Zeitgemäße Webserver-Konfiguration

Ein Serviervorschlag

Protokolle

HTTP

Seit 1991

TLS 1.0

1999

TLS 1.1

2006

TLS 1.2

2008

HTTP/S

SPDY

2009

HTTP/2

2012 .. 2015

HTTP/2

2012 .. 2015

Motivation

2016

Szenarien

Status Quo

SSLLabs

https://www.ssllabs.com/

QUALYS® SSL LABS
Home
Projects
Qualys.com
Contact

You are here: Home > Projects > SSL Server Test

SSL Server Test

This free online service performs a deep analysis of the configuration of any SSL web server on the public Internet. **Please note that the information you submit here is used only to provide you the service. We don't use the domain names or the test results, and we never will.**

Hostname: cert.at

Submit

□ Do not show the results on the boards

Recently Seen

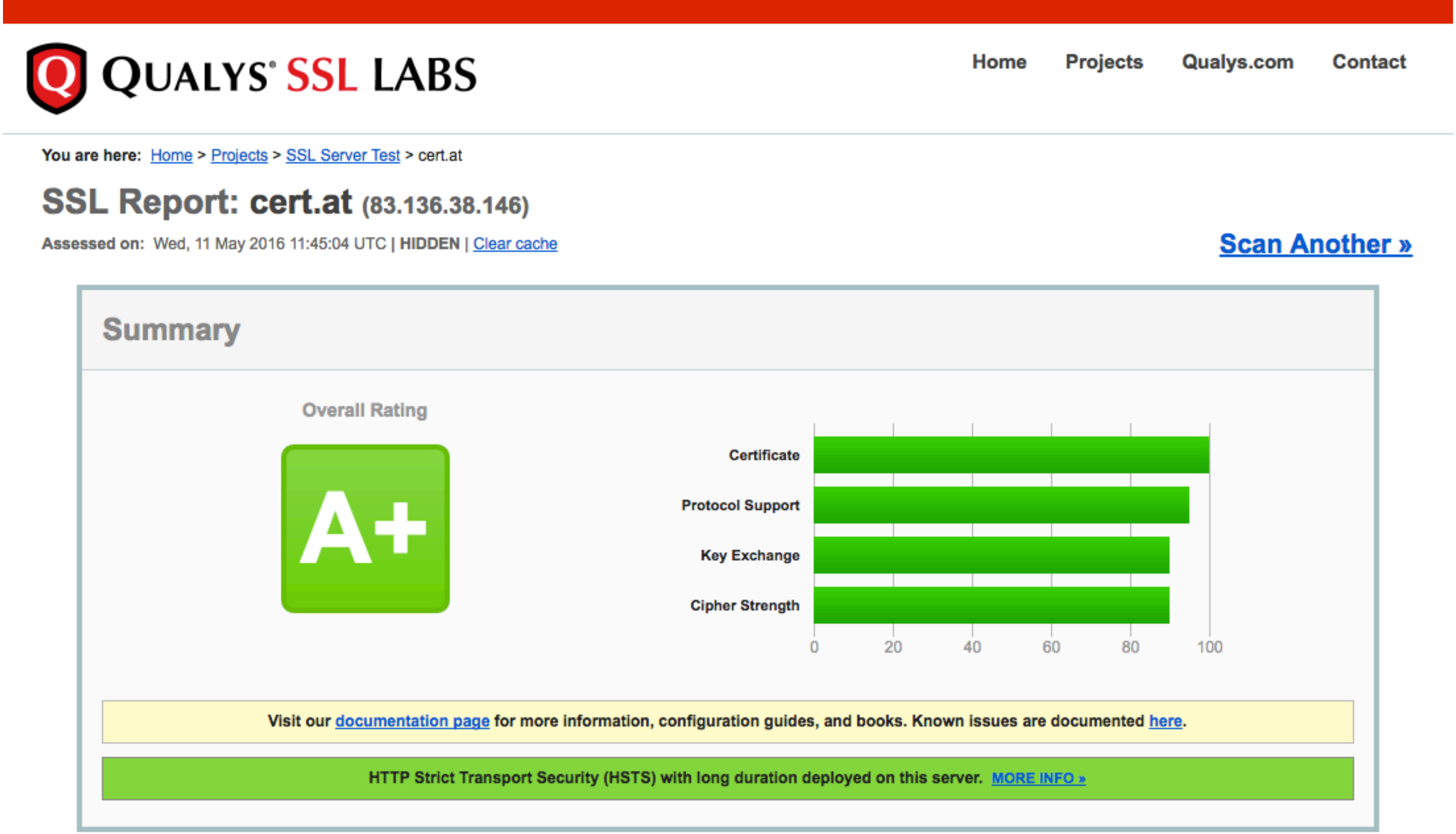
www.covenantwebsitedesign.co ...	
sa-receiver.sematext.com	
drentsmuseum.nl	
qa.compliancehr.com	
microsoftonline.com	
www.hnly88885720.com	Err
ra2.dnow.com	

Recent Best

bportal.zmr.register.gv.at	A+
email.freenet.de	A+
testservices.cb-logistics.nl	A
capi-demo.voxco.com	A
clientapps.compliancehr.com	A
exegetes.eu.org	A-
view.northcountry.org	B

Recent Worst

mail.uesdgq.edu.ec	T
desktop.amadeusri.com	F
www.scnsoft.com	F
sip.dnow.com	T
mail.sttar.ac.id	T
www.wus.cv.osb.overheid.nl	F
demoapi.ttpcenter.ru	T



You are here: Home > Projects > SSL Server Test > cert.at

SSL Report: cert.at (83.136.38.146)

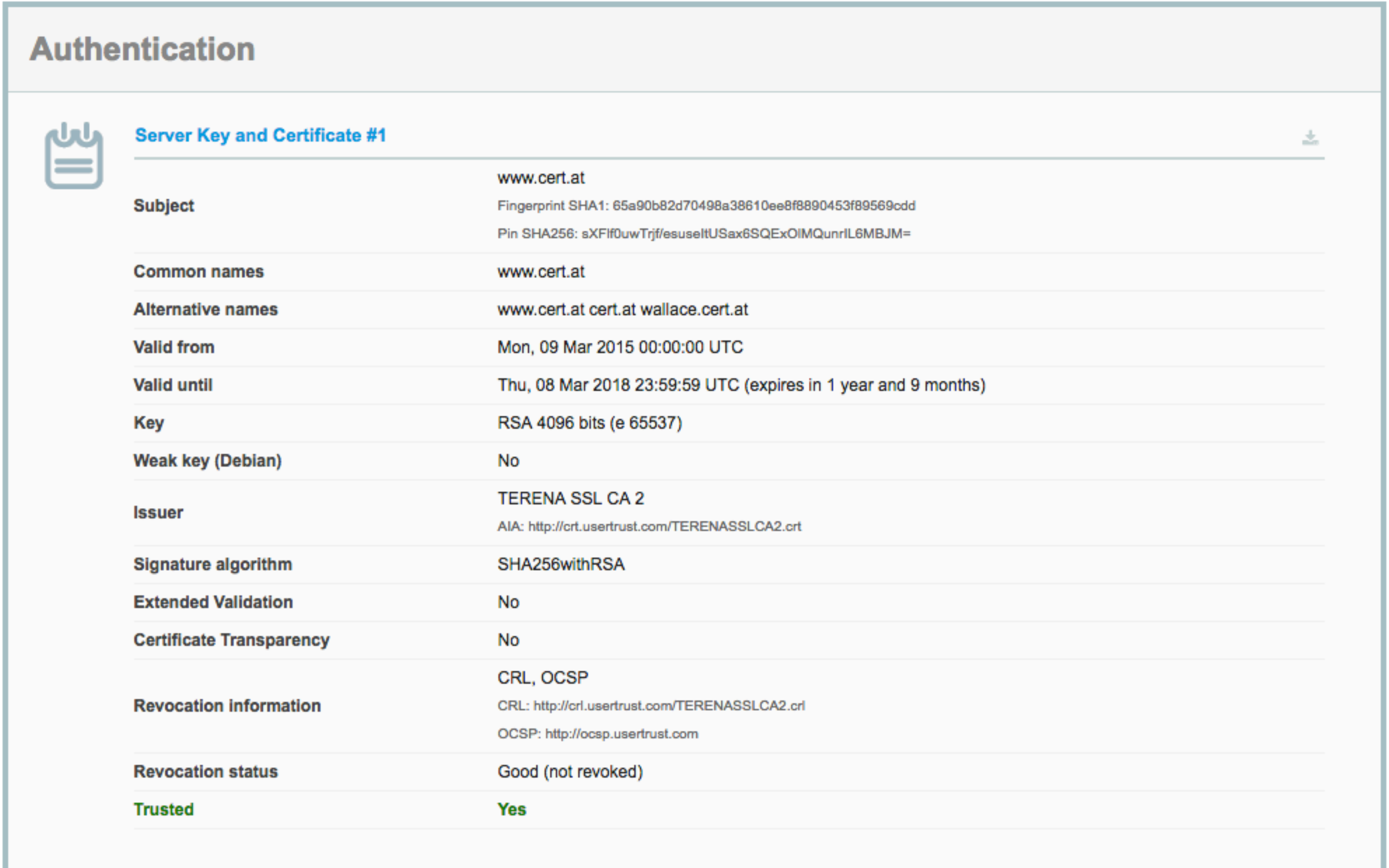
Assessed on: Wed, 11 May 2016 11:45:04 UTC | HIDDEN | Clear cache

Summary

Overall Rating

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

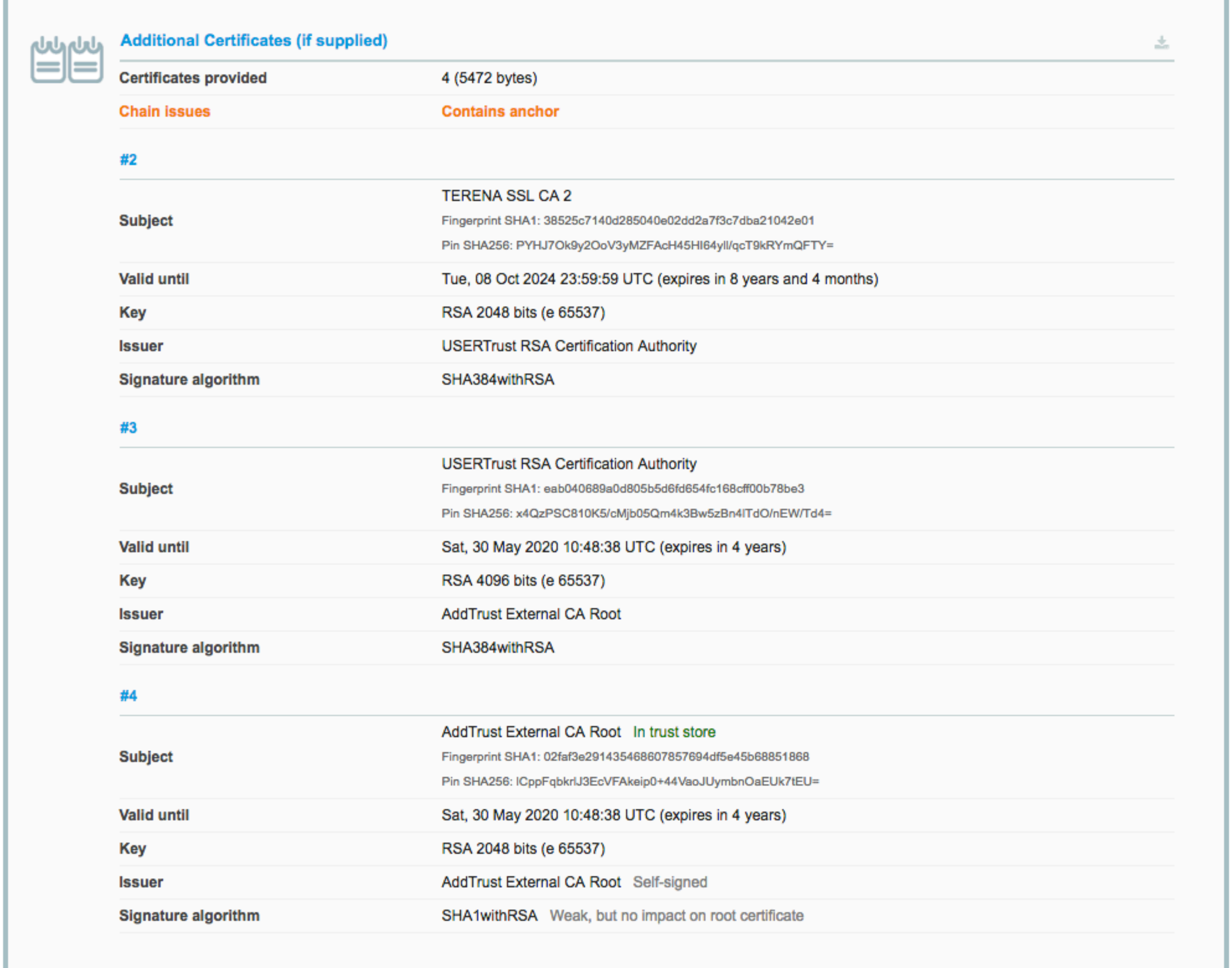
HTTP Strict Transport Security (HSTS) with long duration deployed on this server. MORE INFO »



Authentication

Server Key and Certificate #1

Subject	www.cert.at Fingerprint SHA1: 65a90b82d70498a38610ee8f8890453f89569cdd Pin SHA256: sXFlf0uwTrjf/esuseltUSax6SQExOIMQunrIL6MBJM=
Common names	www.cert.at
Alternative names	www.cert.at cert.at wallace.cert.at
Valid from	Mon, 09 Mar 2015 00:00:00 UTC
Valid until	Thu, 08 Mar 2018 23:59:59 UTC (expires in 1 year and 9 months)
Key	RSA 4096 bits (e 65537)
Weak key (Debian)	No
Issuer	TERENA SSL CA 2 AIA: http://crt.usertrust.com/TERENASSLCA2.crt
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	No
Revocation information	CRL, OCSP CRL: http://crl.usertrust.com/TERENASSLCA2.crl OCSP: http://ocsp.usertrust.com
Revocation status	Good (not revoked)
Trusted	Yes



Additional Certificates (if supplied)

