I LEARNED SOMETHING NEW TODAY!

Just one developer helping another ;-)

Using self-signed certificates with QZ Tray

April 20, 2017

QZ Tray is an amazing printing tool for your browser. It allows your websites to print receipts including bar-codes using thermal printers.

The only problem is that getting it all set up correctly can be a bit tricky especially if you want to suppress the untrusted dialogs/prompts that pop up when using the free version.

Lucky for us, their solution is open source and from version 2.02 they allow developers to recompile the source with a self signed certificate that would suppress these popups. This is great if you cannot afford the $400 annual price tag, but getting it set up could be a painful process because they don't offer step by step instructions, and other articles on the subject are incomplete.

I successfully managed to recompile the binaries using a self signed certificate and thought it might be useful if I provide step by step instructions on how to get it done.

This guide will explain how to recompile the windows binaries only. But this should give you enough insight to be able to compile for Linux and Apple as well. The biggest part is to get the certificates all correct which is what I will be focusing on.

Note: Additional QZ Tray compiling information can be found on their *Compiling Wiki* page

Section 1: Recompiling and Signing Instructions

Step 1 - Installing QZ Dependencies

Before you continue, you should install the required dependencies and configure them correctly to allow you to recompile the application successfully.
To install the dependencies simply follow the instructions from the QA Tray website (HERE)

Step 2 - Clone the source code

Instructions on cloning the source code is available HERE
Note: Once the source code has been cloned, you need to pull the latest code using:

```
cd tray
git pull
```

Step 3 - Install OpenSSL

OpenSSL is used to create our self signed certificate and private key. OpenSSL is not officially supported for windows but you can install the third-party OpenSSL binaries from https://slproweb.com/products/Win32OpenSSL.html

Step 4 - Generating Certificates

Note: When using self signed certificates you do not need to worry about the trusted intermediate certificate, all you need is a certificate and a private key.

a) Run OpenSSL as administrator and use the following command to generate your key and certificate:

```
openssl req -x509 -newkey rsa:2048 -keyout key.pem -out cert.pem -days 11499 -nodes
```

You are required to input various information for the certificate to be correctly generated.

Here are some examples:

Country Name (2 letter code) [XX] : Your 2 letter country code, e.g. US

State or Province Name (full name) [Some-State] : Your state e.g. California

Locality Name (eg, city) ▯ : Your city e.g. San Fransisco

Organization Name (eg, company) [Internet Widgits Pty Ltd]: Your company name, e.g. Some Company Ltd.

Organizational Unit Name (eg, section) ▯: Department Name e.g. IT

Common Name (e.g. server FQDN or YOUR name) ▯: THIS ENTRY IS IMPORTANT, this should be your domain name in wildcard format an example of this would be "***.mywebsitedomain.com***"

Email Address ▯: Your email address

This command generates a certificate that is valid for 30 years, but you can adjust the days parameter to fit your needs. Note that the days parameter cannot be larger than **11499**

b) Once we have our certificate and key generated we should convert the key to the correct format. This is done by running the following command in OpenSSL.

```
openssl pkcs12 -inkey key.pem -in cert.pem -export -out privateKey.pfx
```

You will be prompted to enter (and confirm) a password for your private key, remember to use a secure password.

NOTE: Your certificates will be generated in the same folder where the OPENSSL exe file is located. This is most likely "c:\OpenSSL-Win64\bin" but could be different on version installed and also if you changed the installation path.

Step 5 - Recompile the binaries using our new certificate

Because this tutorial is for the Windows binaries we will be using **ant** to compile our code...

1) Run CMD prompt as Administrator.

2) Navigate to your QZ Tray source code

For example, if your cloned repository is located in "c:\src\tray"

```
cd C:\src\tray\
```

3) Run **ant** and include the new certificate parameter:

Assuming ant is located in "c:\ant" and certificates are located in "c:\OpenSSL-Win64\bin"...

```
c:\ant\bin\ant nsis -Dauthcert.use="c:\OpenSSL-Win64\bin\cert.pem"
```

Re-compiling finished

Your new installation will be located in the "out" folder of your cloned repository: "c:\src\tray\out\"

Section 2: QZ Tray Integration into ASP.Net

Step 1 - Getting Started

Follow the getting started instructions on the QZ Website

Step 2a - Signing the Messages (Client Side)

REMEMBER: Because we are using a self signed certificate we do not need to worry about the intermediate certificate.

