

Macoun

Applied Crypto Hardening

@MacLemon

System-Administration

Datenschutz & Privatsphäre

Sicher nach iOS

Macoun 2011, Klaus M. Rodewig

Torwächter und Schlüsselmeister

2012, @MacLemon

NSURLConnection: Safety First!

Macoun 2013, Alex v. Below, @MacLemon

Datenschutz und Apps

Macoun 2014, Thomas Biedorf

Samstag, 15:00, kleiner Saal

Sicher ganz einfach

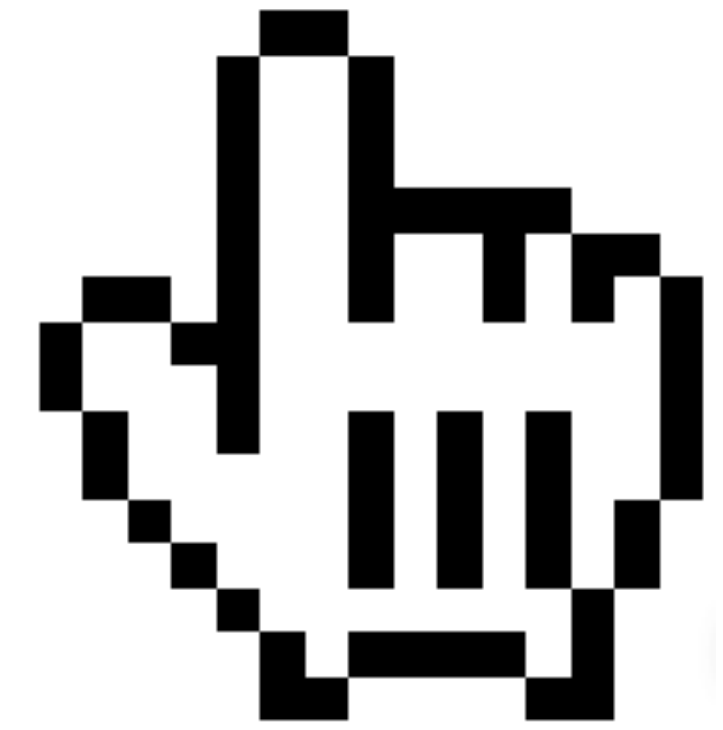
Macoun 2014, Klaus M. Rodewig

Sonntag, 11:00, Terrassensaal

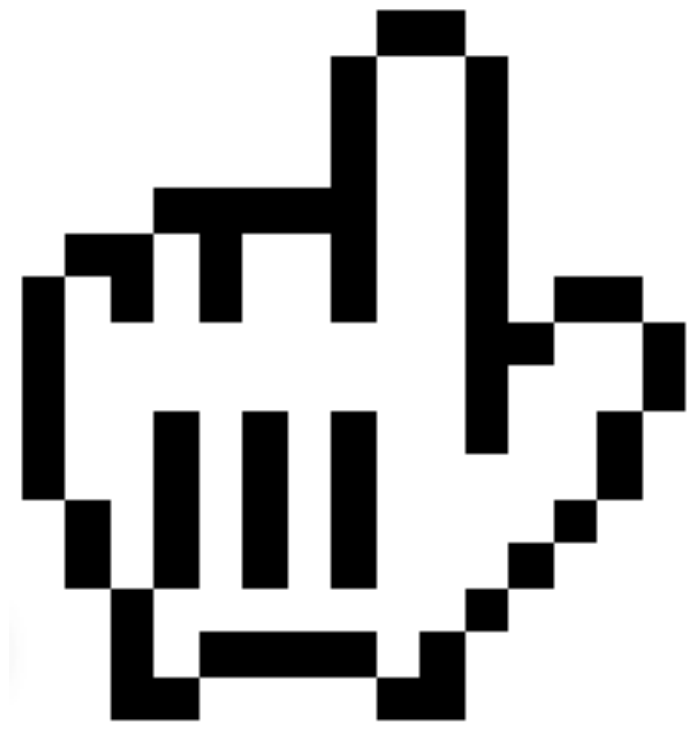
Datenschutz

Gespeicherte Daten

Daten in Bewegung



Deine Apps



Deine Infrastruktur

Stundenwiederholung

Verschlüsselung

Vier Ziele



Vertraulichkeit

2 Integrität

Authentizität

4 Nichtabstreitbarkeit

Geschichte

SSLv1

1994

1970

2014



SSLv2

1995

1970

2014



SSLv3

1996

1970

2014



TLS 1.0



TLS 1.1



TLS 1.2



Transportverschlüsselung

TLS 1.2

TLS 1.1

TLS 1.0

~~SSLv3~~

~~SSLv2~~

OS X Support 10.6 - 10.8

TLS 1.2

TLS 1.1

TLS 1.0

~~SSLv3~~

~~SSLv2~~

OS X Support 10.9+

TLS 1.2

TLS 1.1

TLS 1.0

~~SSLv3~~

~~SSLv2~~

iOS Support seit 5.0

TLS 1.2

TLS 1.1

TLS 1.0

~~SSLv3~~

~~SSLv2~~



<http://istheinternetonfire.com/>

Yep.

Weitergehen...



