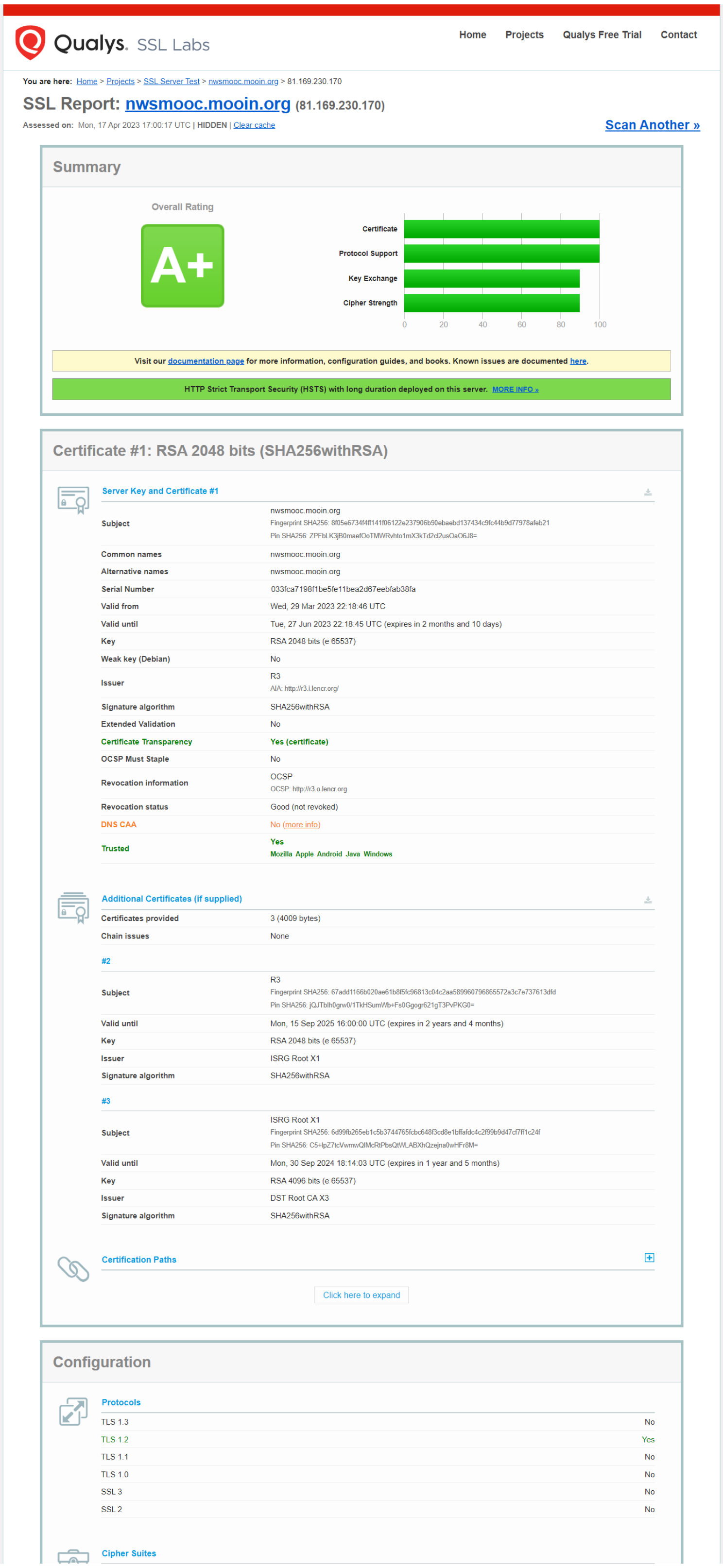
Aufgabe A

Testen Sie den Server nwsmooc.mooin.org mit der SSL-Testseite von Qualys und erklären Sie die Ergebnisse. Erklären Sie für eine weitere Webpräsenz, die als "Recent Worst" bewertet wird, was bei dieser nicht stimmt. "Recent Worst" ist eine Liste auf der rechten Seite der Testseite. Zur besseren Nachvollziehbarkeit bitte Screenshots hinzufügen.

Antwort

Ergebnisse für `nwsmooc.mooin.org`:

Allgemeines Rating A+.



You are here: Home > Projects > SSL Server Test > nwsmooc.mooin.org > 81.169.230.170

SSL Report: nwsmooc.mooin.org (81.169.230.170)

Assessed on: Mon, 17 Apr 2023 17:00:17 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.

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

Certificate #1: RSA 2048 bits (SHA256withRSA)

Server Key and Certificate #1

Subject	nwsmooc.mooin.org Fingerprint SHA256: 8f05e6734f4ff141f06122e237906b90ebaebd137434c9fc44b9d77978afeb21 Pin SHA256: ZPFbLK3jB0maefOoTMWRvhto1mX3kTd2cl2usOaO6J8=
Common names	nwsmooc.mooin.org
Alternative names	nwsmooc.mooin.org
Serial Number	033fca7198f1be5fe11bea2d67eebfab38fa
Valid from	Wed, 29 Mar 2023 22:18:46 UTC
Valid until	Tue, 27 Jun 2023 22:18:45 UTC (expires in 2 months and 10 days)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	R3 AIA: http://r3.i.lencr.org/
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	Yes (certificate)
OCSP Must Staple	No
Revocation information	OCSP OCSP: http://r3.o.lencr.org
Revocation status	Good (not revoked)
DNS CAA	No (more info)
Trusted	Yes Mozilla Apple Android Java Windows

Additional Certificates (if supplied)

Certificates provided	3 (4009 bytes)
Chain issues	None
#2	
Subject	R3 Fingerprint SHA256: 67add1166b020ae61b8f5fc96813c04c2aa589960796865572a3c7e737613dfd Pin SHA256: jQJTbIh0grw0/1TkHSumWb+Fs0Ggogr621gT3PvPKG0=
Valid until	Mon, 15 Sep 2025 16:00:00 UTC (expires in 2 years and 4 months)
Key	RSA 2048 bits (e 65537)
Issuer	ISRG Root X1
Signature algorithm	SHA256withRSA
#3	
Subject	ISRG Root X1 Fingerprint SHA256: 6d99fb265eb1c5b3744765fcbc648f3cd8e1bffafdc4c2f99b9d47cf7ff1c24f Pin SHA256: C5+lpZ7tcVwmwQIMcRtPbsQtWLABXhQzejna0wHFr8M=
Valid until	Mon, 30 Sep 2024 18:14:03 UTC (expires in 1 year and 5 months)
Key	RSA 4096 bits (e 65537)
Issuer	DST Root CA X3
Signature algorithm	SHA256withRSA

Certification Paths

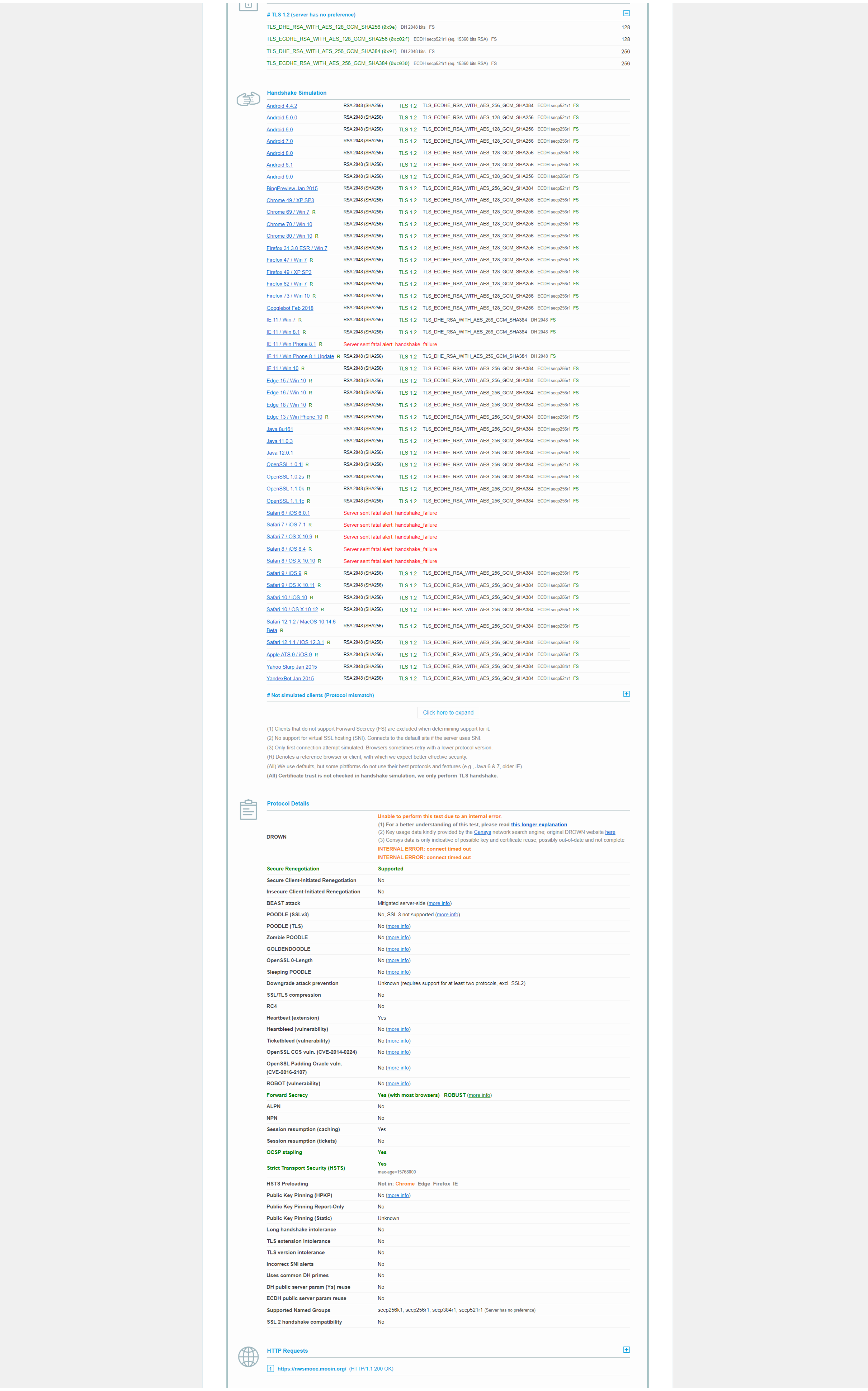
Click here to expand

Configuration

Protocols

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

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 secp521r1 (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 secp521r1 (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	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Android 7.0	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Android 8.0	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Android 8.1	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Android 9.0	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
BingPreview Jan 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp521r1 FS
Chrome 49 / XP SP3	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Chrome 69 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Chrome 70 / Win 10	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Chrome 80 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2	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	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Firefox 49 / XP SP3	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Firefox 62 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Firefox 73 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2	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	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	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	DH 2048 FS
IE 11 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
Edge 15 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
Edge 16 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
Edge 18 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
Edge 13 / Win Phone 10 R	RSA 2048 (SHA256)	TLS 1.2	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 secp521r1 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	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
Safari 9 / OS X 10.11 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
Safari 10 / iOS 10 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
Safari 10 / OS X 10.12 R	RSA 2048 (SHA256)	TLS 1.2	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	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	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
Apple ATS 9 / iOS 9 R	RSA 2048 (SHA256)	TLS 1.2	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 secp521r1 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).