Certificates provided	4 (5472 bytes)
Chain issues	**Contains anchor**

#2

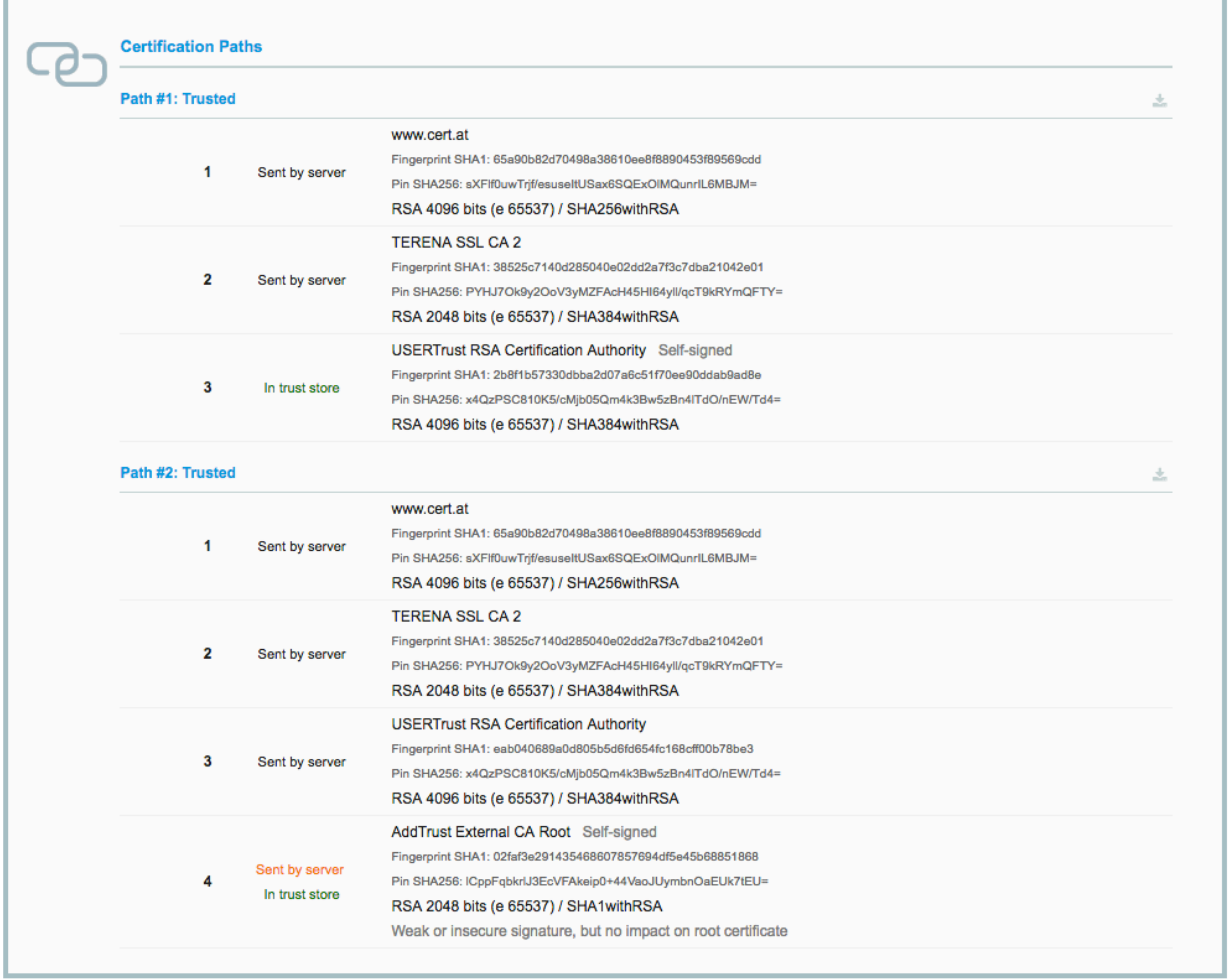
Subject	TERENA SSL CA 2 Fingerprint SHA1: 38525c7140d285040e02dd2a7f3c7dba21042e01 Pin SHA256: PYHJ7Ok9y2OoV3yMZFAcH45HI64yll/qcT9kRYmQFTY=
Valid until	Tue, 08 Oct 2024 23:59:59 UTC (expires in 8 years and 4 months)
Key	RSA 2048 bits (e 65537)
Issuer	USERTrust RSA Certification Authority
Signature algorithm	SHA384withRSA

#3

Subject	USERTrust RSA Certification Authority Fingerprint SHA1: eab040689a0d805b5d6fd654fc168cff00b78be3 Pin SHA256: x4QzPSC810K5/cMjb05Qm4k3Bw5zBn4lTdO/nEW/Td4=
Valid until	Sat, 30 May 2020 10:48:38 UTC (expires in 4 years)
Key	RSA 4096 bits (e 65537)
Issuer	AddTrust External CA Root
Signature algorithm	SHA384withRSA

#4

Subject	AddTrust External CA Root In trust store Fingerprint SHA1: 02faf3e291435468607857694df5e45b68851868 Pin SHA256: lCppFqbkrlJ3EcVFAkeip0+44VaoJUymbnOaEUk7tEU=
Valid until	Sat, 30 May 2020 10:48:38 UTC (expires in 4 years)
Key	RSA 2048 bits (e 65537)
Issuer	AddTrust External CA Root Self-signed
Signature algorithm	SHA1withRSA Weak, but no impact on root certificate



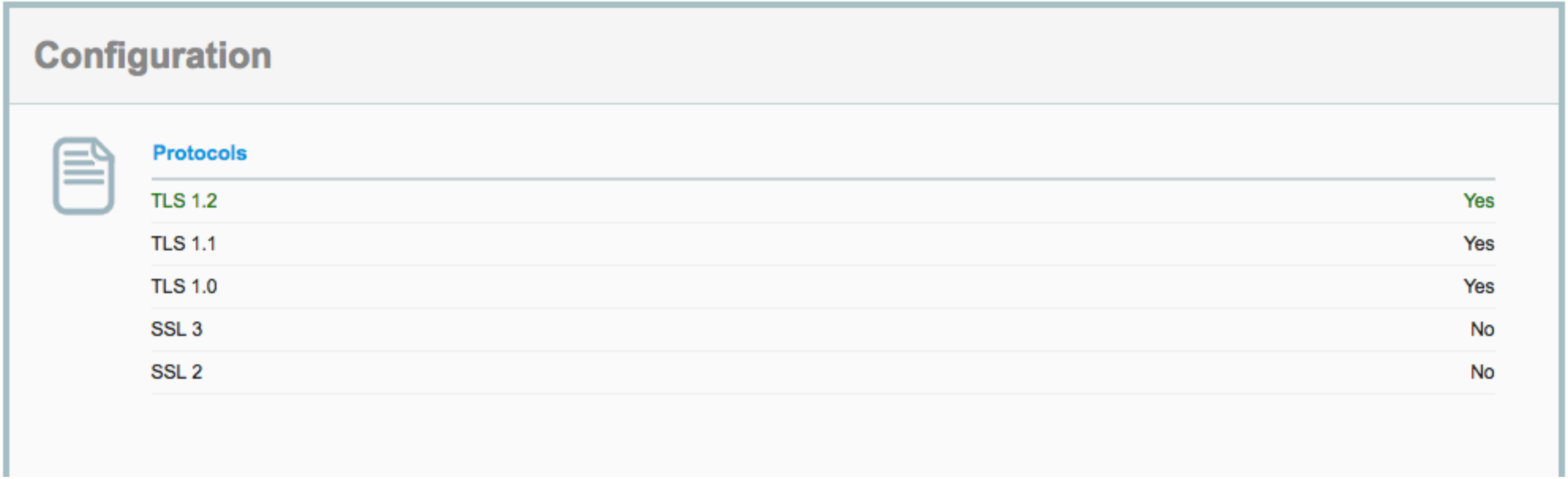
Certification Paths

Path #1: Trusted

1	Sent by server	www.cert.at Fingerprint SHA1: 65a90b82d70498a38610ee8f8890453f89569cdd Pin SHA256: sXFlf0uwTrjf/esuseltUSax6SQExOIMQunrIL6MBJM= RSA 4096 bits (e 65537) / SHA256withRSA
2	Sent by server	TERENA SSL CA 2 Fingerprint SHA1: 38525c7140d285040e02dd2a7f3c7dba21042e01 Pin SHA256: PYHJ7Ok9y2OoV3yMZFAcH45HI64yll/qcT9kRYmQFTY= RSA 2048 bits (e 65537) / SHA384withRSA
3	In trust store	USERTrust RSA Certification Authority Self-signed Fingerprint SHA1: 2b8f1b57330dbba2d07a6c51f70ee90ddab9ad8e Pin SHA256: x4QzPSC810K5/cMjb05Qm4k3Bw5zBn4lTdO/nEW/Td4= RSA 4096 bits (e 65537) / SHA384withRSA

Path #2: Trusted

1	Sent by server	www.cert.at Fingerprint SHA1: 65a90b82d70498a38610ee8f8890453f89569cdd Pin SHA256: sXFlf0uwTrjf/esuseltUSax6SQExOIMQunrIL6MBJM= RSA 4096 bits (e 65537) / SHA256withRSA
2	Sent by server	TERENA SSL CA 2 Fingerprint SHA1: 38525c7140d285040e02dd2a7f3c7dba21042e01 Pin SHA256: PYHJ7Ok9y2OoV3yMZFAcH45HI64yll/qcT9kRYmQFTY= RSA 2048 bits (e 65537) / SHA384withRSA
3	Sent by server	USERTrust RSA Certification Authority Fingerprint SHA1: eab040689a0d805b5d6fd654fc168cff00b78be3 Pin SHA256: x4QzPSC810K5/cMjb05Qm4k3Bw5zBn4lTdO/nEW/Td4= RSA 4096 bits (e 65537) / SHA384withRSA
4	Sent by server In trust store	AddTrust External CA Root Self-signed Fingerprint SHA1: 02faf3e291435468607857694df5e45b68851868 Pin SHA256: lCppFqbkrlJ3EcVFAkeip0+44VaoJUymbnOaEUk7tEU= 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