For basic setup instructions please read this page first: https://qz.io/wiki/2.0-signing-messages

QZ Tray offers multiple ways to sign messages, in this example I will demonstrate the **Direct method** because its the easiest way to get it working.

1) Edit ***qz.security.setCertificatePromise()*** to use your self signed Certificate.

```
<script>
    /// Authentication setup ///
    qz.security.setCertificatePromise(function(resolve, reject) {
        //Preferred method - from server
//        $.ajax("assets/signing/digital-certificate.txt").then(resolve, reject);

        //Alternate method 1 - anonymous
//        resolve();

        //Alternate method 2 - direct
        resolve("-----BEGIN CERTIFICATE-----\n" +
                "MIIFAzCCAuugAwIBAgICEAIwDQYJKoZIhvcNAQEFBQAwgZgxCzAJBgNVBAYTAlVT\n" +
                "MQswCQYDVQQIDAJOWTEbMBkGA1UECgwSUVogSW5kdXN0cmllcywgTExDMRswGQYD\n" +
                "VQQLDBJRWiBJbmR1c3RyaWVzLCBMTEMxGTAXBgNVBAMMEHF6aW5kdXN0cmllcy5j\n" +
                "b20xJzAlBgkqhkiG9w0BCQEWGHN1cHBvcnRAcXppbmR1c3RyaWVzLmNvbTAeFw0x\n" +
                "NTAzMTkwMjM4NDVaFw0yNTAzMTkwMjM4NDVaMHMxCzAJBgNVBAYTAkFBMRMwEQYD\n" +
                "VQQIDApTb21lIFN0YXRlMQ0wCwYDVQQKDAREZW1vMQ0wCwYDVQQLDAREZW1vMRIw\n" +
                "EAYDVQQDDAlsb2NhbGhvc3QxHTAbBgkqhkiG9w0BCQEWDnJvb3RAbG9jYWxob3N0\n" +
                "MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAtFzbBDRTDHHmlSVQLqjY\n" +
                "aoGax7ql3XgRGdhZlNEJPZDs5482ty34J4sI2ZK2yC8YkZ/x+WCSveUgDQIVJ8oK\n" +
                "D4jtAPxqHnfSr9RAbvB1GQoiYLxhfxEp/+zfB9dBKDTRZR2nJm/mMsavY2DnSzLp\n" +
                "t7PJOjt3BdtISRtGMRsWmRHRfy882msBxsYug22odnT1OdaJQ54bWJT5iJnceBV2\n" +
                "1oOqWSg5hU1MupZRxxHbzI61EpTLlxXJQ7YNSwwiDzjaxGrufxc4eZnzGQ1A8h1u\n" +
                "jTaG84S1MWvG7BfcPLW+sya+PkrQWMOCIgXrQnAsUgqQrgxQ8Ocq3G4X9UvBy5VR\n" +
                "CwIDAQABo3sweTAJBgNVHRMEAjAAMCwGCWCGSAGG+EIBDQQfFh1PcGVuU1NMIEdl\n" +
                "bmVyYXRlZCBDZXJ0aWZpY2F0ZTAdBgNVHQ4EFgQUpG420UhvfwAFMr+8vf3pJunQ\n" +
                "gH4wHwYDVR0jBBgwFoAUkKZQt4TUuepf8gWEE3hF6Kl1VFwwDQYJKoZIhvcNAQEF\n" +
                "BQADggIBAFXr6G1g7yYVHg6uGfh1nK2jhpKBAOA+OtZQLNHYlBgoAuRRNWdE9/v4\n" +
                "J/3Jeid2DAyihm2j92qsQJXkyxBgdTLG+ncILlRElXvG7IrOh3tq/TttdzLcMjaR\n" +
                "8w/AkVDLNL0z35shNXih2F9JlbNRGqbVhC7qZl+V1BITfx6mGc4ayke7C9Hm57X0\n" +
                "ak/NerAC/QXNs/bF17b+zsUt2ja5NVS8dDSC4JAkM1dD64Y26leYbPybB+FgOxFu\n" +
                "wou9gFxzwbdGLCGboi0lNLjEysHJBi90KjPUETbzMmoilHNJXw7egIo8yS5eq8RH\n" +
                "i2lS0GsQjYFMvplNVMATDXUPm9MKpCbZ7IlJ5eekhWqvErddcHbzCuUBkDZ7wX/j\n" +
                "unk/3DyXdTsSGuZk3/fLEsc4/YTujpAjVXiA1LCooQJ7SmNOpUa66TPz9O7Ufkng\n" +
                "+CoTSACmnlHdP7U9WLr5TYnmL9eoHwtb0hwENe1oFC5zClJoSX/7DRexSJfB7YBf\n" +
                "vn6JA2xy4C6PqximyCPisErNp85GUcZfo33Np1aywFv9H+a83rSUcV6kpE/jAZio\n" +
                "5qLpgIOisArj1HTM6goDWzKhLiR/AeG3IJvgbpr9Gr7uZmfFyQzUjvkJ9cybZRd+\n" +
                "G8azmpBBotmKsbtbAU/I/LVk8saeXznshOVVpDRYtVnjZeAneso7\n" +
                "-----END CERTIFICATE-----\n");
    });
```