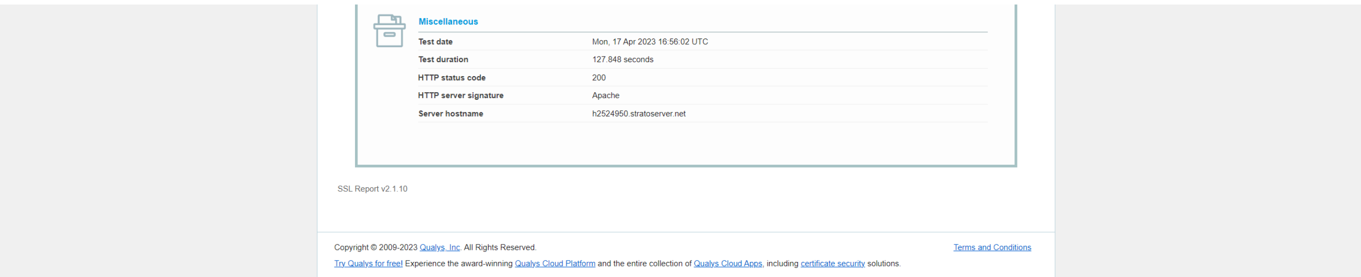
(All) Certificate trust is not checked in handshake simulation, we only perform TLS handshake.

Protocol Details

DROWN	**Unable to perform this test due to an internal error.** **(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 not complete **INTERNAL ERROR: connect timed out** **INTERNAL ERROR: connect timed out**
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	No
NPN	No
Session resumption (caching)	Yes
Session resumption (tickets)	No
OCSP stapling	**Yes**
Strict Transport Security (HSTS)	**Yes** max-age=15768000
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)	Unknown
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	secp256k1, secp256r1, secp384r1, secp521r1 (Server has no preference)
SSL 2 handshake compatibility	No

HTTP Requests

1 https://nwsmooc.mooin.org/ (HTTP/1.1 200 OK)



Miscellaneous

Test date	Mon, 17 Apr 2023 16:56:02 UTC
Test duration	127.848 seconds
HTTP status code	200
HTTP server signature	Apache
Server hostname	h2524950.stratoserver.net

SSL Report v2.1.10

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.

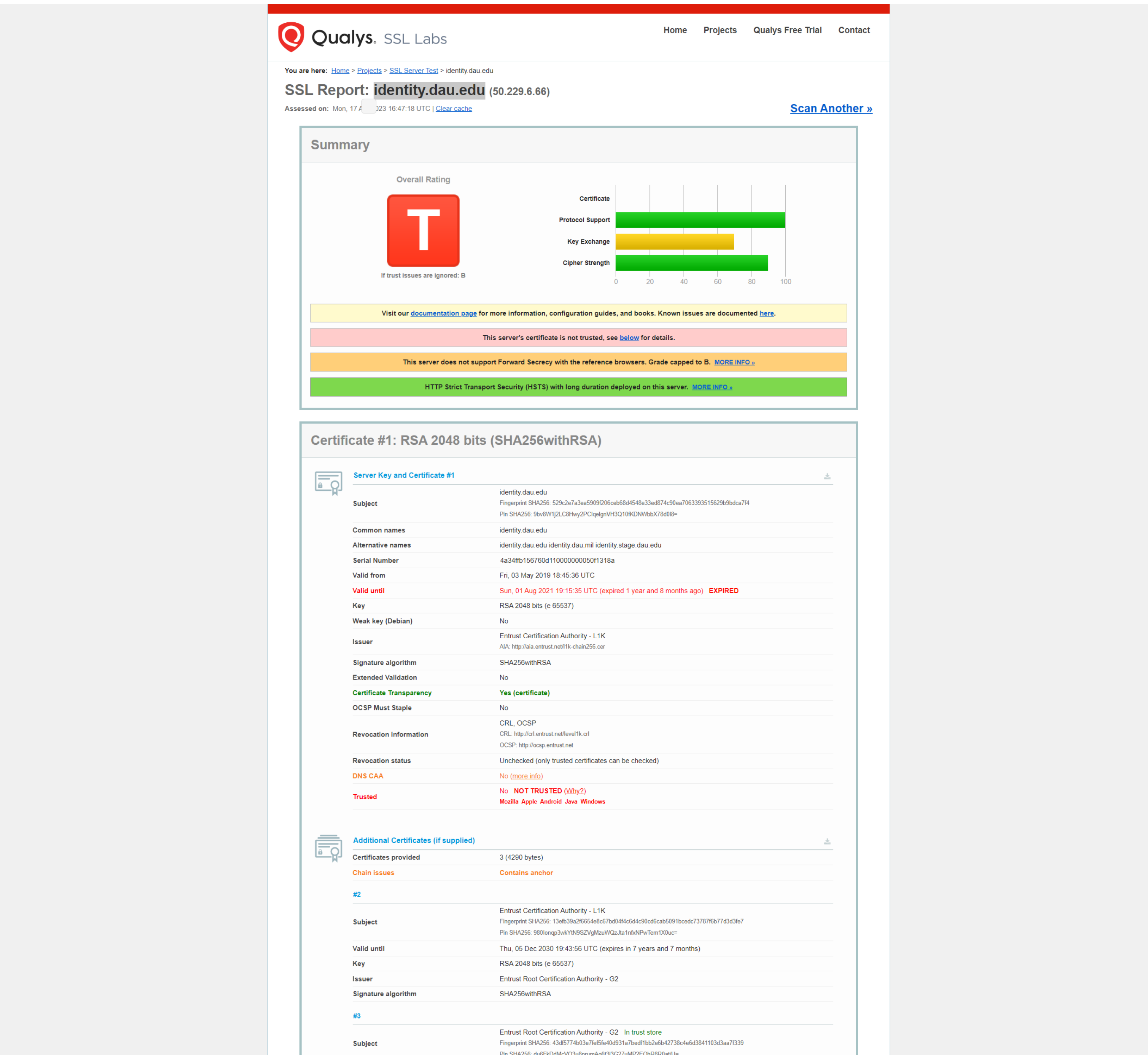
Dies entspricht einem guten Rating.

Potentielle Verbesserungen die vorgeschlagen werden:

- Fehlender DNS CAA Record im DNS Record des Servers. Hiermit kann eine ausstellende CA sicherstellen, dass sie ein Zertifikat für die richtige Seite ausstellt, indem sie überprüft ob sie im DNS record als ausstellende CA gelistet wird. Dies soll verhindern, dass jemand ein gültiges Zertifikat für eine Seite ausstellt, bei welcher er nicht in Kontrolle des DNS Eintrages ist.
- Einige ältere Clients werden nicht mehr unterstützt, dies kann je nach Ausrichtung der Seite zu ungewünschten Problemen führen.
- Der Server indiziert keine Präferenz für die stärksten verfügbaren Ciphersuites, unterstütz jedoch nur moderne.

Ergebnisse für `identity.dau.edu`:

Allgemeines Rating : T



You are here: Home > Projects > SSL Server Test > identity.dau.edu

SSL Report: identity.dau.edu (50.229.6.66)

Assessed on: Mon, 17 A 023 16:47:18 UTC | Clear cache

Scan Another »

Summary

If trust issues are ignored: B

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 does not support Forward Secrecy with the reference browsers. Grade capped to B. MORE INFO »

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

Certificate #1: RSA 2048 bits (SHA256withRSA)

Server Key and Certificate #1

Subject	identity.dau.edu Fingerprint SHA256: 529c2e7a3ea5909f206ceb68d4548e33ed874c90ea7063393515629b9bdca7f4 Pin SHA256: 9bv8W1j2LC8Hwy2PCIqelgnVH3Q10fKDNWbbX78d0I8=
Common names	identity.dau.edu
Alternative names	identity.dau.edu identity.dau.mil identity.stage.dau.edu
Serial Number	4a34ffb156760d110000000050f1318a
Valid from	Fri, 03 May 2019 18:45:36 UTC
Valid until	Sun, 01 Aug 2021 19:15:35 UTC (expired 1 year and 8 months ago) EXPIRED
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	Entrust Certification Authority - L1K AIA: http://aia.entrust.net/l1k-chain256.cer
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	Yes (certificate)
OCSP Must Staple	No
Revocation information	CRL, OCSP CRL: http://crl.entrust.net/level1k.crl OCSP: http://ocsp.entrust.net
Revocation status	Unchecked (only trusted certificates can be checked)
DNS CAA	No (more info)
Trusted	No NOT TRUSTED (Why?) Mozilla Apple Android Java Windows

Additional Certificates (if supplied)

Certificates provided	3 (4290 bytes)
Chain issues	Contains anchor
#2	
Subject	Entrust Certification Authority - L1K Fingerprint SHA256: 13efb39a2f6654e8c67bd04f4c6d4c90cd6cab5091bcedc73787f6b77d3d3fe7 Pin SHA256: 980Ionqp3wkYtN9SZVgMzuWQzJta1nfxNPwTem1X0uc=
Valid until	Thu, 05 Dec 2030 19:43:56 UTC (expires in 7 years and 7 months)
Key	RSA 2048 bits (e 65537)
Issuer	Entrust Root Certification Authority - G2
Signature algorithm	SHA256withRSA
#3	
Subject	Entrust Root Certification Authority - G2 In trust store Fingerprint SHA256: 43df5774b03e7fef5fe40d931a7bedf1bb2e6b42738c4e6d3841103d3aa7f339 Pin SHA256: du6FkDdMcVQ3u8prumAo6t3i3G27uMP2EOhR8R0at/U=

