Using TQSL (ARRL Log Book of the World) Certificates for Online Authentication

At the September 2013 DCC, Heikki Hannikainen, OH7LZB, presented on Friday morning a talk about authenticating amateur radio services on the Internet.

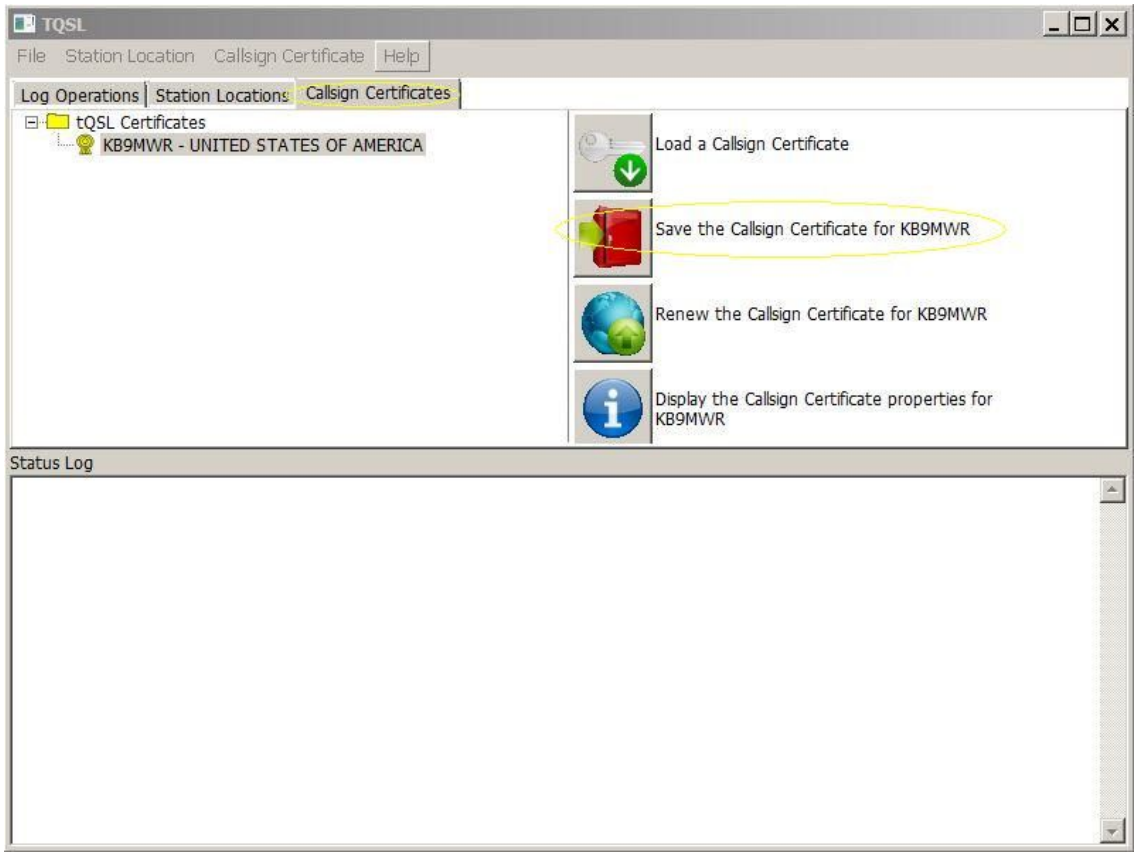
Some of the interesting sites allow you transmit RF, directly or indirectly. Such as IRLP, EchoLink, Allstar APRS-IS, remotehamradio.com etc. And there is more potential for that. I.e. text messages for DMR, APRS, SDR, and remotely operated stations.

Presently each such service has a different manual authentication method.