<https://isitchristmas.com/>

NEIN

Voraussetzungen

RSA Schlüsselpaar

4096bit

Zertifikat

SHA-256

Server

Konfiguration

Ciphersuites

TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
DHE-RSA-AES256-GCM-SHA384

\$ openssl ciphers ALL

ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA:ECDHE-ECDSA-AES256-SHA:SRP-DSS-AES-256-CBC-SHA:SRP-RSA-AES-256-CBC-SHA:SRP-AES-256-CBC-SHA:DHE-DSS-AES256-GCM-SHA384:DHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES256-SHA256:DHE-DSS-AES256-SHA256:DHE-RSA-AES256-SHA:DHE-DSS-AES256-SHA:DHE-RSA-CAMELLIA256-SHA:DHE-DSS-CAMELLIA256-SHA:AECDH-AES256-SHA:ADH-AES256-GCM-SHA384:ADH-AES256-SHA256:ADH-AES256-SHA:ADH-CAMELLIA256-SHA:ECDH-RSA-AES256-GCM-SHA384:ECDH-ECDSA-AES256-GCM-SHA384:ECDH-RSA-AES256-SHA384:ECDH-ECDSA-AES256-SHA384:ECDH-RSA-AES256-SHA:ECDH-ECDSA-AES256-SHA:AES256-GCM-SHA384:AES256-SHA256:AES256-SHA:CAMELLIA256-SHA:PSK-AES256-CBC-SHA:ECDHE-RSA-DES-CBC3-SHA:ECDHE-ECDSA-DES-CBC3-SHA:SRP-DSS-3DES-EDE-CBC-SHA:SRP-RSA-3DES-EDE-CBC-SHA:SRP-3DES-EDE-CBC-SHA:EDH-RSA-DES-CBC3-SHA:EDH-DSS-DES-CBC3-SHA:AECDH-DES-CBC3-SHA:ADH-DES-CBC3-SHA:ECDH-RSA-DES-CBC3-SHA:ECDH-ECDSA-DES-CBC3-SHA:DES-CBC3-SHA:PSK-3DES-EDE-CBC-SHA:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-SHA256:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA:ECDHE-ECDSA-AES128-SHA:SRP-DSS-AES-128-CBC-SHA:SRP-RSA-AES-128-CBC-SHA:SRP-AES-128-CBC-SHA:DHE-DSS-AES128-GCM-SHA256:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES128-SHA256:DHE-DSS-AES128-SHA256:DHE-RSA-AES128-SHA:DHE-DSS-AES128-SHA:DHE-RSA-SEED-SHA:DHE-DSS-SEED-SHA:DHE-RSA-CAMELLIA128-SHA:DHE-DSS-CAMELLIA128-SHA:AECDH-AES128-SHA:ADH-AES128-GCM-SHA256:ADH-AES128-SHA256:ADH-AES128-SHA:ADH-SEED-SHA:ADH-CAMELLIA128-SHA:ECDH-RSA-AES128-GCM-SHA256:ECDH-ECDSA-AES128-GCM-SHA256:ECDH-RSA-AES128-SHA256:ECDH-ECDSA-AES128-SHA256:ECDH-RSA-AES128-SHA:ECDH-ECDSA-AES128-SHA:AES128-GCM-SHA256:AES128-SHA256:AES128-SHA:SEED-SHA:CAMELLIA128-SHA:PSK-AES128-CBC-SHA:ECDHE-RSA-RC4-SHA:ECDHE-ECDSA-RC4-SHA:AECDH-RC4-SHA:ADH-RC4-MD5:ECDH-RSA-RC4-SHA:ECDH-ECDSA-RC4-SHA:RC4-SHA:RC4-MD5:PSK-RC4-SHA:EDH-RSA-DES-CBC-SHA:EDH-DSS-DES-CBC-SHA:ADH-DES-CBC-SHA:DES-CBC-SHA:EXP-EDH-RSA-DES-CBC-SHA:EXP-EDH-DSS-DES-CBC-SHA:EXP-ADH-DES-CBC-SHA:EXP-DES-CBC-SHA:EXP-RC2-CBC-MD5:EXP-ADH-RC4-MD5:EXP-RC4-MD5

DHE-RSA-AES256-GCM-SHA384 : DHE-RSA-AES256-SHA256 : ECDHE-RSA-AES256-GCM-SHA384 : ECDHE-RSA-AES256-SHA384 : DHE-RSA-CAMELLIA256-SHA : DHE-RSA-AES256-SHA : ECDHE-RSA-AES256-SHA

Testen

https*secure*

http*stinkt*

Testen

Testen, Testen, Testen

Webserver

<https://SSLLabs.com/>

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.**

Domain name:

☐ Do not show the results on the boards

Recently Seen

[opdrachtenregister.org](#)

[horisen.info](#)

[irphe.fr](#)

[fsf.org](#)

Recent Best

[cofone.org](#)

A+

[fischer-markenschuh.net](#)

A

[sip.fiskeridir.no](#)

A

[s2.derky.nl](#)

A

Recent Worst

[tasklifecycle.de](#)

F

[fbnhffmnn.de](#)

F

[asurion.com](#)

F

[enescousa.com](#)

F

You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > macoun.de

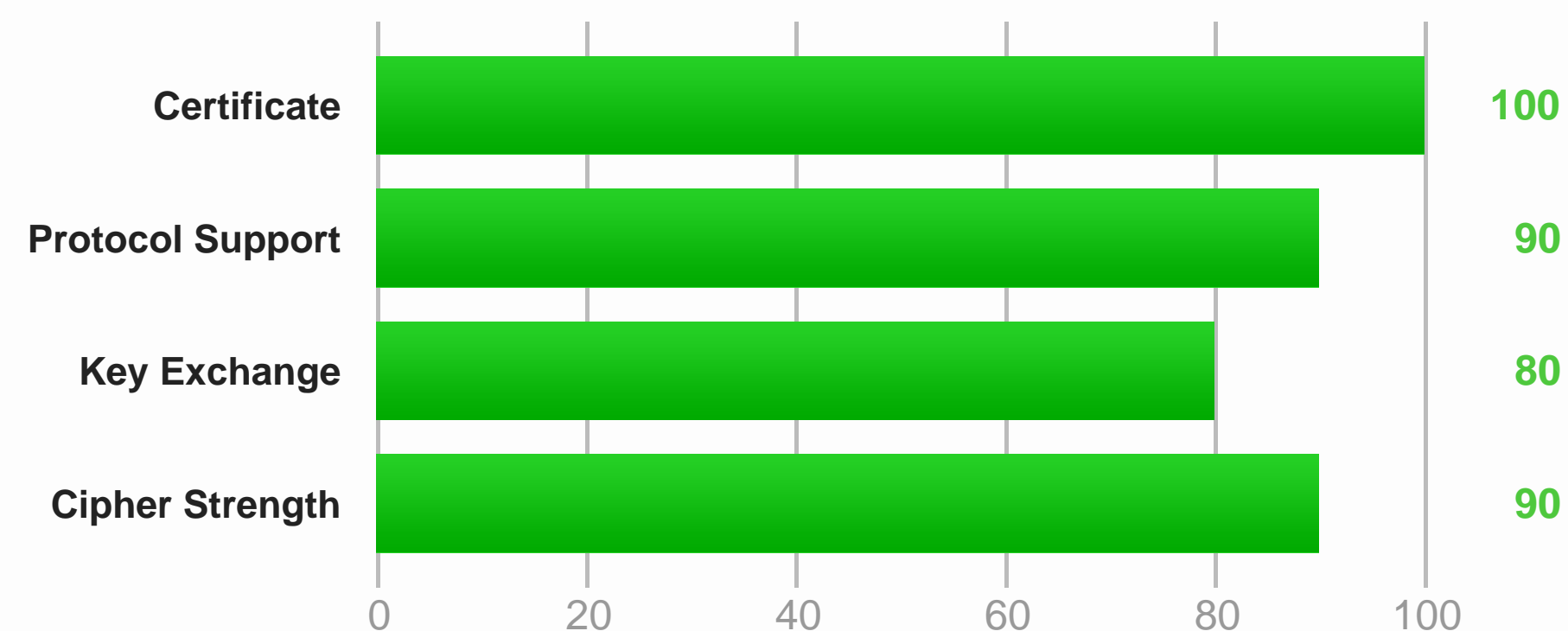
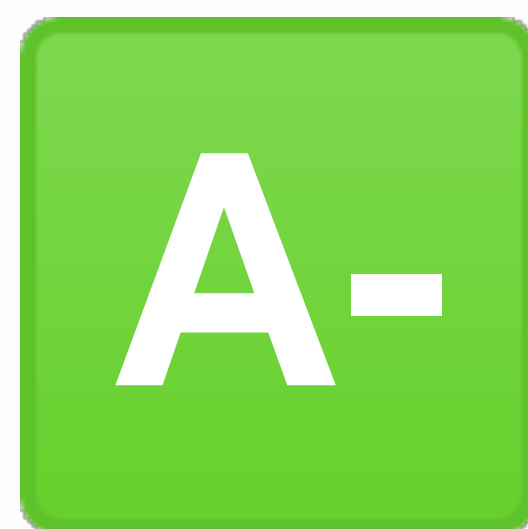
SSL Report: macoun.de (95.143.172.231)

