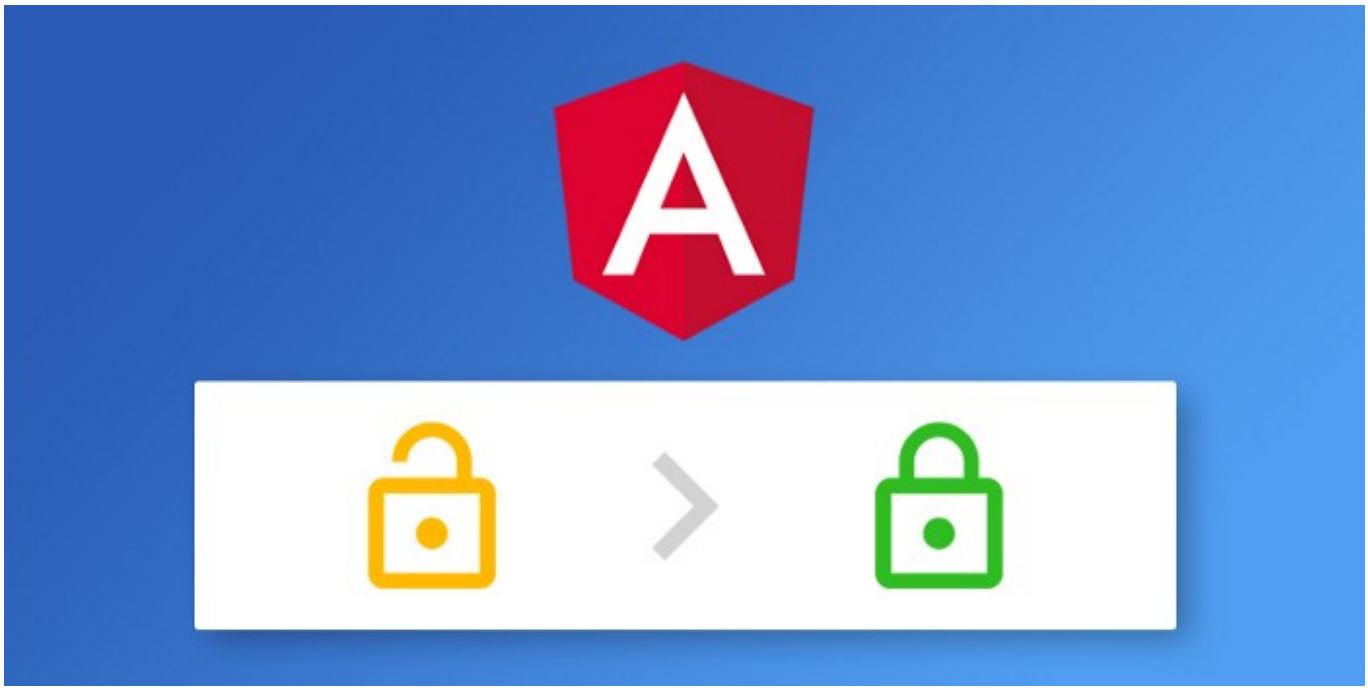
Ruben Vermeulen

Follow 102 Followers About

Running Angular CLI over HTTPS with a Trusted Certificate

 Ruben Vermeulen Feb 25, 2018 · 4 min read



Running an Angular application over a secure connection is pretty straight forward. There are plenty of tutorials how you can enable this. However, you can run into some problems.

most common problems.

Let's get started!

Enabling SSL

The Angular CLI provides us with three parameters we can pass along with the *ng serve command* to enable and configure SSL.

```
// enable or disable SSL
--ssl <boolean: defaults to false>

// path to root certificate
--ssl-cert <string: defaults to "ssl/server.crt">

// path to private key
--ssl-key <string: defaults to "ssl/server.key">
```

ANGULAR 6 REQUIRES YOU TO DEFINE THE PARAMS: `--ssl-cert` AND `--ssl-key`.