Die TLS Ampel

TLS 1.3

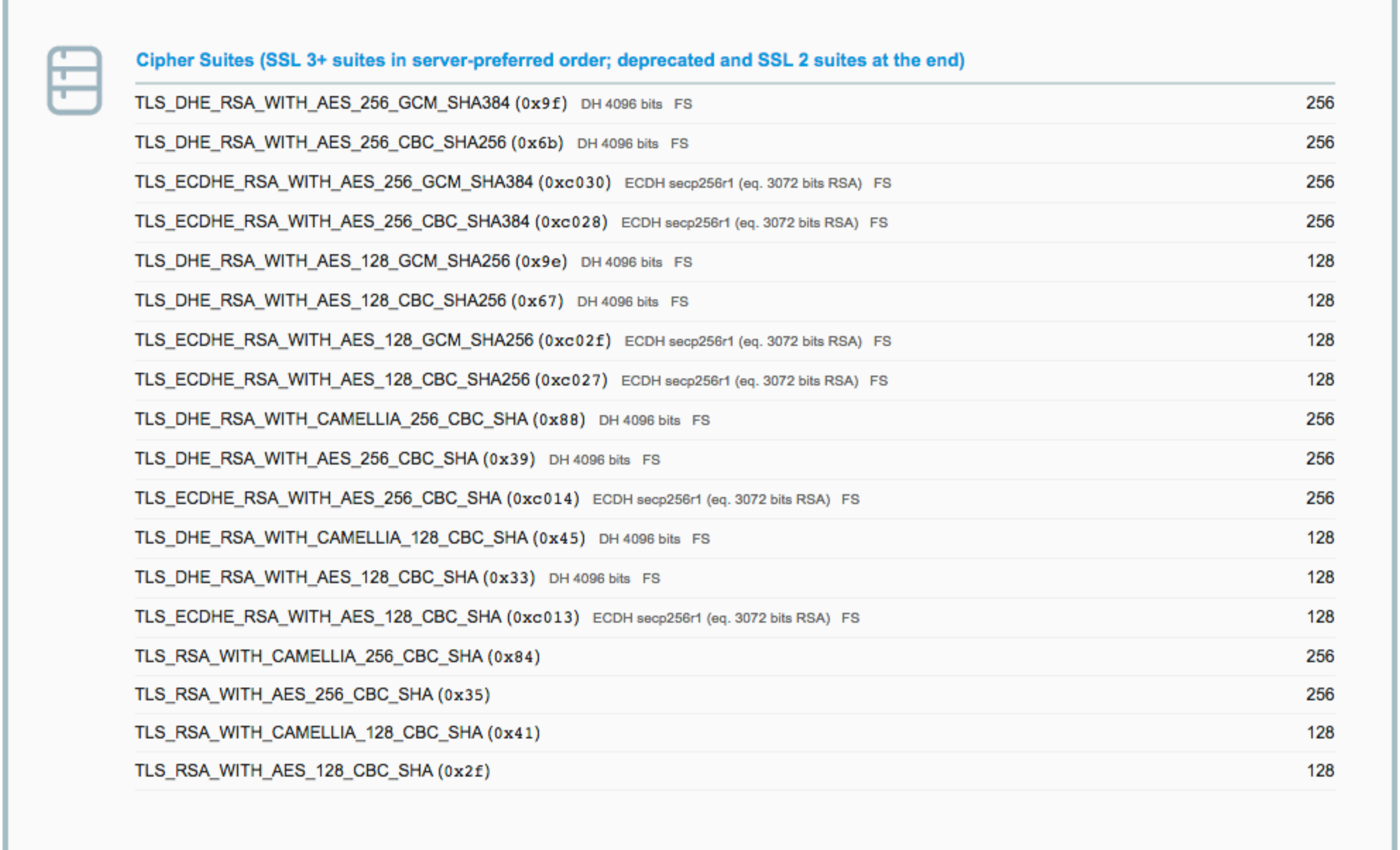
TLS 1.2

TLS 1.1

TLS 1.0

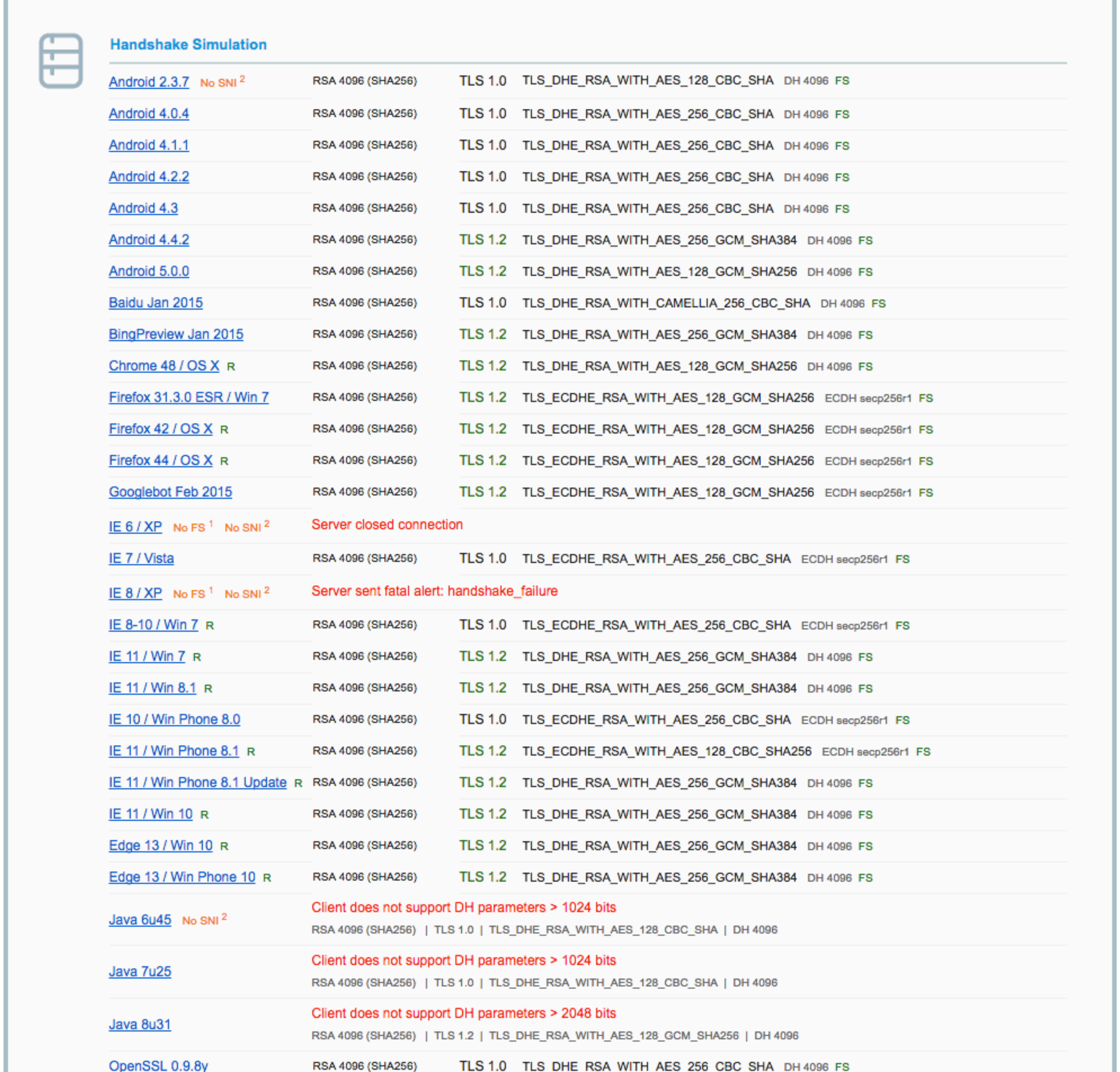
~~SSLv3~~

~~SSLv2~~



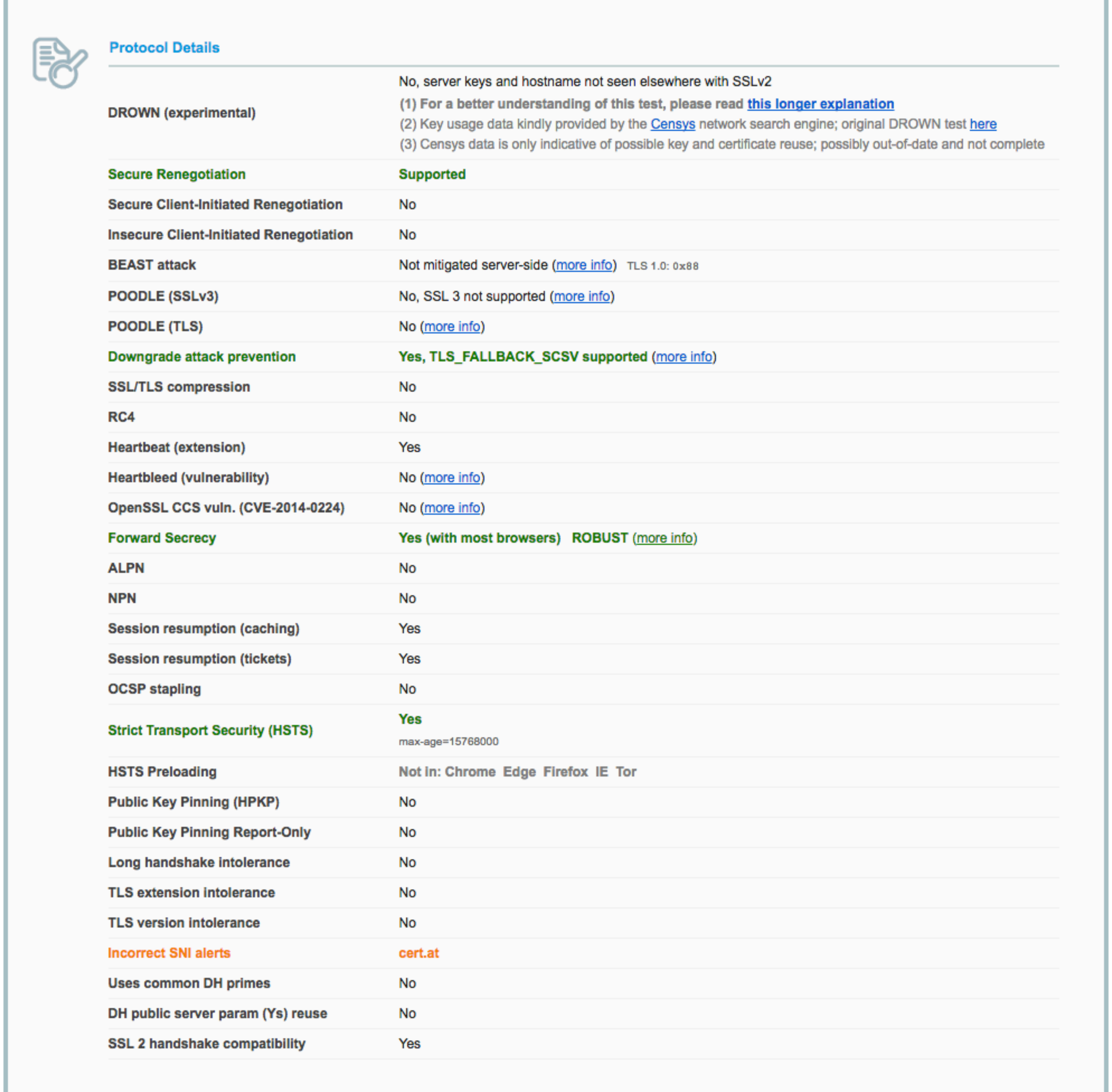
Cipher Suites (SSL 3+ suites in server-preferred order; deprecated and SSL 2 suites at the end)

TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f)	DH 4096 bits FS	256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x6b)	DH 4096 bits FS	256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	ECDH secp256r1 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)	ECDH secp256r1 (eq. 3072 bits RSA) FS	256
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e)	DH 4096 bits FS	128
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x67)	DH 4096 bits FS	128
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	ECDH secp256r1 (eq. 3072 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)	ECDH secp256r1 (eq. 3072 bits RSA) FS	128
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0x88)	DH 4096 bits FS	256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39)	DH 4096 bits FS	256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	ECDH secp256r1 (eq. 3072 bits RSA) FS	256
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (0x45)	DH 4096 bits FS	128
TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33)	DH 4096 bits FS	128
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	ECDH secp256r1 (eq. 3072 bits RSA) FS	128
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (0x84)		256
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)		256
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (0x41)		128
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)		128



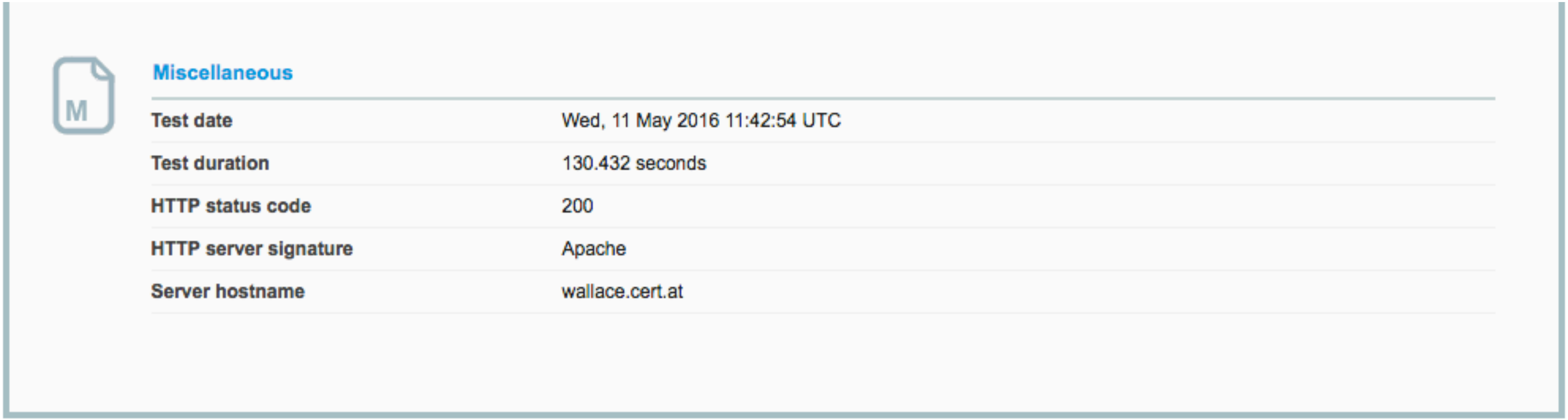
Handshake Simulation

Android 2.3.7 No SNI [2]	RSA 4096 (SHA256)	TLS 1.0	TLS_DHE_RSA_WITH_AES_128_CBC_SHA	DH 4096	FS
Android 4.0.4	RSA 4096 (SHA256)	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA	DH 4096	FS
Android 4.1.1	RSA 4096 (SHA256)	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA	DH 4096	FS
Android 4.2.2	RSA 4096 (SHA256)	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA	DH 4096	FS
Android 4.3	RSA 4096 (SHA256)	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA	DH 4096	FS
Android 4.4.2	RSA 4096 (SHA256)	TLS 1.2	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	DH 4096	FS
Android 5.0.0	RSA 4096 (SHA256)	TLS 1.2	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	DH 4096	FS
Baidu Jan 2015	RSA 4096 (SHA256)	TLS 1.0	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA	DH 4096	FS
BingPreview Jan 2015	RSA 4096 (SHA256)	TLS 1.2	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	DH 4096	FS
Chrome 48 / OS X R	RSA 4096 (SHA256)	TLS 1.2	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	DH 4096	FS
Firefox 31.3.0 ESR / Win 7	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Firefox 42 / OS X R	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Firefox 44 / OS X R	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Googlebot Feb 2015	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
IE 6 / XP No FS [1] No SNI [2]	Server closed connection				
IE 7 / Vista	RSA 4096 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1	FS
IE 8 / XP No FS [1] No SNI [2]	Server sent fatal alert: handshake_failure				
IE 8-10 / Win 7 R	RSA 4096 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1	FS
IE 11 / Win 7 R	RSA 4096 (SHA256)	TLS 1.2	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	DH 4096	FS
IE 11 / Win 8.1 R	RSA 4096 (SHA256)	TLS 1.2	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	DH 4096	FS
IE 10 / Win Phone 8.0	RSA 4096 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1	FS
IE 11 / Win Phone 8.1 R	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	ECDH secp256r1	FS
IE 11 / Win Phone 8.1 Update R	RSA 4096 (SHA256)	TLS 1.2	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	DH 4096	FS
IE 11 / Win 10 R	RSA 4096 (SHA256)	TLS 1.2	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	DH 4096	FS
Edge 13 / Win 10 R	RSA 4096 (SHA256)	TLS 1.2	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	DH 4096	FS
Edge 13 / Win Phone 10 R	RSA 4096 (SHA256)	TLS 1.2	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	DH 4096	FS
Java 6u45 No SNI [2]	Client does not support DH parameters > 1024 bits RSA 4096 (SHA256)	TLS 1.0	TLS_DHE_RSA_WITH_AES_128_CBC_SHA	DH 4096	
Java 7u25	Client does not support DH parameters > 1024 bits RSA 4096 (SHA256)	TLS 1.0	TLS_DHE_RSA_WITH_AES_128_CBC_SHA	DH 4096	
Java 8u31	Client does not support DH parameters > 2048 bits RSA 4096 (SHA256)	TLS 1.2	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	DH 4096	
OpenSSL 0.9.8y	RSA 4096 (SHA256)	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA	DH 4096	FS



Protocol Details

DROWN (experimental)	No, server keys and hostname not seen elsewhere with SSLv2 (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 test here (3) Censys data is only indicative of possible key and certificate reuse; possibly out-of-date and not complete
Secure Renegotiation	Supported
Secure Client-Initiated Renegotiation	No
Insecure Client-Initiated Renegotiation	No
BEAST attack	Not mitigated server-side (more info) TLS 1.0: 0x88
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)	Yes
Heartbleed (vulnerability)	No (more info)
OpenSSL CCS vuln. (CVE-2014-0224)	No (more info)
Forward Secrecy	Yes (with most browsers) ROBUST (more info)
ALPN	No
NPN	No
Session resumption (caching)	Yes
Session resumption (tickets)	Yes
OCSP stapling	No
Strict Transport Security (HSTS)	Yes max-age=15768000
HSTS Preloading	Not in: Chrome Edge Firefox IE Tor
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	cert.at
Uses common DH primes	No
DH public server param (Ys) reuse	No
SSL 2 handshake compatibility	Yes



Miscellaneous

Test date	Wed, 11 May 2016 11:42:54 UTC
Test duration	130.432 seconds
HTTP status code	200
HTTP server signature	Apache
Server hostname	wallace.cert.at

