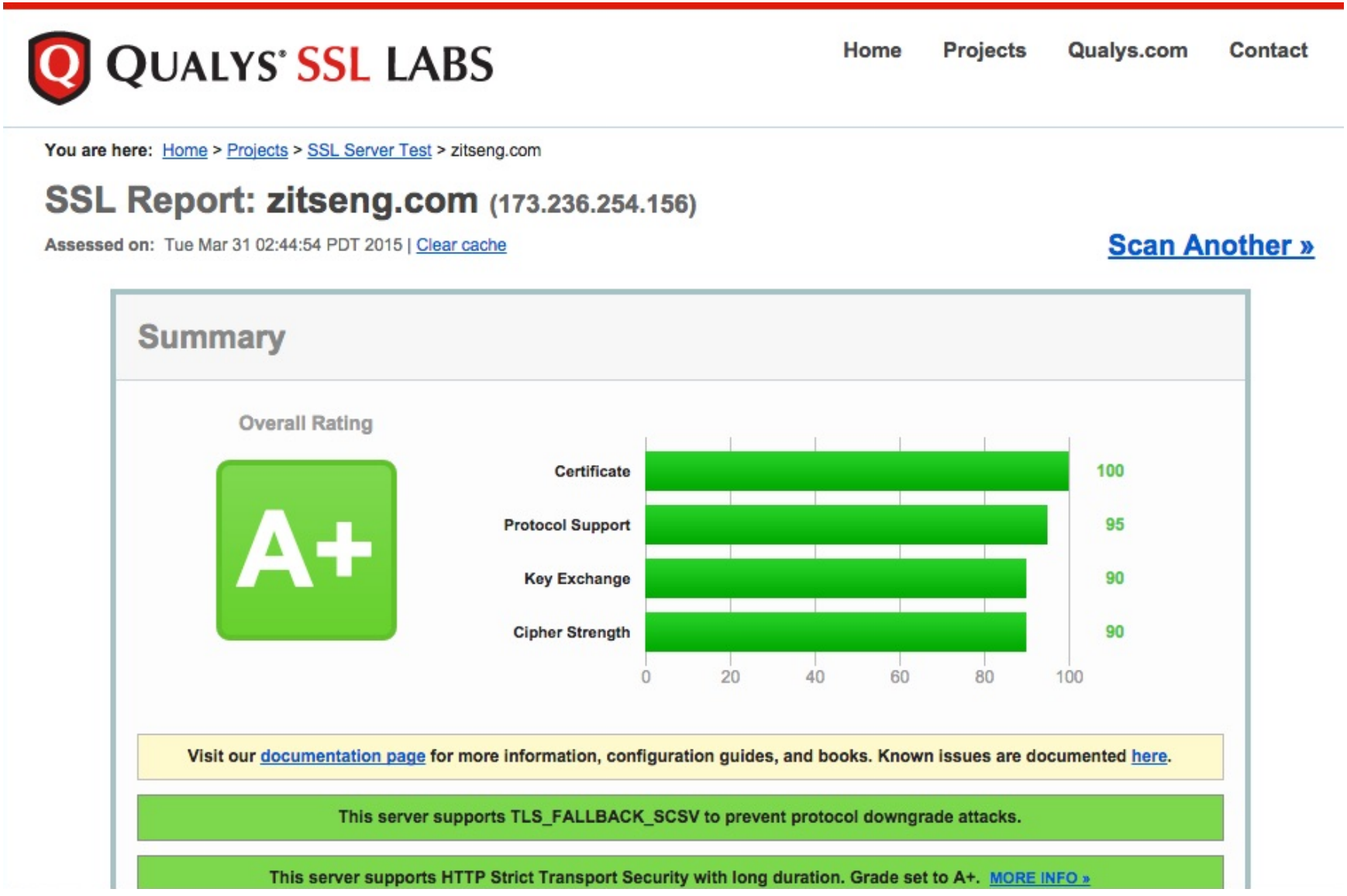
SSL Server Rating Guide for TLS Client Certificate Authentication

Research Seminar in Cryptography

September 7, 2016

Automated TLS Configuration Testing

Automated TLS Configuration Testing



Automated TLS Configuration Testing

Automated TLS Configuration Testing

SSL Report: www.ut.ee (193.40.5.73)

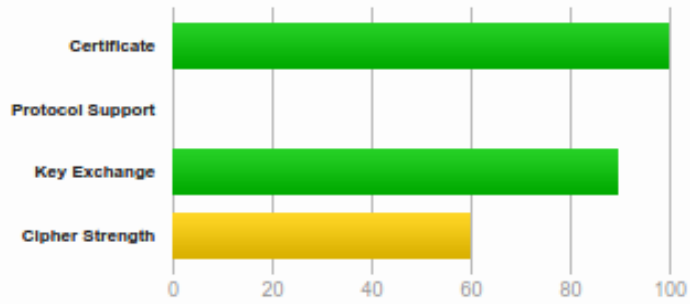
Assessed on: Thu, 01 Sep 2016 14:05:29 UTC | Hide | Clear cache

Scan Another »

Summary

Overall Rating

F



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

This server is vulnerable to the OpenSSL Padding Oracle vulnerability (CVE-2016-2107) and insecure. Grade set to F.