Valid until	Sat, 07 Dec 2030 17:55:54 UTC (expires in 7 years and 7 months)
Key	RSA 2048 bits (e 65537)
Issuer	Entrust Root Certification Authority - G2 Self-signed
Signature algorithm	SHA256withRSA

Certification Paths

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

Cipher Suites

TLS 1.2 (suites in server-preferred order)

TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c) WEAK	128
TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d) WEAK	256
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) WEAK	128
TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c) WEAK	128
TLS_RSA_WITH_AES_256_CBC_SHA (0x35) WEAK	256
TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d) WEAK	256

Handshake Simulation

Android 4.4.2	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_128_GCM_SHA256 No FS
Android 5.0.0	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_128_GCM_SHA256 No FS
Android 6.0	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_128_GCM_SHA256 No FS
Android 7.0	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_128_GCM_SHA256 No FS
Android 8.0	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_128_GCM_SHA256 No FS
Android 8.1	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_128_GCM_SHA256 No FS
Android 9.0	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_128_GCM_SHA256 No FS
BingPreview Jan 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_128_GCM_SHA256 No FS
Chrome 49 / XP SP3	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_128_GCM_SHA256 No FS
Chrome 69 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_128_GCM_SHA256 No FS
Chrome 70 / Win 10	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_128_GCM_SHA256 No FS
Chrome 80 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_128_GCM_SHA256 No FS
Firefox 31.3.0 ESR / Win 7	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_128_CBC_SHA No FS
Firefox 47 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_128_CBC_SHA No FS
Firefox 49 / XP SP3	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_128_CBC_SHA No FS
Firefox 62 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_128_CBC_SHA No FS
Firefox 73 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_128_CBC_SHA No FS
Googlebot Feb 2018	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_128_GCM_SHA256 No FS
IE 11 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_128_GCM_SHA256 No FS
IE 11 / Win 8.1 R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_128_GCM_SHA256 No FS
IE 11 / Win Phone 8.1 R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_128_CBC_SHA No FS
IE 11 / Win Phone 8.1 Update R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_128_GCM_SHA256 No FS
IE 11 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_128_GCM_SHA256 No FS
Edge 15 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_128_GCM_SHA256 No FS
Edge 16 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_128_GCM_SHA256 No FS
Edge 18 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_128_GCM_SHA256 No FS
Edge 13 / Win Phone 10 R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_128_GCM_SHA256 No FS
Java 8u161	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_128_GCM_SHA256 No FS
Java 11.0.3	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_128_GCM_SHA256 No FS
Java 12.0.1	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_128_GCM_SHA256 No FS
OpenSSL 1.0.1l R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_128_GCM_SHA256 No FS
OpenSSL 1.0.2s R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_128_GCM_SHA256 No FS
OpenSSL 1.1.0k R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_128_GCM_SHA256 No FS
OpenSSL 1.1.1c R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_128_GCM_SHA256 No FS
Safari 6 / iOS 6.0.1	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_128_CBC_SHA No FS
Safari 7 / iOS 7.1 R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_128_CBC_SHA No FS
Safari 7 / OS X 10.9 R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_128_CBC_SHA No FS
Safari 8 / iOS 8.4 R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_128_CBC_SHA No FS
Safari 8 / OS X 10.10 R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_128_CBC_SHA No FS
Safari 9 / iOS 9 R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_128_GCM_SHA256 No FS
Safari 9 / OS X 10.11 R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_128_GCM_SHA256 No FS
Safari 10 / iOS 10 R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_128_GCM_SHA256 No FS
Safari 10 / OS X 10.12 R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_128_GCM_SHA256 No FS
Safari 12.1.2 / MacOS 10.14.6 Beta R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_128_GCM_SHA256 No FS
Safari 12.1.1 / iOS 12.3.1 R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_128_GCM_SHA256 No FS
Apple ATS 9 / iOS 9 R	Server sent fatal alert: handshake_failure		
Yahoo Slurp Jan 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_128_GCM_SHA256 No FS
YandexBot Jan 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_128_GCM_SHA256 No 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.

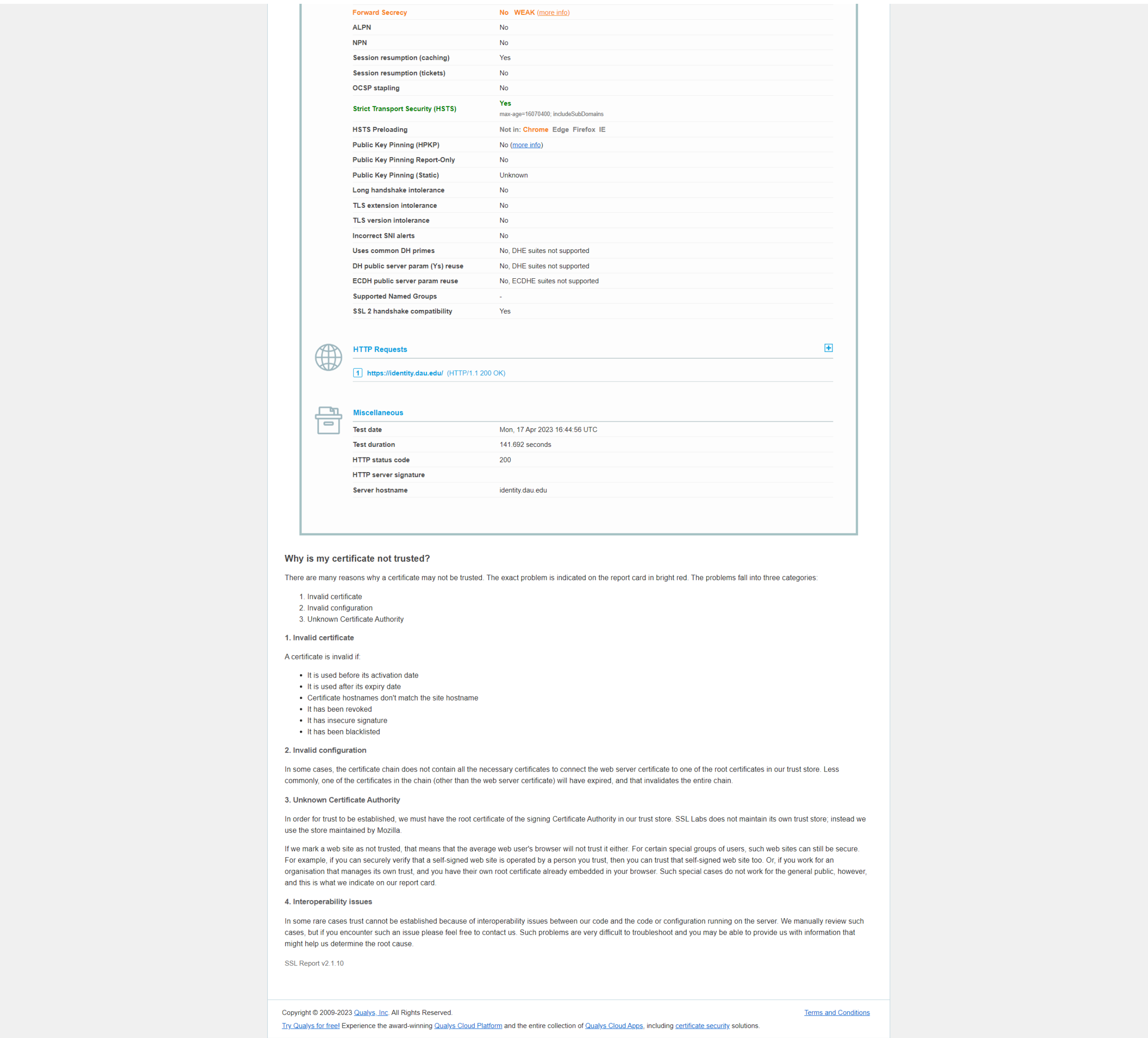
(R) Denotes a reference browser or client, with which we expect better effective security.

(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	**Unable to perform this test due to an internal error.** **(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 not complete **INTERNAL ERROR: connect timed out** **INTERNAL ERROR: connect timed out**
Secure Renegotiation	**Supported**
Secure Client-Initiated Renegotiation	Yes
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) TLS 1.2 : 0x002f
GOLDENDOODLE	No (more info) TLS 1.2 : 0x002f
OpenSSL 0-Length	No (more info) TLS 1.2 : 0x002f
Sleeping POODLE	No (more info) TLS 1.2 : 0x002f
Downgrade attack prevention	Unknown (requires support for at least two protocols, excl. SSL2)
SSL/TLS compression	No
RC4	No
Heartbeat (extension)	No
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	No WEAK (more info)
ALPN	No
NPN	No
Session resumption (caching)	Yes
Session resumption (tickets)	No
OCSP stapling	No
Strict Transport Security (HSTS)	Yes max-age=16070400; includeSubDomains
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)	Unknown
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
ECDH public server param reuse	No, ECDHE suites not supported
Supported Named Groups	-
SSL 2 handshake compatibility	Yes

HTTP Requests

1 https://identity.dau.edu/ (HTTP/1.1 200 OK)

Miscellaneous

Test date	Mon, 17 Apr 2023 16:44:56 UTC
Test duration	141.692 seconds
HTTP status code	200
HTTP server signature	
Server hostname	identity.dau.edu

Why is my certificate not trusted?

There are many reasons why a certificate may not be trusted. The exact problem is indicated on the report card in bright red. The problems fall into three categories:

1. Invalid certificate
2. Invalid configuration
3. Unknown Certificate Authority

1. Invalid certificate

A certificate is invalid if:

- It is used before its activation date
- It is used after its expiry date
- Certificate hostnames don't match the site hostname
- It has been revoked
- It has insecure signature
- It has been blacklisted

2. Invalid configuration

In some cases, the certificate chain does not contain all the necessary certificates to connect the web server certificate to one of the root certificates in our trust store. Less commonly, one of the certificates in the chain (other than the web server certificate) will have expired, and that invalidates the entire chain.

3. Unknown Certificate Authority

In order for trust to be established, we must have the root certificate of the signing Certificate Authority in our trust store. SSL Labs does not maintain its own trust store; instead we use the store maintained by Mozilla.