2) Edit ***qz.security.setSignaturePromise()*** to use your server-side signing method.

```
        /// Returns signed message ///
        qz.security.setSignaturePromise(function (toSign) {
            return function (resolve, reject) {
                PageMethods.SignMessage(toSign, resolve, reject);
            };
        });
```

Step 2b - Signing the Messages (Server Side)

Note: Make sure that your webpage that you want to print from inherits from the following ***CustomPage*** class instead of just the normal `System.Web.UI.Page`

```
using System;
using System.Collections.Generic;
using System.Linq;
using System.Security.Cryptography;
using System.Security.Cryptography.X509Certificates;
using System.Text;
using System.Web;
using System.Web.Services;

namespace YourNameSpace
{
    public class CustomPage : System.Web.UI.Page
    {
        [WebMethod]
        public static object SignMessage(string message)
        {
            // How to associate a private key with the X509Certificate2 class in .net
            // openssl pkcs12 -export -inkey private-key.pem -in digital-certificate.txt -out private

            string KEY = "PATH-TO-YOUR-PRIVATE-KEY-LOCATION (privateKey.pfx)";
            string PASS = "YOUR-PRIVATE-KEY-PASSWORD-HERE";

            var cert = new X509Certificate2(KEY, PASS, X509KeyStorageFlags.MachineKeySet | X509KeySto
            RSACryptoServiceProvider csp = (RSACryptoServiceProvider)cert.PrivateKey;

            byte[] data = new ASCIIEncoding().GetBytes(message);
            byte[] hash = new SHA1Managed().ComputeHash(data);

            string response = Convert.ToBase64String(csp.SignHash(hash, CryptoConfig.MapNameToOID("SH
            return response;
        }
    }
}
```

And that folks, is all you need!

LABELS: QZ TRAY **SHARE**

Comments

Unknown · April 4, 2018 at 3:51 AM

I have done all steps but it showing popup again. What I have to do with Re-compiling finished build in "c:\src\tray\out\". Need to install QZ tray 2.0 downloaded from web site?

Riaan van der Linde · April 4, 2018 at 12:51 PM

Hey Riyas,
You need to install the msi from the out folder that you just compiled. If its still showing the popup each time I suspect that the certificate that you generated is invalid. Can you see the certificate information (I think on the second popup you are able to see the certificate details somewhere)
Check that the valid to date is correct, also check the domain of the certificate, it has to match up with your actual website domain.

REPLY

Unknown · April 6, 2018 at 2:16 PM

Hi!
Thanks for the amazing tutorial! You are really doing wonders.
I am stuck on section 5 of part 1 where you recompile binaries with the newly created certificates.

