

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

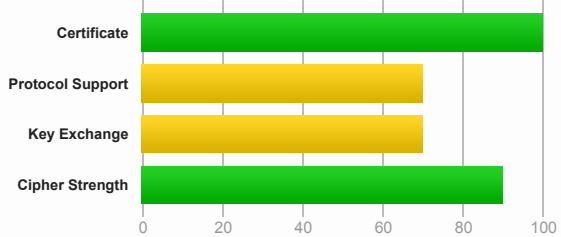
SSL Report: fao.ge.ch (160.53.144.72)

Assessed on: Wed, 16 Sep 2020 11:17:03 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](#).

This server supports weak Diffie-Hellman (DH) key exchange parameters. Grade capped to B. [MORE INFO »](#)

Server sent invalid HSTS policy. See below for further information.

This server supports TLS 1.0 and TLS 1.1. Grade capped to B. [MORE INFO »](#)

Certificate #1: RSA 4096 bits (SHA256withRSA)



Server Key and Certificate #1



Subject	*.ge.ch Fingerprint SHA256: 850b8d44d03348f5b8cc2aa43179109ac2bdd99a4f2f9fd6ebe7e38d146dfe Pin SHA256: yNNettkphbaM/qewe89s6r3Eg2uQsPWkMWOrDDpJIH0=
Common names	*.ge.ch
Alternative names	*.ge.ch ge.ch
Serial Number	32f9adabf93099055f42050f8ecbec7f097202b1
Valid from	Fri, 13 Dec 2019 10:50:11 UTC
Valid until	Mon, 13 Dec 2021 10:50:11 UTC (expires in 1 year and 2 months)
Key	RSA 4096 bits (e 65537)
Weak key (Debian)	No
Issuer	SwissSign Server Gold CA 2014 - G22 AIA: http://swissign.net/cgi-bin/authority/download/E7F1E7FD2E53AD11E5811A57A4738F127D98C8AE
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	Yes (certificate)
OCSP Must Staple	No
Revocation information	CRL, OCSP CRL: http://crl.swissign.net/E7F1E7FD2E53AD11E5811A57A4738F127D98C8AE OCSP: http://gold-server-g2.ocsp.swissign.net/E7F1E7FD2E53AD11E5811A57A4738F127D98C8AE
Revocation status	Good (not revoked)
DNS CAA	No (more info)
Trusted	Yes Mozilla Apple Android Java Windows



Additional Certificates (if supplied)



Certificates provided	3 (5596 bytes)
Chain issues	Contains anchor

#2

Additional Certificates (if supplied)



Subject	SwissSign Server Gold CA 2014 - G22 Fingerprint SHA256: 561dc78351f5e7ee5a464ac6e58a0d164ef2768f98f02e6ee65501120fcd9c5e Pin SHA256: skyozdmp140lJrHv/Rijq3v2/yQ1nyfFyBIa9uOKuw8=
Valid until	Sat, 15 Sep 2029 14:09:12 UTC (expires in 8 years and 11 months)
Key	RSA 2048 bits (e 65537)
Issuer	SwissSign Gold CA - G2
Signature algorithm	SHA256withRSA

#3

Subject	SwissSign Gold CA - G2 In trust store 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	Yes
TLS 1.0	Yes
SSL 3	No
SSL 2	No



Cipher Suites

TLS 1.2 (suites in server-preferred order)



TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	ECDH secp384r1 (eq. 7680 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	ECDH secp384r1 (eq. 7680 bits RSA) FS WEAK	128
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)	ECDH secp384r1 (eq. 7680 bits RSA) FS WEAK	128
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	ECDH secp384r1 (eq. 7680 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	ECDH secp384r1 (eq. 7680 bits RSA) FS WEAK	256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)	ECDH secp384r1 (eq. 7680 bits RSA) FS WEAK	256
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c)	WEAK	128
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_GCM_SHA384 (0x9d)	WEAK	256
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)	WEAK	256
TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d)	WEAK	256
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (0x41)	WEAK	128
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (0x84)	WEAK	256
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e)	DH 1024 bits FS WEAK	128
TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33)	DH 1024 bits FS WEAK	128
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x67)	DH 1024 bits FS WEAK	128
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f)	DH 1024 bits FS WEAK	256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39)	DH 1024 bits FS WEAK	256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x6b)	DH 1024 bits FS WEAK	256
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (0x45)	DH 1024 bits FS WEAK	128
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0x88)	DH 1024 bits FS WEAK	256

Cipher Suites

TLS 1.1 (suites in server-preferred order)



TLS 1.0 (suites in server-preferred order)