QUALYS® SSL LABS
Home
Projects
Qualys.com
Contact
Scan Another >>

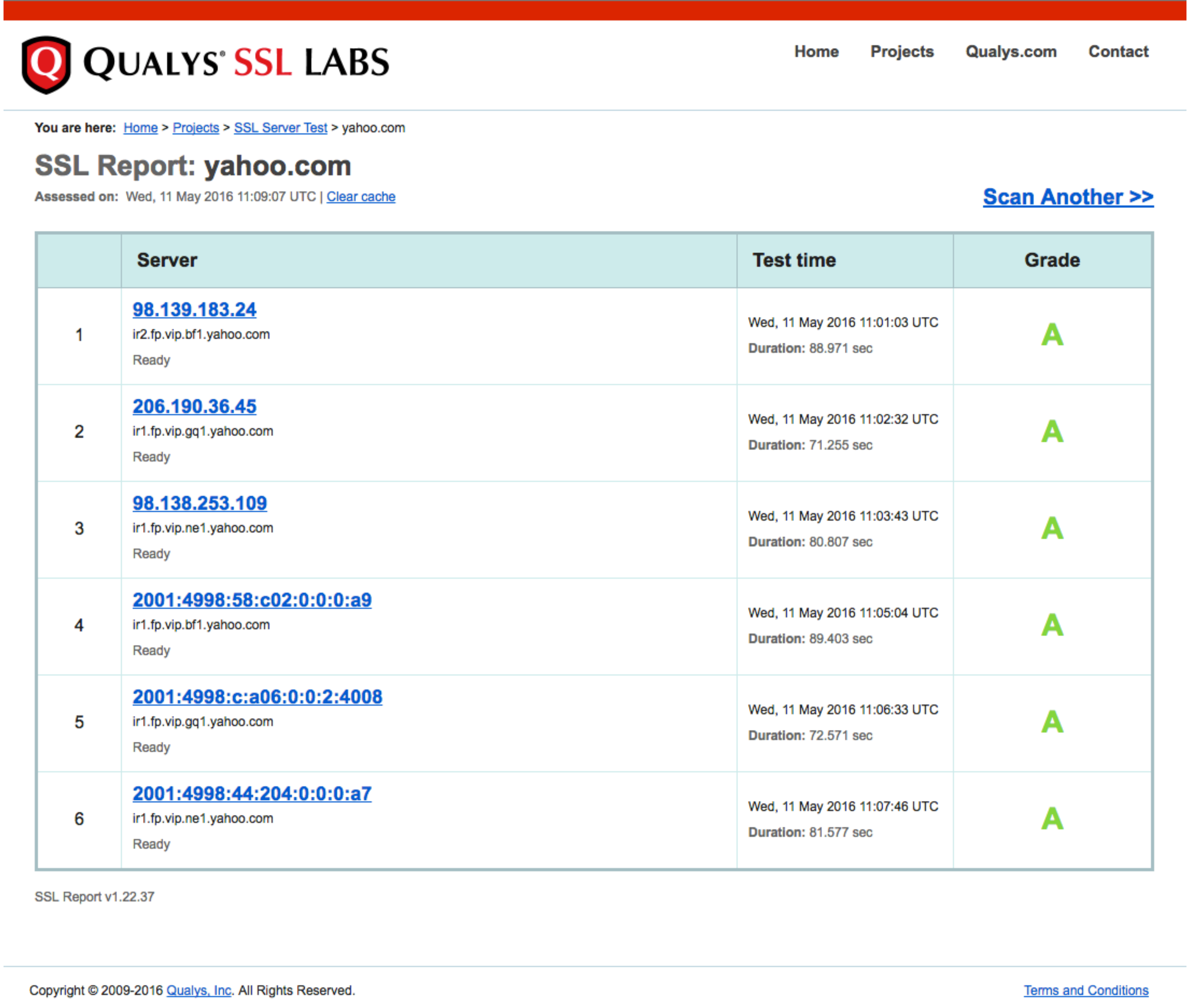
You are here: Home > Projects > SSL Server Test > maclemon.at

SSL Report: maclemon.at

Assessed on: Fri, 29 Apr 2016 15:50:24 UTC | **HIDDEN** | Clear cache

	Server	Test time	Grade
1	2001:470:6f:4ca:9a26:fb93:ba1c:e29a Ready	Fri, 29 Apr 2016 15:44:58 UTC **Duration:** 157.904 sec	A+
2	86.59.70.21 pandora.maclemon.at Ready	Fri, 29 Apr 2016 15:47:36 UTC **Duration:** 168.489 sec	A+

SSL Report v1.22.37



You are here: Home > Projects > SSL Server Test > yahoo.com

SSL Report: yahoo.com

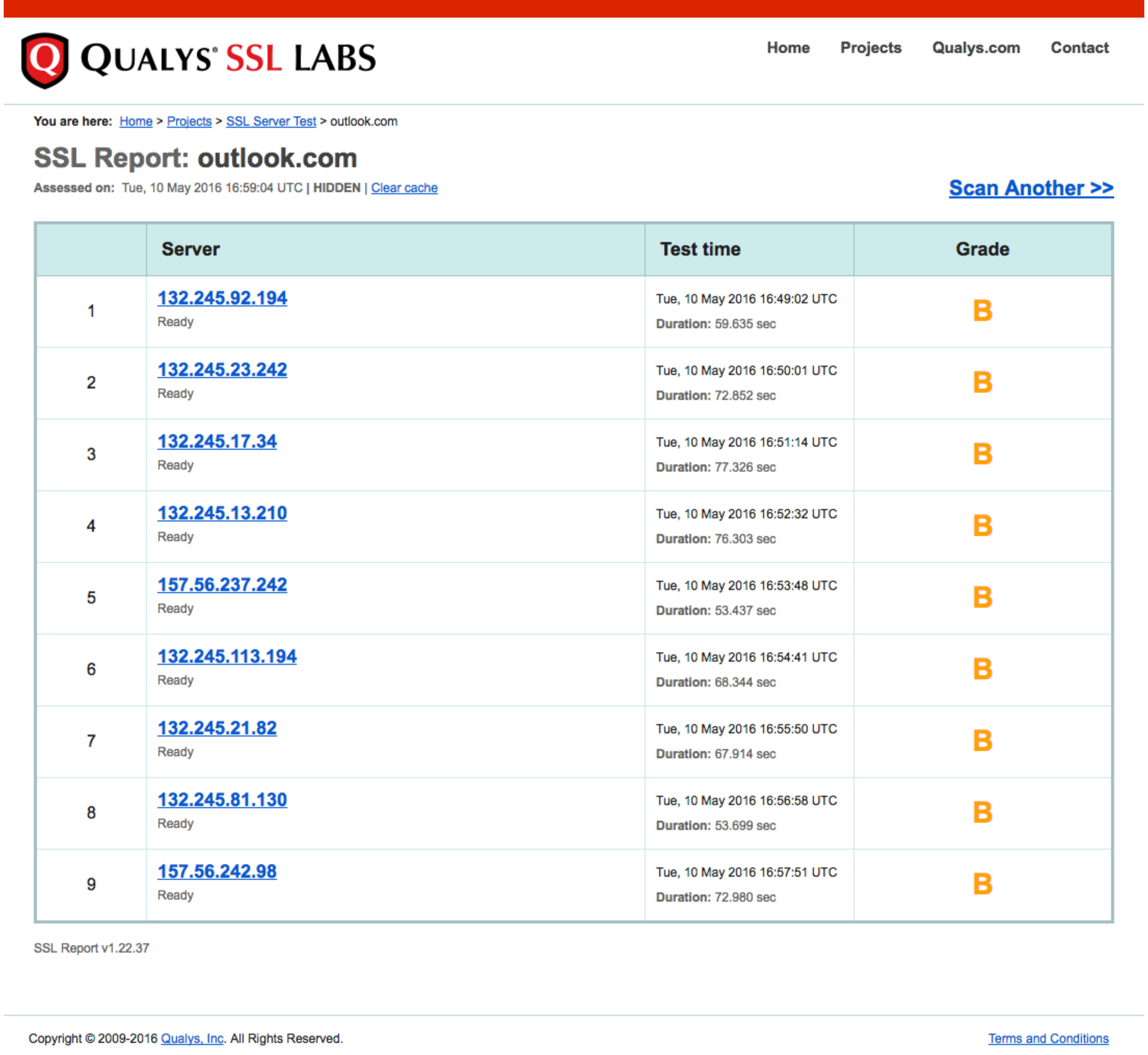
Assessed on: Wed, 11 May 2016 11:09:07 UTC | Clear cache

Scan Another >>

	Server	Test time	Grade
1	98.139.183.24 ir2.fp.vip.bf1.yahoo.com Ready	Wed, 11 May 2016 11:01:03 UTC **Duration:** 88.971 sec	A
2	206.190.36.45 ir1.fp.vip.gq1.yahoo.com Ready	Wed, 11 May 2016 11:02:32 UTC **Duration:** 71.255 sec	A
3	98.138.253.109 ir1.fp.vip.ne1.yahoo.com Ready	Wed, 11 May 2016 11:03:43 UTC **Duration:** 80.807 sec	A
4	2001:4998:58:c02:0:0:0:a9 ir1.fp.vip.bf1.yahoo.com Ready	Wed, 11 May 2016 11:05:04 UTC **Duration:** 89.403 sec	A
5	2001:4998:c:a06:0:0:2:4008 ir1.fp.vip.gq1.yahoo.com Ready	Wed, 11 May 2016 11:06:33 UTC **Duration:** 72.571 sec	A
6	2001:4998:44:204:0:0:0:a7 ir1.fp.vip.ne1.yahoo.com Ready	Wed, 11 May 2016 11:07:46 UTC **Duration:** 81.577 sec	A

SSL Report v1.22.37

Terms and Conditions



QUALYS® SSL LABS

Home Projects Qualys.com Contact

You are here: Home > Projects > SSL Server Test > outlook.com

SSL Report: outlook.com

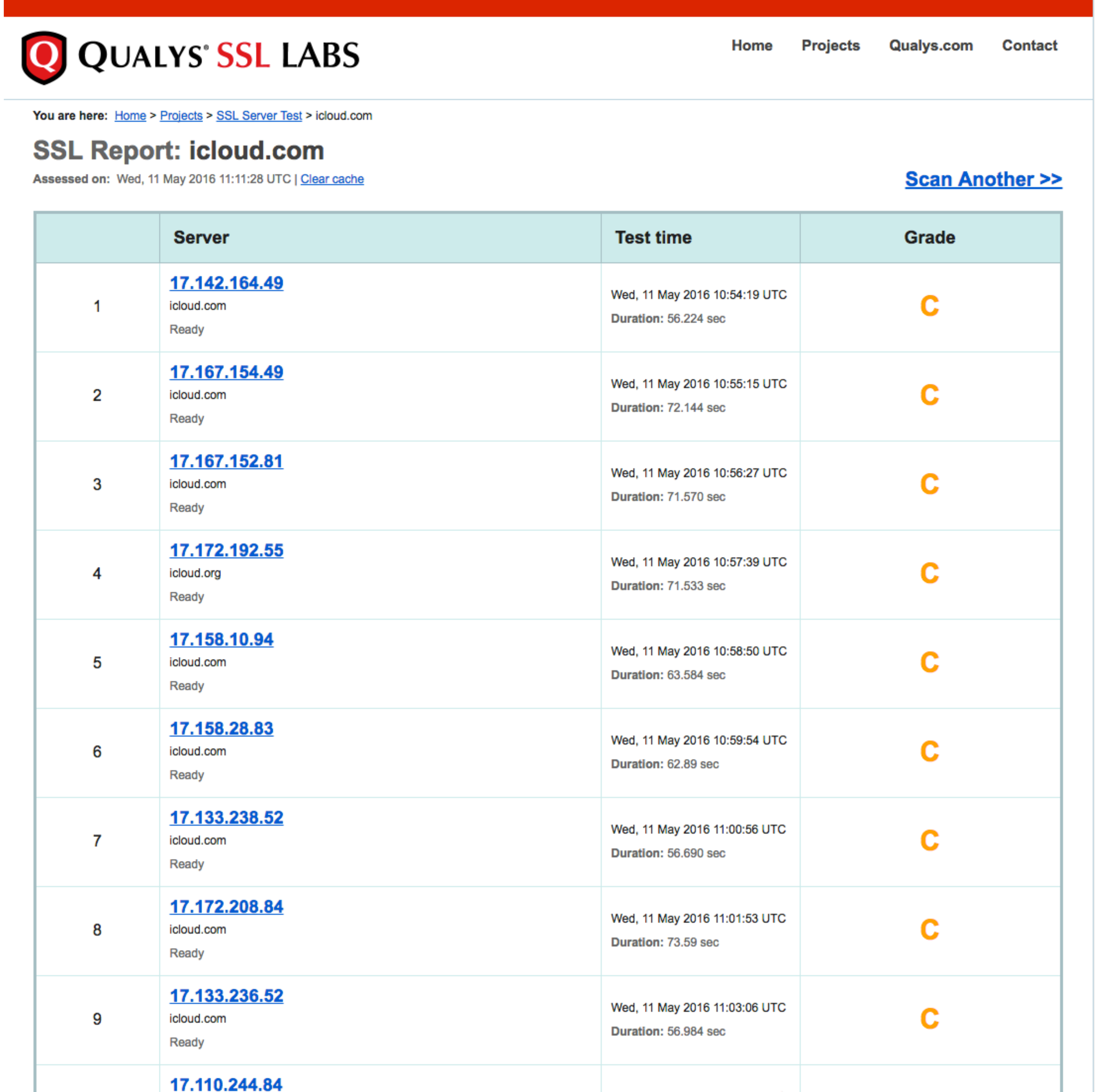
Assessed on: Tue, 10 May 2016 16:59:04 UTC | **HIDDEN** | Clear cache

Scan Another >>

	Server	Test time	Grade
1	132.245.92.194 Ready	Tue, 10 May 2016 16:49:02 UTC **Duration:** 59.635 sec	B
2	132.245.23.242 Ready	Tue, 10 May 2016 16:50:01 UTC **Duration:** 72.852 sec	B
3	132.245.17.34 Ready	Tue, 10 May 2016 16:51:14 UTC **Duration:** 77.326 sec	B
4	132.245.13.210 Ready	Tue, 10 May 2016 16:52:32 UTC **Duration:** 76.303 sec	B
5	157.56.237.242 Ready	Tue, 10 May 2016 16:53:48 UTC **Duration:** 53.437 sec	B
6	132.245.113.194 Ready	Tue, 10 May 2016 16:54:41 UTC **Duration:** 68.344 sec	B
7	132.245.21.82 Ready	Tue, 10 May 2016 16:55:50 UTC **Duration:** 67.914 sec	B
8	132.245.81.130 Ready	Tue, 10 May 2016 16:56:58 UTC **Duration:** 53.699 sec	B
9	157.56.242.98 Ready	Tue, 10 May 2016 16:57:51 UTC **Duration:** 72.980 sec	B

