SSL Report: egov.comune.cefalu.pa.it (156.54.128.60)

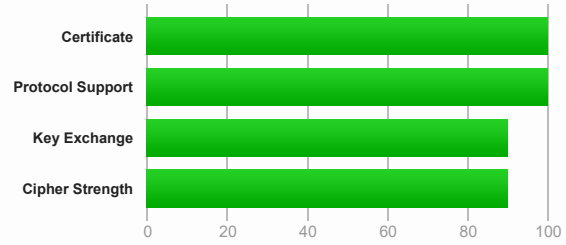
Assessed on: Wed, 22 Dec 2021 11:21:14 UTC | **HIDDEN** | Clear cache

Scan Another »

Summary

Overall Rating

A



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

This site works only in browsers with SNI support.

Certificate #1: RSA 2048 bits (SHA256withRSA)

Server Key and Certificate #1

Subject	egov.comune.cefalu.pa.it Fingerprint SHA256: 3d37ea80c1e1c16e4e1993f6a692576ebd0d93f4992c426cb08c07ec18a74298 Pin SHA256: lzyQmitJS/bLqUD96nDXc14H+j7I01I9Apx+jz3gBsI=
Common names	egov.comune.cefalu.pa.it
Alternative names	egov.comune.cefalu.pa.it www.egov.comune.cefalu.pa.it
Serial Number	4af29fd4ca2023c2979295001e10ccea
Valid from	Thu, 25 Feb 2021 00:00:00 UTC
Valid until	Sun, 27 Mar 2022 23:59:59 UTC (expires in 3 months and 5 days)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	Trustico RSA DV CA AIA: http://crt.comodoca.com/TrusticoRSADVCA.crt
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	Yes (certificate)
OCSP Must Staple	No
Revocation information	CRL, OCSP CRL: http://crl.comodoca.com/TrusticoRSADVCA.crl OCSP: http://ocsp.comodoca.com
Revocation status	Good (not revoked)
DNS CAA	No (more info)
Trusted	Yes Mozilla Apple Android Java Windows

Additional Certificates (if supplied)

Certificates provided	3 (4439 bytes)
Chain issues	Incorrect order

#2

Additional Certificates (if supplied)

Subject	COMODO RSA Certification Authority Fingerprint SHA256: 38392f17ce7b682c198d29c6e71d2740964a2074c8d2558e6cff64c27823f129 Pin SHA256: grX4Ta9HpZx6tSHkmCrvpApTQGo67CYDnvprLg5yRME=
Valid until	Sun, 31 Dec 2028 23:59:59 UTC (expires in 7 years)
Key	RSA 4096 bits (e 65537)
Issuer	AAA Certificate Services
Signature algorithm	SHA384withRSA

#3

Subject	Trustico RSA DV CA Fingerprint SHA256: 33cfb062cd2951e4dd1a256bed156bea53f290d039deefb85be95e1901216a36 Pin SHA256: B/bkhTDI5DJw6nXXzz0RfEQettWUxxESQlnc8VMZ4uk=
Valid until	Wed, 08 Sep 2027 23:59:59 UTC (expires in 5 years and 8 months)
Key	RSA 2048 bits (e 65537)
Issuer	COMODO RSA Certification Authority
Signature algorithm	SHA384withRSA

Certification Paths

Click here to expand

Certificate #2: RSA 1024 bits (MD5withRSA) No SNI

Click here to expand

Configuration

Protocols

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

(*) Experimental: Server negotiated using No-SNI

Cipher Suites

TLS 1.2 (server has no preference)

TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e) DH 2048 bits FS	128
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) ECDH sect571r1 (eq. 15360 bits RSA) FS	128
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f) DH 2048 bits FS	256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) ECDH sect571r1 (eq. 15360 bits RSA) FS	256

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_128_GCM_SHA256	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