If we mark a web site as not trusted, that means that the average web user's browser will not trust it either. For certain special groups of users, such web sites can still be secure. For example, if you can securely verify that a self-signed web site is operated by a person you trust, then you can trust that self-signed web site too. Or, if you work for an organisation that manages its own trust, and you have their own root certificate already embedded in your browser. Such special cases do not work for the general public, however, and this is what we indicate on our report card.

4. Interoperability issues

In some rare cases trust cannot be established because of interoperability issues between our code and the code or configuration running on the server. We manually review such cases, but if you encounter such an issue please feel free to contact us. Such problems are very difficult to troubleshoot and you may be able to provide us with information that might help us determine the root cause.

SSL Report v2.1.10

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.

Dies entspricht einem "schreklichen" (terrible) Rating. Jedoch nur wenn man berücksichtigt, das das Zertifikat ein selbst ausgestelltes ist.

Weitere Probleme:

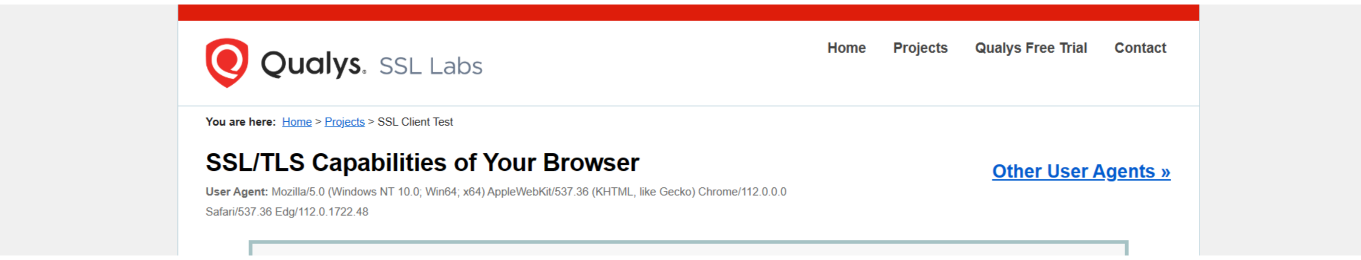
- Das Zertifikat ist seit 2021 abgelaufen.
- Es werden schwache Ciphersuites unterstützt (sollte man im Webserver deaktivieren)
-

Aufgabe b)

Führen Sie den Client-Test von Qualys aus und erklären Sie die Ergebnisse.

Antwort

Ergebnis mit Edge:

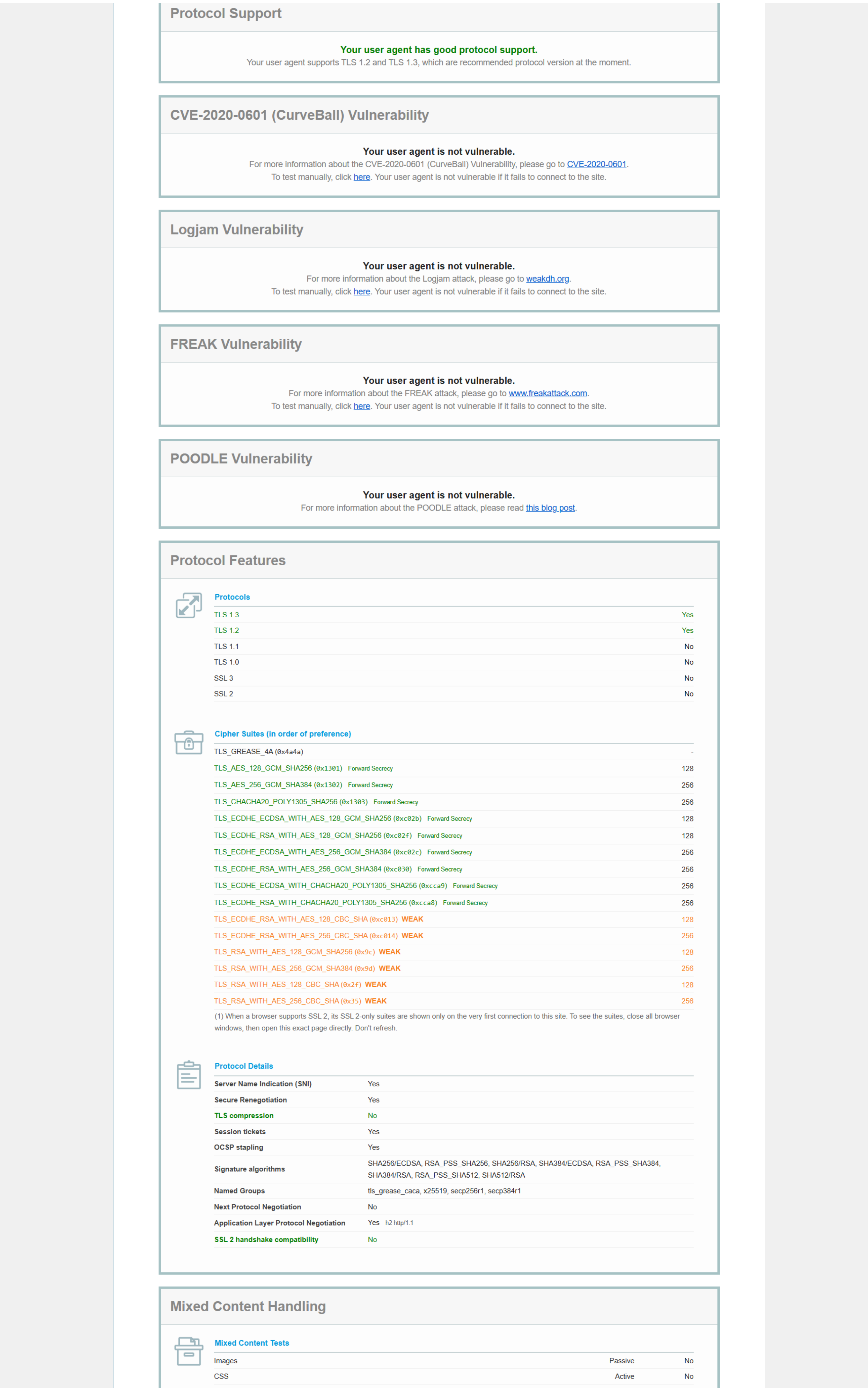


You are here: Home > Projects > SSL Client Test

SSL/TLS Capabilities of Your Browser

Other User Agents »

User Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.0.0 Safari/537.36 Edg/112.0.1722.48



Protocol Support

Your user agent has good protocol support.
Your user agent supports TLS 1.2 and TLS 1.3, which are recommended protocol version at the moment.

CVE-2020-0601 (CurveBall) Vulnerability

Your user agent is not vulnerable.
For more information about the CVE-2020-0601 (CurveBall) Vulnerability, please go to CVE-2020-0601.
To test manually, click here. Your user agent is not vulnerable if it fails to connect to the site.

Logjam Vulnerability

Your user agent is not vulnerable.
For more information about the Logjam attack, please go to weakdh.org.
To test manually, click here. Your user agent is not vulnerable if it fails to connect to the site.

FREAK Vulnerability

Your user agent is not vulnerable.
For more information about the FREAK attack, please go to www.freakattack.com.
To test manually, click here. Your user agent is not vulnerable if it fails to connect to the site.

POODLE Vulnerability

Your user agent is not vulnerable.
For more information about the POODLE attack, please read this blog post.

Protocol Features

Protocols

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

Cipher Suites (in order of preference)

TLS_GREASE_4A (0x4a4a)	-
TLS_AES_128_GCM_SHA256 (0x1301) Forward Secrecy	128
TLS_AES_256_GCM_SHA384 (0x1302) Forward Secrecy	256
TLS_CHACHA20_POLY1305_SHA256 (0x1303) Forward Secrecy	256
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
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8) Forward Secrecy	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) **WEAK**	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) **WEAK**	256
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c) **WEAK**	128
TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d) **WEAK**	256
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) **WEAK**	128
TLS_RSA_WITH_AES_256_CBC_SHA (0x35) **WEAK**	256

(1) When a browser supports SSL 2, its SSL 2-only suites are shown only on the very first connection to this site. To see the suites, close all browser windows, then open this exact page directly. Don't refresh.

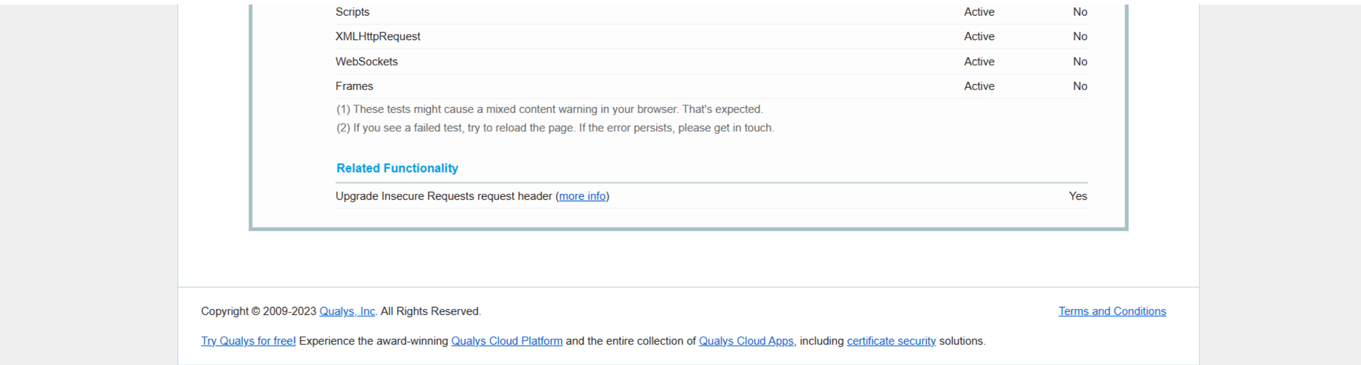
Protocol Details

Server Name Indication (SNI)	Yes
Secure Renegotiation	Yes
TLS compression	No
Session tickets	Yes
OCSP stapling	Yes
Signature algorithms	SHA256/ECDSA, RSA_PSS_SHA256, SHA256/RSA, SHA384/ECDSA, RSA_PSS_SHA384, SHA384/RSA, RSA_PSS_SHA512, SHA512/RSA
Named Groups	tls_grease_caca, x25519, secp256r1, secp384r1
Next Protocol Negotiation	No
Application Layer Protocol Negotiation	Yes h2 http/1.1
SSL 2 handshake compatibility	No

Mixed Content Handling

Mixed Content Tests

Images	Passive	No
CSS	Active	No



Scripts	Active	No
XMLHttpRequest	Active	No
WebSockets	Active	No
Frames	Active	No

(1) These tests might cause a mixed content warning in your browser. That's expected.
(2) If you see a failed test, try to reload the page. If the error persists, please get in touch.

