Creating self signed certificates with makecert.exe for development

September 3, 2014 - Elizabeth Andrews (https://blog.jayway.com/author/elizabethandrews/) - .Net (https://blog.jayway.com/category/net/) / Security (https://blog.jayway.com/category/security-2/) - 101 Comments (https://blog.jayway.com/2014/09/03/creating-self-signed-certificates-with-makecert-exe-for-development/#comments)

If you've ever had the need of creating self signed certificates you may start out feeling like it's not a straightforward stroll in the park, so here is a blog post that might help you to get started. I will be going through the basics of creating self signed X.509 certificates (Root, server & client) using makecert.exe.
For the complete makecert.exe parameter reference click here (http://msdn.microsoft.com/en-us/library/bfsktky3%28v=vs.110%29.aspx).

I'm using a PC with Windows 8.1 Pro and Visual Studio Premium 2013.

Certificate Authority (CA)

Normally most companies would just buy their certificates from a trusted third party certificate authority such as GoDaddy or Verisign, but for development and testing, this might not be the first thing one wants to

do. Instead you can create your own self signed certificates, starting with a root CA that can be used to sign other certificates. *(For example ssl certificates for servers and clients)*. When you do this, the certificates are not trusted by default. You must therefore add the root CA to your machine's Trusted Root Certification Authorities Store through the Microsoft Management Console.

NOTE: You can add these two parameters: -sr LocalMachine ^ and -ss Root ^ to the upcoming command batch file, if you want to install the certificate directly into the LocalMachine's Trusted Root Certification Authorities. **BE SURE** to run the Developer Command Prompt as administrator or it will fail. We will however go through how to do this manually so you get a more basic understanding.

The ^ symbol I add to the following cmd batch files means "escape the next line", this makes it more readable instead of one long command string.

Let's do all of this step by step:
Open an empty notepad document and copy and paste the following into notepad:

Aspect Oriented Programming (https://blog.jayway.com/category/aspect-oriented-programming/)
Assistants (https://blog.jayway.com/category/assistants/)
Augmented Reality (https://blog.jayway.com/category/augmented-reality/)
Automotive (https://blog.jayway.com/category/automotive/)
C++ (https://blog.jayway.com/category/c/)
Cloud (https://blog.jayway.com/category/cloud/)
Cocoa (https://blog.jayway.com/category/cocoa/)
Competence Development (https://blog.jayway.com/category/competence-development/)
Data Science (https://blog.jayway.com/category/data-science/)
Design (https://blog.jayway.com/category/design/)
DevOps (https://blog.jayway.com/category/devops/)

```
makecert.exe ^
-n "CN=CARoot" ^
-r ^
-pe ^
-a sha512 ^
-len 4096 ^
-cy authority ^
-sv CARoot.pvk ^
CARoot.cer

pvk2pfx.exe ^
-pvk CARoot.pvk ^
-spc CARoot.cer ^
-pfx CARoot.pfx ^
-po Test123
```

This may or may not look a bit frightening or incomprehensive at first, but let me
walk you through what is going on here: First we create a certificate with makecert.exe, then we use pvk2pfx.exe to copy the public key and private key
information from the .pvk and .cer into a .pfx (personal information exchange) file.

NOTE: Never share your root .pvk or .pfx files if you want to stay secure! The .pvk file contains your private key for your .cer certificate and the .pfx file contains both the certificate .cer and the private key .pvk, which means that others can sign new certificates with your certificate without your consent. The only file you can share is the .cer file, which only contains the public key.

The makecert.exe parameters:

Dynamic languages (https://blog.jayway.com/category/dynamic-languages/)
Embedded (https://blog.jayway.com/category/embedded/)
Events (https://blog.jayway.com/category/events/)
Functional programming (https://blog.jayway.com/category/functional-programming/)
Generics (https://blog.jayway.com/category/swift/generics/)
Graphics (https://blog.jayway.com/category/graphics/)
iOS (https://blog.jayway.com/category/ios/)
IoT (https://blog.jayway.com/category/iot/)
Java (https://blog.jayway.com/category/java/)
JavaScript (https://blog.jayway.com/category/javascript/)
Kotlin (https://blog.jayway.com/category/kotlin/)

- -n “CN=CARoot” → Subject’s certificate name and must be formatted as the standard: “CN=Your CA Name Here”
  You can also add more than one in the -n parameter for example: “-n “CA=CARoot,O=My Organization,OU=Dev,C=Denmark” and so on.
  Reference:
    - CN = commonName (for example, “CN=My Root CA”)
    - OU = organizationalUnitName (for example, “OU=Dev”)
    - O = organizationName (for example, “O=Jayway”)
    - L = localityName (for example, “L=San Francisco”)
    - S = stateOrProvinceName (for example, “S=CA”)
    - C = countryName (for example, “C=US”)
- -r → Indicates that this certificate is self signed
- -pe → The generated private key is exportable and can be included in the certificate
- -a sha512 → We declare which signature algorithm we will be using (**DO NOT** use the sha1 algoritm, it is [no longer secure](https://konklone.com/post/why-google-is-hurrying-the-web-to-kill-sha-1))
- -len 4096 → The generated key length in bits
- -cy authority → Specifies that this is a certificate authority
- -sv CARoot.pvk → The subject’s .pvk private key file
- CARoot.cer → The certificate file

Optional: install certificate directly into the Trusted Root CA store

- -sr LocalMachine → The subject’s certificate store location
- -ss Root → The certificate store name