Handshake Simulation

Android 2.3.7 No SNI ²	RSA 4096 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA	No FS
Android 4.0.4	RSA 4096 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp384r1 FS
Android 4.1.1	RSA 4096 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp384r1 FS
Android 4.2.2	RSA 4096 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp384r1 FS
Android 4.3	RSA 4096 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp384r1 FS
Android 4.4.2	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp384r1 FS
Android 5.0.0	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp384r1 FS
Android 6.0	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp384r1 FS
Android 7.0	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp384r1 FS
Android 8.0	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp384r1 FS
Android 8.1	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp384r1 FS
Android 9.0	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp384r1 FS
Baidu Jan 2015	RSA 4096 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp384r1 FS
BingPreview Jan 2015	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp384r1 FS
Chrome 49 / XP SP3	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp384r1 FS
Chrome 69 / Win 7 R	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp384r1 FS
Chrome 70 / Win 10	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp384r1 FS
Chrome 80 / Win 10 R	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp384r1 FS
Firefox 31.3.0 ESR / Win 7	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp384r1 FS
Firefox 47 / Win 7 R	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp384r1 FS
Firefox 49 / XP SP3	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp384r1 FS
Firefox 62 / Win 7 R	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp384r1 FS
Firefox 73 / Win 10 R	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp384r1 FS
Googlebot Feb 2018	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp384r1 FS
IE 7 / Vista	RSA 4096 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp384r1 FS
IE 8 / XP No FS ¹ No SNI ²			Server sent fatal alert: handshake_failure	
IE 8-10 / Win 7 R	RSA 4096 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp384r1 FS
IE 11 / Win 7 R	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp384r1 FS
IE 11 / Win 8.1 R	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp384r1 FS
IE 10 / Win Phone 8.0	RSA 4096 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp384r1 FS
IE 11 / Win Phone 8.1 R	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp384r1 FS
IE 11 / Win Phone 8.1 Update R	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp384r1 FS
IE 11 / Win 10 R	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp384r1 FS
Edge 15 / Win 10 R	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp384r1 FS
Edge 16 / Win 10 R	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp384r1 FS
Edge 18 / Win 10 R	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp384r1 FS
Edge 13 / Win Phone 10 R	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp384r1 FS
Java 6u45 No SNI ²	RSA 4096 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA	No FS
Java 7u25	RSA 4096 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp384r1 FS
Java 8u161	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp384r1 FS
Java 11.0.3	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp384r1 FS
Java 12.0.1	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp384r1 FS
OpenSSL 0.9.8y	RSA 4096 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA	No FS
OpenSSL 1.0.1l R	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp384r1 FS
OpenSSL 1.0.2s R	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp384r1 FS
OpenSSL 1.1.0k R	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp384r1 FS
OpenSSL 1.1.1c R	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp384r1 FS
Safari 5.1.9 / OS X 10.6.8	RSA 4096 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp384r1 FS
Safari 6 / iOS 6.0.1	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp384r1 FS
Safari 6.0.4 / OS X 10.8.4 R	RSA 4096 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp384r1 FS

Handshake Simulation

Safari 7 / iOS 7.1 R	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp384r1	FS
Safari 7 / OS X 10.9 R	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp384r1	FS
Safari 8 / iOS 8.4 R	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp384r1	FS
Safari 8 / OS X 10.10 R	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp384r1	FS
Safari 9 / iOS 9 R	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp384r1	FS
Safari 9 / OS X 10.11 R	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp384r1	FS
Safari 10 / iOS 10 R	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp384r1	FS
Safari 10 / OS X 10.12 R	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp384r1	FS
Safari 12.1.2 / MacOS 10.14.6 Beta R	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp384r1	FS
Safari 12.1.1 / iOS 12.3.1 R	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp384r1	FS
Apple ATS 9 / iOS 9 R	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp384r1	FS
Yahoo Slurp Jan 2015	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp384r1	FS
YandexBot Jan 2015	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp384r1	FS

Not simulated clients (Protocol mismatch)

[IE 6 / XP](#) No FS¹ No SNI² Protocol mismatch (not simulated)

(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	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 complete
Secure Renegotiation	Supported
Secure Client-Initiated Renegotiation	Yes
Insecure Client-Initiated Renegotiation	No
BEAST attack	Not mitigated server-side (more info) TLS 1.0: 0xc013
POODLE (SSLv3)	No, SSL 3 not supported (more info)
POODLE (TLS)	No (more info)
Zombie POODLE	No (more info) TLS 1.2: 0xc013
GOLDENDOODLE	No (more info) TLS 1.2: 0xc013
OpenSSL 0-Length	No (more info) TLS 1.2: 0xc013
Sleeping POODLE	No (more info) TLS 1.2: 0xc013
Downgrade attack prevention	Yes, TLS_FALLBACK_SCSV supported (more info)
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	Weak key exchange WEAK
ALPN	No
NPN	No
Session resumption (caching)	Yes
Session resumption (tickets)	No
OCSF stapling	No
Strict Transport Security (HSTS)	Invalid Server provided more than one HSTS header
HSTS Preloading	Not in: Chrome Edge Firefox IE
Public Key Pinning (HPKP)	No (more info)
Public Key Pinning Report-Only	No

Protocol Details

Public Key Pinning (Static)	No (more info)
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	Yes
ECDH public server param reuse	No
Supported Named Groups	secp384r1, secp256r1, x25519 (server preferred order)
SSL 2 handshake compatibility	Yes



HTTP Requests



- 1 <https://fao.ge.ch/> (HTTP/1.1 302 Moved Temporarily)
- 2 <https://fao.ge.ch/captcha?t=5cadce5f86d8a24485a9d988e9e21c12> (HTTP/1.1 301 Moved Permanently)
- 3 <https://fao.ge.ch/captcha?t=5cadce5f86d8a24485a9d988e9e21c12> (HTTP/1.1 200 OK)



Miscellaneous

Test date	Wed, 16 Sep 2020 11:14:22 UTC
Test duration	161.498 seconds
HTTP status code	200
HTTP server signature	Apache
Server hostname	cds.ge.ch