Related Functionality

Upgrade Insecure Requests request header (more info)	Yes

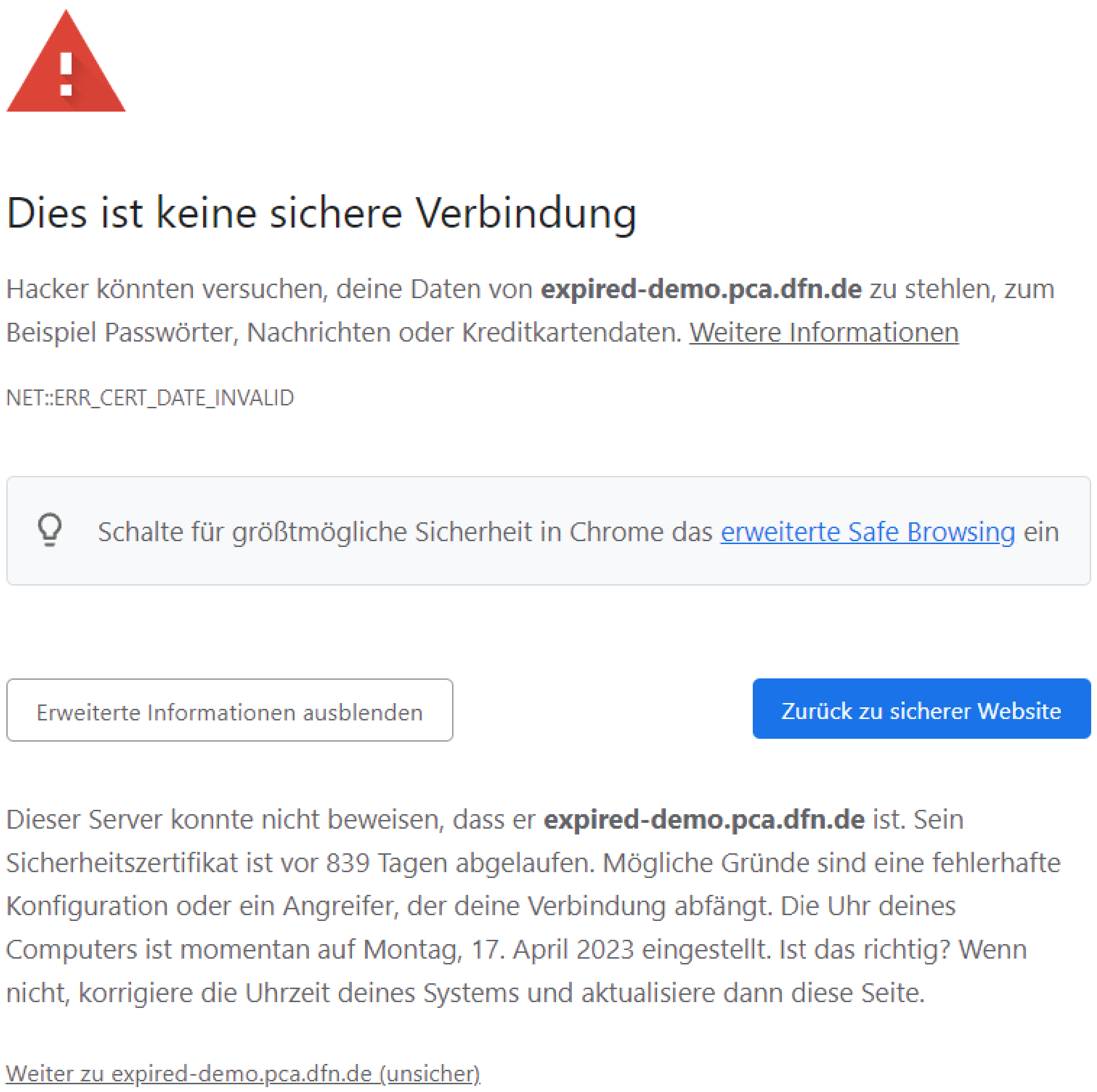
- Der Browser unterstützt aktuelle Protokolle.
- Er ist nicht anfällig für die folgenden Vulns: CurveBall, Logjam, FREAK und POODLE
- Es werden aktuelle aber auch einige als schwach eingestellte Ciphersuites akzeptiert, dies kann ein Sicherheitsrisiko darstellen.
- Gängige features (WebSockets, CSS ...) werden unterstützt

Aufgabe c)

Rufen Sie die Testwebseiten https://expired-demo.pca.dfn.de/ sowie https://revoked-demo.pca.dfn.de/ mit Firefox und mit Google Chrome auf. Erklären Sie, was passiert. Sind die Resultate bei allen vier Tests so wie erwartet?

Der Browser Lehnt die Verbindung mit den Seiten ab, da die Zertifikate abgelaufen sind (Kann durch den user mit einer weiteren Bestätigung ignoriert werden)

Chrome:



Dies ist keine sichere Verbindung

Hacker könnten versuchen, deine Daten von **expired-demo.pca.dfn.de** zu stehlen, zum Beispiel Passwörter, Nachrichten oder Kreditkartendaten. Weitere Informationen

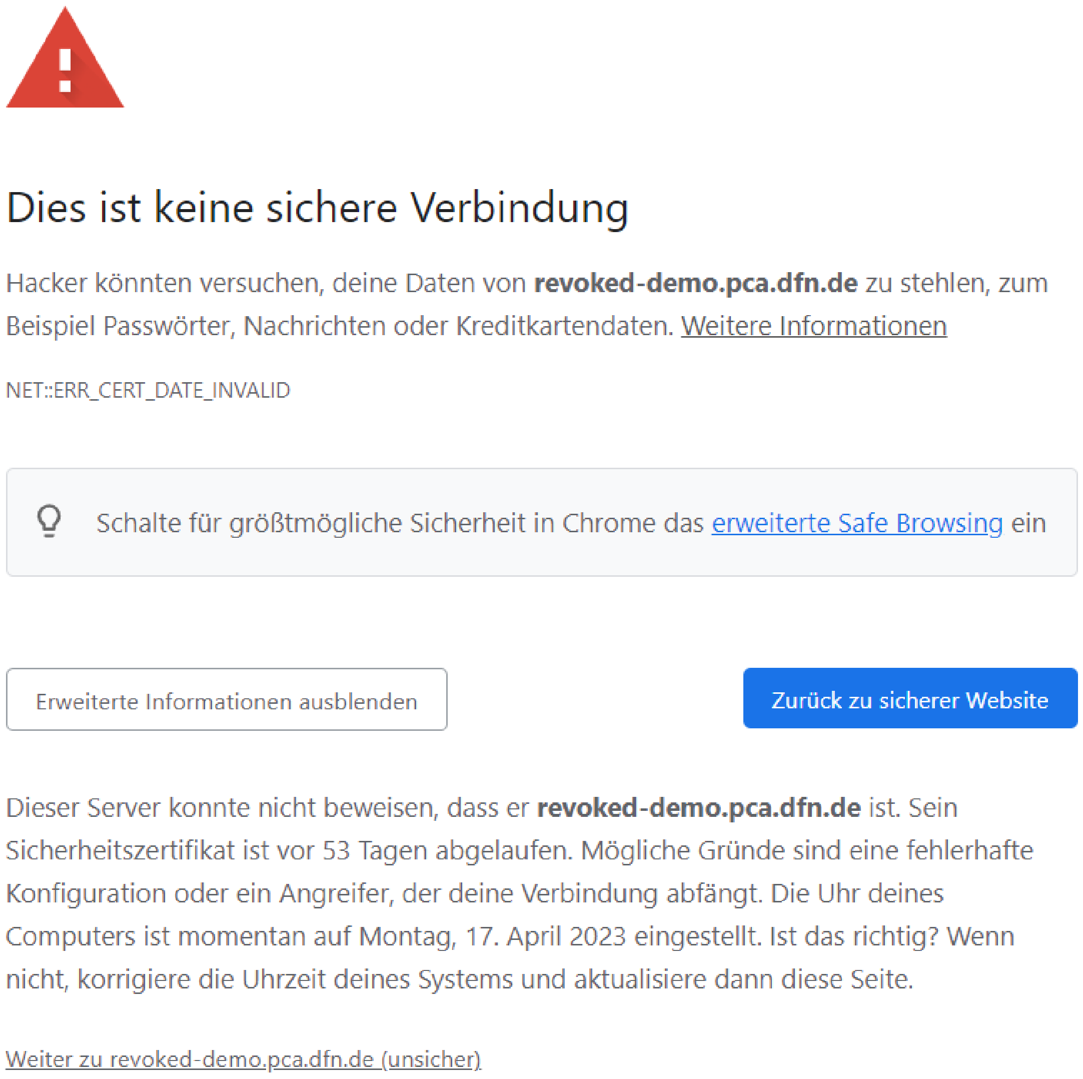
NET::ERR_CERT_DATE_INVALID

Schalte für größtmögliche Sicherheit in Chrome das erweiterte Safe Browsing ein

Erweiterte Informationen ausblenden
Zurück zu sicherer Website

Dieser Server konnte nicht beweisen, dass er **expired-demo.pca.dfn.de** ist. Sein Sicherheitszertifikat ist vor 839 Tagen abgelaufen. Mögliche Gründe sind eine fehlerhafte Konfiguration oder ein Angreifer, der deine Verbindung abfängt. Die Uhr deines Computers ist momentan auf Montag, 17. April 2023 eingestellt. Ist das richtig? Wenn nicht, korrigiere die Uhrzeit deines Systems und aktualisiere dann diese Seite.