Assessed on: Sat Sep 27 00:19:12 UTC 2014 | **HIDDEN** | [Clear cache](#)

[Scan Another »](#)

Summary

Overall Rating



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

Certificate uses SHA1. When renewing, ensure you upgrade to SHA256. [MORE INFO »](#)

The server does not support Forward Secrecy with the reference browsers. Grade reduced to A-. [MORE INFO »](#)

This site works only in browsers with SNI support.

Configuration



Protocols

| | |
|--------------------|-----|
| TLS 1.2 | Yes |
| TLS 1.1 | Yes |
| TLS 1.0 | Yes |
| SSL 3 ² | Yes |
| SSL 2 | No |

(2) This site requires support for virtual SSL hosting, but SSL 2.0 and SSL 3.0 do not support this feature.



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

| | |
|--|-----|
| TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f) DH 1024 bits (p: 128, g: 1, Ys: 128) FS | 256 |
| TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x6b) DH 1024 bits (p: 128, g: 1, Ys: 128) FS | 256 |
| TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) DH 1024 bits (p: 128, g: 1, Ys: 128) FS | 256 |
| TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0x88) DH 1024 bits (p: 128, g: 1, Ys: 128) FS | 256 |
| TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x0a) DH 1024 bits (p: 128, g: 1, Ys: 128) FS | 128 |



Handshake Simulation

| | | | | |
|--|-----------------------------------|--|-------|-------------------|
| Android 2.3.7 No SNI ² | TLS 1.0 | TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33) | FS | 128 |
| Android 4.0.4 | TLS 1.0 | TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) | FS | 256 |
| Android 4.1.1 | TLS 1.0 | TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) | FS | 256 |
| Android 4.2.2 | TLS 1.0 | TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) | FS | 256 |
| Android 4.3 | TLS 1.0 | TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) | FS | 256 |
| Android 4.4.2 | TLS 1.2 | TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f) | FS | 256 |
| BingBot Dec 2013 No SNI ² | TLS 1.0 | TLS_RSA_WITH_AES_256_CBC_SHA (0x35) | No FS | 256 |
| BingPreview Jun 2014 | TLS 1.0 | TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) | FS | 256 |
| Chrome 36 / Win 7 R | TLS 1.2 | TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) | FS | 256 |
| Firefox 24.2.0 ESR / Win 7 | TLS 1.0 | TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) | FS | 256 |
| Firefox 31 / OS X R | TLS 1.2 | TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) | FS | 256 |
| Googlebot Jun 2014 | TLS 1.0 | TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) | FS | 256 |
| IE 6 / XP No FS ¹ No SNI ² | Protocol or cipher suite mismatch | | | Fail ³ |
| IE 7 / Vista | TLS 1.0 | TLS_RSA_WITH_AES_256_CBC_SHA (0x35) | No FS | 256 |
| IE 8 / XP No FS ¹ No SNI ² | Protocol or cipher suite mismatch | | | Fail ³ |

| | |
|---|---|
| Secure Client-Initiated Renegotiation | No |
| Insecure Client-Initiated Renegotiation | No |
| BEAST attack | Not mitigated server-side (more info) SSL 3: 0x39, TLS 1.0: 0x39 |
| TLS compression | No |
| RC4 | No |
| Heartbeat (extension) | Yes |
| Heartbleed (vulnerability) | No (more info) |
| OpenSSL CCS vuln. (CVE-2014-0224) | No (more info) |
| Forward Secrecy | With some browsers (more info) |
| Next Protocol Negotiation | No |
| Session resumption (caching) | Yes |
| Session resumption (tickets) | Yes |
| OCSP stapling | No |
| Strict Transport Security (HSTS) | No |
| Long handshake intolerance | No |
| TLS extension intolerance | No |
| TLS version intolerance | TLS 2.98 |
| SSL 2 handshake compatibility | Yes |