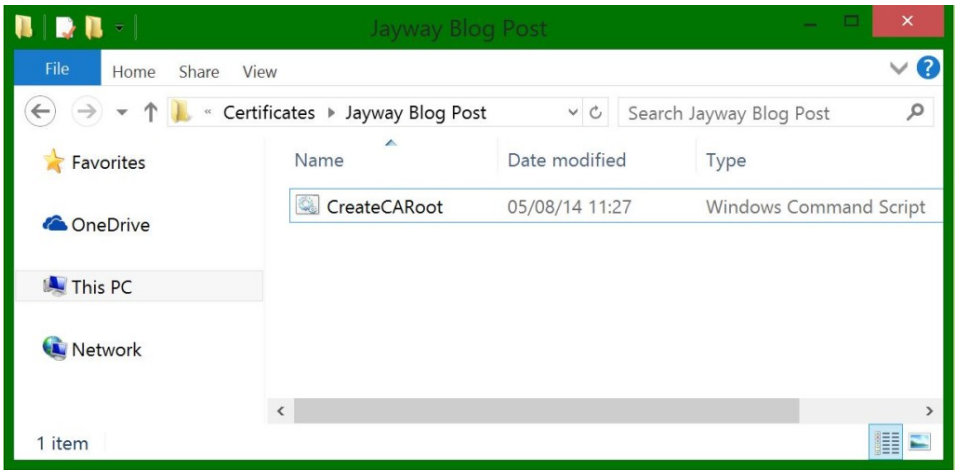
The pvk2pfx.exe parameters:

- -pvk CARoot.pvk → The name of the .pvk file
- -spc CARoot.cer → The name of the .cer file
- -pfx CARoot.pfx → The name of the -pfx file

Linux (https://blog.jayway.com/category/linux/)
Machine Learning (https://blog.jayway.com/category/data-science/machine-learning/)
Other (https://blog.jayway.com/category/other/)
python (https://blog.jayway.com/category/python/)
React (https://blog.jayway.com/category/web/react/)
Scala (https://blog.jayway.com/category/scala/)
Security (https://blog.jayway.com/category/security-2/)
Swift (https://blog.jayway.com/category/swift/)
SwiftUI (https://blog.jayway.com/category/swift/swiftui/)
Testing (https://blog.jayway.com/category/testing/)
Tips & Tricks (https://blog.jayway.com/category/tips-and-tricks/)
Tools & Workflows (https://blog.jayway.com/ca

- -po Test123 ➜ The password for the .pfx file

Save the document as “CreateCARoot.cmd” which will create a command batch file. *(You can call it what you want as long as you remember the .cmd ending which will make it a Windows Command Script)*



(http://blog.jayway.com/wp-content/uploads/2014/09/1.-CreateCARoot-batch-file.jpg)

Open a Visual Studio Developer Command Prompt – this is where makecert.exe lives, and navigate to the folder that contains the batch file and run the cmd file

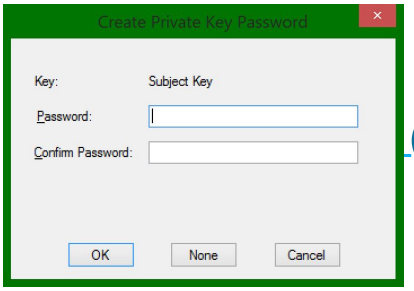
(http://blog.jayway.com/wp-content/uploads/2014/09/2.-DevPrompt1.jpg)

tegory/tools-and-workflows/)
Tutorial (https://blog.jayway.com/category/tutorial/)
Uncategorized (https://blog.jayway.com/category/uncategorized/)
Unity (https://blog.jayway.com/category/unity/)
User Experience (https://blog.jayway.com/category/user-experience/)
VR/AR (https://blog.jayway.com/category/vrar/)
Wearables (https://blog.jayway.com/category/wearables/)
Web (https://blog.jayway.com/category/web/)

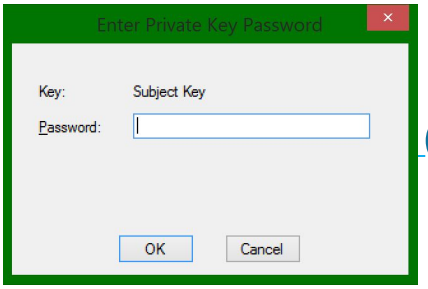
TAGS

.Net (https://blog.jayway.com/tag/net/) Android (https://blog.jayway.com/tag/android/)

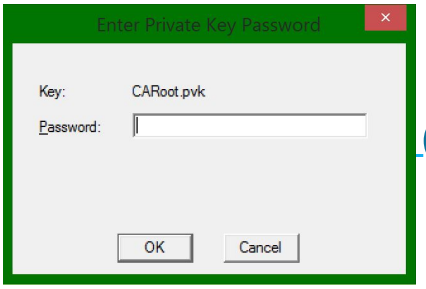
It should now prompt you to enter some passwords. *(This is where we create and use the .pvk private key, so these need to match for success)*



(http://blog.jayway.com/wp-content/uploads/2014/09/3.-DevPrompt2.jpg)



(http://blog.jayway.com/wp-content/uploads/2014/09/4.-DevPrompt3.jpg)



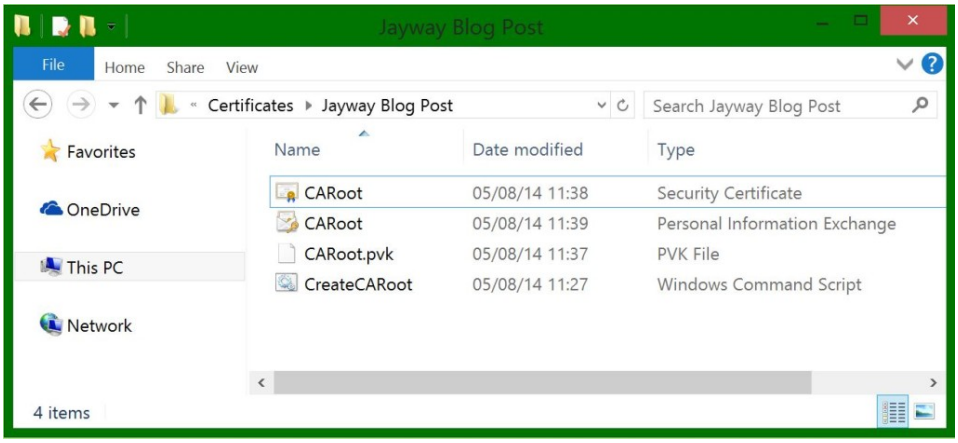
(http://blog.jayway.com/wp-content/uploads/2014/09/5.-DevPrompt4.jpg)