SSL Report v1.22.37

Terms and Conditions



You are here: Home > Projects > SSL Server Test > icloud.com

SSL Report: icloud.com

Assessed on: Wed, 11 May 2016 11:11:28 UTC | Clear cache

Scan Another >>

	Server	Test time	Grade
1	17.142.164.49 icloud.com Ready	Wed, 11 May 2016 10:54:19 UTC Duration: 56.224 sec	C
2	17.167.154.49 icloud.com Ready	Wed, 11 May 2016 10:55:15 UTC Duration: 72.144 sec	C
3	17.167.152.81 icloud.com Ready	Wed, 11 May 2016 10:56:27 UTC Duration: 71.570 sec	C
4	17.172.192.55 icloud.org Ready	Wed, 11 May 2016 10:57:39 UTC Duration: 71.533 sec	C
5	17.158.10.94 icloud.com Ready	Wed, 11 May 2016 10:58:50 UTC Duration: 63.584 sec	C
6	17.158.28.83 icloud.com Ready	Wed, 11 May 2016 10:59:54 UTC Duration: 62.89 sec	C
7	17.133.238.52 icloud.com Ready	Wed, 11 May 2016 11:00:56 UTC Duration: 56.690 sec	C
8	17.172.208.84 icloud.com Ready	Wed, 11 May 2016 11:01:53 UTC Duration: 73.59 sec	C
9	17.133.236.52 icloud.com Ready	Wed, 11 May 2016 11:03:06 UTC Duration: 56.984 sec	C
	17.110.244.84		

QUALYS® SSL LABS
Home
Projects
Qualys.com
Contact
Scan Another »

You are here: Home > Projects > SSL Server Test > openbsd.org

SSL Report: openbsd.org (129.128.5.194)

Assessed on: Fri, 29 Apr 2016 15:49:34 UTC | **HIDDEN** | Clear cache

Assessment failed: Unable to connect to the server

Known Problems

There are some errors that we cannot fix properly in the current version. They will be addressed in the next generation version, which is currently being developed.

- **No secure protocols supported** - if you get this message, but you know that the site supports SSL, wait until the cache expires on its own, then try again, making sure the hostname you enter uses the "www" prefix (e.g., "www.ssllabs.com", not just "ssllabs.com").
- **no more data allowed for version 1 certificate** - the certificate is invalid; it is declared as version 1, but uses extensions, which were introduced in version 3. Browsers might ignore this problem, but our parser is strict and refuses to proceed. We'll try to find a different parser to avoid this problem.
- **Failed to obtain certificate** and **Internal Error** - errors of this type will often be reported for servers that use connection rate limits or block connections in response to unusual traffic. Problems of this type are very difficult to diagnose. If you have access to the server being tested, before reporting a problem to us, please check that there is no rate limiting or IDS in place.
- **NetScaler issues** - some NetScaler versions appear to reject SSL handshakes that do not include certain suites or handshakes that use a few suites. If the test is failing and there is a NetScaler load balancer in place, that's most likely the reason.
- **Unexpected failure** - our tests are designed to fail when unusual results are observed. This usually happens when there are multiple TLS servers behind the same IP address. In such cases we can't provide accurate results, which is why we fail.

Common Error Messages

QUALYS SSL LABS
Home
Projects
Qualys.com
Contact
Scan Another »
T
Certificate
Protocol Support
Key Exchange
Cipher Strength
0
20
40
60
80
100

You are here: Home > Projects > SSL Server Test > openbsd.org

SSL Report: openbsd.org (129.128.5.194)

Assessed on: Wed, 11 May 2016 13:51:13 UTC | **HIDDEN** | Clear cache

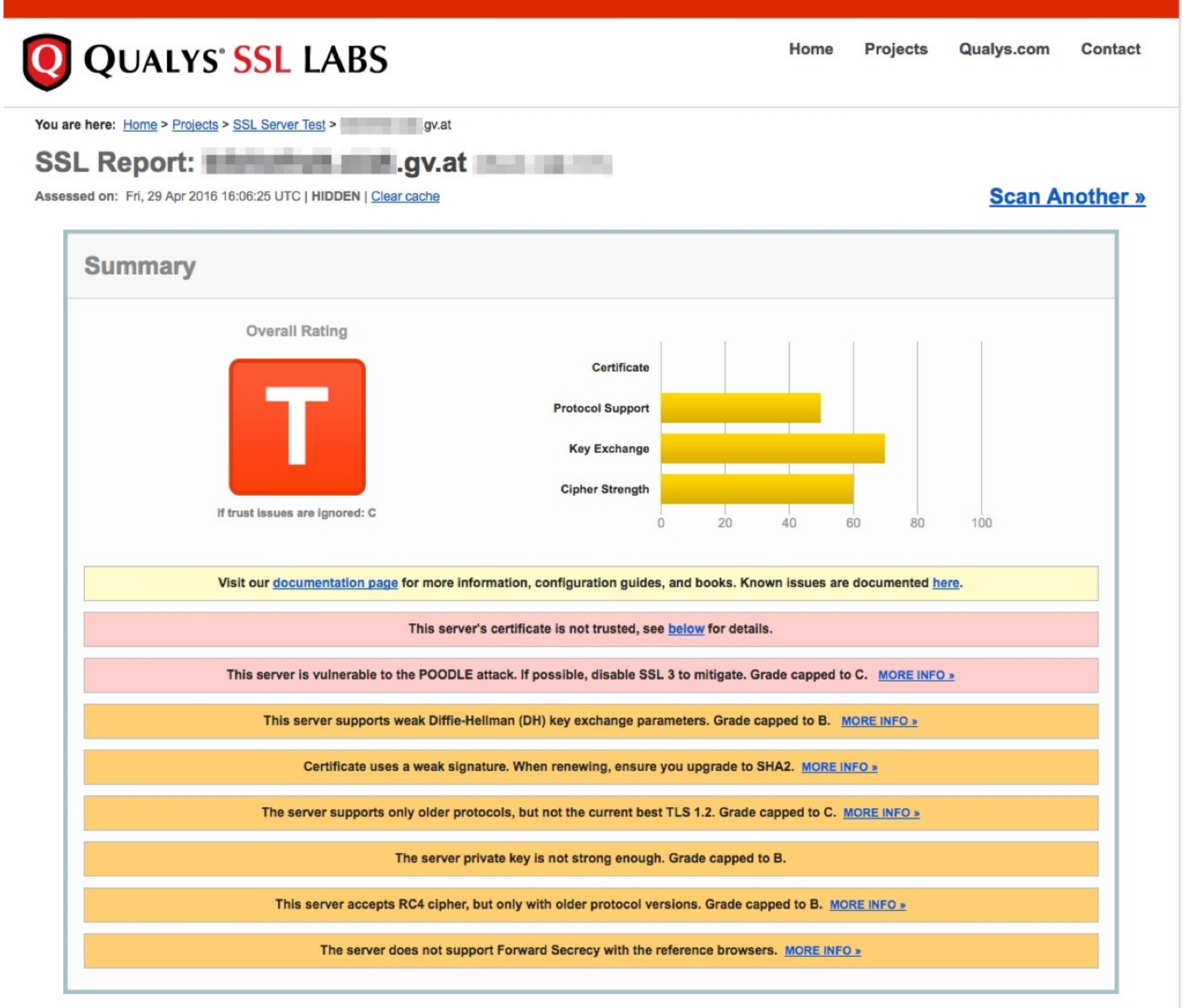
Summary

Overall Rating

If trust issues are ignored: A

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

This server's certificate is not trusted, see below for details.



You are here: Home > Projects > SSL Server Test > [redacted]gv.at

SSL Report: [redacted].gv.at [redacted]

Assessed on: Fri, 29 Apr 2016 16:06:25 UTC | HIDDEN | Clear cache

Scan Another »

Summary

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

This server's certificate is not trusted, see below for details.

This server is vulnerable to the POODLE attack. If possible, disable SSL 3 to mitigate. Grade capped to C. MORE INFO »

This server supports weak Diffie-Hellman (DH) key exchange parameters. Grade capped to B. MORE INFO »

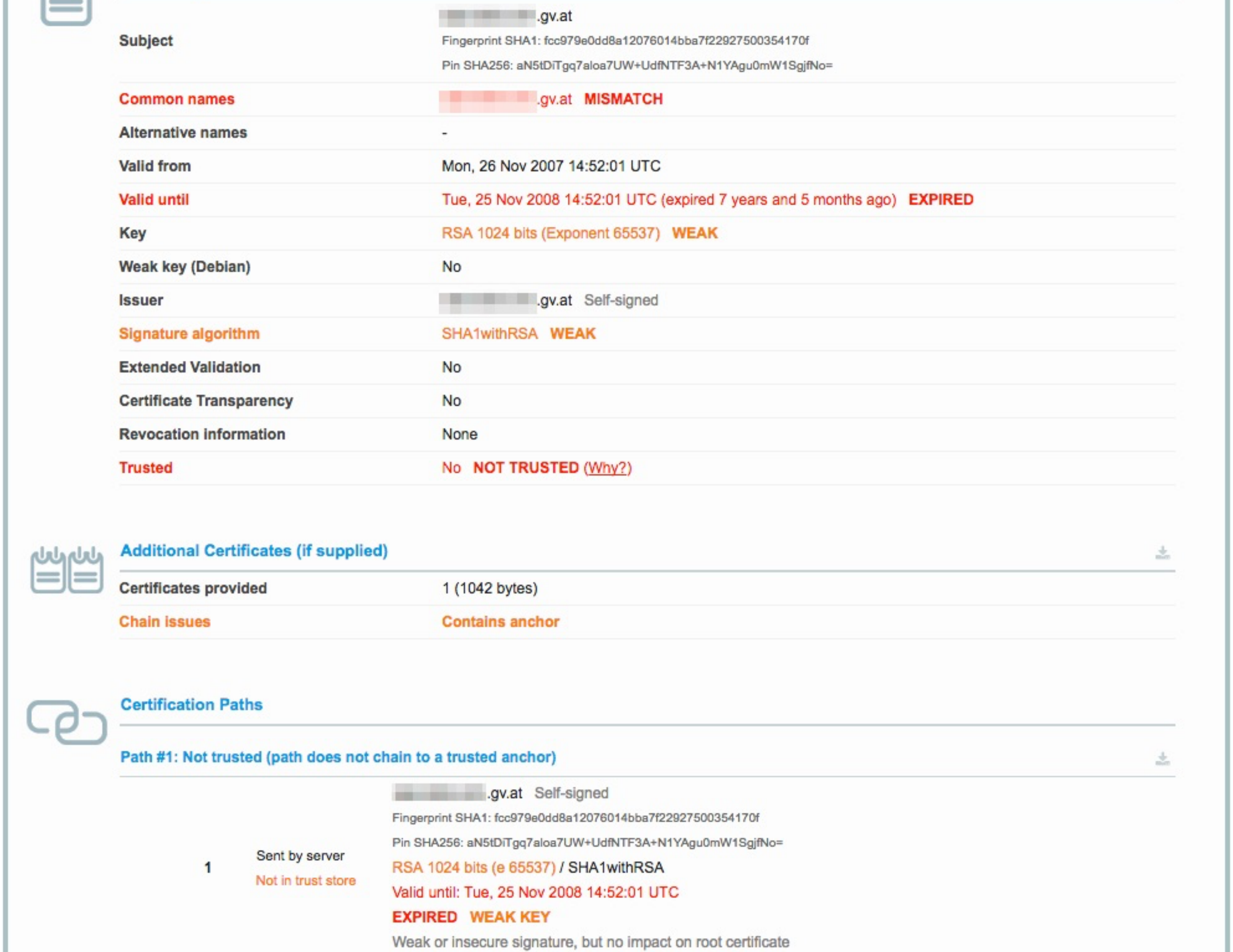
Certificate uses a weak signature. When renewing, ensure you upgrade to SHA2. MORE INFO »

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

The server private key is not strong enough. Grade capped to B.

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 »



Subject	[redacted].gv.at Fingerprint SHA1: fcc979e0dd8a12076014bba7f22927500354170f Pin SHA256: aN5tDiTgq7aloa7UW+UdfNTF3A+N1YAgu0mW1SgjfNo=
Common names	[redacted].gv.at **MISMATCH**
Alternative names	-
Valid from	Mon, 26 Nov 2007 14:52:01 UTC
Valid until	Tue, 25 Nov 2008 14:52:01 UTC (expired 7 years and 5 months ago) **EXPIRED**
Key	RSA 1024 bits (Exponent 65537) **WEAK**
Weak key (Debian)	No
Issuer	[redacted].gv.at Self-signed
Signature algorithm	SHA1withRSA **WEAK**
Extended Validation	No
Certificate Transparency	No
Revocation information	None
Trusted	No **NOT TRUSTED** (Why?)