You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > nsa.gov

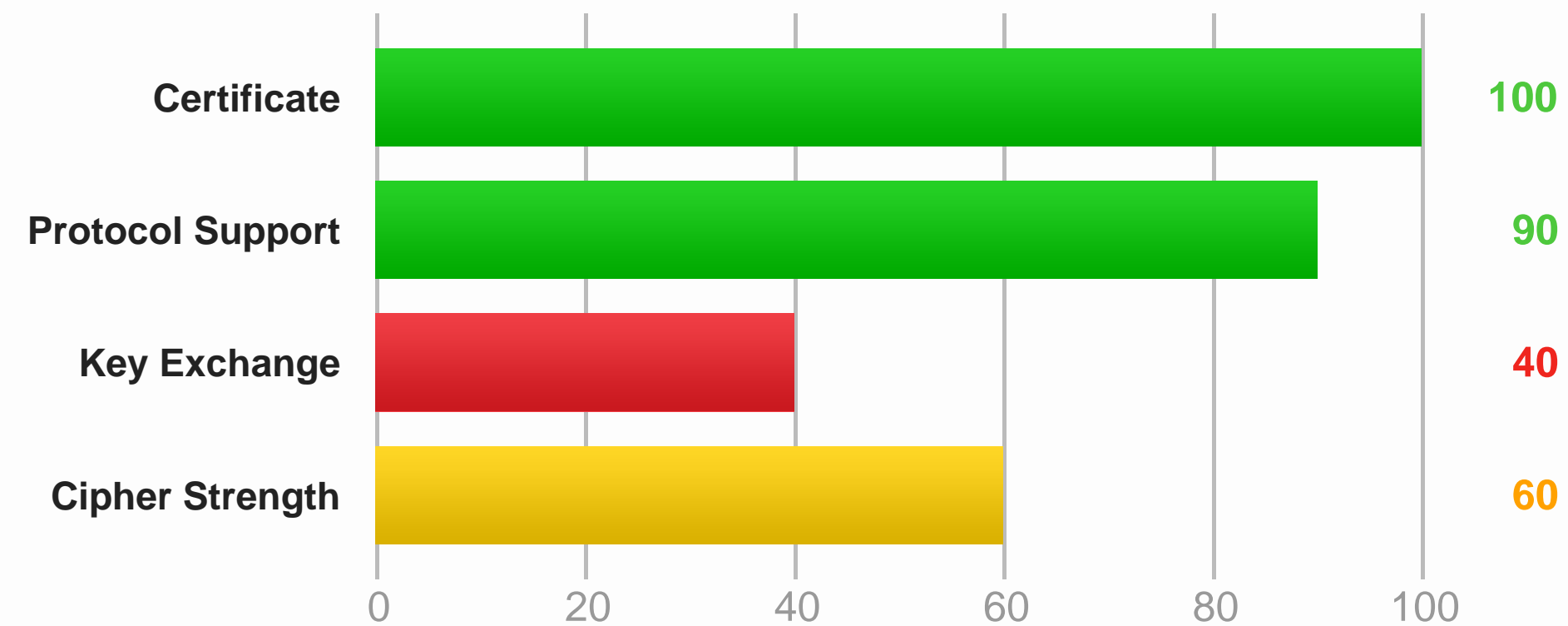
SSL Report: nsa.gov (23.39.50.161)

Assessed on: Fri Sep 26 18:23:02 UTC 2014 | [Clear cache](#)

[Scan Another »](#)

Summary

Overall Rating



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

Certificate uses SHA1. When renewing, ensure you upgrade to SHA256. [MORE INFO »](#)

The server does not support Forward Secrecy with the reference browsers. [MORE INFO »](#)

You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > openbsd.org

SSL Report: openbsd.org (129.128.5.194)

Assessed on: Fri Sep 26 13:36:00 UTC 2014 | **HIDDEN** | [Clear cache](#)

[Scan Another »](#)

Assessment failed: Unable to connect to 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

You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > openbsd.org

SSL Report: openbsd.org (129.128.5.194)

Assessed on: Fri Sep 26 13:36:00 UTC 2014 | **HIDDEN** | [Clear cache](#)

[Scan Another »](#)

Assessment failed: Unable to connect to 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



<https://isitchristmas.com/>

You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > isitchristmas.com

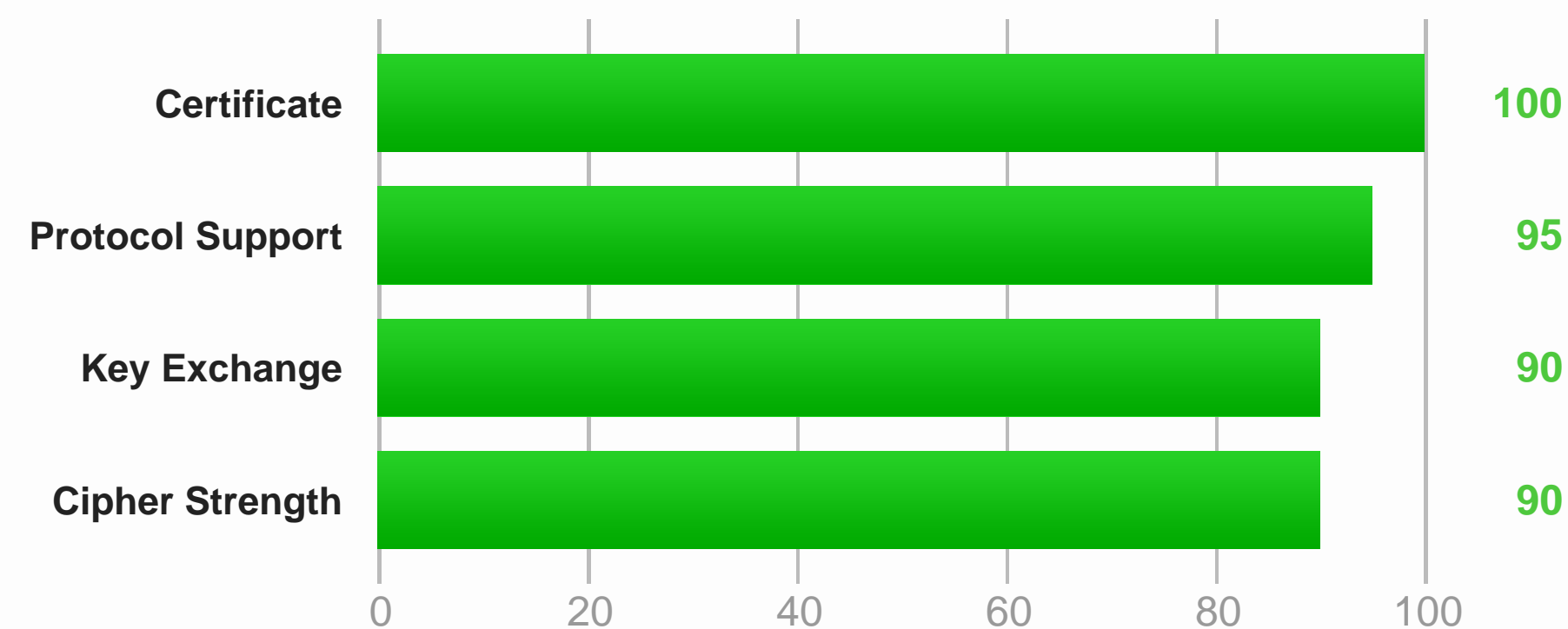
SSL Report: isitchristmas.com (54.235.64.112)

Assessed on: Mon Jul 28 06:42:17 UTC 2014 | [Clear cache](#)

[Scan Another »](#)

Summary

Overall Rating



Documentation: [SSL/TLS Deployment Best Practices](#), [SSL Server Rating Guide](#), and [OpenSSL Cookbook](#).