(http://blog.jayway.com/wp-content/uploads/2014/09/6.-DevPrompt5.jpg)

(http://blog.jayway.com/wp-content/uploads/2014/09/6.-DevPrompt52.jpg)

aop (https://blog.jayway.com/tag/aop/) automated testing (https://blog.jayway.com/tag/automated-testing/) aws (https://blog.jayway.com/tag/aws/) azure (https://blog.jayway.com/tag/azure/) C# (https://blog.jayway.com/tag/c/) clojure (https://blog.jayway.com/tag/clojure/) conference (https://blog.jayway.com/tag/conference/) frameworks (https://blog.jayway.com/tag/frameworks/) functional programming (https://blog.jayway.com/tag/functional-programming/) git (https://blog.jayway.com/tag/git/) http (https://blog.jayway.com/tag/http/) iOS (https://blog.jayway.com/tag/ios/) iphone (https://blog.jayway.com/tag/iphone/) Java (https://blog.jayway.com/tag/j

You should now have 3 new files: CARoot.cer, CARoot.pfx and CARoot.pvk in the folder where your batch files are.



(http://blog.jayway.com/wp-content/uploads/2014/09/7.-CARootCertfiles.jpg)

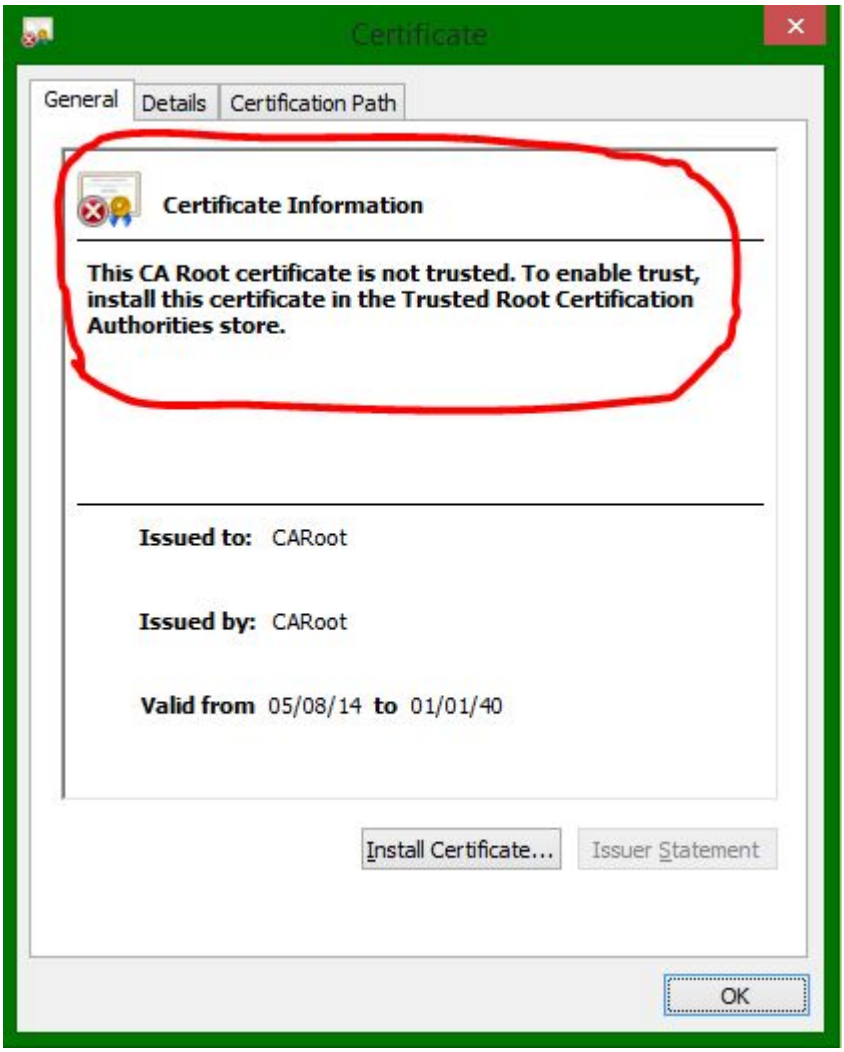
Making It Trusted

(This is a manual walk through if you didn't include the -sr and -ss parameters)

Open your new CARoot.cer file by double clicking it and see that it is not trusted.

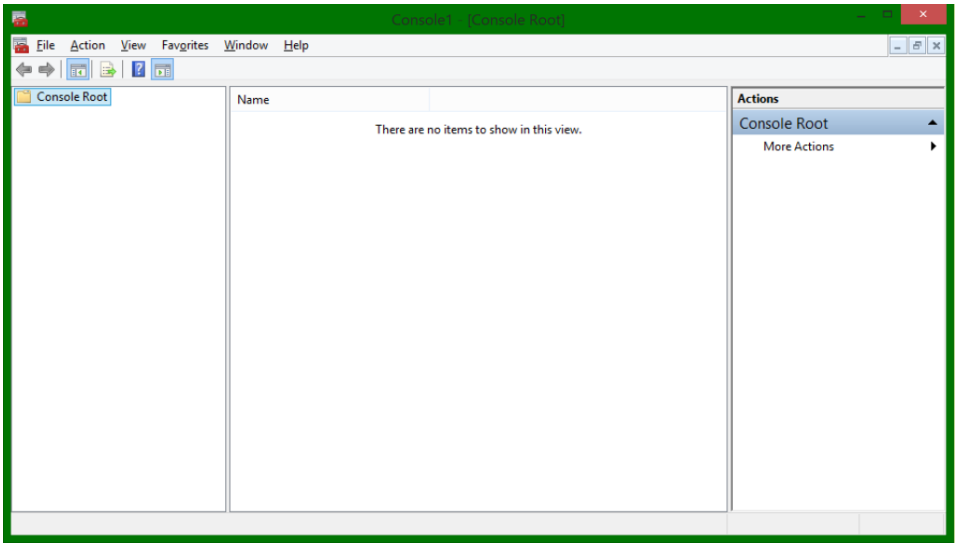
ava/) javascript (https://blog.jayway.com/tag/javascript/) jayview (https://blog.jayway.com/tag/jayview/) junit (https://blog.jayway.com/tag/junit/) maven (https://blog.jayway.com/tag/maven/) metro (https://blog.jayway.com/tag/metro/) mobile (https://blog.jayway.com/tag/mobile/) node.js (https://blog.jayway.com/tag/node-js/) objective-c (https://blog.jayway.com/tag/objective-c/) open source (https://blog.jayway.com/tag/open-source/) performance (https://blog.jayway.com/tag/performance/) powermock (https://blog.jayway.com/tag/powermock/)