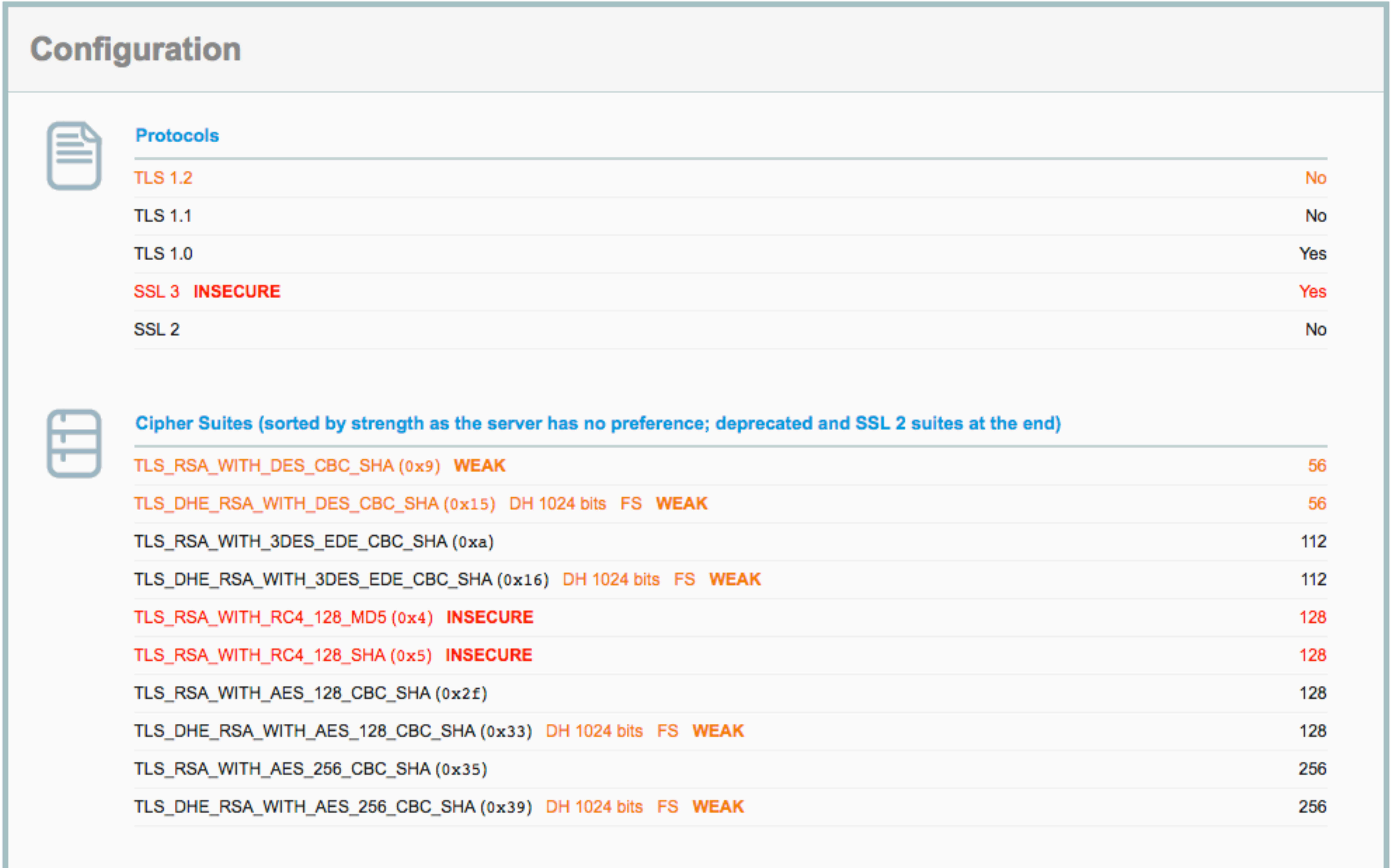
Additional Certificates (if supplied)

Certificates provided	1 (1042 bytes)
Chain issues	Contains anchor

Certification Paths

Path #1: Not trusted (path does not chain to a trusted anchor)

1	Sent by server Not in trust store	[redacted].gv.at Self-signed Fingerprint SHA1: fcc979e0dd8a12076014bba7f22927500354170f Pin SHA256: aN5tDiTgq7aloa7UW+UdfNTF3A+N1YAgu0mW1SgjfNo= RSA 1024 bits (e 65537) / SHA1withRSA Valid until: Tue, 25 Nov 2008 14:52:01 UTC **EXPIRED** **WEAK KEY** 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 (sorted by strength as the server has no preference; deprecated and SSL 2 suites at the end)

TLS_RSA_WITH_DES_CBC_SHA (0x9) **WEAK**	56
TLS_DHE_RSA_WITH_DES_CBC_SHA (0x15) DH 1024 bits FS **WEAK**	56
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa)	112
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x16) DH 1024 bits FS **WEAK**	112
TLS_RSA_WITH_RC4_128_MD5 (0x4) **INSECURE**	128
TLS_RSA_WITH_RC4_128_SHA (0x5) **INSECURE**	128
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	128
TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33) DH 1024 bits FS **WEAK**	128
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)	256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) DH 1024 bits FS **WEAK**	256

HTTP Response Header

Security Headers

https://securityheaders.io

securityheaders.io
Home
About
Scan

Scan your site now

cert.at

□ Hide results

Grand Totals

A+	52,631
A	58,483
B	43,164
C	2,170
D	36,204
E	188,265
F	192,728
R	136,670
Total	710,315

Recent Scans

www.nubix.nl	E
rungo.idnes.cz	F
vyvoj1.larx.cz	A
sso.yatun.cz	E
www.file.io	F
www.fidelity.com	F
bistrodengi.ru	B
wien52.at	F
orf.at	F

Hall of Fame

vyvoj1.larx.cz	A
www.wetterstation-...	A+
securityheaders.io	A
penfold.fr	A
www.slevomat.cz	A+
raspi.madavi.de	A
addons.mozilla.org	A
www.handicapmaster...	A+
www.michalspacek.c...	A

Hall of Shame

rungo.idnes.cz	F
www.file.io	F
www.fidelity.com	F
wien52.at	F
orf.at	F
onlinebanking.nati...	F
uk.passion-radio.c...	F
www.auctiva.com	F
ac2.happyforever.c...	F

A scotthelme.co.uk project - CC-BY-SA 4.0

securityheaders.io
Home
About
Scan your site now
Scan
☐ Hide results

cert.at

Security Report Summary

E

Site:	http://cert.at/ - (Scan again over https)
IP Address:	83.136.38.146
Report Time:	11 May 2016 12:22:50 UTC
Headers:	X-Frame-Options Content-Security-Policy X-XSS-Protection X-Content-Type-Options

securityheaders.io
Home
About
Scan
Hide results

Scan your site now

https://cert.at

Security Report Summary

D

Site:	https://cert.at/
IP Address:	83.136.38.146
Report Time:	11 May 2016 14:03:29 UTC
Headers:	X-Frame-Options Strict-Transport-Security Content-Security-Policy Public-Key-Pins X-XSS-Protection X-Content-Type-Options

Raw Headers

HTTP/1.1	200 OK
Date	Wed, 11 May 2016 14:03:28 GMT
Server	Apache

securityheaders.io
Home
About
Scan
□ Hide results

Scan your site now

http://maclemon.at

Security Report Summary

R

Redirect:	Click here to follow the redirect to https://maclemon.at/.
Site:	http://maclemon.at/ - (Scan again over https)
IP Address:	2001:470:6f:4ca:9a26:fb93:ba1c:e29a
Report Time:	11 May 2016 14:08:02 UTC
Headers:	X-Frame-Options X-Content-Type-Options X-XSS-Protection Content-Security-Policy

Raw Headers

HTTP/1.1	301 Moved Permanently
Server	nginx
Date	Wed, 11 May 2016 14:08:02 GMT

securityheaders.io
Home
About
Scan
☐ Hide results

Scan your site now

https://maclemon.at/

Security Report Summary

A+

Site:	https://maclemon.at/
IP Address:	2001:470:6f:4ca:9a26:fb93:ba1c:e29a
Report Time:	27 Mar 2016 11:55:16 UTC
Headers:	✓ X-Frame-Options ✓ X-Content-Type-Options ✓ X-XSS-Protection ✓ Strict-Transport-Security ✓ Public-Key-Pins ✓ Content-Security-Policy

Raw Headers

HTTP/1.1	200 OK
Server	nginx
Date	Sun, 27 Mar 2016 11:55:14 GMT

Raw Headers

HTTP/1.1	200 OK
Server	nginx
Date	Sun, 27 Mar 2016 11:55:14 GMT
Content-Type	text/html; charset=utf-8
Content-Length	134619
Last-Modified	Fri, 15 Jan 2016 12:15:53 GMT
Connection	keep-alive
Vary	Accept-Encoding
ETag	"5698e2f9-20ddb"
X-Frame-Options	DENY
X-Content-Type-Options	nosniff
X-XSS-Protection	1; mode=block
strict-transport-security	max-age=31104000; includeSubDomains; preload
Public-Key-Pins	max-age=2592000; pin-sha256="rFfvG6DIxgDwHy4qfCVEnDKoFJ2XG3szxQHeeaRv9g8=";pin-sha256="gXaQqXAAR+AjznLZGRIBAYOabhv/lI5Bc+CL9e7Kpmg=";pin-sha256="5noWBr53rhdxeVxcQagM3hqYu+Cw0m34VjrBo1Cu5Ag="
Content-Security-Policy	upgrade-insecure-requests
Accept-Ranges	bytes

Additional Information

Server	This Server header seems to advertise the software being run on the server but you can remove or change this value.
X-Frame-Options	X-Frame-Options tells the browser whether you want to allow your site to be framed or not. By preventing a browser from framing your site you can defend against attacks like clickjacking.
X-Content-Type-Options	X-Content-Type-Options stops a browser from trying to MIME-sniff the content type and forces it to stick with the declared content-type. This helps to reduce the danger of drive-by downloads. The only valid value for this header is "X-Content-Type-Options: nosniff".
X-XSS-Protection	X-XSS-Protection sets the configuration for the cross-site scripting filters built into most browsers. The best configuration is "X-XSS-Protection: 1; mode=block".
strict-transport-security	HTTP Strict Transport Security is an excellent feature to support on your site and strengthens your implementation of TLS by getting the User Agent to enforce the use of HTTPS.
Public-Key-Pins	HTTP Public Key Pinning protects your site from MiTM attacks using rogue X.509 certificates. By whitelisting only the identities that the browser should trust, your users are protected in the event a certificate authority is compromised. Analyse this policy in more detail.
Content-Security-Policy	Content Security Policy is an effective measure to protect your site from XSS attacks. By whitelisting sources of approved content, you can prevent the browser from loading malicious assets. Analyse this policy in more detail.

```
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
X-XSS-Protection: 1;mode=block
```

```
# CSP
Content-Security-Policy
"default-src 'self'; upgrade-
insecure-requests";
```

HTTPS only

```
# HSTS
strict-transport-security "max-age=31104000";
                                     includeSubDomains; preload;

# HPKP
Public-Key-Pins "pin-sha256=\"YOUR_HASH=\"; pin-sha256=
\"YOUR_BACKUP_HASH=\"; max-age=7776000; report-uri=\"https://
YOUR.REPORT.URL\""
```

```
curl -I https://maclemon.at/
```

[-4|-6]

```
$ curl -I https://maclemon.at/
HTTP/2.0 200
server:nginx
date:Sun, 27 Mar 2016 12:50:15 GMT
content-type:text/html; charset=utf-8
content-length:134619
last-modified:Fri, 15 Jan 2016 12:15:53 GMT
vary:Accept-Encoding
etag:"5698e2f9-20ddb"
x-frame-options:DENY
x-content-type-options:nosniff
x-xss-protection:1; mode=block
strict-transport-security:max-age=31104000; includeSubDomains; preload
public-key-pins:max-age=2592000; pin-
sha256="rFfvG6DIxgDwHy4qfCVEnDKoFJ2XG3szxQHeeaRv9g8=";pin-sha256="gXaQqXAAR
+AjznLZGRlBAYOabhv/II5Bc+CL9e7Kpmg=";pin-sha256="5noWBr53rhdxeVxcQagM3hqYu
+Cw0m34VjrBo1Cu5Ag="
content-security-policy:upgrade-insecure-requests
accept-ranges:bytes
```

```
wget -S -O/dev/null https://maclemon.at/
```

[-4|-6]

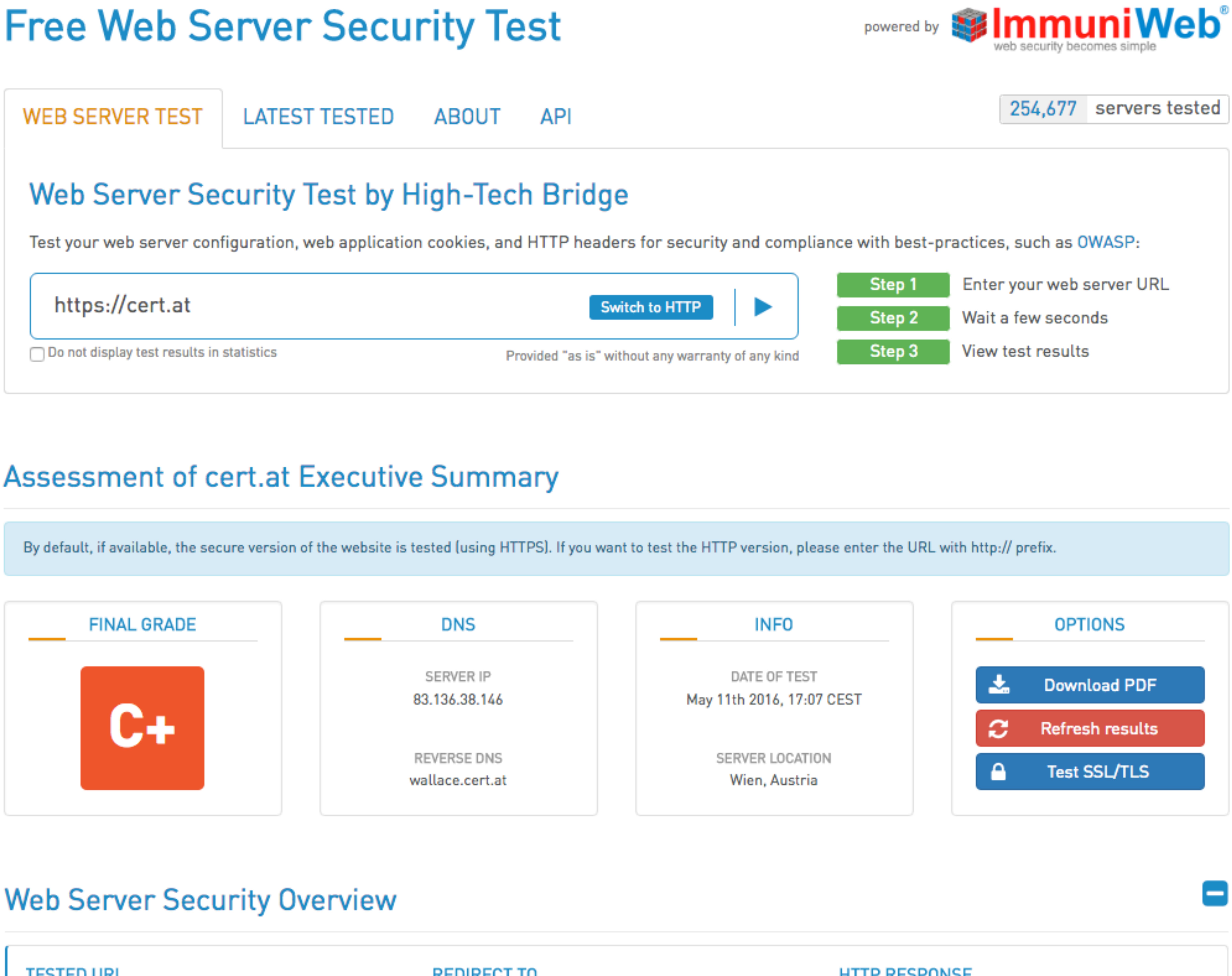
```
$ wget -S -O/dev/null https://maclemon.at/
--2016-03-27 14:49:46--  https://maclemon.at/
Resolving maclemon.at (maclemon.at)... 86.59.70.21, 2001:470:6f:4ca:9a26:fb93:ba1c:e29a
Connecting to maclemon.at (maclemon.at)|86.59.70.21|:443... connected.
HTTP request sent, awaiting response...
  HTTP/1.1 200 OK
  Server: nginx
  Date: Sun, 27 Mar 2016 12:49:46 GMT
  Content-Type: text/html; charset=utf-8
  Content-Length: 134619
  Last-Modified: Fri, 15 Jan 2016 12:15:53 GMT
  Connection: keep-alive
  Vary: Accept-Encoding
  ETag: "5698e2f9-20ddb"
  X-Frame-Options: DENY
  X-Content-Type-Options: nosniff
  X-XSS-Protection: 1; mode=block
  strict-transport-security: max-age=31104000; includeSubDomains; preload
  Public-Key-Pins: max-age=2592000; pin-sha256="rFfvG6DIxgDwHy4qfCVEnDKoFJ2XG3szxQHeeaRv9g8=";pin-sha256="gXaQqXAAR
+AjznLZGRlBAYOabhv/II5Bc+CL9e7Kpmg=";pin-sha256="5noWBr53rhdxeVxcQagM3hqYu+Cw0m34VjrBo1Cu5Ag="
  Content-Security-Policy: upgrade-insecure-requests
  Accept-Ranges: bytes
Length: 134619 (131K) [text/html]
Saving to: ‘/dev/null’

/dev/null                                                                      100%
[=============================================================================>] 131.46K   509KB/s    in 0.3s

2016-03-27 14:49:47 (509 KB/s) - ‘/dev/null’ saved [134619/134619]
```