Weiter zu expired-demo.pca.dfn.de (unsicher)



Dies ist keine sichere Verbindung

Hacker könnten versuchen, deine Daten von **revoked-demo.pca.dfn.de** zu stehlen, zum Beispiel Passwörter, Nachrichten oder Kreditkartendaten. Weitere Informationen

NET::ERR_CERT_DATE_INVALID

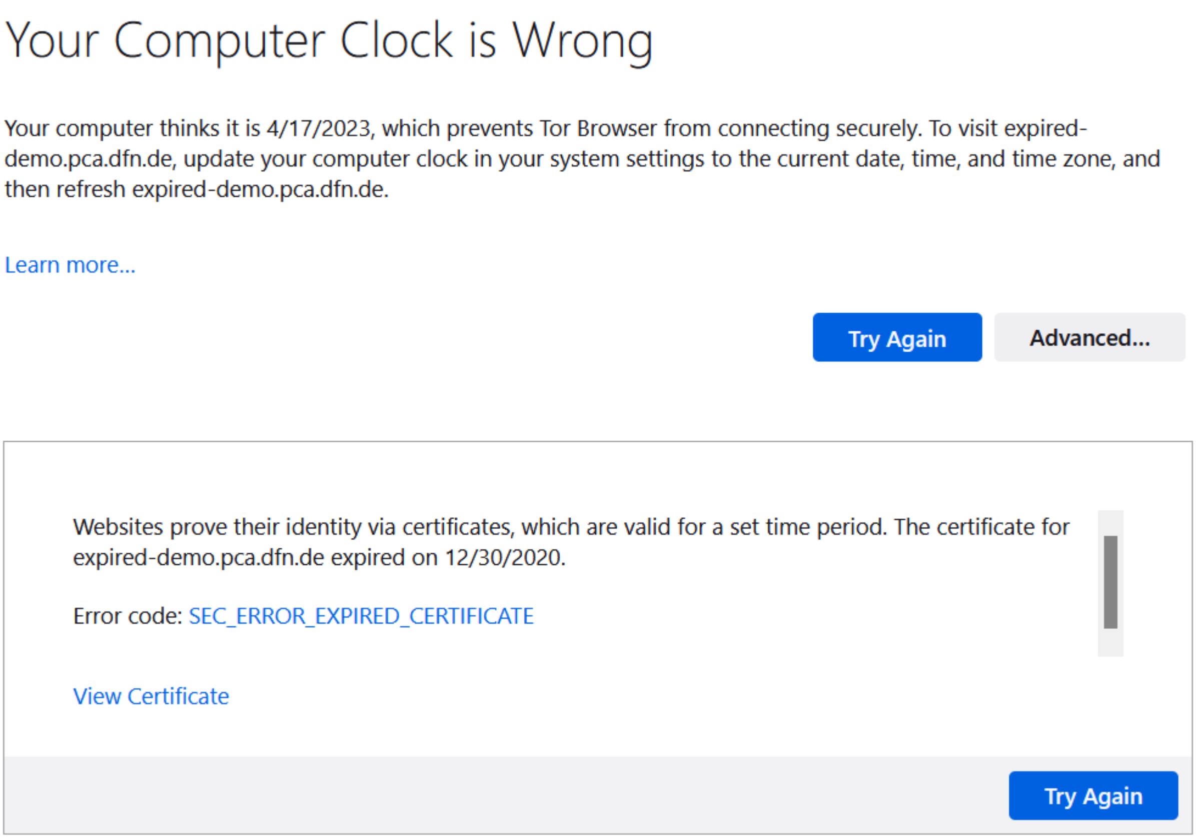
Schalte für größtmögliche Sicherheit in Chrome das erweiterte Safe Browsing ein

Erweiterte Informationen ausblenden
Zurück zu sicherer Website

Dieser Server konnte nicht beweisen, dass er **revoked-demo.pca.dfn.de** ist. Sein Sicherheitszertifikat ist vor 53 Tagen abgelaufen. Mögliche Gründe sind eine fehlerhafte Konfiguration oder ein Angreifer, der deine Verbindung abfängt. Die Uhr deines Computers ist momentan auf Montag, 17. April 2023 eingestellt. Ist das richtig? Wenn nicht, korrigiere die Uhrzeit deines Systems und aktualisiere dann diese Seite.

Weiter zu revoked-demo.pca.dfn.de (unsicher)

Firefox:



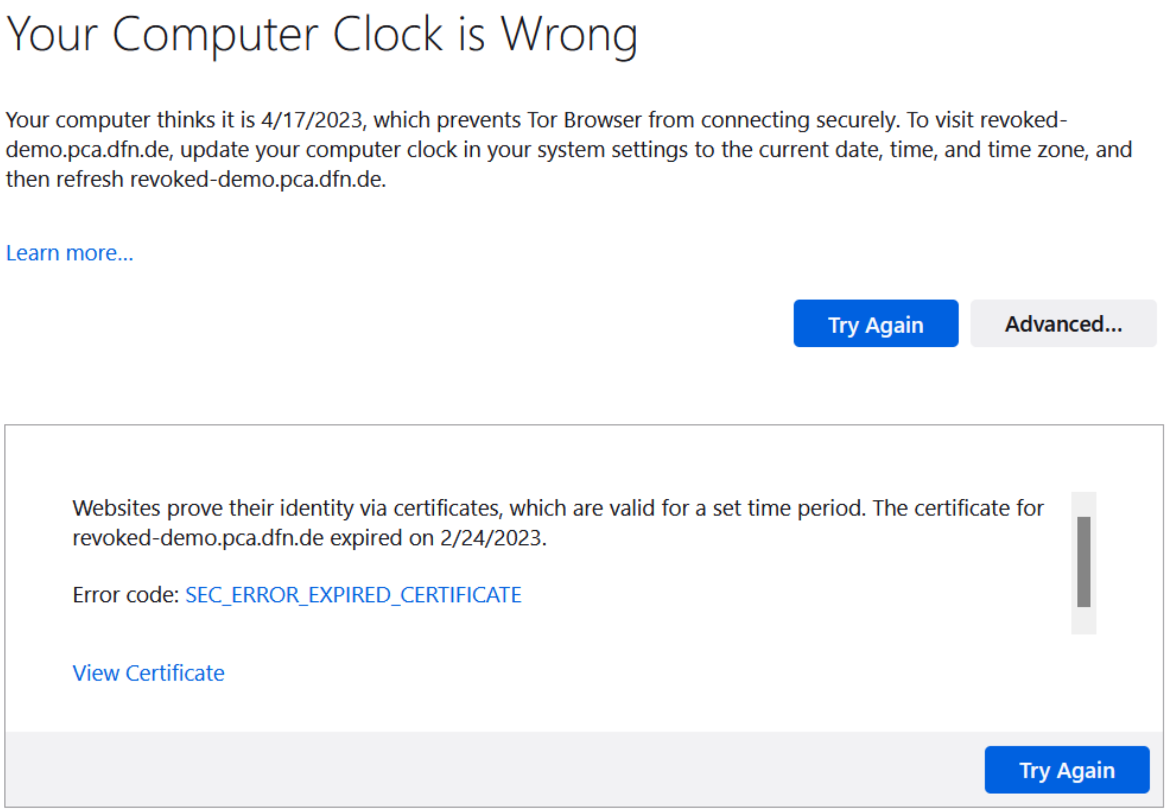
Your Computer Clock is Wrong

Your computer thinks it is 4/17/2023, which prevents Tor Browser from connecting securely. To visit expired-demo.pca.dfn.de, update your computer clock in your system settings to the current date, time, and time zone, and then refresh expired-demo.pca.dfn.de.

Learn more…

Websites prove their identity via certificates, which are valid for a set time period. The certificate for expired-demo.pca.dfn.de expired on 12/30/2020.

Error code: SEC_ERROR_EXPIRED_CERTIFICATE



Your Computer Clock is Wrong

Your computer thinks it is 4/17/2023, which prevents Tor Browser from connecting securely. To visit revoked-demo.pca.dfn.de, update your computer clock in your system settings to the current date, time, and time zone, and then refresh revoked-demo.pca.dfn.de.

Websites prove their identity via certificates, which are valid for a set time period. The certificate for revoked-demo.pca.dfn.de expired on 2/24/2023.

Error code: SEC_ERROR_EXPIRED_CERTIFICATE

Alle Zeigen den gleichen Fehler an, vermutlich weil das zurückgezogene Zertifikat mittlerweile auch abgelaufen ist.

Aufgabe d)

d) Installieren Sie VeraCrypt auf Ihrem Rechner. Hierzu erhalten Sie zusätzlich eine VeraCrypt-Datei. In der Datei ist ein normaler und ein versteckter Container zu finden, die jeweils eine Datei enthalten. Das Passwort für den normalen Container ist der Exponent e des RSA-Schlüssels vom nwsmooc.mooin.org-Server. Dokumentieren Sie Ihre Vorgehensweise mit Screenshots und geben Sie anschließend das im versteckten Container gefundene Kennwort an.