This server supports HTTP Strict Transport Security with long duration. Grade set to A+. [MORE INFO »](#)

This server is not vulnerable to the [Heartbleed attack](#).

Experimental: This server is not vulnerable to the OpenSSL CCS vulnerability (CVE-2014-0224).

You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > ecb.europa.eu

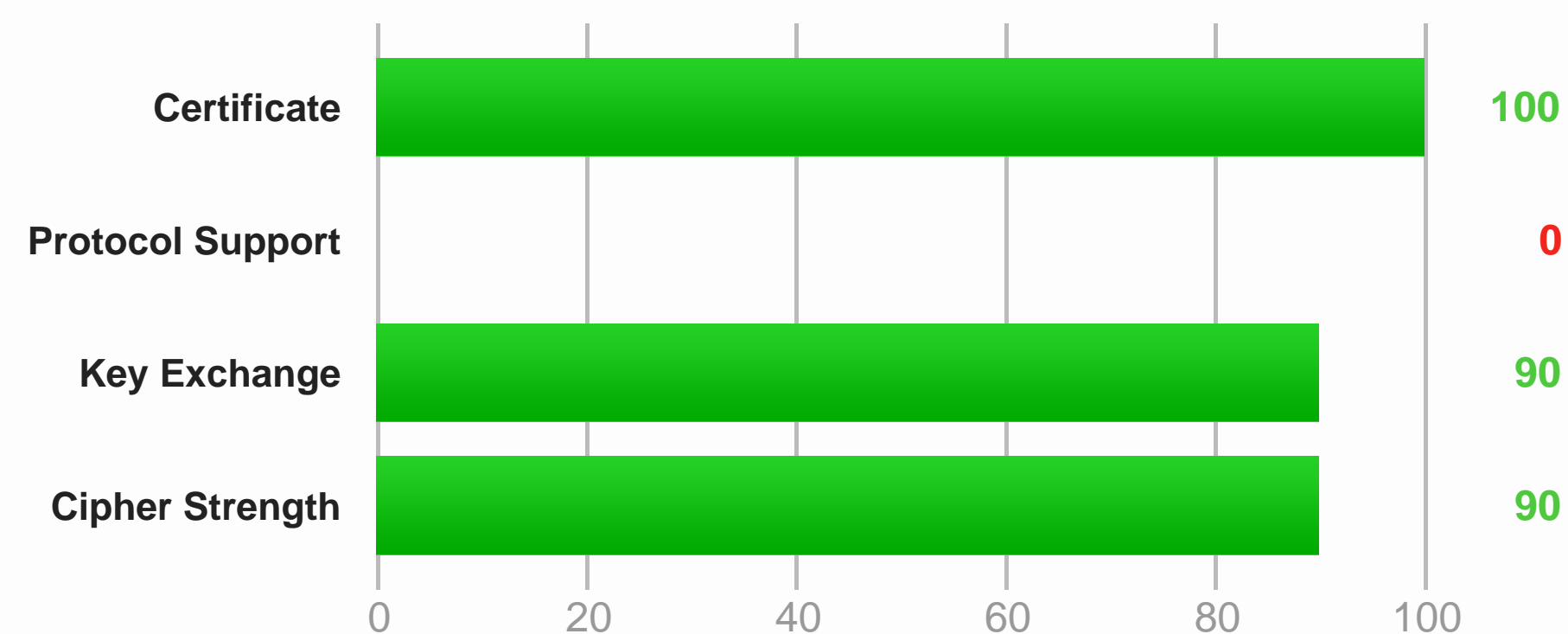
SSL Report: ecb.europa.eu (184.25.151.166)

Assessed on: Sat Sep 27 00:27:51 UTC 2014 | **HIDDEN** | [Clear cache](#)

[Scan Another »](#)

Summary

Overall Rating



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

This server supports SSL 2, which is obsolete and insecure. Grade set to F.

Certificate uses SHA1. When renewing, ensure you upgrade to SHA256. [MORE INFO »](#)

The server does not support Forward Secrecy with the reference browsers. [MORE INFO »](#)