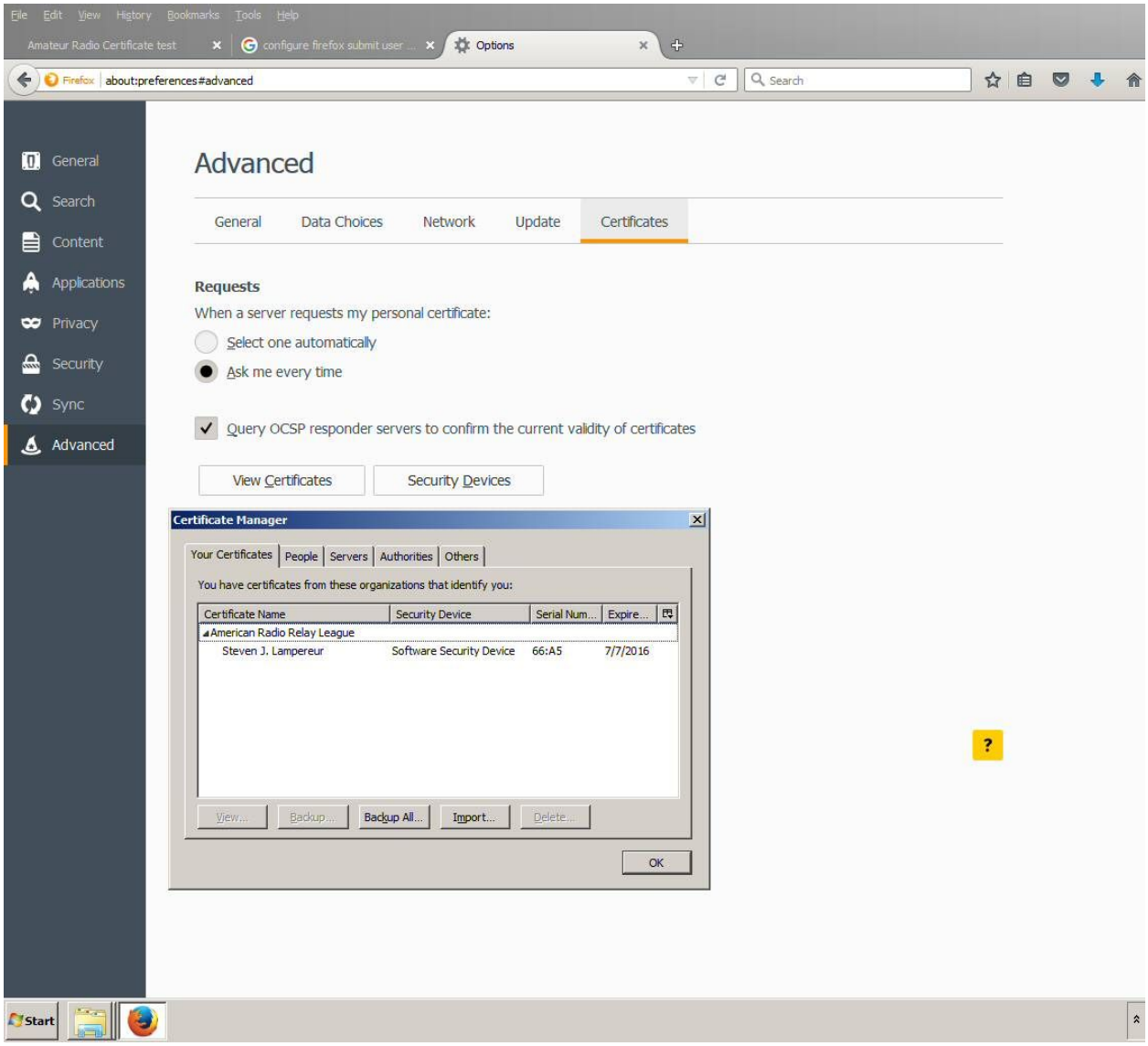
The ARRL Log of the World Certificate conforms to the X.509 standard used all over the internet. It may be installed on web browser, and used to log into web services. Any third party can technically validate that the web user connecting really has an ARRL LoTW certificate. Anyone implementing this method on their website to restrict access to hams, does not get access to the users private key. This is the same crypto used by banks and the military. The ARRL doesn't need to do any additional work to make this happen. Websites implementing this do not need to query the ARRL anything about the user. No single point of failure.

There are plenty of developers who would be happy to create new web services for hams. They just don't have the time or motivation to go through all the license papers to manually authenticate them.
http://sigspace.wordpress.com/2013/09/21/tapr-dcc-authenticating-amateur-radio-services-on-the-internet/ - Providing authenticated amateur radio services on the Internet - OH7LZB
http://www.youtube.com/watch?v=7anDmQQfyu8 Video presentation from the DCC
Notes on setting up a OpenVPN server that uses LoTW keys
http://authtest.aprs.fi - authentication demo site
https://github.com/hessu/ham-cert-web-demo - Apache configuration and PHP scripts