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 »

Automated TLS Configuration Testing

Automated TLS Configuration Testing

SSL Report: mailhost.ut.ee (193.40.5.66)

Assessed on: Thu, 01 Sep 2016 14:23:15 UTC | Hide | Clear cache

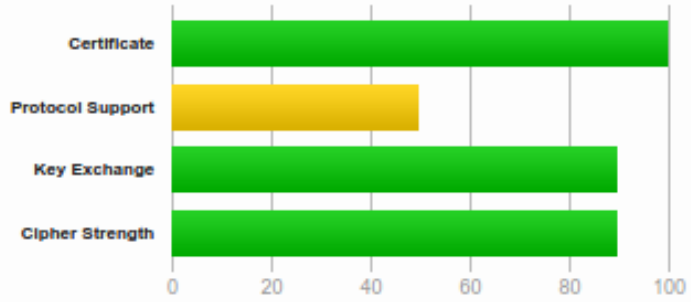
Scan Another »

Summary

Overall Rating

C

No support for TLS 1.2, which is the only secure protocol version. MORE »



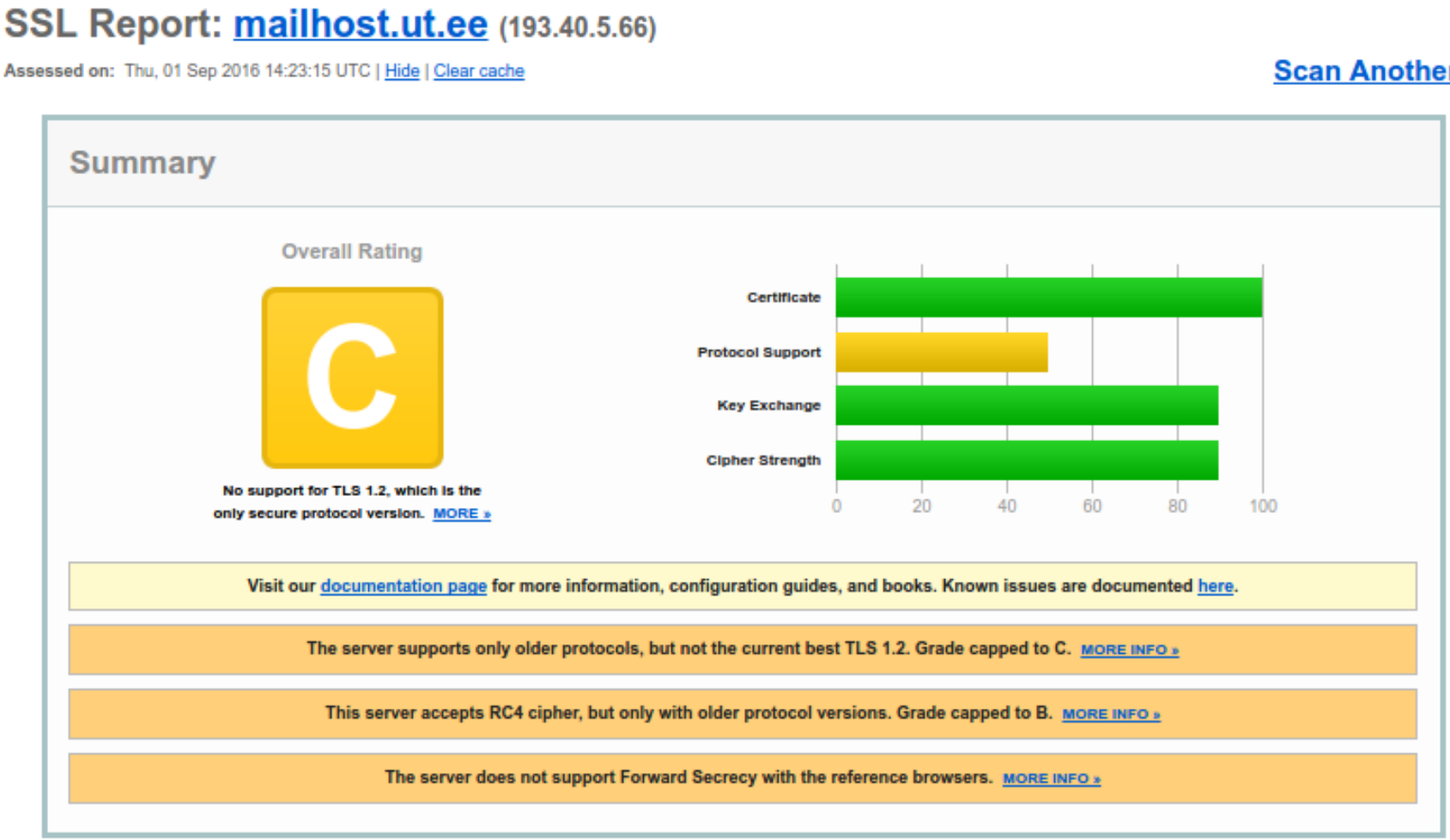
Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