programming (https://blog.jayway.com/tag/pr



(http://blog.jayway.com/wp-content/uploads/2014/09/8.-UntrustedCert2.jpg)

To make it trusted on your machine open up the Microsoft Management Console. *(Find it by searching for mmc in start)*

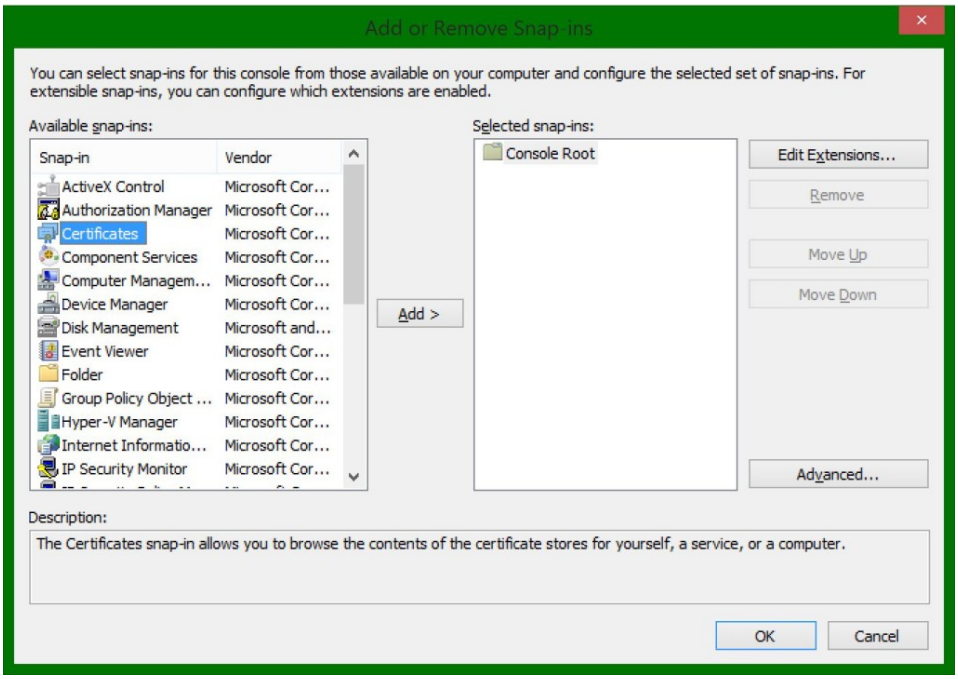


(http://blog.jayway.com/wp-content/uploads/2014/09/mmc-console.png)

ogramming/) rest (https://blog.jayway.com/tag/rest/) Ruby (https://blog.jayway.com/tag/ruby/) scala (https://blog.jayway.com/tag/scala/) spring (https://blog.jayway.com/tag/spring/) testing (https://blog.jayway.com/tag/testing-2/) tips (https://blog.jayway.com/tag/tips/) tools (https://blog.jayway.com/tag/tools/) tutorial (https://blog.jayway.com/tag/tutorial/) web (https://blog.jayway.com/tag/web/) windows (https://blog.jayway.com/tag/windows/) windows 8 (https://blog.jayway.com/tag/windows-8/) windows phone (https://blog.jayway.com/tag/windows-phone/) windows

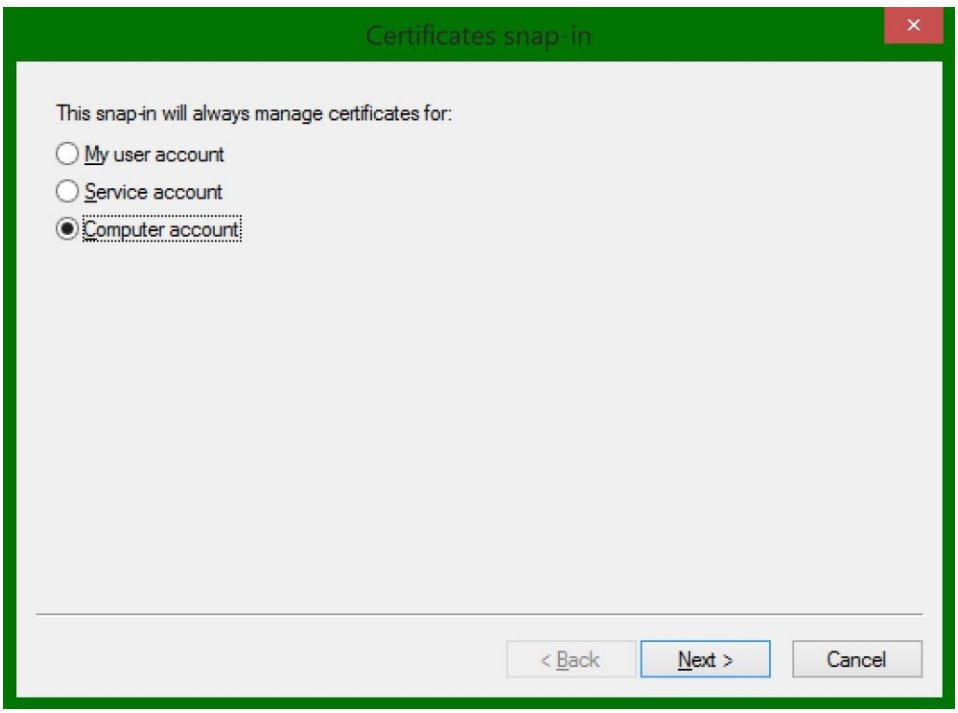
Go to File → Add/Remove Snap-in

Double-click Certificates in the list to the left



(http://blog.jayway.com/wp-content/uploads/2014/09/9.-MMC1.jpg)