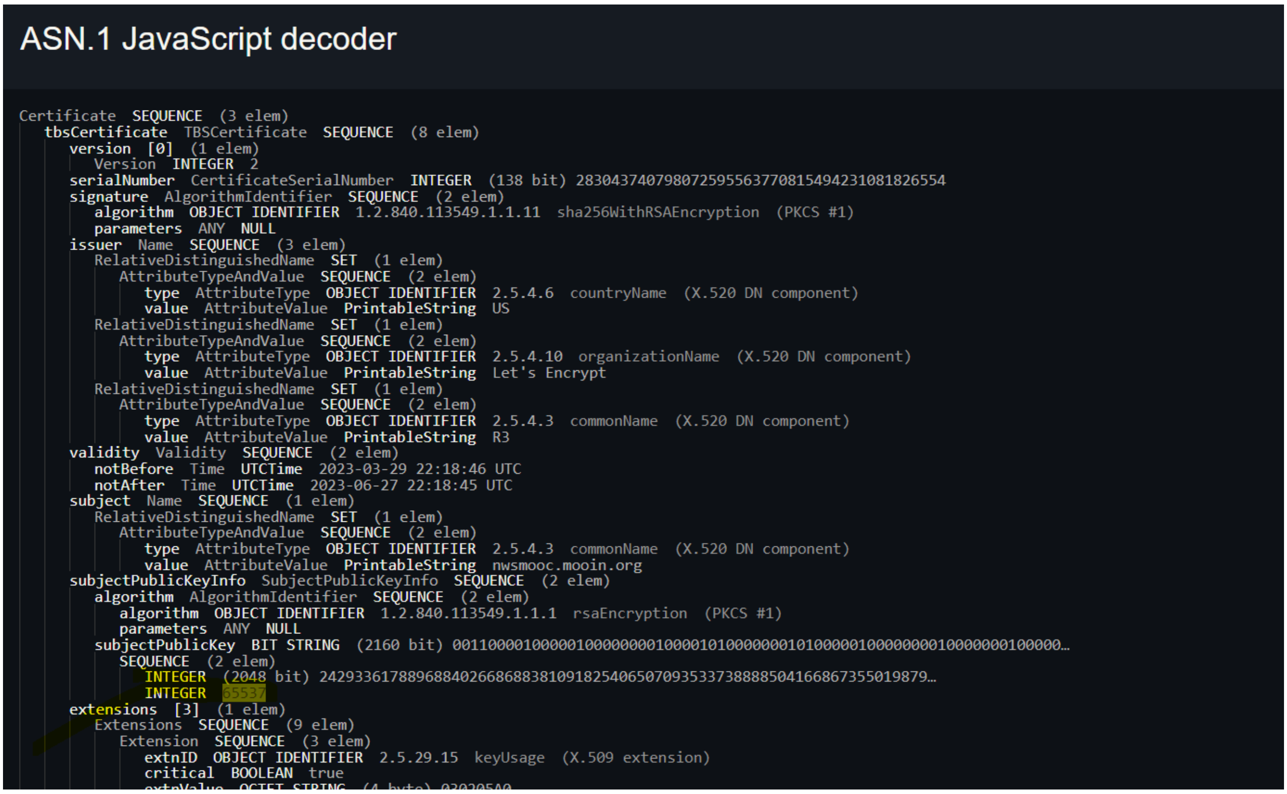
Tipp: Zur Bedienung von VeraCrypt können Sie sich beispielsweise eine

e) Installieren Sie SilentEye auf Ihrem Rechner und untersuchen Sie die bereitgestellten Beispieldateien. Eine Datei enthält ein verstecktes Kennwort, die andere eine Datei. Die notwendigen Einstellungen können Sie der Aufgabe mit VeraCrypt entnehmen. Dokumentieren Sie Ihre Vorgehensweise mit Screenshots und geben Sie das gefundene Kennwort an.

Vorgehen:

1. Zertifikat im Browser herunterladen.

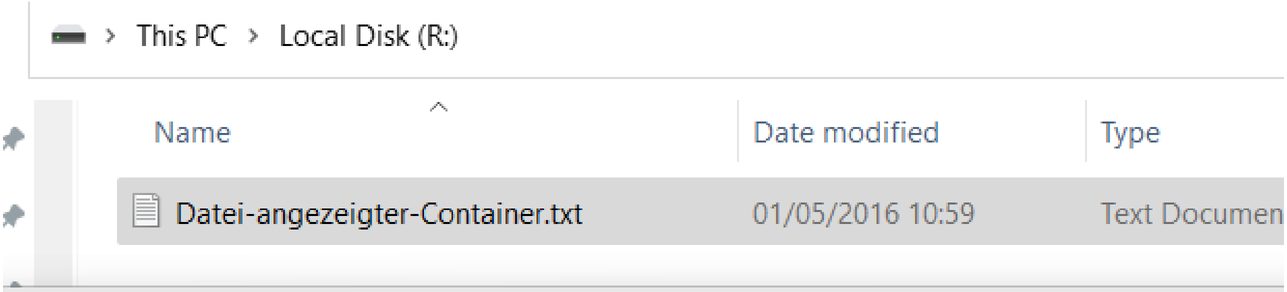
2. Zertifikat im ASN.1 browser decodiern und exponent extrahieren.

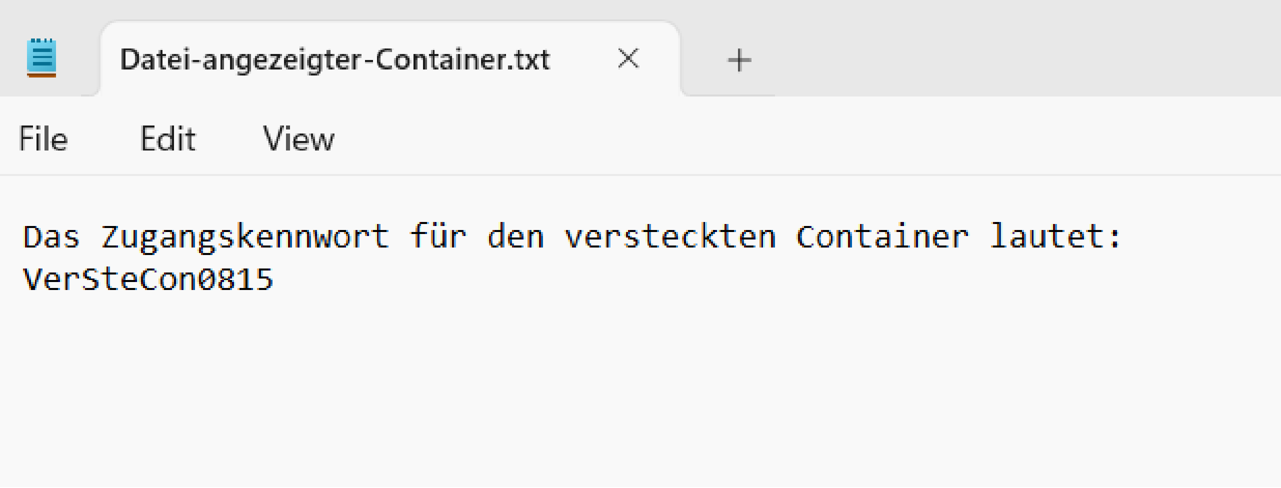


ASN.1 JavaScript decoder

```
Certificate  SEQUENCE  (3 elem)
   tbsCertificate  TBSCertificate  SEQUENCE  (8 elem)
      version  [0]  (1 elem)
         Version  INTEGER  2
      serialNumber  CertificateSerialNumber  INTEGER  (138 bit) 283043740798072595563770815494231081826554
      signature  AlgorithmIdentifier  SEQUENCE  (2 elem)
         algorithm  OBJECT IDENTIFIER  1.2.840.113549.1.1.11  sha256WithRSAEncryption  (PKCS #1)
         parameters  ANY  NULL
      issuer  Name  SEQUENCE  (3 elem)
         RelativeDistinguishedName  SET  (1 elem)
            AttributeTypeAndValue  SEQUENCE  (2 elem)
               type  AttributeType  OBJECT IDENTIFIER  2.5.4.6  countryName  (X.520 DN component)
               value  AttributeValue  PrintableString  US
         RelativeDistinguishedName  SET  (1 elem)
            AttributeTypeAndValue  SEQUENCE  (2 elem)
               type  AttributeType  OBJECT IDENTIFIER  2.5.4.10  organizationName  (X.520 DN component)
               value  AttributeValue  PrintableString  Let's Encrypt
         RelativeDistinguishedName  SET  (1 elem)
            AttributeTypeAndValue  SEQUENCE  (2 elem)
               type  AttributeType  OBJECT IDENTIFIER  2.5.4.3  commonName  (X.520 DN component)
               value  AttributeValue  PrintableString  R3
      validity  Validity  SEQUENCE  (2 elem)
         notBefore  Time  UTCTime  2023-03-29 22:18:46 UTC
         notAfter  Time  UTCTime  2023-06-27 22:18:45 UTC
      subject  Name  SEQUENCE  (1 elem)
         RelativeDistinguishedName  SET  (1 elem)
            AttributeTypeAndValue  SEQUENCE  (2 elem)
               type  AttributeType  OBJECT IDENTIFIER  2.5.4.3  commonName  (X.520 DN component)
               value  AttributeValue  PrintableString  nwsmooc.mooin.org
      subjectPublicKeyInfo  SubjectPublicKeyInfo  SEQUENCE  (2 elem)
         algorithm  AlgorithmIdentifier  SEQUENCE  (2 elem)
            algorithm  OBJECT IDENTIFIER  1.2.840.113549.1.1.1  rsaEncryption  (PKCS #1)
            parameters  ANY  NULL
         subjectPublicKey  BIT STRING  (2160 bit) 0011000010000010000000010000101000000001010000010000000010000000100000…
            SEQUENCE  (2 elem)
               INTEGER  (2048 bit) 242933617889688402668688381091825406507093533738888504166867355019879…
               INTEGER  65537
      extensions  [3]  (1 elem)
         Extensions  SEQUENCE  (9 elem)
            Extension  SEQUENCE  (3 elem)
               extnID  OBJECT IDENTIFIER  2.5.29.15  keyUsage  (X.509 extension)
               critical  BOOLEAN  true
               extnValue  OCTET STRING  (4 byte) 030205A0
```

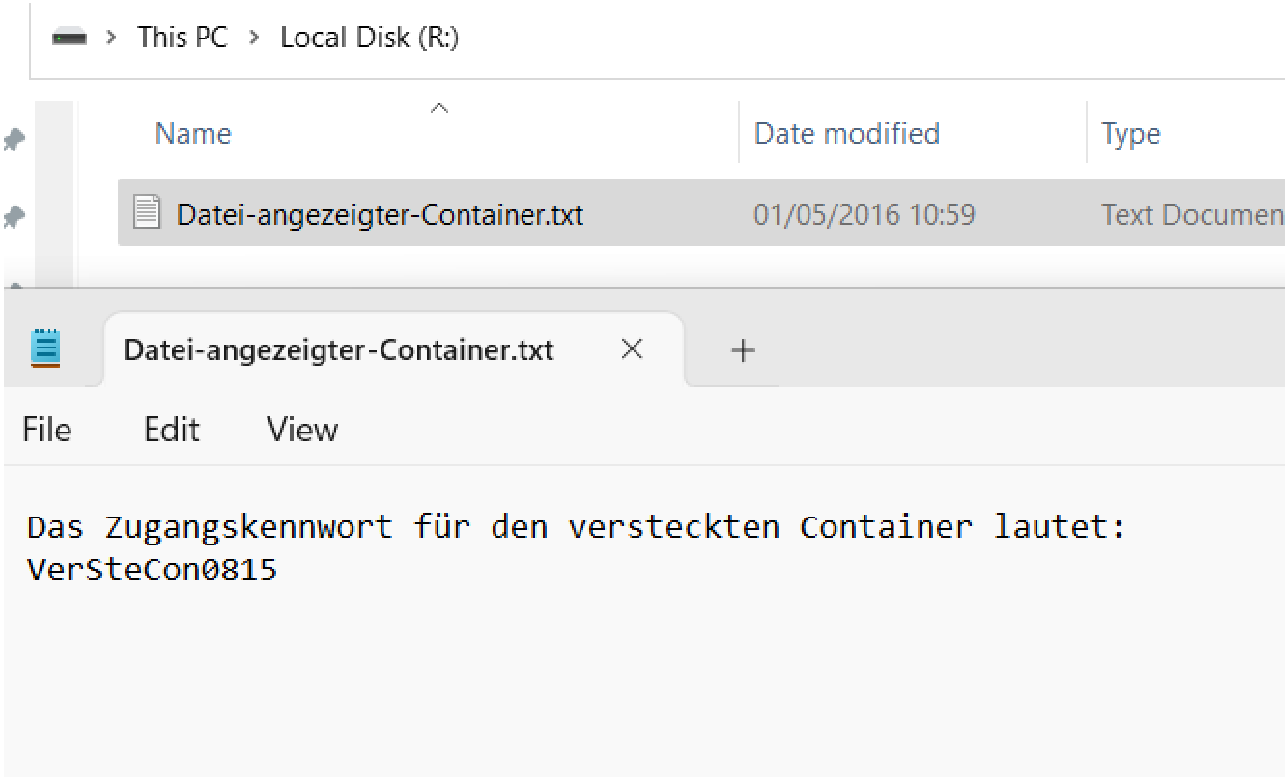
3. Container mit exponenten in VeraCrypt mounten





```
Das Zugangskennwort für den versteckten Container lautet:
VerSteCon0815
```