High Tech Bridge

https://www.htbridge.com/websec/



Free Web Server Security Test

254,677 servers tested

Web Server Security Test by High-Tech Bridge

Test your web server configuration, web application cookies, and HTTP headers for security and compliance with best-practices, such as OWASP:

https://cert.at

□ Do not display test results in statistics

Provided "as is" without any warranty of any kind

Step 1 Enter your web server URL

Step 2 Wait a few seconds

Step 3 View test results

Assessment of cert.at Executive Summary

By default, if available, the secure version of the website is tested (using HTTPS). If you want to test the HTTP version, please enter the URL with http:// prefix.

FINAL GRADE	DNS	INFO	OPTIONS
C+	SERVER IP 83.136.38.146 REVERSE DNS wallace.cert.at	DATE OF TEST May 11th 2016, 17:07 CEST SERVER LOCATION Wien, Austria	Download PDF Refresh results Test SSL/TLS

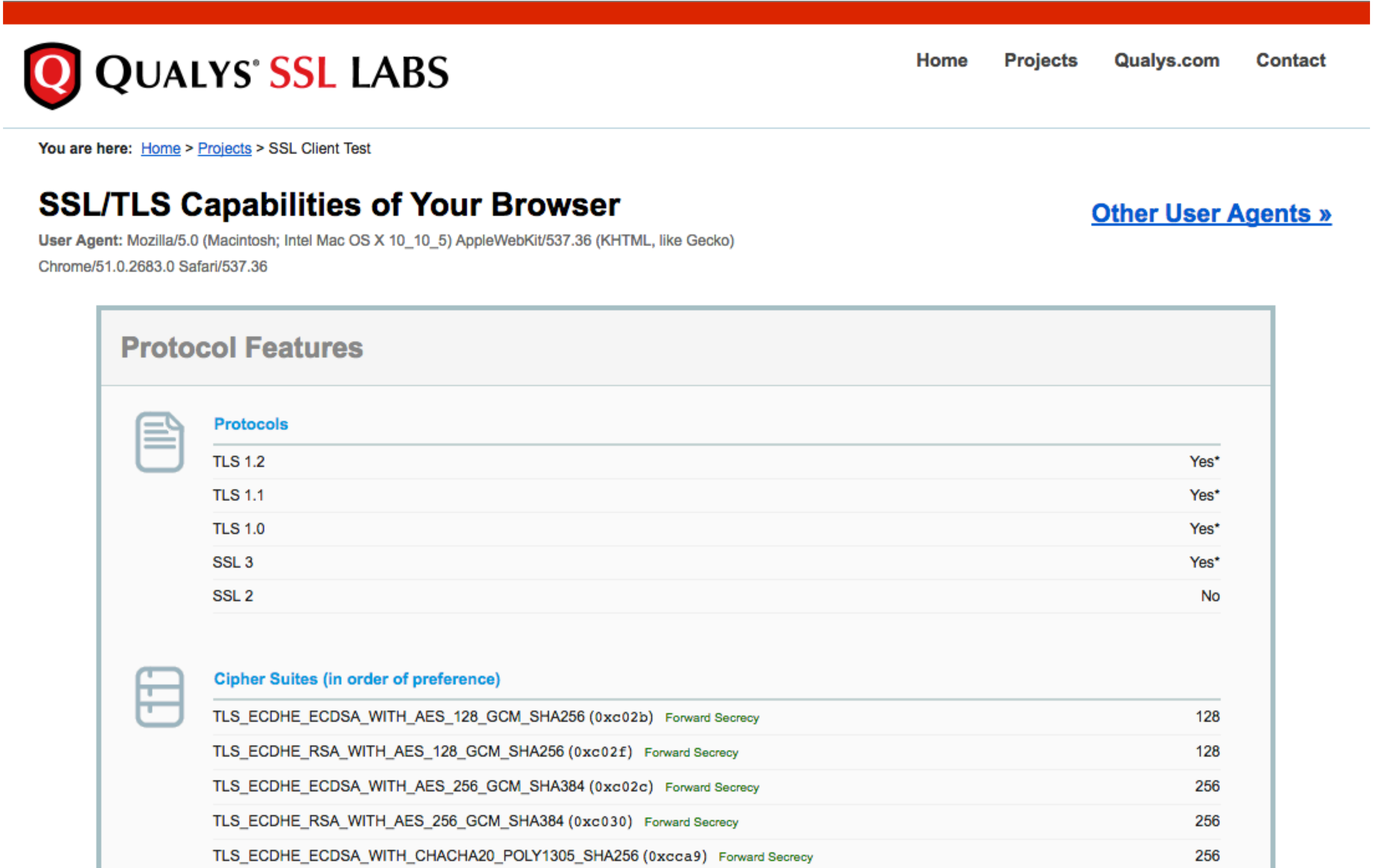
Web Server Security Overview

TESTED URL REDIRECT TO HTTP RESPONSE

Browser

Qualys SSLLabs

https://www.ssllabs.com/ssltest/viewMyClient.html



You are here: Home > Projects > SSL Client Test

SSL/TLS Capabilities of Your Browser

Other User Agents »

User Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_5) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2683.0 Safari/537.36

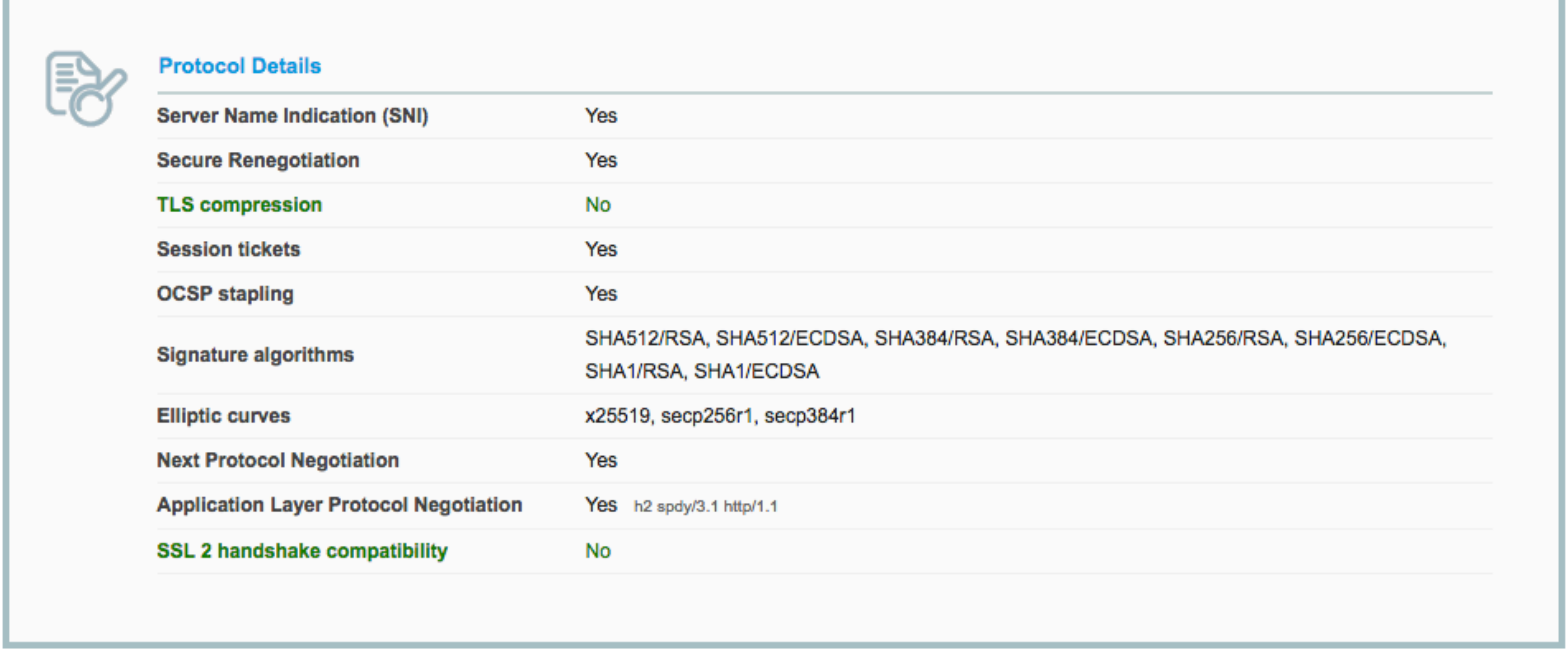
Protocol Features

Protocols

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

Cipher Suites (in order of preference)

TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b) Forward Secrecy	128
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) Forward Secrecy	128
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c) Forward Secrecy	256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) Forward Secrecy	256
TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca9) Forward Secrecy	256

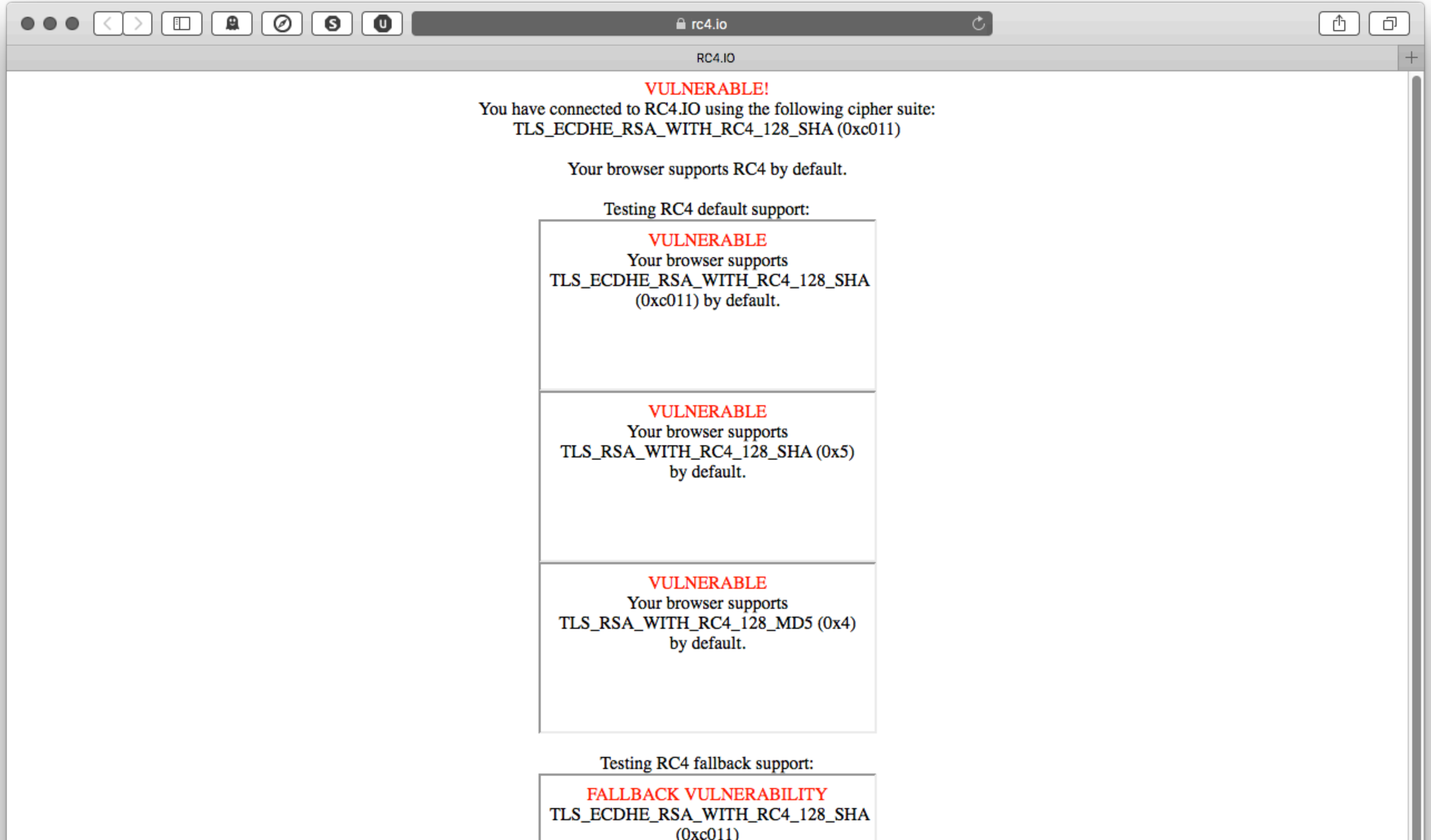


Protocol Details

Server Name Indication (SNI)	Yes
Secure Renegotiation	Yes
TLS compression	No
Session tickets	Yes
OCSP stapling	Yes
Signature algorithms	SHA512/RSA, SHA512/ECDSA, SHA384/RSA, SHA384/ECDSA, SHA256/RSA, SHA256/ECDSA, SHA1/RSA, SHA1/ECDSA
Elliptic curves	x25519, secp256r1, secp384r1
Next Protocol Negotiation	Yes
Application Layer Protocol Negotiation	Yes h2 spdy/3.1 http/1.1
SSL 2 handshake compatibility	No

RC4 Test

https://rc4.io/



VULNERABLE!
You have connected to RC4.IO using the following cipher suite:
TLS_ECDHE_RSA_WITH_RC4_128_SHA (0xc011)

Your browser supports RC4 by default.