Handshake Simulation

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
Chrome 70 / Win 10	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
IE 11 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	DH 2048 FS
IE 11 / Win 8.1 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	DH 2048 FS
IE 11 / Win Phone 8.1 R	Server sent fatal alert: handshake_failure			
IE 11 / Win Phone 8.1 Update R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	DH 2048 FS
IE 11 / Win 10 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
Java 8u161	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_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
Java 12.0.1	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
OpenSSL 1.0.1l 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
Safari 6 / iOS 6.0.1	Server sent fatal alert: handshake_failure			
Safari 7 / iOS 7.1 R	Server sent fatal alert: handshake_failure			
Safari 7 / OS X 10.9 R	Server sent fatal alert: handshake_failure			
Safari 8 / iOS 8.4 R	Server sent fatal alert: handshake_failure			
Safari 8 / OS X 10.10 R	Server sent fatal alert: handshake_failure			
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
Safari 9 / OS X 10.11 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
Safari 12.1.2 / MacOS 10.14.6 Beta R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
Safari 12.1.1 / iOS 12.3.1 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
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) 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

DROWN

IP Address	Port	Export	Special	Status
156.54.128.60	443	Yes	Yes	Not checked (same host)
93.64.233.58	443	Yes	Yes	Not vulnerable

Protocol Details

217.58.210.107	443	Yes	Yes	Not vulnerable
2.118.200.203	443	Yes	Yes	Not vulnerable
85.18.241.211	443	Yes	Yes	Not vulnerable
95.231.104.3	443	Yes	Yes	Not vulnerable
185.56.8.65	443	Yes	Yes	Not vulnerable
212.46.67.82	443	Yes	Yes	Not vulnerable
82.187.255.203	443	Yes	Yes	Not vulnerable
156.54.128.61	443	Yes	Yes	Not vulnerable
82.59.56.50	443	Yes	Yes	Not vulnerable
80.23.240.139	443	Yes	Yes	Not vulnerable
93.64.240.182	443	Yes	Yes	Not vulnerable
82.104.148.19	443	Yes	Yes	Not vulnerable
93.94.95.34	443	Yes	Yes	Not vulnerable
156.54.128.66	443	Yes	Yes	Not vulnerable
156.54.128.64	443	Yes	Yes	Not vulnerable
88.49.235.210	443	Yes	Yes	Not vulnerable
5.98.195.181	443	Yes	Yes	Not vulnerable
178.211.69.178	443	Yes	Yes	Not vulnerable
156.54.128.59	443	Yes	Yes	Not vulnerable
195.78.209.3	443	Yes	Yes	Not vulnerable
80.88.89.218	443	Yes	Yes	Not vulnerable
83.149.158.7	443	Yes	Yes	Not vulnerable
95.110.168.252	443	Yes	Yes	Not vulnerable
82.91.182.236	443	Yes	Yes	Not vulnerable
80.21.214.156	443	Yes	Yes	Not checked
109.239.253.227	443	Yes	Yes	Not checked
156.54.128.62	443	Yes	Yes	Not checked
46.44.235.70	443	Yes	Yes	Not checked
94.82.124.241	443	Yes	Yes	Not checked
95.110.187.153	443	Yes	Yes	Not checked
188.13.51.9	443	Yes	Yes	Not checked
109.239.250.2	443	Yes	Yes	Not checked
156.54.128.63	443	Yes	Yes	Not checked
95.110.168.111	443	Yes	Yes	Not checked
37.206.183.22	443	Yes	Yes	Not checked
83.211.17.52	443	No	No	Not checked
109.73.181.92	443	Yes	Yes	Not checked
79.59.36.211	443	Yes	Yes	Not checked
94.138.188.128	443	Yes	Yes	Not checked
37.206.203.122	443	Yes	Yes	Not checked
93.64.205.149	443	Yes	Yes	Not checked
87.23.249.90	443	Yes	Yes	Not checked
5.158.71.86	443	Yes	Yes	Not checked
82.143.32.18	443	Yes	Yes	Not checked
88.59.143.251	443	Yes	Yes	Not checked
88.37.153.26	443	Yes	Yes	Not checked
93.63.239.11	443	Yes	Yes	Not checked
188.95.77.123	443	Yes	Yes	Not checked
37.186.221.108	443	Yes	Yes	Not checked
95.231.157.145	443	Yes	Yes	Not checked
62.94.56.54	443	Yes	Yes	Not checked
195.31.193.11	443	Yes	Yes	Not checked
94.83.163.187	443	Yes	Yes	Not checked
217.141.144.35	443	Yes	Yes	Not checked
178.248.146.80	443	Yes	Yes	Not checked
46.228.248.25	443	Yes	Yes	Not checked
95.110.168.247	443	Yes	Yes	Not checked
93.88.107.35	443	Yes	Yes	Not checked
156.54.128.58	443	Yes	Yes	Not checked
213.26.146.100	443	Yes	Yes	Not checked
94.91.164.130	443	Yes	Yes	Not checked
85.45.210.93	443	Yes	Yes	Not checked
85.39.205.206	443	Yes	Yes	Not checked
81.117.231.5	443	Yes	Yes	Not checked
85.33.200.140	443	Yes	Yes	Not checked
2.118.192.163	443	Yes	Yes	Not checked
195.78.209.8	443	Yes	Yes	Not checked
82.143.39.64	443	Yes	Yes	Not checked
88.45.122.78	443	Yes	Yes	Not checked
109.71.237.13	443	Yes	Yes	Not checked
217.59.157.198	443	Yes	Yes	Not checked
85.39.36.18	443	Yes	Yes	Not checked
212.46.65.44	443	Yes	Yes	Not checked
185.56.8.32	443	Yes	Yes	Not checked
151.0.199.26	443	Yes	Yes	Not checked
195.45.77.22	443	Yes	Yes	Not checked
95.231.157.138	443	Yes	Yes	Not checked

