Your web browser trusts a lot of certification authorities and chained sub-authorities, and it does so blindly. "[Subordinate or intermediate certification authorities](http://en.wikipedia.org/wiki/Intermediate_certificate_authorities)" are a little known device: The root CAs in your browser can delegate permission to issue certificates to an unlimited amount of subordinate CAs ([SCA](http://www.linuxsecurity.com/component/option,com_dictionary/task,view/id,411/)) just by signing their certificate, not by borrowing their precious private key to them. You can even buy yourself such a CA from [GeoTrust](http://geotrust.com/enterprise-ssl-certificates/georoot/) or [elsewhere](http://www.sslshopper.com/article-trusted-root-signing-certificates.html). You may also want to obtain them from [CNNIC](http://googleonlinesecurity.blogspot.de/2015/03/maintaining-digital-certificate-security.html).

Here's a friendly [example of a certificate issued by an ICA](https://opacplus.bsb-muenchen.de/). You never knew your browser trusts the Bavarian National Library, right? It is unclear how many intermediate certification authorities really exist, and yet each of them has god-like power to impersonate any https web site using a [Man in the Middle](http://en.wikipedia.org/wiki/Man-in-the-middle_attack) (MITM) attack scenario. [Researchers at Princeton are acknowledging this problem](http://www.freedom-to-tinker.com/blog/sjs/web-security-trust-models) and recommending Certificate Patrol. Revealing the inner workings of [X.509](http://en.wikipedia.org/wiki/X.509) to end users is still considered too hard, but only getting familiar with this will really help you get in control. That's why Certificate Patrol gives you insight of what is happening.

If you still think a MITM attack is unlikely to happen to you, [read this user report](http://bitsandchaos.wordpress.com/2010/03/29/certificate-patrol-can-really-save-your-pocket/). Somebody noticed a company called MarkMonitor has taken control over the Internet's most essential services and brands. [Here's a copy of the story](http://patrol.psyced.org/markmonitor) for your convenience. Again, CertPatrol seems to be your best bet in defense of your civil liberties. **News:** [Tina Membe also considers the X.509 certification architecture hopelessly insecure](https://medium.com/@pepelephew/how-to-intercept-all-wire-voice-and-video-calls-13da1246675c) which now in 2017, considering [the many woes of X.509](https://en.wikipedia.org/wiki/X.509#Security) is a [quite](https://blogs.fsfe.org/larma/2017/signal-backdoors/) common expertise.

Certificate Patrol doesn't actually work in Thunderbird. [Here's an interesting workaround](http://forums.mozillazine.org/viewtopic.php?f=39&t=2687657) if you want to pin down the certificate of your mail server.