

You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > ind.millenniumbcp.pt

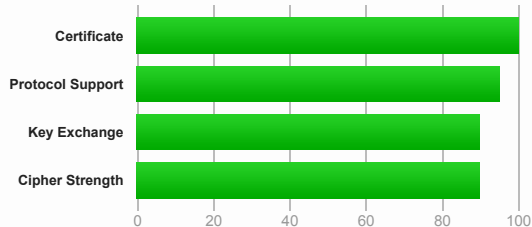
## SSL Report: ind.millenniumbcp.pt (193.53.22.233)

Assessed on: Mon, 25 Feb 2019 10:47:50 UTC | [Hide](#) | [Clear cache](#)

[Scan Another »](#)

### Summary

Overall Rating



Visit our [documentation page](#) for more information, configuration guides, and books. Known issues are documented [here](#).

Server sent invalid HSTS policy. See below for further information.

Renegotiation test has been disabled temporarily due to an Apache httpd 2.4.37 bug. [MORE INFO »](#)

### Certificate #1: RSA 2048 bits (SHA256withRSA)



#### Server Key and Certificate #1



<b>Subject</b>	ind.millenniumbcp.pt Fingerprint SHA256: f8853c531289b0ba1dde87a0d9174b1375ed21e823ef547f3b316e23b0398977 Pin SHA256: X9SnliuSMq9Krz1uhpAhcUkjdgSjKLP6k4QajuGAIRk=
<b>Common names</b>	ind.millenniumbcp.pt
<b>Alternative names</b>	ind.millenniumbcp.pt
<b>Serial Number</b>	00d8f279549c0b33bf0000000054cf764f
<b>Valid from</b>	Mon, 18 Feb 2019 09:56:57 UTC
<b>Valid until</b>	Thu, 18 Feb 2021 10:26:55 UTC (expires in 1 year and 11 months)
<b>Key</b>	RSA 2048 bits (e 65537)
<b>Weak key (Debian)</b>	No
<b>Issuer</b>	Entrust Certification Authority - L1M AIA: http://aia.entrust.net/11m-chain256.cer
<b>Signature algorithm</b>	SHA256withRSA
<b>Extended Validation</b>	Yes
<b>Certificate Transparency</b>	Yes (certificate)
<b>OCSP Must Staple</b>	No
<b>Revocation information</b>	CRL, OCSP CRL: http://crl.entrust.net/level1m.crl OCSP: http://ocsp.entrust.net
<b>Revocation status</b>	Good (not revoked)
<b>DNS CAA</b>	No ( <a href="#">more info</a> )
<b>Trusted</b>	Yes Mozilla Apple Android Java Windows



#### Additional Certificates (if supplied)



<b>Certificates provided</b>	4 (5712 bytes)
<b>Chain issues</b>	Contains anchor
<b>#2</b>	
<b>Subject</b>	Entrust Certification Authority - L1M Fingerprint SHA256: 75c5b3f01fd1f51a2c447ab7c785d72e69fa9c472c08571e7eadf3b8eabae70c Pin SHA256: VYZwGJkq3NN01YRI2RGIST1mqTWG8zDcRf1/KAN6l=
<b>Valid until</b>	Tue, 15 Oct 2030 15:55:03 UTC (expires in 11 years and 7 months)

## Additional Certificates (if supplied)



Key	RSA 2048 bits (e 65537)
Issuer	Entrust Root Certification Authority - G2
Signature algorithm	SHA256withRSA

#3

Subject	Entrust Root Certification Authority - G2 Fingerprint SHA256: 6b143c2005d5539cc22eab5f772db2a9fe87467feffa07fc0a9f7d28274ca7a Pin SHA256: du6FkDdMcVQ3u8prumAo6t3i3G27uMP2EOhR8R0at/U=
Valid until	Mon, 23 Sep 2024 01:31:53 UTC (expires in 5 years and 6 months)
Key	RSA 2048 bits (e 65537)
Issuer	Entrust Root Certification Authority
Signature algorithm	SHA256withRSA