Protocol Details

	83.211.61.22	443	Yes	Yes	Not checked
	178.20.39.146	443	Yes	Yes	Not checked
	195.45.77.19	443	Yes	Yes	Not checked
	85.37.183.20	443	Yes	Yes	Not checked
	88.56.122.195	443	Yes	Yes	Not checked
	194.243.188.43	443	Yes	Yes	Not checked
	62.94.5.150	443	Yes	Yes	Not checked
	85.44.206.197	443	Yes	Yes	Not checked
	95.253.240.174	443	Yes	Yes	Not checked
	213.82.107.163	443	Yes	Yes	Not checked
	212.78.1.85	443	Yes	Yes	Not checked
	194.243.217.18	443	Yes	Yes	Not checked
	46.44.235.66	443	Yes	Yes	Not checked
	88.49.7.180	443	Yes	Yes	Not checked
	37.186.221.115	443	Yes	Yes	Not checked
	217.59.152.61	443	Yes	Yes	Not checked
	87.22.73.1	443	Yes	Yes	Not checked

(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 incomplete
(4) We perform real-time key reuse checks, but stop checking after first confirmed vulnerability
(5) The "Special" column indicates vulnerable OpenSSL version; "Export" refers to export cipher suites

INTERNAL ERROR: Too many hosts to check all

Secure Renegotiation	**Supported**
Secure Client-Initiated Renegotiation	No
Insecure Client-Initiated Renegotiation	No
BEAST attack	Mitigated server-side (more info)
POODLE (SSLv3)	No, SSL 3 not supported (more info)
POODLE (TLS)	No (more info)
Zombie POODLE	No (more info)
GOLDENDOODLE	No (more info)
OpenSSL 0-Length	No (more info)
Sleeping POODLE	No (more info)
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)	No (more info)
ROBOT (vulnerability)	No (more info)
Forward Secrecy	**Yes (with most browsers) ROBUST** (more info)
ALPN	Yes http/1.1
NPN	No
Session resumption (caching)	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 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
DH public server param (Ys) reuse	No
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)

Protocol Details

SSL 2 handshake compatibility	Yes

HTTP Requests

1 **https://egov.comune.cefalu.pa.it/** (HTTP/1.1 302 Found)

2 **https://egov.comune.cefalu.pa.it/hh/index.php?jvs=0&acc=1** (HTTP/1.1 200 OK)

Miscellaneous

Test date	Wed, 22 Dec 2021 11:16:45 UTC
Test duration	269.455 seconds
HTTP status code	200
HTTP server signature	Apache/2.4.23 (Unix) OpenSSL/1.0.2k PHP/5.6.31
Server hostname	-

SSL Report v2.1.8

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

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