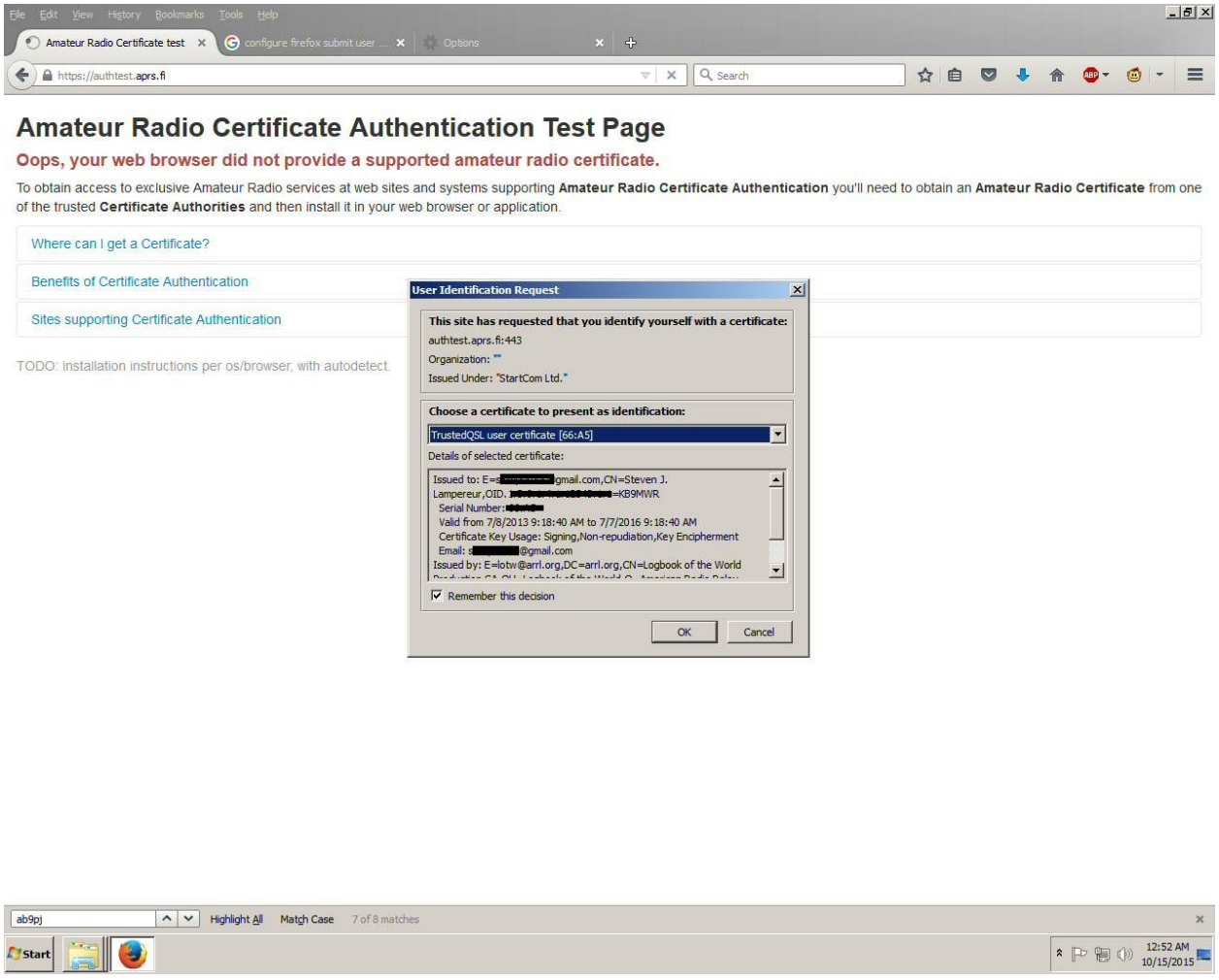
To save your P12 certificate out of the TQSL program