Choose Computer account and just go next, finish and OK



(http://blog.jayway.com/wp-content/uploads/2014/09/10.-MMC2.jpg)

Open the Trusted Root Certification Authorities → Certificates

Here you can see all of the currently trusted certificates that Windows trusts.

phone 7 (https://blog.jayway.com/tag/windows-phone-7/) windows phone 8.1 (https://blog.jayway.com/tag/windows-phone-8-1/) winrt (https://blog.jayway.com/tag/winrt/) wp7dev (https://blog.jayway.com/tag/wp7dev/) xaml (https://blog.jayway.com/tag/xaml/)

AUTHORS

Adam Tibbing (https://blog.jayway.com/author/adam-tibbingjayway-com/) (1)

Albin Theander (https://blog.jayway.com/author/albintheander/) (1)

Alexander Persson (https://blog.jayway.com/author/alexanderpersson/) (8)

Amir Moulavi (https://blog.jayway.com/author/amirmoulavi/) (7)

Anders Ericsson (https://blog.jayway.com/author/andersericsson/) (8)

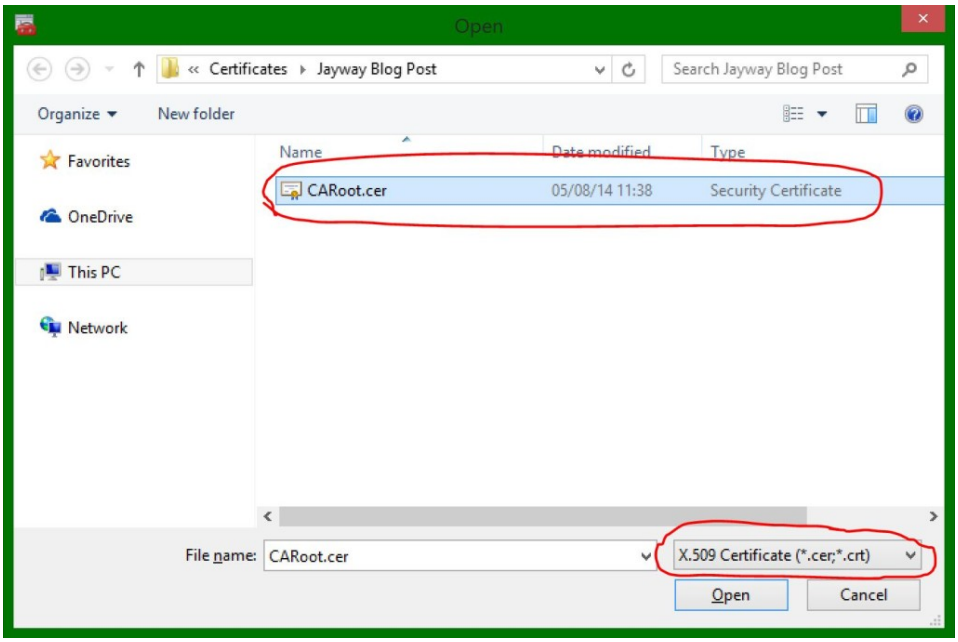
Anders Eriksson (https://blog.jayway.com/au

(Alot of them ship with Windows out of the box)

Now right-click the Certificates folder → All tasks → Import…

The certificate Import Wizard will pop up.

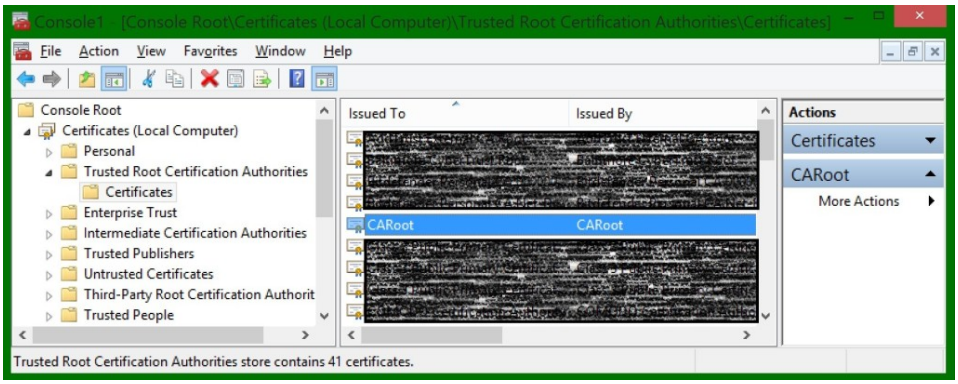
Go next → Browse to find the CARoot.cer file we created earlier



(http://blog.jayway.com/wp-content/uploads/2014/09/MMC-CARoot.jpg)