Since I am using a mac, what are the steps I need to follow? How do i run ant for recompilation? Any solution would be GREATLY appreciated!

Thanks
Kazi

Riaan van der Linde · April 11, 2018 at 2:23 PM

Hi Kazi, apologies for the late reply.
I have not tried to compile on Mac, but looking at the instructions on this page: https://qz.io/wiki/compiling it does seem that you will need to use ANT as well.

The only difference seem to be

ant pkgbuild # <-- Apple installer

instead of

ant nsis # <-- Windows installer

REPLY

Unknown · April 6, 2018 at 2:16 PM

This comment has been removed by the author.

REPLY

Marco Peroni · April 10, 2018 at 10:37 AM

Wonderful, it works! Thank you so much for sharing it !

Riaan van der Linde · April 11, 2018 at 2:10 PM

That's great Marco! I'm glad it helped.

REPLY

Unknown · May 2, 2018 at 5:28 AM

This comment has been removed by the author.

REPLY

Unknown · May 2, 2018 at 5:29 AM

Hey mate, can you help me achieve the same with Angular 4 (typescript). It would be of great help !

Riaan van der Linde · May 2, 2018 at 1:05 PM

Hi Angad,

I wish I could help but im not that familiar with Angular.
I assume all the steps would be the same except for Step 2b

REPLY

Unknown · August 1, 2018 at 9:15 AM

Hello Riaan, nice work here! This is the easiest tutorial to follow i found. I've followed every step but i'm getting 'untrusted website' warning when popup shows. Any ideas on what might be happening?

REPLY

Unknown · November 24, 2018 at 8:49 AM

Hi,

Nice post!

I've been able to compile and my site is already displaying in the list of trusted sites (it no longer also shows the Allow site trust box), but when I send print, it still displays the dialog to trust the print.

REPLY

PlaynowGames · December 6, 2018 at 4:38 AM

Hey man, Nice tutorial, I follow tutorial and it's work great! but I have some issues with images, when I open a page with image the window print show again..just in page where have images... do you have any trick? thx!