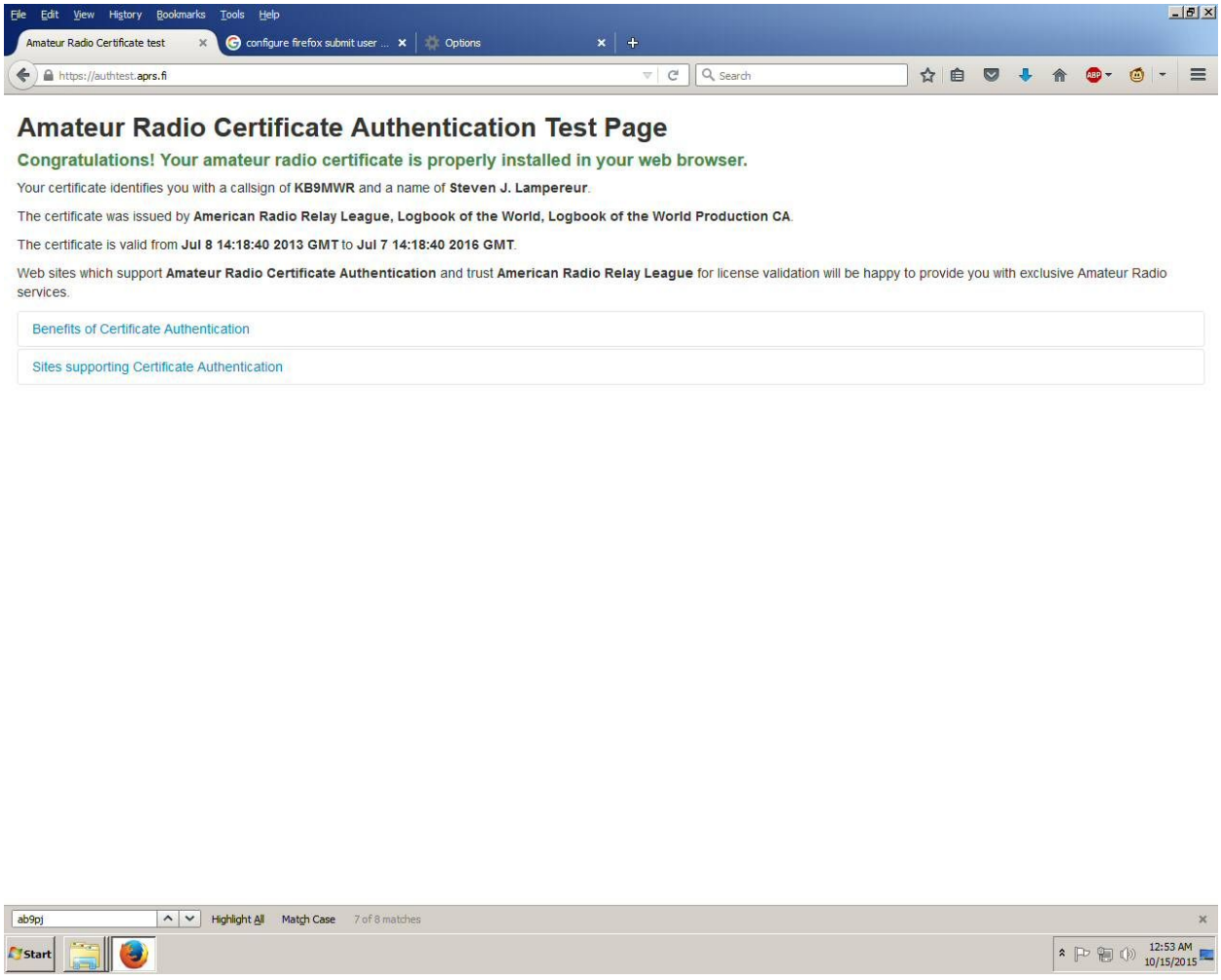


Then add the LoTW CALLSIGN.P12 file to your browser like so. Options -> Advanced -> Certificates in FireFox



In the future websites seeking authentication will show this.


File Edit View History Bookmarks Tools Help
Amateur Radio Certificate test
configure firefox submit user ....
Options
https://authtest.aprs.fi
Search
Amateur Radio Certificate Authentication Test Page
Oops, your web browser did not provide a supported amateur radio certificate.
To obtain access to exclusive Amateur Radio services at web sites and systems supporting Amateur Radio Certificate Authentication you'll need to obtain an Amateur Radio Certificate from one of the trusted Certificate Authorities and then install it in your web browser or application.
Where can I get a Certificate?
Benefits of Certificate Authentication
Sites supporting Certificate Authentication
TODO: installation instructions per os/browser, with autodetect.
User Identification Request
This site has requested that you identify yourself with a certificate:
authtest.aprs.fi:443
Organization: ""
Issued Under: "StartCom Ltd."
Choose a certificate to present as identification:
TrustedQSL user certificate [66:A5]
Details of selected certificate:
Issued to: E=[redacted]gmail.com,CN=Steven J. Lampereur,OID.[redacted]=KB9MWR
Serial Number:[redacted]
Valid from 7/8/2013 9:18:40 AM to 7/7/2016 9:18:40 AM
Certificate Key Usage: Signing,Non-repudiation,Key Encipherment
Email: [redacted]@gmail.com
Issued by: E=lotw@arrl.org,DC=arrl.org,CN=Logbook of the World
Remember this decision
OK
Cancel
ab9pj
Highlight All
Match Case
7 of 8 matches
Start
12:52 AM
10/15/2015


File Edit View History Bookmarks Tools Help
Amateur Radio Certificate test
configure firefox submit user ...
Options
https://authtest.aprs.fi
Search
Amateur Radio Certificate Authentication Test Page
Congratulations! Your amateur radio certificate is properly installed in your web browser.
Your certificate identifies you with a callsign of KB9MWR and a name of Steven J. Lampereur.
The certificate was issued by American Radio Relay League, Logbook of the World, Logbook of the World Production CA.
The certificate is valid from Jul 8 14:18:40 2013 GMT to Jul 7 14:18:40 2016 GMT.
Web sites which support Amateur Radio Certificate Authentication and trust American Radio Relay League for license validation will be happy to provide you with exclusive Amateur Radio services.
Benefits of Certificate Authentication
Sites supporting Certificate Authentication
ab9pj
Highlight All
Match Case
7 of 8 matches
Start
12:53 AM
10/15/2015