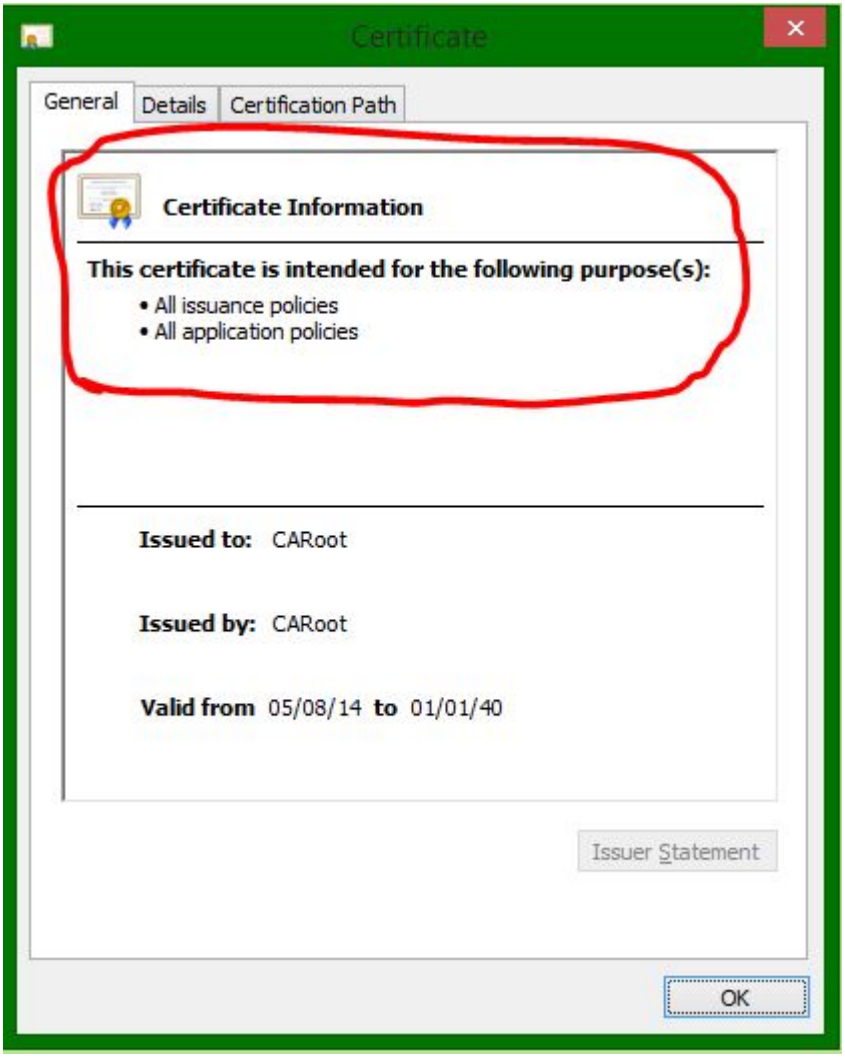
Keep going next until finish where a message box should appear saying "The import was successful".

Your CARoot certificate should now be in you Trusted Root Certification Authorities store.



Open the CARoot (double-click) and see that it is now trusted by your computer.

thor/anderseriksson/) (2)
Anders Haahr (https://blog.jayway.com/author/anders-haahrjayway-com/) (1)
Anders Janmyr (https://blog.jayway.com/author/andersjanmyr/) (57)
Anders Poulsen (https://blog.jayway.com/author/anderspoulsen/) (28)
Andreas Ekberg (https://blog.jayway.com/author/andreasekberg/) (4)
Andreas Hammar (https://blog.jayway.com/author/andreashammar/) (60)
Andreas Nilsson (https://blog.jayway.com/author/andreasnilsson/) (2)
Andreas Ronge (https://blog.jayway.com/author/andreasronge/) (6)
Anton Fagerberg (https://blog.jayway.com/author/antonfagerberg/) (6)
August Alfredsson (https://blog.jayway.com/author/august-alfredssondevoteam-com/) (1)
Binh Tu (https://blog.jayway.com/author/binhtu/) (2)
Björn Antonsson (https://blog.jayway.com/au



(http://blog.jayway.com/wp-content/uploads/2014/09/13.-TrustedCert2.jpg)

Server Certificates

Next up we need a certificate to handle SSL on the server. We will create this with a new command batch file in notepad just like before, this time with these parameters:

thor/bjornantonsson/) (1)
Björn Carlsson (https://blog.jayway.com/author/bjorncarlsson/) (6)
Björn Granvik (https://blog.jayway.com/author/bjorngranvik/) (29)
Carl Nordenfelt (https://blog.jayway.com/author/carl-nordenfeltjayway-com/) (4)
Carl-Emil Kjellstrand (https://blog.jayway.com/author/carlemilkjellstrand/) (14)
Christian Hedin (https://blog.jayway.com/author/christianhedin/) (4)
Christian Jacobsen (https://blog.jayway.com/author/christianjacobsen/) (16)
Daniel Kleveros (https://blog.jayway.com/author/danielkleveros/) (4)
Darius Katz (https://blog.jayway.com/author/dariuskatz/) (5)
Davor Crnomat (https://blog.jayway.com/author/davorcrnomat/) (5)
Dennis Overhage (https://blog.jayway.com/author/dennis-overhagejayway-com/) (2)
Einar Valgeirsson (https://blog.jayway.com/au

```
makecert.exe ^
-n "CN=yourdomain.com" ^
-iv CARoot.pvk ^
-ic CARoot.cer ^
-pe ^
-a sha512 ^
-len 4096 ^
-b 01/01/2014 ^
-e 01/01/2016 ^
-sky exchange ^
-eku 1.3.6.1.5.5.7.3.1 ^
-sv %1.pvk ^
%1.cer

pvk2pfx.exe ^
-pvk %1.pvk ^
-spc %1.cer ^
-pfx %1.pfx ^
-po Test123
```

NOTE: The CN must match your domain otherwise the browsers won't trust your SSL certificate and warn the end user not to proceed to your website

You will recognize most of the parameters, but let me explain the new ones:

- -n "CN=yourdomain.com" for example → Change this to your domain name in order to connect the SSL server certificate to a specific web server domain. (Examples: "CN=www.yourdomain.com", "CN=yourdomain.com" or the wildcard that will match all urls ending in your domain "CN=*.yourdomain.com".)
  You can also add more than one in the -n parameter for example: "-n

thor/einar-valgeirssonjayway-com/) (2)
Elizabeth Andrews (https://blog.jayway.com/author/elizabethandrews/) (6)
Erik Ogenvik (https://blog.jayway.com/author/erikhjortsberg/) (5)
Ester Ytterbrink (https://blog.jayway.com/author/esterytterbrink/) (2)
Fredrik Frodlund (https://blog.jayway.com/author/fredrikfrodlund/) (5)
Fredrik Nannestad (https://blog.jayway.com/author/fredrik/) (1)
Fredrik Olsson (https://blog.jayway.com/author/fredrikolsson/) (31)
Frida Bredberg (https://blog.jayway.com/author/fridabredberg/) (1)
Gina Adamova (https://blog.jayway.com/author/gina-adamovajayway-com/) (1)
Gustaf Nilklint (https://blog.jayway.com/author/gustafnilklint/) (2)
Gustaf Nilsson Kotte (https://blog.jayway.com/author/gustafnilssonkotte/) (12)
Håkan Reis (https://blog.jayway.com/au

"CA=CARoot,O=My Organization,OU=Dev,C=Denmark" and so on. Reference:

  - CN = commonName (for example, "CN=My Root CA")
  - OU = organizationalUnitName (for example, "OU=Dev")
  - O = organizationName (for example, "O=Jayway")
  - L = localityName (for example, "L=San Francisco")
  - S = stateOrProvinceName (for example, "S=CA")
  - C = countryName (for example, "C=US")
- %1 → A command line parameter and will be whatever you type in after .cmd, this will be the file name of your .cer, .pvk and .pfx files
- -iv CARoot.pvk → Issuer's (The CA that signed it) .pvk private key file
- -ic CARoot.cer → The issuer's certificate file
- -b 01/01/2014 → Start of the period where the certificate is valid
- -e 01/01/2016 → End of the valid period
- -sky exchange → Indicates that the key is for key encryption and key exchange
- -eku 1.3.6.1.5.5.7.3.1 → Server authentication OID (Object Identifier). Identifies that this is an SSL Server certificate.

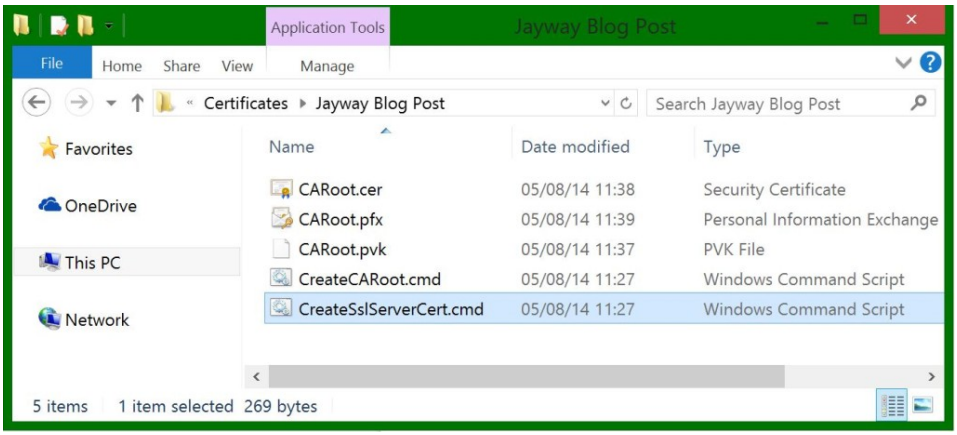
Optional: Install server certificate directly into the LocalMachine Personal certificate store

NOTE: This will only install the .cer file into the MMC, in order to import the .pfx file you will have to do it manually.

- -sr LocalMachine → The subject's certificate store location
- -ss My → The certificate store name that will store the output certificate

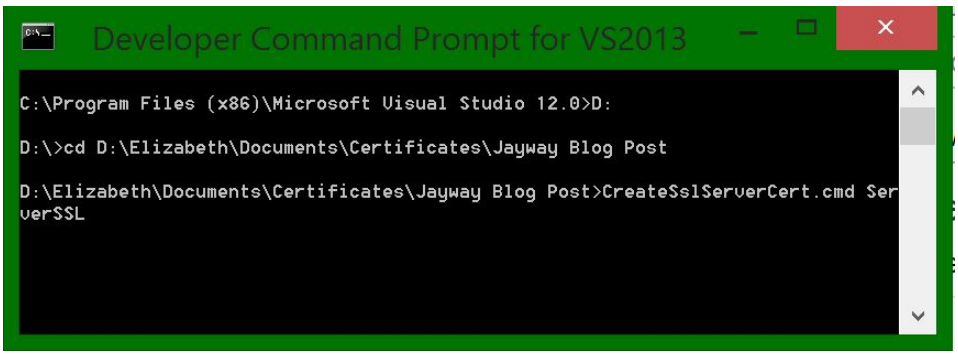
This will create a SSL certificate to use on your server and will be signed by your CARoot authority.

thor/hakanreis/) (37)
Hang Ruan (https://blog.jayway.com/author/hangruan/) (3)
Hanna Sahle (https://blog.jayway.com/author/hannasahle/) (1)
Hannes Gruber (https://blog.jayway.com/author/hannesgruber/) (3)
Henrik Andersson (https://blog.jayway.com/author/henrikandersson/) (3)
Henrik Bernstrom (https://blog.jayway.com/author/henrik-bernstromdevoteam-com/) (5)
Henrik Feldt (https://blog.jayway.com/author/henrikfeldt/) (5)
Henrik Larne (https://blog.jayway.com/author/henriklarne/) (2)
Henrik Lundahl (https://blog.jayway.com/author/henriklundahl/) (4)
Fredrik Henriksson (https://blog.jayway.com/author/fredrik-henricssonjayway-com/) (2)
Hugo Hjerten (https://blog.jayway.com/author/hugo-hjertenjayway-com/) (3)