Example #1

```
ng serve —-ssl true
```

1. SSL is enabled
2. Check whether there is a certificate and private key in the default *ssl* folder
3. If nothing is found, the CLI will generate his own certificate and private key

Example #2

```
ng serve \
    --ssl true \
    --ssl-cert "/home/john/ssl/example.crt" \
    --ssl-key "/home/john/ssl/example.key"
```

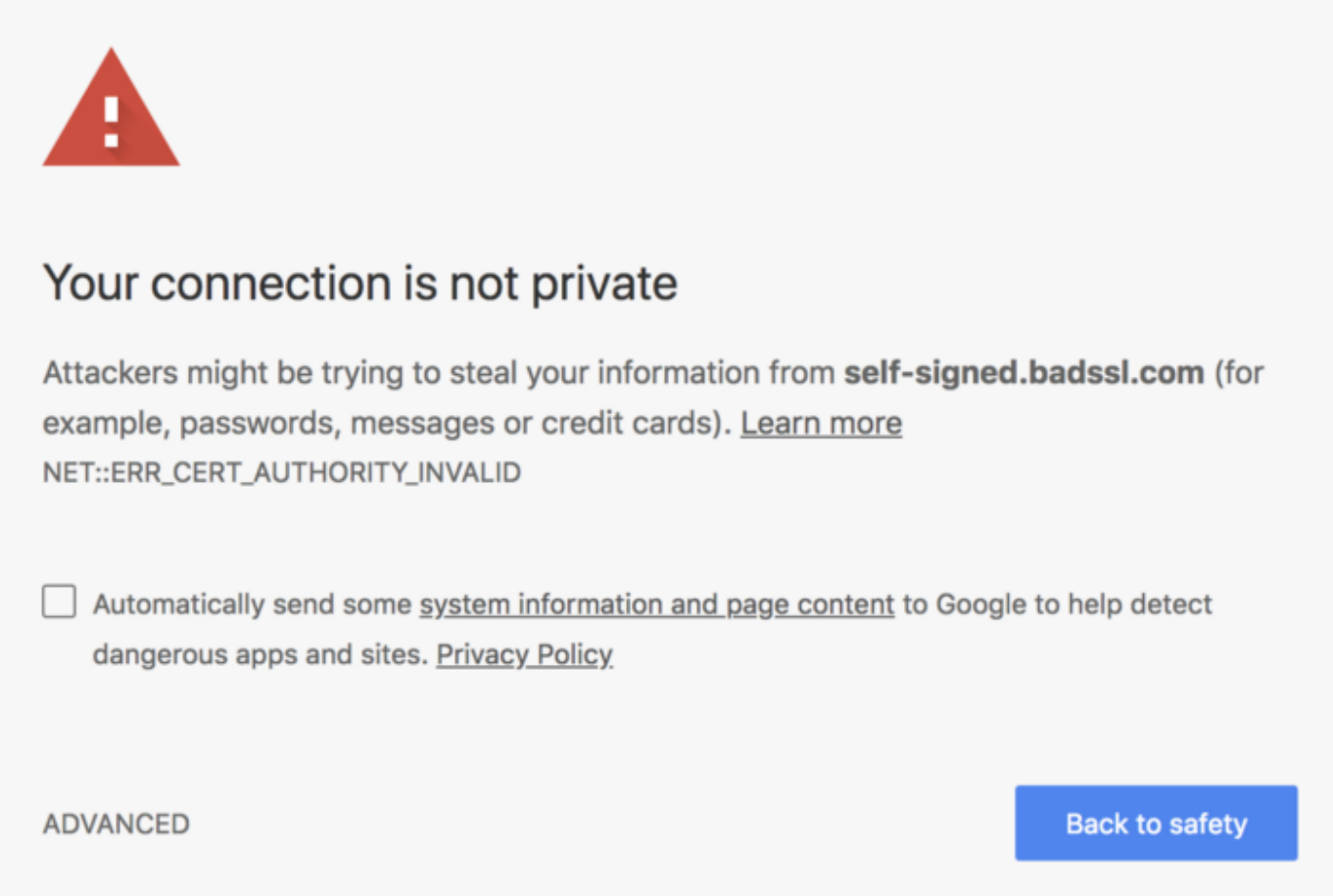
2. Check whether there is a certificate and private key in the given path

