrect SNI alerts No Incorrect SNI al	Heartbleed (vulnerability)	No (more info)		
OpenSSL Padding Oracle vuln. (CVE-2016-2107) ROBOT (vulnerability) No (more info) Forward Secrecy With some browsers (more info) ALPN Yes http/1.1 No No Session resumption (caching) No (IDs assigned but not accepted) Session resumption (tickets) Yes 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 (Static) No (more info) No (more info) Public Key Pinning (Static) No (more info) TLS extension intolerance No TLS version intolerance No Incorrect SNI alerts No Uses common DH primes No	Ticketbleed (vulnerability)	No (more info)		
ROBOT (vulnerability) No (more info) Forward Secrecy With some browsers (more info) ALPN Yes http/1.1 NPN No Session resumption (caching) No (IDs assigned but not accepted) Session resumption (tickets) Yes 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 (Static) No (more info) TLS extension intolerance No TLS version intolerance No Incorrect SNI alerts No Uses common DH primes No	OpenSSL CCS vuln. (CVE-2014-0224)	No (more info)		
Forward Secrecy With some browsers (more info) ALPN Yes http/1.1 NPN No No Session resumption (caching) No (IDs assigned but not accepted) Session resumption (tickets) Yes 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 Incorrect SNI alerts No Uses common DH primes No	OpenSSL Padding Oracle vuln. (CVE-2016-2107)	No (more info)		
ALPN Yes http://.1 NPN No No Session resumption (caching) No (IDs assigned but not accepted) Session resumption (tickets) Yes 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 (Static) No (more info) Public Key Pinning (Static) No (more info) TLS extension intolerance No TLS version intolerance No Incorrect SNI alerts No No No No No No No No No No No No No	ROBOT (vulnerability)	No (more info)		
No (IDs assigned but not accepted) Session resumption (caching) No (IDs assigned but not accepted) Session resumption (tickets) Yes 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	Forward Secrecy	With some browsers (more info)		
Session resumption (caching) No (IDs assigned but not accepted) Session resumption (tickets) Yes 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 Incorrect SNI alerts No Uses common DH primes No	ALPN	Yes http/1.1		
Session resumption (tickets) 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 (Static) No (more info) Long handshake intolerance No TLS extension intolerance No Incorrect SNI alerts No No No No No No No No No N	NPN	No		
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 Incorrect SNI alerts No Uses common DH primes No	Session resumption (caching)	No (IDs assigned but not accepted)		
Strict Transport Security (HSTS) No HSTS Preloading Not in: Chrome Edge Firefox IE Public Key Pinning (HPKP) No (more info) Public Key Pinning (Static) No (more info) Long handshake intolerance No TLS extension intolerance No Incorrect SNI alerts No No No No No No No No No N	Session resumption (tickets)	Yes		
HSTS Preloading Not in: Chrome Edge Firefox IE Public Key Pinning (HPKP) No (more info) Public Key Pinning Report-Only No (more info) Long handshake intolerance No TLS extension intolerance No Incorrect SNI alerts No No No No No No No No No N	OCSP stapling	No		
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 Incorrect SNI alerts No No No No No No No No No N	Strict Transport Security (HSTS)	No		
Public Key Pinning Report-Only No (more info) Long handshake intolerance No TLS extension intolerance No Incorrect SNI alerts No Uses common DH primes No	HSTS Preloading	Not in: Chrome Edge Firefox IE		
Public Key Pinning (Static) Long handshake intolerance No TLS extension intolerance No Incorrect SNI alerts No Uses common DH primes No	Public Key Pinning (HPKP)	No (more info)		
Long handshake intolerance No TLS extension intolerance No TLS version intolerance No Incorrect SNI alerts No Uses common DH primes No	Public Key Pinning Report-Only	No		
TLS extension intolerance No TLS version intolerance No Incorrect SNI alerts No Uses common DH primes No	Public Key Pinning (Static)	No (more info)		
TLS version intolerance No Incorrect SNI alerts No Uses common DH primes No	Long handshake intolerance	No		
Incorrect SNI alerts No Uses common DH primes No	TLS extension intolerance	No		
Uses common DH primes No	TLS version intolerance	No		
·	Incorrect SNI alerts	No		
DH public server param (Ys) reuse No	Uses common DH primes	No		
	DH public server param (Ys) reuse	No		

Protocol Details ECDH public server param reuse No Supported Named Groups sect283k1, sect283r1, sect409k1, sect409r1, sect571k1, sect571r1, secp256k1, secp256r1, secp384r1, secp521r1, brainpoolP256r1, brainpoolP384r1, brainpoolP512r1 (Server has no preference) SSL 2 handshake compatibility No HTTP Requests 1 https://mastercard.com/ (HTTP/1.1 301 Moved Permanently)



Miscellaneous

Test date	Fri, 22 Oct 2021 19:14:07 UTC
Test duration	83.517 seconds
HTTP status code	301
HTTP forwarding	https://www.mastercard.com
HTTP server signature	Apache
Server hostname	www.purchasewithpurpose.net.ma

SSL Report v2.1.8

Copyright © 2009-2021 Qualys, Inc. All Rights Reserved.

Terms and Conditions

Iry Qualys for free! Experience the award-winning Qualys Cloud Platform and the entire collection of Qualys Cloud Apps, including certificate security solutions.