Configuration



Protocols

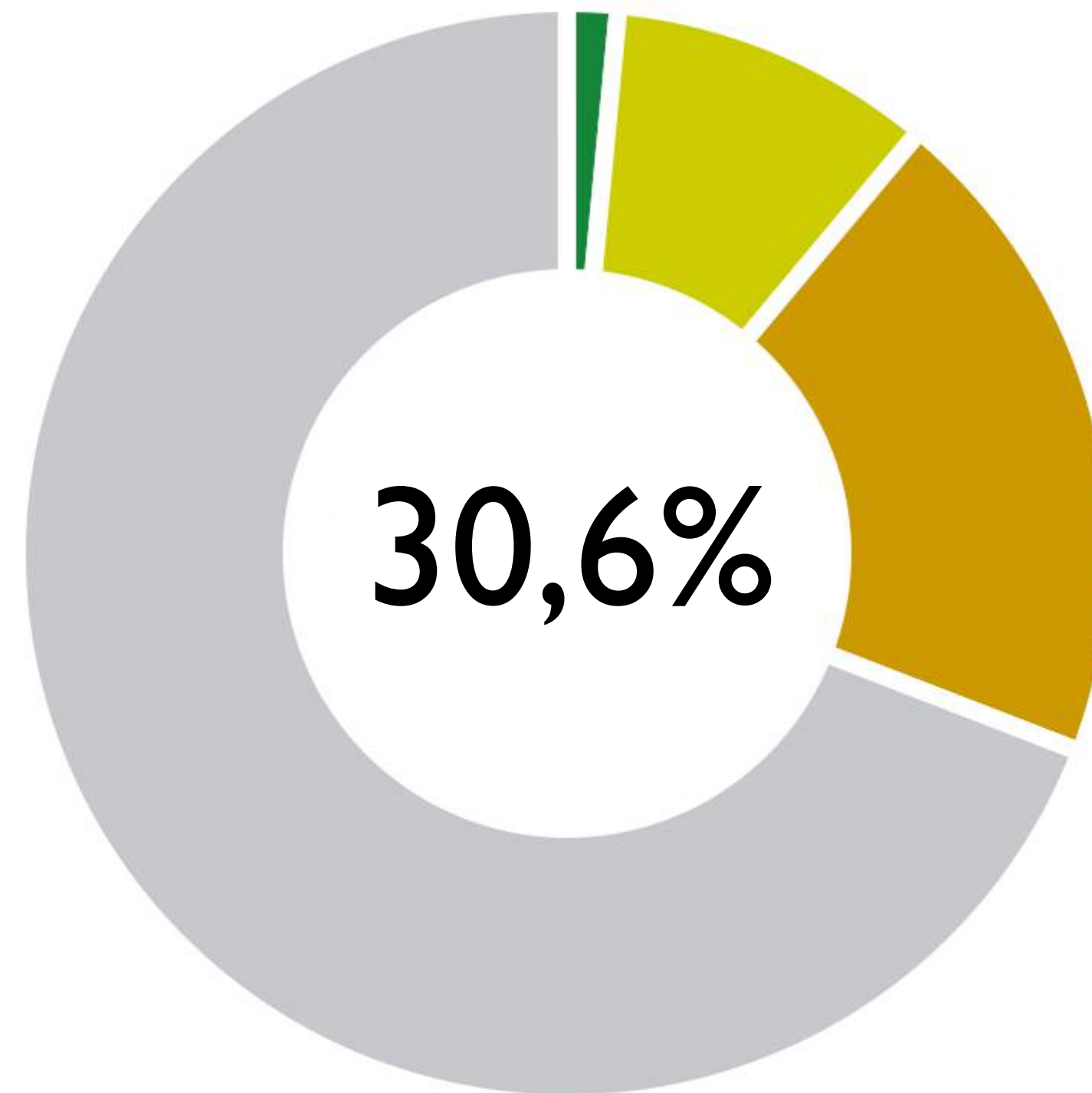
| | |
|----------------|-----|
| TLS 1.2 | Yes |
| TLS 1.1 | Yes |
| TLS 1.0 | Yes |
| SSL 3 | Yes |
| SSL 2 INSECURE | Yes |



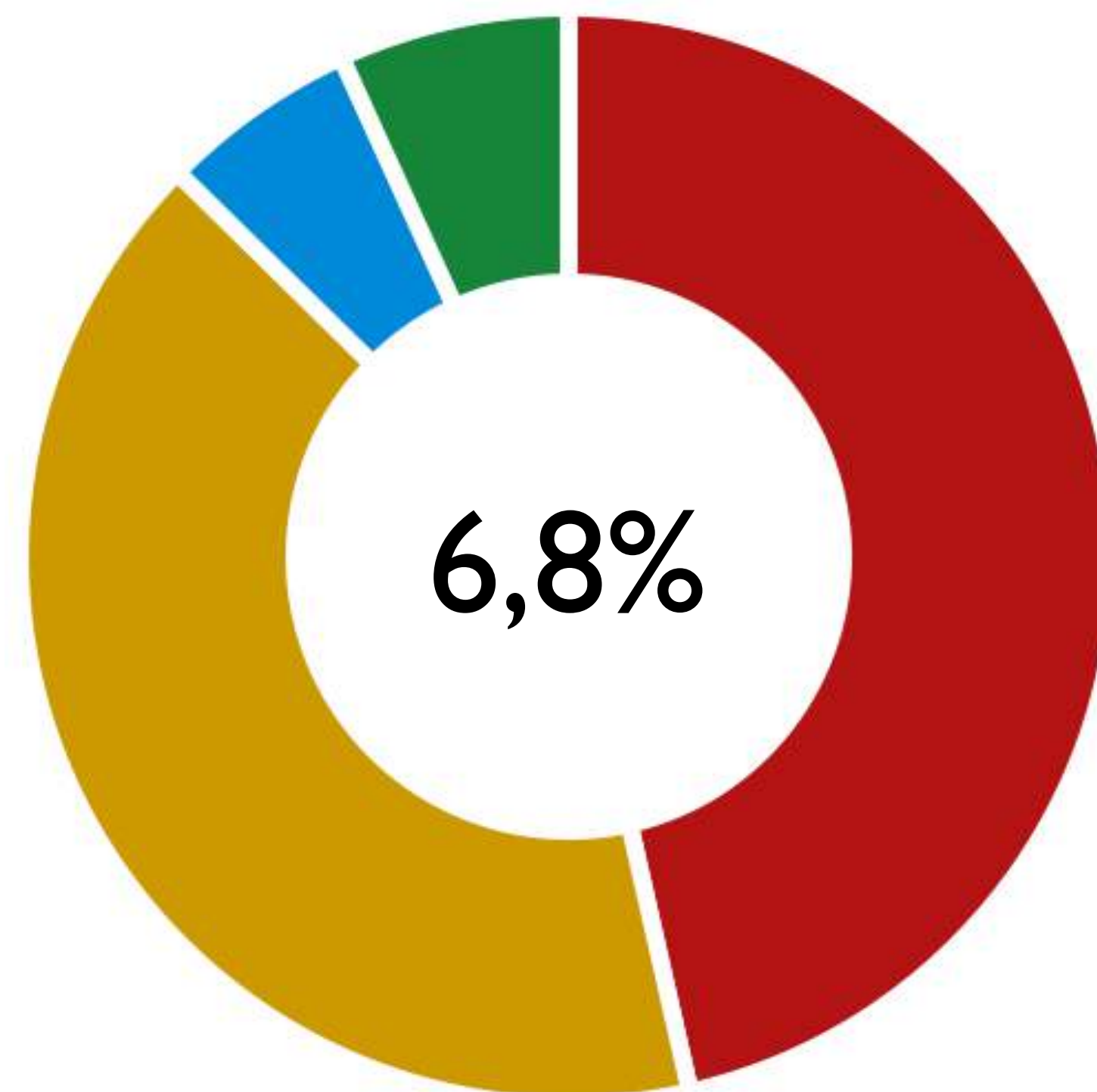
Cipher Suites (SSL 3+ suites in server-preferred order; deprecated and SSL 2 suites always at the end)

| | |
|--|-----|
| TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) | 128 |
| TLS_RSA_WITH_AES_256_CBC_SHA (0x35) | 256 |
| TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa) | 112 |
| TLS_RSA_WITH_RC4_128_MD5 (0x4) | 128 |
| TLS_RSA_WITH_RC4_128_SHA (0x5) | 128 |
| SSL CK RC4_128_WITH_MD5 (0x10080) INSECURE | 128 |