3. If nothing is found, the CLI will generate his own certificate and private key

Problems

1. The browser doesn't trust our certificate, so we get a warning
2. Disconnect and restart loop

Certificate is not trusted



This problem is pretty easy to bypass. We can just ignore the warning and continue to visit our application.

If you don't experience the second problem and you can live with the fact you have an untrusted certificate, you can just stop right here and keep on developing your awesome application.

that listens to the event that restarts the application when a piece of code has changed. Along with the disconnect, the application restarts several times over and over again.

Disconnect and restart loop

Several people have/had this problem. There's an issue reported in Github in the Angular repository.

Issue: https://github.com/angular/angular-cli/issues/5826

Solution

To solve all the problems, the only thing we need is for our browser to trust our certificate. For some reason the Angular CLI doesn't have any problems when we use a trusted certificate. So this means by using a trusted certificate both problems are solved.

Trusted secure connection

Requirements

OS X

You should be all set. OS X has by default openssl installed.

Windows 10

Install openssl. I recommend using the *Git bash*. It has openssl preinstalled. *Git Bash* is bundled with the *Git* installer.

https://git-scm.com/

Step 1: Generate a certificate

Clone the following repository on your local machine and run the *generate.sh* script in either the *terminal* or *Git Bash*. The repository contains all necessary configuration for

https://github.com/RubenVermeulen/generate-trusted-ssl-certificate

```
git clone https://github.com/RubenVermeulen/generate-trusted-ssl-certificate.git

cd generate-trusted-ssl-certificate

bash generate.sh
```

You should now have a *server.crt* and a *server.key* file in the repository folder.

Step 2: Install the certificate

We have to make sure the browser trust our certificate, so we're going to install it on our local machine.

OS X

1. Double click on the certificate (server.crt)
2. Select your desired keychain (*login* should suffice)
3. Add the certificate
4. Open *Keychain Access* if it isn't already open
5. Select the keychain you chose earlier
6. You should see the certificate *localhost*
7. Double click on the certificate
8. Expand *Trust*
9. Select the option *Always Trust* in *When using this certificate*
10. Close the certificate window

The certificate is now installed.

1. Double click on the certificate (server.crt)
2. Click on the button “Install Certificate …”
3. Select whether you want to store it on user level or on machine level
4. Click “Next”
5. Select “Place all certificates in the following store”
6. Click “Browse”
7. Select “Trusted Root Certification Authorities”
8. Click “Ok”
9. Click “Next”
10. Click “Finish”
11. If you get a prompt, click “Yes”

The certificate is now installed.

Step 3: Configure the application

Now our certificate is ready to be consumed we have to make sure our application uses the correct certificate.

Create a folder *ssl* in the application folder.

```
angular-app:
   - e2e
   - src
   - ssl
   .angular-cli.json
```

Copy the private key and root certificate from step 1 into the *ssl* folder. Make sure the file names are like this:

Before we run our application, make sure you have restarted your browser and updated the *start* script in *package.json*.

```
"start": "ng serve --ssl true"
```

ANGULAR 6 REQUIRES YOU TO DEFINE THE PARAMS: `--ssl-cert` AND `--ssl-key`.

The only thing we know have to do, is run our application.

```
npm start
```

You should now have a fully working application with a trusted certificate.

Feedback is appreciated!

. . .

Website: https://rubenvermeulen.be
Twitter: https://twitter.com/rubverm
Github: https://github.com/RubenVermeulen
LinkedIn: https://www.linkedin.com/in/ruben-vermeulen/

Ssl Angular Angular Cli Typescript Https