

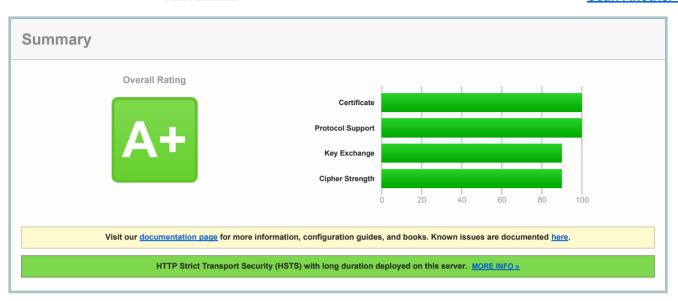
Home Projects Qualys.com Contact

You are here: Home > Projects > SSL Server Test > www.ed.gov > 184.94.214.145

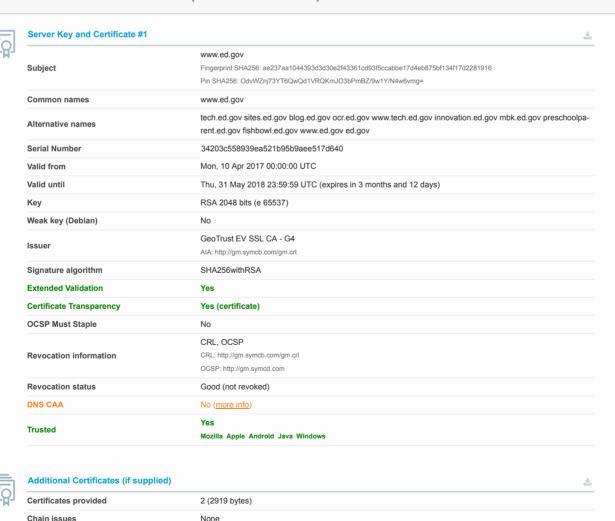
# SSL Report: <u>www.ed.gov</u> (184.94.214.145)

Assessed on: Mon, 19 Feb 2018 16:29:18 UTC | Hide | Clear cache

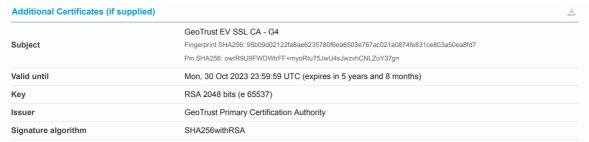
## Scan Another »



# Certificate #1: RSA 2048 bits (SHA256withRSA)



#2





**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  |

For TLS 1.3 tests, we currently support draft version 18.



## **Cipher Suites**

| # TLS 1.2 (suites in server-preferred order)   | _   |
|--|-----|
| 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_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ECDH secp256r1 (eq. 3072 bits RSA) FS    | 256 |
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ECDH secp256r1 (eq. 3072 bits RSA) FS    | 128 |
| TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d) WEAK  | 256 |
| TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d) WEAK  | 256 |
| TLS_RSA_WITH_AES_256_CBC_SHA (0x35) WEAK   | 256 |
| TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c) WEAK  | 128 |
| TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c) WEAK  | 128 |
| TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) WEAK   | 128 |



### **Handshake Simulation**

| Android 4.4.2              | RSA 2048 (SHA256) | TLS 1.2 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS |
|----------------------------|-------------------|---|
| Android 5.0.0              | RSA 2048 (SHA256) | TLS 1.2 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 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 |
| BingPreview Jan 2015       | RSA 2048 (SHA256) | TLS 1.2 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS |
| Chrome 49 / XP SP3         | RSA 2048 (SHA256) | TLS 1.2 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS |
| Chrome 57 / Win 7 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 53 / Win 7 R       | RSA 2048 (SHA256) | TLS 1.2 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS |
| Googlebot Feb 2015         | RSA 2048 (SHA256) | TLS 1.2 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS |
| <u>IE 11 / Win 7</u> R     | RSA 2048 (SHA256) | TLS 1.2 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 ECDH secp256r1 FS |
| <u>IE 11 / Win 8.1</u> R   | RSA 2048 (SHA256) | TLS 1.2 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 ECDH secp256r1 FS |
| IE 11 / Win Phone 8.1 R    | RSA 2048 (SHA256) | TLS 1.2 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 ECDH secp256r1 FS |
|                            |                   |   |