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

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 »

Automated TLS Configuration Testing



Qualys SSL Labs "SSL Server Rating Guide"
(`https://www.ssllabs.com/downloads/SSL_Server_Rating_Guide.pdf`)

TLS CCA Configuration Testing

Service provider	Spare	Request	Depth	Timeout	Privacy	Resume	Bind	Validity
Banking:								
citadele.ee	0	optional	3	–	–	+	+	OCSP
krediidipank.ee	5	optional	2	–	–	+	+	OCSP
seb.ee	2	optional	2	–	–	+	+	OCSP
tbb.ee	4	require	3	–	+	–	–*	OCSP
unicreditbank.ee	0	require	5	–	–	+	?	?
versobank.com	0	optional	3	40 sec	–	+	?	?
Education:								
e-ope.ee	4	optional	3	–	–	+	+	–
eek.ee	0	require	2	–	+	–	?	?
ekool.eu	0	optional	2	–*	+	–	–	–
emu.ee	0	require	2	–	+	–	–	OCSP 2007
tlu.ee	0	require	2	9 hour	–	+	–	?
Government:								
ariregister.rik.ee	0	optional	6	–	+	–	–	CRL
digidoc.sk.ee	4	require	2	–	+	–	–	OCSP
e-register.ee	0	require	3	–	+	–	–	OCSP
e-toimik.ee	0	optional	2	–	+	–	–	OCSP
eesti.ee	5	require	2	–*	+	–	–	OCSP
emta.ee	0	optional	3	–	–	+	–	OCSP

TLS CCA Configuration Testing

Service provider	Spare	Request	Depth	Timeout	Privacy	Resume	Bind	Validity
Banking:								
citadele.ee	0	optional	3	–	–	+	+	OCSP
krediidipank.ee	5	optional	2	–	–	+	+	OCSP
seb.ee	2	optional	2	–	–	+	+	OCSP
tbb.ee	4	require	3	–	+	–	–*	OCSP
unicreditbank.ee	0	require	5	–	–	+	?	?
versobank.com	0	optional	3	40 sec	–	+	?	?
Education:								
e-ope.ee	4	optional	3	–	–	+	+	–
eek.ee	0	require	2	–	+	–	?	?
ekool.eu	0	optional	2	–*	+	–	–	–
emu.ee	0	require	2	–	+	–	–	OCSP 2007
tlu.ee	0	require	2	9 hour	–	+	–	?
Government:								
ariregister.rik.ee	0	optional	6	–	+	–	–	CRL
digidoc.sk.ee	4	require	2	–	+	–	–	OCSP
e-register.ee	0	require	3	–	+	–	–	OCSP
e-toimik.ee	0	optional	2	–	+	–	–	OCSP
eesti.ee	5	require	2	–*	+	–	–	OCSP
emta.ee	0	optional	3	–	–	+	–	OCSP

"Practical Issues with TLS Client Certificate Authentication"
(`https://eprint.iacr.org/2013/538.pdf`)

Tasks

Tasks

- Study the paper “Practical Issues with TLS Client Certificate Authentication”

Tasks

- Study the paper “Practical Issues with TLS Client Certificate Authentication”
- In your report describe:

Tasks

- Study the paper "Practical Issues with TLS Client Certificate Authentication"
- In your report describe:
  - what TLS CCA configuration options could be tested

Tasks

- Study the paper "Practical Issues with TLS Client Certificate Authentication"
- In your report describe:
  - what TLS CCA configuration options could be tested
  - what scores should be assigned to the tests

Tasks

- Study the paper "Practical Issues with TLS Client Certificate Authentication"
- In your report describe:
  - what TLS CCA configuration options could be tested
  - what scores should be assigned to the tests
  - describe how the tests could be implemented in an automated manner

Tasks

- Study the paper "Practical Issues with TLS Client Certificate Authentication"
- In your report describe:
  - what TLS CCA configuration options could be tested
  - what scores should be assigned to the tests
  - describe how the tests could be implemented in an automated manner
  - sketch GUI of example test result

Tasks

- Study the paper "Practical Issues with TLS Client Certificate Authentication"
- In your report describe:
  - what TLS CCA configuration options could be tested
  - what scores should be assigned to the tests
  - describe how the tests could be implemented in an automated manner
  - sketch GUI of example test result
- For an example refer to "SSL Server Rating Guide"