REPLY

Unknown · January 3, 2019 at 8:33 AM

I was able to tick Allow on the Pop Up but it is not sending to the printer.

```
qz.security.setSignaturePromise(function (toSign) {
return function (resolve, reject) {
PageMethods.SignMessage(toSign, resolve, reject);
};
});

qz.security.setCertificatePromise(function(resolve, reject) {


//Alternate method 2 - direct
resolve("-----BEGIN CERTIFICATE-----\n" +
"MIID5DCCAsygAwIBAgIJAJyA6TwbEDEnMA0GCSqGSIb3DQEBCwUAMIGFMQswCQYD\n"+
"VQQGEwJORzEOMAwGA1UECAwFTGFnb3MxDjAMBgNVBAcMBUxhZ29zMREwDwYDVQQK\n"+
"DAhXaXJlcGljazELMAkGA1UECwwCSVQxEDAOBgNVBAMMB2Jhc2h0ZW0xJDAiBgkq\n"+
"hkiG9w0BCQEWFXRvcGVhZGViYXNzQHlhaG9vLmNvbTAgFw0xOTAxMDIyMjQ3Mzha\n"+
"GA8yMDUwMDYyNzIyNDczOFowgYUxCzAJBgNVBAYTAk5HMQ4wDAYDVQQIDAVMYWdv\n"+
"czEOMAwGA1UEBwwFTGFnb3MxETAPBgNVBAoMCFdpcmVwaWNrMQswCQYDVQQLDAJJ\n"+
"VDEQMA4GA1UEAwwHYmFzaHRlbTEkMCIGCSqGSIb3DQEJARYVdG9wZWFkZWJhc3NA\n"+
"eWFob28uY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAq8SkaCCA\n"+
"zQ0MWfznmhp+ZD40BKAl/M/YuvslaIqFslrGCq+okkTG0lZ6T2f7wDUIHQ+xt3yO\n"+
"eOT6ZapMkHc/UIcP1F4CDL/tqXUgE6JuQtGiaBbL/yZJgKLUSWBWtjUsUxo65V5e\n"+
"mDrTxWS2cA/pnZ+3M8K1WFGqVYq19oWWd1whR5KKmAIC8TaPLZLh5wkQjHsBDf4U\n"+
"oSjRbPyvXsMZlrJOngzThNH8mfWVBuhQtjBeavWXCjO/q/seVBDGP+Dj2Wg5OG4P\n"+
"KlNsTGwbKdIU7E5Q+nbKJiTCkaUJKD9mdv+yzLqZXnZ1RYWOfbBt3xMEfE31muwj\n"+
"0PH7vQUwLmFSIwIDAQABo1MwUTAdBgNVHQ4EFgQUkMNMUT0Pxeh+Lfnjlynn5AYq\n"+
"lzkwHwYDVR0jBBgwFoAUkMNMUT0Pxeh+Lfnjlynn5AYqlzkwDwYDVR0TAQH/BAUw\n"+
"AwEB/zANBgkqhkiG9w0BAQsFAAOCAQEAKrSM3g9k9550rv9N9Si8AR0Oh4pyrE+x\n"+
"mgRam4ij2dZJEqHy7popUM+uYbErKW02RakoVvae6KwQ6wWg3VNUVbipSMewfNjR\n"+
"heTrMLdZupu4uVlz/D+r1vn7ZZx77dvr+pCLoGzZ1pNsd0kwcl0X5xzOBCie8KSX\n"+
"Hahp6H8fkx78UnhxzMZ0iaHef1gyhrji0LwlleG5uPm8juPTEgbCKCcq7EJCAT3I\n"+
"5ZTnSe+YQlb8KTVkn+27jnTatWVkcPO9pWT1EkWcs/6Jzjhgp6bFSRmUSk8d8YRS\n"+
"4nkU4xMDIx2MfqE/U0Gxm21cjnlgXvtJZRCmYlabxVp+lOaFQ5XBng==\n"+
"-----END CERTIFICATE-----\n");
});
```

Please how can i implement the above code correctly.
Thanks

REPLY

Unknown · April 17, 2019 at 9:50 AM

Followed all the steps are gone but no printing...Right after the call to websocket.connect the function passed to then does not get called...I am using self signed certificate for localhost...Have toyed with things for a day and a half but no luck so far...Any suggestions to try out are most welcome...Angular 7 application Node on the server side BTW...

REPLY

phongtd · August 18, 2020 at 1:01 AM

BUILD FAILED
G:\tray\ant\windows\installer.xml:25: The following error occurred while executing this line:
G:\tray\ant\windows\installer.xml:43: exec returned: 1

Help me!

REPLY

Sw0rd7 · September 17, 2020 at 8:56 AM

Wow GREAT Blog!! you did my day, excellent, I was able to create the certificate and work just fine!!!!

REPLY

Thant · February 6, 2024 at 9:22 AM

How to get self signed certificate?
"assets/signing/digital-certificate.txt"

I don't understand
REPLY

Zayden Wood · April 11, 2024 at 5:23 AM

Nice

REPLY

To leave a comment, click the button below to sign in with Google.

SIGN IN WITH GOOGLE

Popular posts from this blog

How to update NuGet Package Manager (NPM) in Visual Studio

February 29, 2016

How to update your NuGet package manager in Visual Studio. Follow these steps to update NPM in Visual Studio: Click Tools -> Extensions And Updates Select " Updates" on the left, and then "Visual Studio Gallery" Select NuGet Package Manager and click Update Accept the agreement NuGet Package Manager is now successfully updated

...

SHARE POST A COMMENT READ MORE

Ethereum, the new BitCoin but better!

May 24, 2017

If you are like me you probably want to kick yourself for not getting on the BitCoin train back in the day when it was just taking off. Bitcoin has been making some good gains the last few months but there is a newer "Crypto Currency" making all the headlines these days... And this one is still affordable but growing at an incredible rate. This new blockchain is called Ethereum. Important: The purpose behind this arti …

SHARE 1 COMMENT READ MORE

→

Archive

Labels

Report Abuse