Sichere Seiten



Forward Secrecy



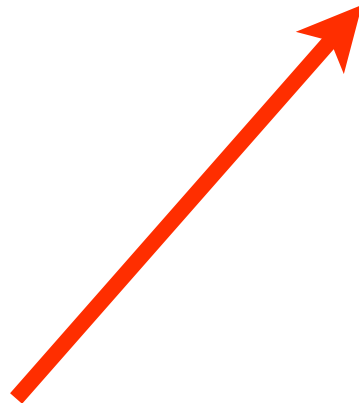
DHE

ECDHE

~~RC4~~

Email

<https://starttls.info/>



Does your mail server support STARTTLS?

If you care about privacy, it should. Read more in the [blog](#).

Test it!

This site is a beta. | Read [about this](#). | Check the [stats](#).

Developed by [Einar Otto Stangvik](#).

Does your mail server support STARTTLS?

If you care about privacy, it should. Read more in the [blog](#).

Results for: macoun.de



Mail server

Result

macoun.de

Grade: B (76.0%)



Certificate

- The certificate is not valid for the server's hostname.

There are validity issues for the certificate. Certificates are seldom verified for SMTP servers, so this doesn't mean that STARTTLS won't be used.

Generally speaking it's a bad practice not to have a valid certificate, and an even worse practice not to verify them. Any attempted encrypted communication is left all but wide open to Man-in-the-Middle attacks.

Does your mail server support STARTTLS?

If you care about privacy, it should. Read more in the [blog](#).

Results for: **ubermorgen.com**



| Mail server | Result |
|-----------------------|---------------------------|
| ubermorgen.com | Grade: A (93.4%) ▼ |

Certificate

- No remarks.

Protocol

- Supports SSLV3.
- Supports TLSV1.
- Supports TLSV1.1.
- Supports TLSV1.2.

Key exchange

- Key size is 4096 bits; that's very good.

Cipher

- Weakest accepted cipher: 128.
- Strongest accepted cipher: 256.

Click the score for details.

[Test another!](#)

This site is a beta. | Read [about this](#). | Check the [stats](#).

Developed by [Einar Otto Stangvik](#).

Does your mail server support STARTTLS?

If you care about privacy, it should. Read more in the [blog](#).

Results for: bnd.bund.de



| Mail server | Result |
|-------------|--------------------|
| mx2.bund.de | Grade: D (44.3%) ▼ |

Certificate

- There is a self-signed certificate in the trust chain. It may be a configuration problem.
- There are one or more fatal problems which causes the certificate not to be trusted.

There are validity issues for the certificate. Certificates are seldom verified for SMTP servers, so this doesn't mean that STARTTLS won't be used.

Generally speaking it's a bad practice not to have a valid certificate, and an even worse practice not to verify them. Any attempted encrypted communication is left all but wide open to Man-in-the-Middle attacks.

Protocol

- Supports SSLV3.
- Supports TLSV1.

Key exchange

- Anonymous Diffie-Hellman is accepted. This is susceptible to Man-in-the-Middle attacks.
- Key size is 2048 bits; that's good.

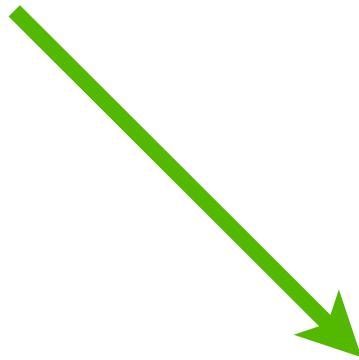
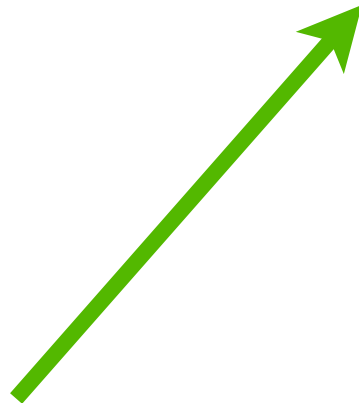
Cipher

- Weakest accepted cipher: 0.
- Strongest accepted cipher: 256.