#4

Subject	Entrust Root Certification Authority <span>In trust store</span> Fingerprint SHA256: 73c176434f1bc6d5ad45b0e76e727287c8de57616c1e6e6141a2b2cbc7d8e4c Pin SHA256: bb+uANN7nNc/j7R95IkXrwDg3d9C286slMF8AnXulJU=
Valid until	Fri, 27 Nov 2026 20:53:42 UTC (expires in 7 years and 9 months)
Key	RSA 2048 bits (e 65537)
Issuer	Entrust Root Certification Authority Self-signed
Signature algorithm	SHA1withRSA Weak, but no impact on root certificate



## Certification Paths

[Click here to expand](#)

## 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 only support RFC 8446.



## Cipher Suites

# TLS 1.2 (suites in server-preferred order)	
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	ECDH secp256r1 (eq. 3072 bits RSA) FS 128
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	ECDH secp256r1 (eq. 3072 bits RSA) FS 128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	ECDH secp256r1 (eq. 3072 bits RSA) FS 256
# TLS 1.1 (suites in server-preferred order)	
# TLS 1.0 (suites in server-preferred order)	



## Handshake Simulation

<a href="#">Android 2.3.7</a> No SNI <sup>2</sup>	Server sent fatal alert: handshake_failure
<a href="#">Android 4.0.4</a>	RSA 2048 (SHA256) TLS 1.0 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
<a href="#">Android 4.1.1</a>	RSA 2048 (SHA256) TLS 1.0 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
<a href="#">Android 4.2.2</a>	RSA 2048 (SHA256) TLS 1.0 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
<a href="#">Android 4.3</a>	RSA 2048 (SHA256) TLS 1.0 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
<a href="#">Android 4.4.2</a>	RSA 2048 (SHA256) TLS 1.2 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
<a href="#">Android 5.0.0</a>	RSA 2048 (SHA256) TLS 1.2 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
<a href="#">Android 6.0</a>	RSA 2048 (SHA256) TLS 1.2 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
<a href="#">Android 7.0</a>	RSA 2048 (SHA256) TLS 1.2 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
<a href="#">Baidu Jan 2015</a>	RSA 2048 (SHA256) TLS 1.0 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS

## Handshake Simulation

<a href="#">BingPreview Jan 2015</a>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">Chrome 49 / XP SP3</a>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">Chrome 69 / Win 7</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">Chrome 70 / Win 10</a>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">Firefox 31.3.0 ESR / Win 7</a>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">Firefox 47 / Win 7</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">Firefox 49 / XP SP3</a>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">Firefox 62 / Win 7</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">Googlebot Feb 2018</a>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">IE 7 / Vista</a>	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp256r1	FS
<a href="#">IE 8 / XP</a> No FS <sup>1</sup> No SNI <sup>2</sup>	Server sent fatal alert: handshake_failure				
<a href="#">IE 8-10 / Win 7</a> R	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp256r1	FS
<a href="#">IE 11 / Win 7</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp256r1	FS
<a href="#">IE 11 / Win 8.1</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp256r1	FS
<a href="#">IE 10 / Win Phone 8.0</a>	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp256r1	FS
<a href="#">IE 11 / Win Phone 8.1</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp256r1	FS
<a href="#">IE 11 / Win Phone 8.1 Update</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp256r1	FS
<a href="#">IE 11 / Win 10</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">Edge 15 / Win 10</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">Edge 13 / Win Phone 10</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">Java 6u45</a> No SNI <sup>2</sup>	Server sent fatal alert: handshake_failure				
<a href="#">Java 7u25</a>	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp256r1	FS
<a href="#">Java 8u161</a>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">OpenSSL 0.9.8y</a>	Server sent fatal alert: handshake_failure				
<a href="#">OpenSSL 1.0.1l</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">OpenSSL 1.0.2e</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">Safari 5.1.9 / OS X 10.6.8</a>	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp256r1	FS
<a href="#">Safari 6 / iOS 6.0.1</a>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp256r1	FS
<a href="#">Safari 6.0.4 / OS X 10.8.4</a> R	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp256r1	FS
<a href="#">Safari 7 / iOS 7.1</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp256r1	FS
<a href="#">Safari 7 / OS X 10.9</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp256r1	FS
<a href="#">Safari 8 / iOS 8.4</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp256r1	FS
<a href="#">Safari 8 / OS X 10.10</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp256r1	FS
<a href="#">Safari 9 / iOS 9</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">Safari 9 / OS X 10.11</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">Safari 10 / iOS 10</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">Safari 10 / OS X 10.12</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">Apple ATS 9 / iOS 9</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">Yahoo Slurp Jan 2015</a>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">YandexBot Jan 2015</a>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS

### # Not simulated clients (Protocol mismatch)

[IE 6 / XP](#) No FS<sup>1</sup> No SNI<sup>2</sup> 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

	No, server keys and hostname not seen elsewhere with SSLv2
DROWN	(1) For a better understanding of this test, please read <a href="#">this longer explanation</a> (2) Key usage data kindly provided by the <a href="#">Censys</a> network search engine; original DROWN website <a href="#">here</a> (3) Censys data is only indicative of possible key and certificate reuse; possibly out-of-date and not complete
BEAST attack	No mitigated server-side ( <a href="#">more info</a> ) TLS 1.0: 0xc013
POODLE (SSLv3)	No, SSL 3 not supported ( <a href="#">more info</a> )
POODLE (TLS)	No ( <a href="#">more info</a> )
Downgrade attack prevention	Yes, TLS_FALLBACK_SCSV supported ( <a href="#">more info</a> )
SSL/TLS compression	No

## Protocol Details

RC4	No
Heartbeat (extension)	No
Heartbleed (vulnerability)	No ( <a href="#">more info</a> )
Ticketbleed (vulnerability)	No ( <a href="#">more info</a> )
OpenSSL CCS vuln. (CVE-2014-0224)	No ( <a href="#">more info</a> )
OpenSSL Padding Oracle vuln. (CVE-2016-2107)	No ( <a href="#">more info</a> )
ROBOT (vulnerability)	No ( <a href="#">more info</a> )
<b>Forward Secrecy</b>	<b>Yes (with most browsers) ROBUST</b> ( <a href="#">more info</a> )
ALPN	No
NPN	No
Session resumption (caching)	Yes
Session resumption (tickets)	No
OCSP stapling	No
<b>Strict Transport Security (HSTS)</b>	<b>Invalid</b> Server provided more than one HSTS header
HSTS Preloading	Not in: Chrome Edge Firefox IE
Public Key Pinning (HPKP)	No ( <a href="#">more info</a> )
Public Key Pinning Report-Only	No
Public Key Pinning (Static)	No ( <a href="#">more info</a> )
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
<b>ECDH public server param reuse</b>	<b>Yes</b>
Supported Named Groups	secp256r1, secp384r1 (server preferred order)
SSL 2 handshake compatibility	Yes



## HTTP Requests



- 1 <https://ind.millenniumbcp.pt/> (HTTP/1.1 302 Redirect)
- 2 <https://ind.millenniumbcp.pt/Pages/VariationsRoot.aspx> (HTTP/1.1 302 Found)
- 3 <https://ind.millenniumbcp.pt/pt/particulares/> (HTTP/1.1 302 Redirect)
- 4 <https://ind.millenniumbcp.pt/pt/particulares/Pages/Welcome.aspx> (HTTP/1.1 200 OK)



## Miscellaneous

Test date	Mon, 25 Feb 2019 10:46:21 UTC
Test duration	88.975 seconds
HTTP status code	200
HTTP server signature	Microsoft-IIS/7.5
Server hostname	-