

Your browser trusts many CAs **by default**

Keychain Access

Click to unlock the System Roots keychain.

Keychains

- login
- Microsoft_Int...diate_Certificates
- Local Items
- System
- System Roots**

Category

- All Items
- Passwords
- Secure Notes
- My Certificates
- Keys
- Certificates**

GeoTrust Global CA
Root certificate authority
Expires: Saturday, May 21, 2022 at 7:00:00 AM Arabian Standard Time
This certificate is valid

| Name | Kind | Expires | Keychain |
|---|--------------------|---------------------------------|---------------------|
| Echoworx Root CA2 | certificate | Oct 7, 2030, 1:49:13 PM | System Roots |
| EE Certification Centre Root CA | certificate | Dec 18, 2030, 2:59:59 AM | System Roots |
| Entrust Root Certification Authority | certificate | Nov 27, 2026, 11:53:42 PM | System Roots |
| Entrust Root Certification Authority - EC1 | certificate | Dec 18, 2037, 6:55:36 PM | System Roots |
| Entrust Root Certification Authority - G2 | certificate | Dec 7, 2030, 8:55:54 PM | System Roots |
| Entrust.net Certification Authority (2048) | certificate | Dec 24, 2019, 9:20:51 PM | System Roots |
| Entrust.net Certification Authority (2048) | certificate | Jul 24, 2029, 5:15:12 PM | System Roots |
| ePKI Root Certification Authority | certificate | Dec 20, 2034, 5:31:27 AM | System Roots |
| Federal Common Policy CA | certificate | Dec 1, 2030, 7:45:27 PM | System Roots |
| GeoTrust Global CA | certificate | May 21, 2022, 7:00:00 AM | System Roots |
| GeoTrust Primary Certification Authority | certificate | Jul 17, 2036, 2:59:59 AM | System Roots |
| GeoTrust Primary Certification Authority - G2 | certificate | Jan 19, 2038, 2:59:59 AM | System Roots |
| GeoTrust Primary Certification Authority - G3 | certificate | Dec 2, 2037, 2:59:59 AM | System Roots |
| Global Chambersign Root | certificate | Sep 30, 2037, 7:14:18 PM | System Roots |
| Global Chambersign Root - 2008 | certificate | Jul 31, 2038, 3:31:40 PM | System Roots |
| GlobalSign | certificate | Mar 18, 2029, 1:00:00 PM | System Roots |
| GlobalSign | certificate | Jan 19, 2038, 6:14:07 AM | System Roots |
| GlobalSign | certificate | Jan 19, 2038, 6:14:07 AM | System Roots |
| GlobalSign | certificate | Dec 15, 2021, 11:00:00 AM | System Roots |
| GlobalSign Root CA | certificate | Jan 28, 2028, 3:00:00 PM | System Roots |
| Go Daddy Class 2 Certification Authority | certificate | Jun 29, 2034, 8:06:20 PM | System Roots |
| Go Daddy Root Certificate Authority - G2 | certificate | Jan 1, 2038, 2:59:59 AM | System Roots |
| Government Root Certification Authority | certificate | Dec 31, 2037, 6:59:59 PM | System Roots |
| Hellenic Academic and Research Institutions RootCA 2011 | certificate | Dec 1, 2031, 4:49:52 PM | System Roots |
| Hongkong Post Root CA 1 | certificate | May 15, 2023, 7:52:29 AM | System Roots |

177 Items

Real attacks

Google Security Blog

The latest news and insights from Google on security and safety on the Internet

An update on attempted man-in-the-middle attacks

August 29, 2011

Posted by Heather Adkins, Information Security Manager

Today we received reports of attempted SSL man-in-the-middle (MITM) attacks against Google users, whereby someone tried to get between them and encrypted Google services. The people affected were primarily located in Iran. The attacker used a fraudulent SSL certificate issued by DigiNotar, a root certificate authority that should not issue certificates for Google (and has since revoked it).

Google Chrome users were protected from this attack because Chrome was able to [detect](#) the fraudulent certificate.

Google Security Blog

The latest news and insights from Google on security and safety on the Internet

Enhancing digital certificate security

January 3, 2013

Posted by Adam Langley, Software Engineer

Late on December 24, Chrome detected and blocked an unauthorized digital certificate for the "*.google.com" domain. We investigated immediately and found the certificate was issued by an [intermediate certificate authority](#) (CA) linking back to TURKTRUST, a Turkish certificate authority. Intermediate CA certificates carry the full authority of the CA, so anyone who has one can use it to create a certificate for any website they wish to impersonate.