

You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > prestations.vd.ch

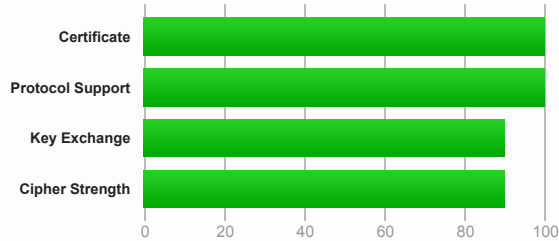
# SSL Report: prestations.vd.ch (145.232.192.146)

Assessed on: Tue, 15 Sep 2020 15:26:29 UTC | [Hide](#) | [Clear cache](#)

[Scan Another »](#)

## 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 »](#)

## Certificate #1: RSA 2048 bits (SHA256withRSA)



### Server Key and Certificate #1



<b>Subject</b>	prestations.vd.ch Fingerprint SHA256: 6a056ddb32a43e8b7b88a7e6e7383db1ea2f365e33c42aa121f546ed45bfe22 Pin SHA256: sQqP2ulKC5Pukp7nsrZuuMHv+j5/dcFparF8bODxPH8=
<b>Common names</b>	prestations.vd.ch
<b>Alternative names</b>	prestations.vd.ch www.prestations.vd.ch
<b>Serial Number</b>	2c8dbbfa5bbc843dcc2e6385466efe6caa1b1399
<b>Valid from</b>	Tue, 10 Dec 2019 09:08:56 UTC
<b>Valid until</b>	Fri, 10 Dec 2021 09:08:56 UTC (expires in 1 year and 2 months)
<b>Key</b>	RSA 2048 bits (e 65537)
<b>Weak key (Debian)</b>	No
<b>Issuer</b>	SwissSign EV Gold CA 2014 - G22 AIA: <a href="http://swissign.net/cgi-bin/authority/download/EEFD46CAF7275E91BC5AB6E787CD0AFA550A2642">http://swissign.net/cgi-bin/authority/download/EEFD46CAF7275E91BC5AB6E787CD0AFA550A2642</a>
<b>Signature algorithm</b>	SHA256withRSA
<b>Extended Validation</b>	Yes
<b>Certificate Transparency</b>	Yes (certificate)
<b>OCSP Must Staple</b>	No
<b>Revocation information</b>	CRL, OCSP CRL: <a href="http://crl.swissign.net/EEFD46CAF7275E91BC5AB6E787CD0AFA550A2642">http://crl.swissign.net/EEFD46CAF7275E91BC5AB6E787CD0AFA550A2642</a> OCSP: <a href="http://gold-ev-g2.ocsp.swissign.net/EEFD46CAF7275E91BC5AB6E787CD0AFA550A2642">http://gold-ev-g2.ocsp.swissign.net/EEFD46CAF7275E91BC5AB6E787CD0AFA550A2642</a>
<b>Revocation status</b>	Good (not revoked)
<b>DNS CAA</b>	No ( <a href="#">more info</a> )
<b>Trusted</b>	Yes Mozilla Apple Android Java Windows



### Additional Certificates (if supplied)



<b>Certificates provided</b>	3 (5589 bytes)
<b>Chain issues</b>	Contains anchor
<b>#2</b>	SwissSign EV Gold CA 2014 - G22
<b>Subject</b>	Fingerprint SHA256: a434aae4e15a5519e9b111fd08ec190fd2adf13bbe30815c6e1606555cb31450 Pin SHA256: mDKR5ptpp7PqVUefxx2Ftq5ymsEuzCEg+EVrLQrQFB8=

### Additional Certificates (if supplied)



Valid until	Sun, 04 Mar 2035 16:16:37 UTC (expires in 14 years and 5 months)
Key	RSA 2048 bits (e 65537)
Issuer	SwissSign Gold CA - G2
Signature algorithm	SHA256withRSA

#3

Subject	SwissSign Gold CA - G2 <a href="#">In trust store</a> Fingerprint SHA256: 62dd0be9b9f50a163ea0f8e75c053b1eca57ea55c8688f647c6881f2c8357b95 Pin SHA256: QPz8KliddzL/ry99s10MzEtpjxO/PO9extQXCICCuAnQ=
Valid until	Sat, 25 Oct 2036 08:30:35 UTC (expires in 16 years and 1 month)
Key	RSA 4096 bits (e 65537)
Issuer	SwissSign Gold CA - G2 Self-signed
Signature algorithm	SHA1withRSA Weak, but no impact on root certificate



### 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_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	ECDH secp256r1 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	ECDH secp256r1 (eq. 3072 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)	ECDH secp256r1 (eq. 3072 bits RSA) FS <b>WEAK</b>	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)	ECDH secp256r1 (eq. 3072 bits RSA) FS <b>WEAK</b>	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	ECDH secp256r1 (eq. 3072 bits RSA) FS <b>WEAK</b>	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	ECDH secp256r1 (eq. 3072 bits RSA) FS <b>WEAK</b>	128
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f)	DH 2048 bits FS	256
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e)	DH 2048 bits FS	128



### Handshake Simulation

<a href="#">Android 4.4.2</a>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
<a href="#">Android 5.0.0</a>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
<a href="#">Android 6.0</a>	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
<a href="#">Android 7.0</a>	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
<a href="#">Android 8.0</a>	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
<a href="#">Android 8.1</a>	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
<a href="#">Android 9.0</a>	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
<a href="#">BingPreview Jan 2015</a>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
<a href="#">Chrome 49 / XP SP3</a>	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
<a href="#">Chrome 69 / Win 7</a> R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
<a href="#">Chrome 70 / Win 10</a>	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
<a href="#">Chrome 80 / Win 10</a> R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
<a href="#">Firefox 31.3.0 ESR / Win 7</a>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS

## Handshake Simulation

<a href="#">Firefox 47 / Win 7</a> R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">Firefox 49 / XP SP3</a>	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
<a href="#">Firefox 62 / Win 7</a> R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
<a href="#">Firefox 73 / Win 10</a> R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
<a href="#">Googlebot Feb 2018</a>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
<a href="#">IE 11 / Win 7</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1	FS
<a href="#">IE 11 / Win 8.1</a> R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1	FS
<a href="#">IE 11 / Win Phone 8.1</a> R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	ECDH secp256r1	FS
<a href="#">IE 11 / Win Phone 8.1 Update</a> R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1	FS
<a href="#">IE 11 / Win 10</a> R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
<a href="#">Edge 15 / Win 10</a> R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
<a href="#">Edge 16 / Win 10</a> R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
<a href="#">Edge 18 / Win 10</a> R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
<a href="#">Edge 13 / Win Phone 10</a> R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
<a href="#">Java 8u161</a>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
<a href="#">Java 11.0.3</a>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
<a href="#">Java 12.0.1</a>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
<a href="#">OpenSSL 1.0.1l</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
<a href="#">OpenSSL 1.0.2s</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
<a href="#">OpenSSL 1.1.0k</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
<a href="#">OpenSSL 1.1.1c</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
<a href="#">Safari 6 / iOS 6.0.1</a>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1	FS
<a href="#">Safari 7 / iOS 7.1</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1	FS
<a href="#">Safari 7 / OS X 10.9</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1	FS
<a href="#">Safari 8 / iOS 8.4</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1	FS
<a href="#">Safari 8 / OS X 10.10</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1	FS
<a href="#">Safari 9 / iOS 9</a> R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
<a href="#">Safari 9 / OS X 10.11</a> R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
<a href="#">Safari 10 / iOS 10</a> R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
<a href="#">Safari 10 / OS X 10.12</a> R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
<a href="#">Safari 12.1.2 / MacOSX 10.14.6 Beta</a> R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
<a href="#">Safari 12.1.1 / iOS 12.3.1</a> R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
<a href="#">Apple ATS 9 / iOS 9</a> R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
<a href="#">Yahoo Slurp Jan 2015</a>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
<a href="#">YandexBot Jan 2015</a>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	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) 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

	No, server keys and hostname not seen elsewhere with SSLv2
<b>DROWN</b>	(1) For a better understanding of this test, please read <a href="#">this longer explanation</a> (2) Key usage data kindly provided by the <a href="#">Censys</a> network search engine; original DROWN website <a href="#">here</a> (3) Censys data is only indicative of possible key and certificate reuse; possibly out-of-date and not complete
<b>Secure Renegotiation</b>	<b>Supported</b>
<b>Secure Client-Initiated Renegotiation</b>	No
<b>Insecure Client-Initiated Renegotiation</b>	No
<b>BEAST attack</b>	Mitigated server-side ( <a href="#">more info</a> )
<b>POODLE (SSLv3)</b>	No, SSL 3 not supported ( <a href="#">more info</a> )
<b>POODLE (TLS)</b>	No ( <a href="#">more info</a> )
<b>Zombie POODLE</b>	No ( <a href="#">more info</a> ) TLS 1.2 : 0xc027

## Protocol Details

GOLDDOODLE	No ( <a href="#">more info</a> )	TLS 1.2 : 0xc027
OpenSSL 0-Length	No ( <a href="#">more info</a> )	TLS 1.2 : 0xc027
Sleeping POODLE	No ( <a href="#">more info</a> )	TLS 1.2 : 0xc027
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 ( <a href="#">more info</a> )	
Ticketbleed (vulnerability)	No ( <a href="#">more info</a> )	
OpenSSL CCS vuln. (CVE-2014-0224)	No ( <a href="#">more info</a> )	
OpenSSL Padding Oracle vuln. (CVE-2016-2107)	No ( <a href="#">more info</a> )	
ROBOT (vulnerability)	No ( <a href="#">more info</a> )	
<b>Forward Secrecy</b>	<b>Yes (with most browsers) ROBUST</b> ( <a href="#">more info</a> )	
ALPN	Yes	http/1.1
NPN	No	
Session resumption (caching)	Yes	
Session resumption (tickets)	No	
OCSP stapling	No	
<b>Strict Transport Security (HSTS)</b>	<b>Yes</b> max-age=157680000	
HSTS Preloading	Not in: Chrome Edge Firefox IE	
Public Key Pinning (HPKP)	No ( <a href="#">more info</a> )	
Public Key Pinning Report-Only	No	
Public Key Pinning (Static)	No ( <a href="#">more info</a> )	
Long handshake intolerance	No	
TLS extension intolerance	No	
TLS version intolerance	TLS 1.152 TLS 2.152	
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	secp256r1, secp384r1, secp224r1, secp521r1 (server preferred order)	
SSL 2 handshake compatibility	No	



## HTTP Requests



- 1 <https://prestations.vd.ch/> (HTTP/1.1 302 Found : Moved Temporarily)
- 2 <https://prestations.vd.ch/100002/> (HTTP/1.1 302 )
- 3 [https://prestations.vd.ch/100018/login?goto\\_disabled=https%3A%2F%2Fprestations.vd.ch%3A443%2F100002%2F](https://prestations.vd.ch/100018/login?goto_disabled=https%3A%2F%2Fprestations.vd.ch%3A443%2F100002%2F) (HTTP/1.1 200 )



## Miscellaneous

Test date	Tue, 15 Sep 2020 15:25:14 UTC
Test duration	74.240 seconds
HTTP status code	200
HTTP server signature	-
Server hostname	-