+

| Handshake Simulation            |                     |   |  |  |
|---------------------------------|---------------------|---|--|--|
| IE 11 / Win Phone 8.1 Update    | R RSA 2048 (SHA256) | TLS 1.2 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 ECDH secp256r1 FS |  |  |
| <u>IE 11 / Win 10</u> R         | RSA 2048 (SHA256)   | TLS 1.2 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS |  |  |
| Edge 13 / Win 10 R              | RSA 2048 (SHA256)   | TLS 1.2 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS |  |  |
| Edge 13 / Win Phone 10 R        | RSA 2048 (SHA256)   | TLS 1.2 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS |  |  |
| Java 8u31                       | RSA 2048 (SHA256)   | TLS 1.2 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS |  |  |
| OpenSSL 1.0.11 R                | RSA 2048 (SHA256)   | TLS 1.2 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS |  |  |
| OpenSSL 1.0.2e R                | RSA 2048 (SHA256)   | TLS 1.2 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS |  |  |
| Safari 6 / iOS 6.0.1            | RSA 2048 (SHA256)   | TLS 1.2 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 ECDH secp256r1 FS |  |  |
| Safari 7 / iOS 7.1 R            | RSA 2048 (SHA256)   | TLS 1.2 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 ECDH secp256r1 FS |  |  |
| <u>Safari 7 / OS X 10.9</u> R   | RSA 2048 (SHA256)   | TLS 1.2 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 ECDH secp256r1 FS |  |  |
| Safari 8 / iOS 8.4 R            | RSA 2048 (SHA256)   | TLS 1.2 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 ECDH secp256r1 FS |  |  |
| <u>Safari 8 / OS X 10.10</u> R  | RSA 2048 (SHA256)   | TLS 1.2 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 ECDH secp256r1 FS |  |  |
| Safari 9 / iOS 9 R              | RSA 2048 (SHA256)   | TLS 1.2 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS |  |  |
| <u>Safari 9 / OS X 10.11</u> R  | RSA 2048 (SHA256)   | TLS 1.2 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS |  |  |
| Safari 10 / iOS 10 R            | RSA 2048 (SHA256)   | TLS 1.2 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS |  |  |
| <u>Safari 10 / OS X 10.12</u> R | RSA 2048 (SHA256)   | TLS 1.2 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS |  |  |
| Apple ATS 9 / iOS 9 R           | RSA 2048 (SHA256)   | TLS 1.2 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS |  |  |
| Yahoo Slurp Jan 2015            | RSA 2048 (SHA256)   | TLS 1.2 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS |  |  |
| YandexBot Jan 2015              | RSA 2048 (SHA256)   | TLS 1.2 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS |  |  |

#### # Not simulated clients (Protocol mismatch)



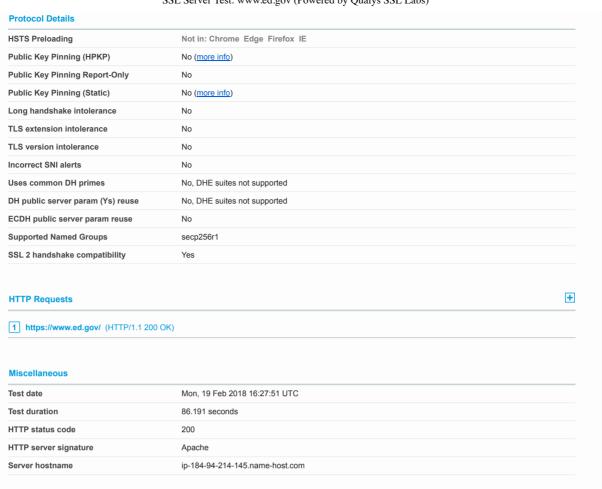
## Click here to expand

- (1) Clients that do not support Forward Secrecy (FS) are excluded when determining support for it.
- $(2) \ No \ support \ for \ virtual \ SSL \ hosting \ (SNI). \ Connects \ to \ the \ default \ site \ if \ the \ server \ uses \ SNI.$
- $(3) \ \ \text{Only first connection attempt simulated. Browsers sometimes retry with a lower protocol version.}$
- (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   | 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 website here (3) Censys data is only indicative of possible key and certificate reuse; possibly out-of-date and not complet |
|---|---|
| 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)  |
| 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.<br>(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)                    | Yes   |
| OCSP stapling                                   | Yes   |
| Strict Transport Security (HSTS)                | <b>Yes</b> max-age=31536000   |



SSL Report v1.30.8

Copyright © 2009-2018 Qualys, Inc. All Rights Reserved.

Terms and Conditions

Qualys is the leading provider of integrated infrastructure security, cloud infrastructure security, endpoint security, devsecops, compliance and web app security solutions.