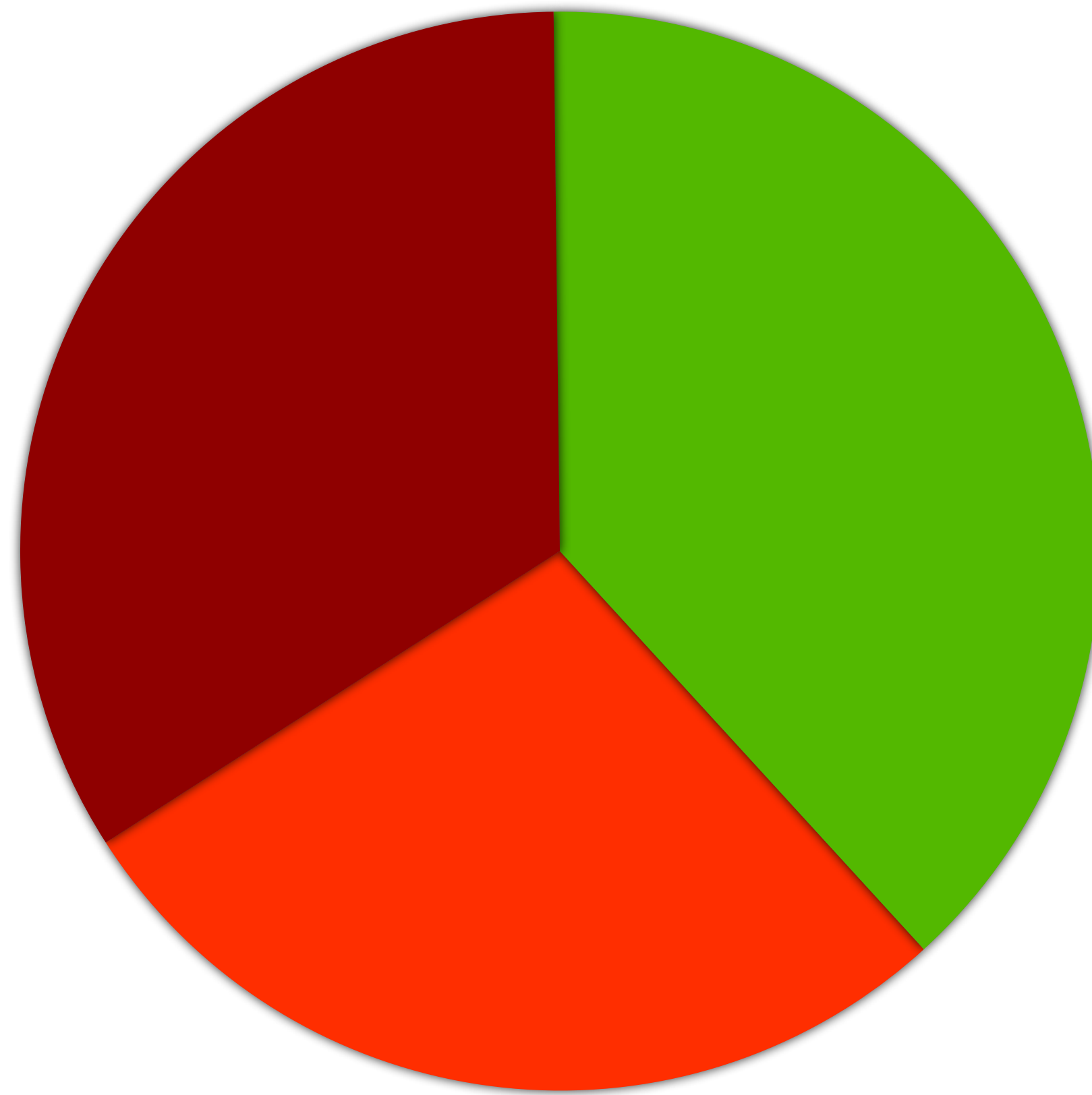
| | |
|-------------|--------------------|
| mx1.bund.de | Grade: D (44.3%) ▼ |
|-------------|--------------------|

Click the score for details.

[Test another!](#)



<https://starttls.info/stats>



38%

Chat

<https://xmpp.net/>

[Score](#)[General](#)[DNS](#)[TLS](#)

IM Observatory client report for jabber.maclemon.at

Test started 2014-09-20 20:38:05 UTC 28 minutes ago.

[Show server to server result](#) | [Permalink to this report](#)

Score

jabber.maclemon.at:5222

Certificate score:



100

Key exchange
score:



100

Protocol score:



95

Cipher score:



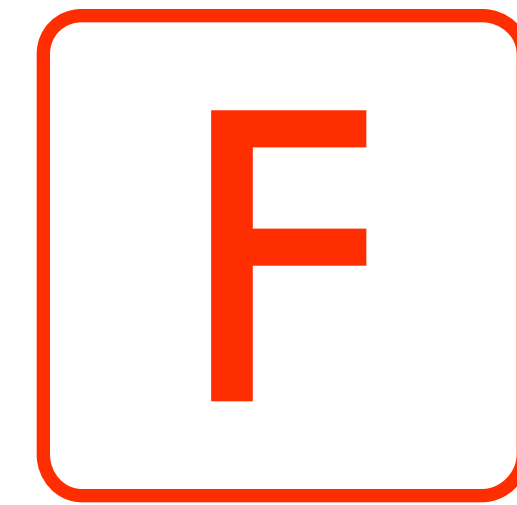
90

Grade:

A



Handlungsbedarf



Verschlüsselung muß Standard sein!





Praktische Einstellungen

Kopieren/Einsetzen

Server Tests

Webserver

Mailserver

Schlüssel

Verfahren

Zufallszahlen

VPN

SSH

PGP/GnuPG

Instant Messaging

Datenbanken







Hausübung

Teste ALLE Server

TLS 1.2 überall

Forward Secrecy

Nur noch verschlüsselte Kommunikation

Fragen?

Links

Applied Crypto Hardening Guide: [https://BetterCrypto.org/
Webseiten/API](https://BetterCrypto.org/Webseiten/API) mit [https: https://SSLLabs.com/](https://SSLLabs.com/)
Mailserver TLS: <https://StartTLS.com/>
Jabber/XMPP TLS: <https://xmpp.net/>



Pepi Zawodsky: <https://MacLemon.at/>
Twitter, ADN @MacLemon

Macoun Referenzen

- 2011: Sicher nach iOS - Klaus M. Rodewig
- 2012: Torwächter und Schlüsselmeister, Pepi Zawodsky
- 2013: NSURLConnection: Safety First! - Alexander von Below
- 2014: Applied Crypto Hardening - Pepi Zawodsky
- 2014: Datenschutz und Apps - Thomas Biedorf
- 2014: Sicher ganz einfach - Klaus M. Rodewig

Danke

Quellennachweis:

Folie Nr.; Titel; Urheber; Datum; Quelle/Link. Rechte.

I: „Macoun Logo“; Chris Hauser; 2009; Macoun GbR.
Unentgeltliche Nutzung im Rahmen der Veranstaltung und Berichterstattung gestattet.

Hand Icon: CC-BY-SA-NC, 3.0 Unported Pepi Zawodsky

Fire Emoji: UTF-8 Character Code F0 9F 94 A5

Christmal Tree Emoji: UTF-8 Character Code F0 9F 8E 84

<https://SSLLabs.com> Screenshots: Used with Permission by Ivan Ristić, erstellt von Pepi Zawodsky

<https://StartTLS.info> Screenshots: Used with Permission by Einar Otto Stangvik, erstellt von Pepi Zawodsky

<https://BetterCrypto.org> Logo, Screenshots und Inhalte: CC-BY-SA 3.0 unported

Hiermit erteilt Pepi Zawodsky Ihnen das einfache, räumlich und zeitlich unbeschränkte Nutzungsrecht, das MacLemon Logo auf beliebige Weise unentgeltlich in beliebigen Medien, Printmedien, Videos, sowie digitale Medien, einschließlich des Internets, zu nutzen. Eine Übertragung des Nutzungsrechts an Dritte ist nicht gestattet.

TLS_DHE_RSA_WITH_AES_256_GCM_SHA384