Testing RC4 default support:

VULNERABLE
Your browser supports TLS_ECDHE_RSA_WITH_RC4_128_SHA (0xc011) by default.

VULNERABLE
Your browser supports TLS_RSA_WITH_RC4_128_SHA (0x5) by default.

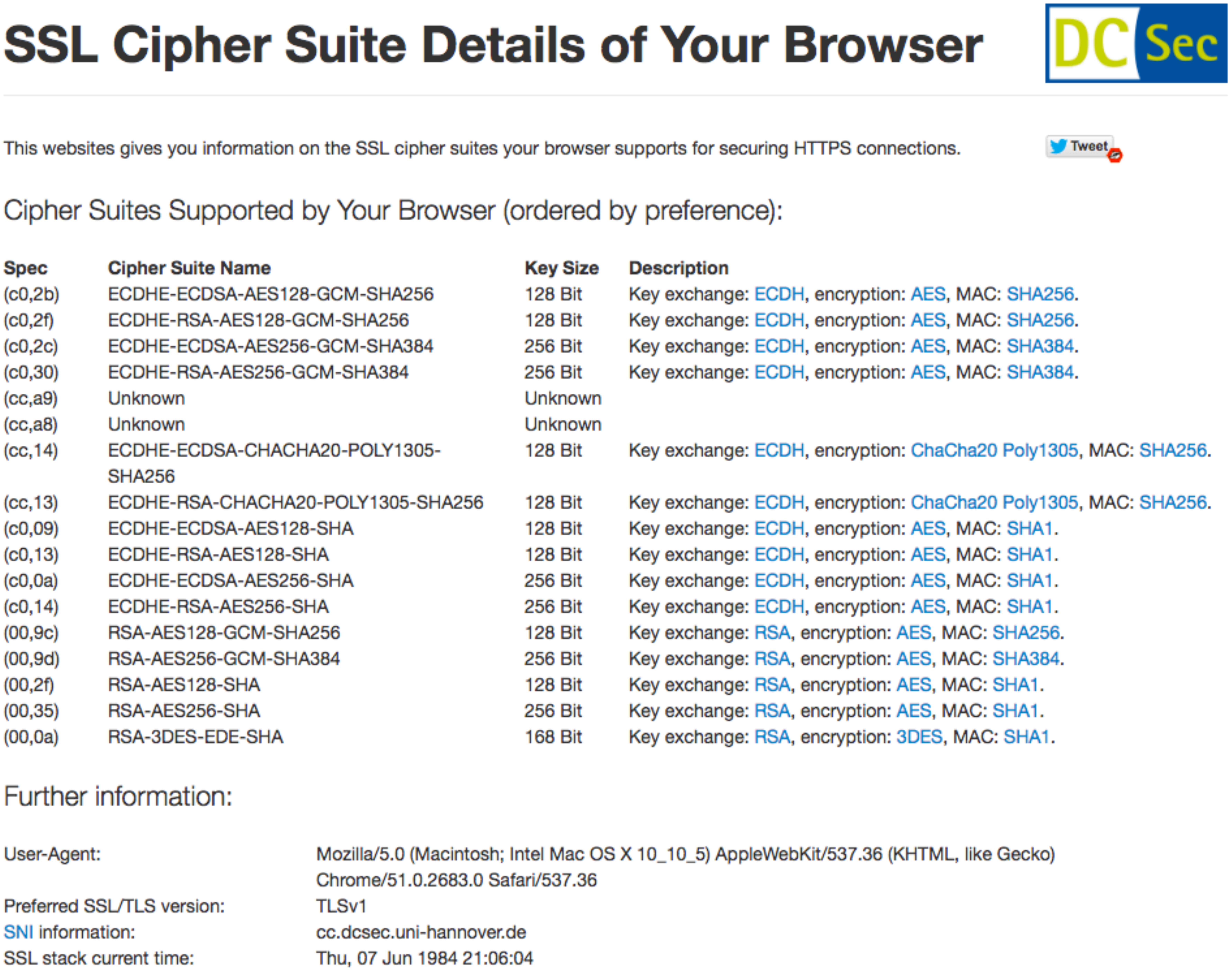
VULNERABLE
Your browser supports TLS_RSA_WITH_RC4_128_MD5 (0x4) by default.

Testing RC4 fallback support:

FALLBACK VULNERABILITY
TLS_ECDHE_RSA_WITH_RC4_128_SHA (0xc011)

Uni-Hannover

https://cc.dcsec.uni-hannover.de/



SSL Cipher Suite Details of Your Browser

This websites gives you information on the SSL cipher suites your browser supports for securing HTTPS connections.

Cipher Suites Supported by Your Browser (ordered by preference):

Spec	Cipher Suite Name	Key Size	Description
(c0,2b)	ECDHE-ECDSA-AES128-GCM-SHA256	128 Bit	Key exchange: ECDH, encryption: AES, MAC: SHA256.
(c0,2f)	ECDHE-RSA-AES128-GCM-SHA256	128 Bit	Key exchange: ECDH, encryption: AES, MAC: SHA256.
(c0,2c)	ECDHE-ECDSA-AES256-GCM-SHA384	256 Bit	Key exchange: ECDH, encryption: AES, MAC: SHA384.
(c0,30)	ECDHE-RSA-AES256-GCM-SHA384	256 Bit	Key exchange: ECDH, encryption: AES, MAC: SHA384.
(cc,a9)	Unknown	Unknown	
(cc,a8)	Unknown	Unknown	
(cc,14)	ECDHE-ECDSA-CHACHA20-POLY1305-SHA256	128 Bit	Key exchange: ECDH, encryption: ChaCha20 Poly1305, MAC: SHA256.
(cc,13)	ECDHE-RSA-CHACHA20-POLY1305-SHA256	128 Bit	Key exchange: ECDH, encryption: ChaCha20 Poly1305, MAC: SHA256.
(c0,09)	ECDHE-ECDSA-AES128-SHA	128 Bit	Key exchange: ECDH, encryption: AES, MAC: SHA1.
(c0,13)	ECDHE-RSA-AES128-SHA	128 Bit	Key exchange: ECDH, encryption: AES, MAC: SHA1.
(c0,0a)	ECDHE-ECDSA-AES256-SHA	256 Bit	Key exchange: ECDH, encryption: AES, MAC: SHA1.
(c0,14)	ECDHE-RSA-AES256-SHA	256 Bit	Key exchange: ECDH, encryption: AES, MAC: SHA1.
(00,9c)	RSA-AES128-GCM-SHA256	128 Bit	Key exchange: RSA, encryption: AES, MAC: SHA256.
(00,9d)	RSA-AES256-GCM-SHA384	256 Bit	Key exchange: RSA, encryption: AES, MAC: SHA384.
(00,2f)	RSA-AES128-SHA	128 Bit	Key exchange: RSA, encryption: AES, MAC: SHA1.
(00,35)	RSA-AES256-SHA	256 Bit	Key exchange: RSA, encryption: AES, MAC: SHA1.
(00,0a)	RSA-3DES-EDE-SHA	168 Bit	Key exchange: RSA, encryption: 3DES, MAC: SHA1.

Further information:

User-Agent:	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_5) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2683.0 Safari/537.36
Preferred SSL/TLS version:	TLSv1
SNI information:	cc.dcsec.uni-hannover.de
SSL stack current time:	Thu, 07 Jun 1984 21:06:04

about:config

chrome://net-internals/

Webserver Konfiguration

bettercrypto·org

https://bettercrypto.org/

BetterCrypto Arbeitstreffen

2016-05-23, 18:00 MESZ, CERT.at

THE APACHE® SOFTWARE FOUNDATION

httpd 2.4

mod_ssl
mod_header

mod_h2

HTTP/2

```
/etc/apache2/httpd.conf
  NameVirtualHost *:443
  # Linux / Windows
  # AcceptFilter http data
  AcceptFilter https data

  # FreeBSD
  # AcceptFilter http httpready
  # AcceptFilter https dataready

/etc/apache2/ports.conf
  Listen 443
```

```
<VirtualHost *:443>
  ServerName www.yoursite.com
  DocumentRoot /var/www/site
  SSLEngine on
  Protocols h2 http/1.1

  SSLCertificateFile /etc/ssl/certs/ssl-cert-snakeoil.pem
  SSLCertificateKeyFile /etc/ssl/private/ssl-cert-snakeoil.key
  SSLCertificateChainFile /etc/apache2/ssl.crt/server-ca.crt

  SSLProtocol All -SSLv2 -SSLv3
  SSLCipherSuite 'EDH+CAMELLIA:EDH+aRSA:EECDH+aRSA+AESGCM:EECDH
+aRSA+SHA384:EECDH+aRSA+SHA256:EECDH:
+CAMELLIA256:+AES256:+CAMELLIA128:+AES128:+SSLv3:!aNULL:!eNULL:!
LOW:!3DES:!MD5:!EXP:!PSK:!DSS:!RC4:!SEED:!ECDSA:CAMELLIA256-
SHA:AES256-SHA:CAMELLIA128-SHA:AES128-SHA'
```

```
  SSLHonorCipherOrder On
  SSLCompression off

  # TLS_DHE_
  SSLDHParametersFile /etc/ssl/dh4096.pem

</VirtualHost>
```

Security Header

```
# For HTTPS only

  # HSTS
  Header always set strict-transport-security "max-
age=15768000"

  # HPKP
  Header always set Public-Key-Pins "pin-sha256=\"YOUR_HASH=
\"; pin-sha256=\"YOUR_BACKUP_HASH=\"; max-age=7776000;
report-uri=\"https://YOUR.REPORT.URL\""
```

```
# For HTTPS and HTTP

    Header always set  X-Frame-Options DENY
    Header always set  X-Content-Type-Options "nosniff"
    Header always set  X-XSS-Protection "1; mode=block"


# CSP
    Header always set Content-Security-Policy "default-src
https: data: 'unsafe-inline' 'unsafe-eval'" always; upgrade-
insecure-requests"
```

HTTP → HTTPS

301

```
# mod_rewrite syntax
<VirtualHost cert.at:80>
  RewriteRule ^/?(.*) https://%{SERVER_NAME}/$1 [R,L]
</VirtualHost>

# mod_alias syntax

<VirtualHost cert.at:80>
  Redirect permanent / https://%{SERVER_NAME}/
</VirtualHost>
```

```
ServerTokens Prod[uctOnly]
```

Server: Apache

nginx 1.10 stable / 1.11 mainline

```
--with-http_ssl_module
```

```
--with-http_v2_module
```

HTTP/2

```
server {
  # listen [2001:470:6f:4ca:9a26:fb93:ba1c:e29a]:443 ssl http2
deferred; # Tux
  listen [2001:470:6f:4ca:9a26:fb93:ba1c:e29a]:443 ssl http2
accept_filter=dataready; # FreeBSD

  server_name maclemon.at;

  ssl_certificate_key /etc/nginx/certificates/maclemon.at.key;
  ssl_certificate /etc/nginx/certificates/maclemon.at_chained.pem;

  ssl_protocols TLSv1 TLSv1.1 TLSv1.2;

  ssl_ciphers EDH+CAMELLIA:EDH+aRSA:EECDH+aRSA+AESGCM:EECDH+aRSA
+SHA384:EECDH+aRSA+SHA256:EECDH:
+CAMELLIA256:+AES256:+CAMELLIA128:+AES128:+SSLv3:!aNULL:!eNULL:!
LOW:!3DES:!MD5:!EXP:!PSK:!DSS:!RC4:!SEED:!IDEA:!
```

```
  ssl_prefer_server_ciphers on;

  # TLS_DHE_
  ssl_dhparam /etc/nginx/dhparam/dh4096.pem;

  # TLS compression is automatically turned OFF in
  # nginx 1.1.6+/1.0.9+ (if OpenSSL 1.0.0+ used)
  # nginx 1.3.2+/1.2.2+ (if older OpenSSL).
  # spdy_headers_comp 0; # SPDY Header Compression off

  ssl_ecdh_curve          secp384r1;

  # Speed improvements to first byte for smaller files.
  ssl_buffer_size 4k;
}
```

Security Header

```
# For HTTPS only

  # HSTS
  add_header strict-transport-security "max-age=31104000;
includeSubDomains; preload" always;

  # HPKP
  add_header Public-Key-Pins 'max-age=2592000; pin-
sha256="rFfvG6DIxgDwHy4qfCVEnDKoFJ2XG3szxQHeeaRv9g8=";pin-
sha256="gXaQqXAAR+AjznLZGRlBAYOabhv/II5Bc+CL9e7Kpmg=";pin-
sha256="5noWBr53rhdxeVxcQagM3hqYu+Cw0m34VjrBo1Cu5Ag="' always;
```

```
# For HTTPS and HTTP

    add_header  X-Frame-Options DENY always;
    add_header  X-Content-Type-Options "nosniff" always;
    add_header  X-XSS-Protection "1; mode=block" always;


# CSP
    add_header Content-Security-Policy "default-src https: data:
'unsafe-inline' 'unsafe-eval' upgrade-insecure-requests" always;
```

HTTP → HTTPS

301

```
server {
    listen [2001:470:6f:4ca:9a26:fb93:ba1c:e29a]:80;
    server_name maclemon.at;
    server_name www.maclemon.at;
    server_name [2001:470:6f:4ca:9a26:fb93:ba1c:e29a];

    return 301 https://maclemon.at$request_uri;
    # return 301 https://$server_name$request_uri;
}
```

```
server_tokens off;
```

Server: nginx

Handlungsbedar F

A

Fragen?

Zeitgemäße Webserver-Konfiguration

`https://media.ccc.de/c/eh16`

`https://maclemon.at/talks`

@leyrer
@MacLemon