4. Den versteckten Container mit dem gefundenen Passwort mounten

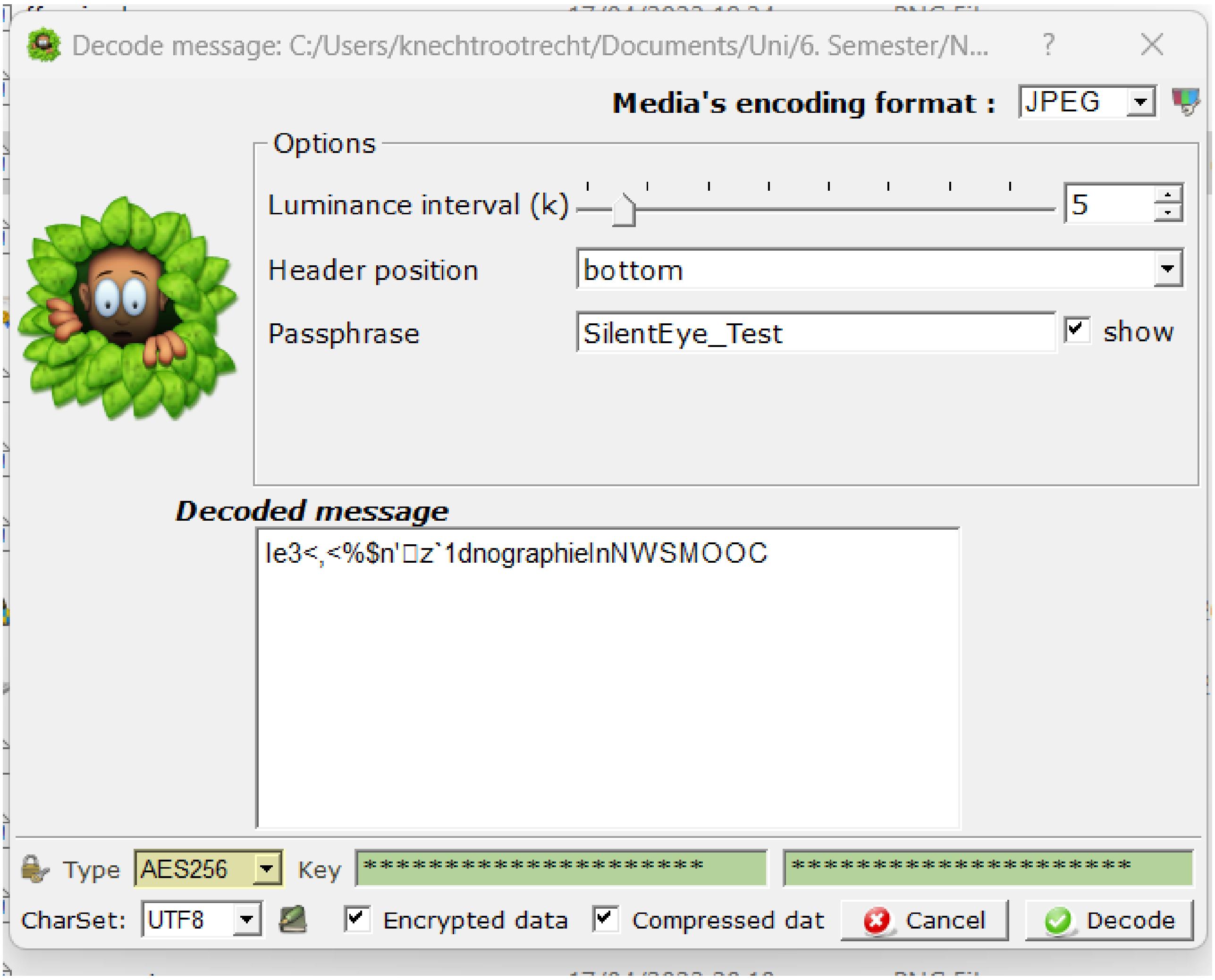


Datei-angezeigter-Container.txt 01/05/2016 10:59 Text Documen

Datei-angezeigter-Container.txt

```
Das Zugangskennwort für den versteckten Container lautet:
VerSteCon0815
```

5. Mittels gefundener Anleitung JPG und bmp Datei entsteganographieren



Decode message: C:/Users/knechtrootrecht/Documents/Uni/6. Semester/N...

Media's encoding format : JPEG

Options

Luminance interval (k): 5

Header position: bottom

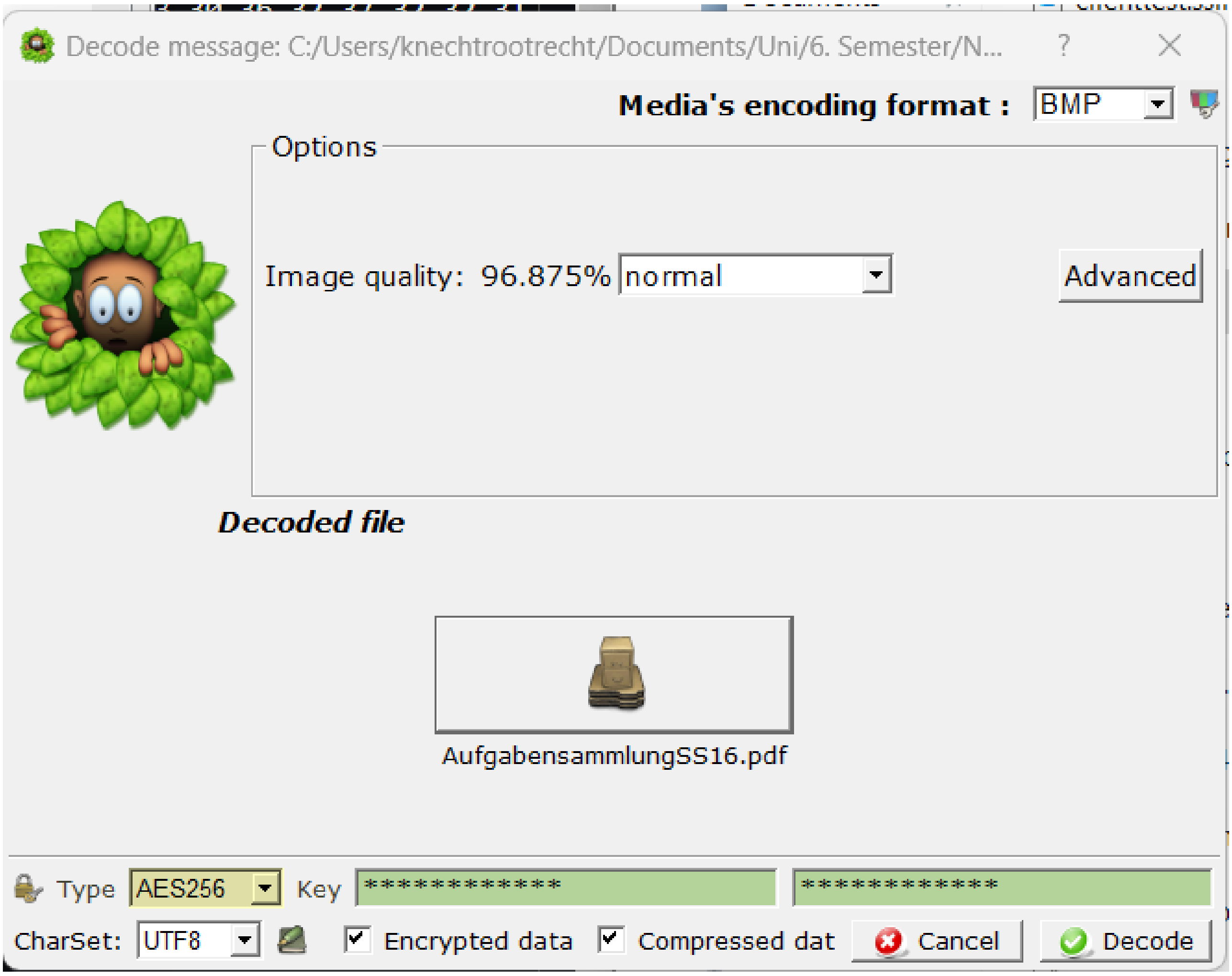
Passphrase: SilentEye_Test ☑ show

Decoded message

```
le3<,<%$n'□z`1dnographielnNWSMOOC
```

Type: AES256 Key: ******************** ********************

CharSet: UTF8 ☑ Encrypted data ☑ Compressed dat



Decode message: C:/Users/knechtrootrecht/Documents/Uni/6. Semester/N...

Media's encoding format : BMP

Options

Image quality: 96.875% normal

Decoded file

AufgabensammlungSS16.pdf

Type AES256 Key ************ ************

CharSet: UTF8 ☑ Encrypted data ☑ Compressed dat