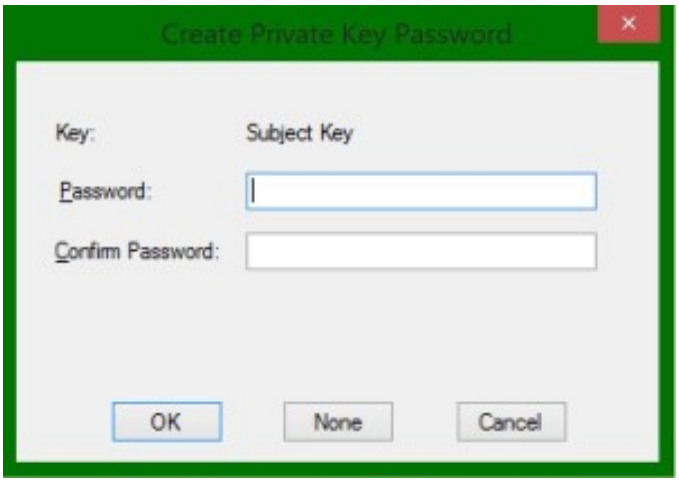
(http://blog.jayway.com/wp-content/uploads/2014/09/15.-ServerSSL-cmd.jpg)

Run it in your Developer Command Prompt the same way as before, only this time type in a name for your certificate after the command. Mine will be: CreateSslServerCert.cmd ServerSSL



(http://blog.jayway.com/wp-content/uploads/2014/09/14.-ServerPrompt.jpg)

Again it will ask you to create your private key password, use it to verify, also give the issuers password *(which is the one you chose when creating your root CA)* and lastly the private key password you choose in the first window.

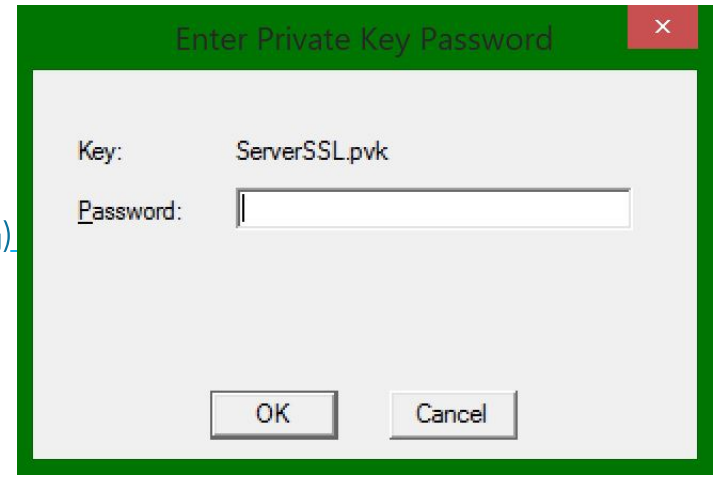


Hugo Josefson (https://blog.jayway.com/author/hugojosefson/) (6)
Jacob Mattsson (https://blog.jayway.com/author/jacobmattsson/) (2)
Jakob Nilsson-Ehle (https://blog.jayway.com/author/jakobnilssonehle/) (4)
Jakob Wolman (https://blog.jayway.com/author/jakobklamra/) (3)
Jan Kronquist (https://blog.jayway.com/author/jankronquist/) (29)
Jan-Olof Eriksson (https://blog.jayway.com/author/janoloferiksson/) (1)
Jens Jakob Jensen (https://blog.jayway.com/author/jensjakobjensen/) (2)
Jens Nordahl (https://blog.jayway.com/author/jensnordahl/) (2)
Jimmie Jensen (https://blog.jayway.com/author/jimmiejensen/) (3)
Jimmy Falkbjer (https://blog.jayway.com/author/jimmyfalkbjer/) (1)
Joacim Löwgren (https://blog.jayway.com/author/joacimlowgren/) (1)
joakim astbrant (https://blog.jayway.com/author/joakimastbrant/) (2)

(http://blog.jayway.com/wp-content/uploads/2014/09/servercert-password1.jpg)

(http://blog.jayway.com/wp-content/uploads/2014/09/servercert-password2.jpg)

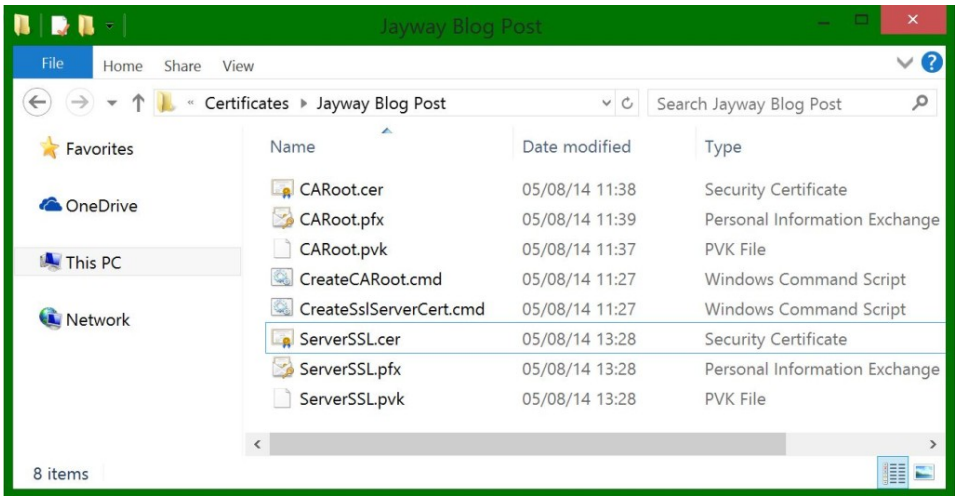
(http://blog.jayway.com/wp-content/uploads/2014/09/servercert-password3.jpg)



(http://blog.jayway.com/wp-content/uploads/2014/09/servercert-password4.jpg)

...aaand voila you now have the ServerSSL certificate files.

Joakim Back (https://blog.jayway.com/author/joakimback/) (1)
Joakim Hogart (https://blog.jayway.com/author/joakimhogart/) (1)
Johan Haleby (https://blog.jayway.com/author/johanhaleby/) (50)
Johan Karlsson (https://blog.jayway.com/author/johankarlsson/) (3)
Johan Lundahl (https://blog.jayway.com/author/johanlundahl/) (5)
Johan Månsson (https://blog.jayway.com/author/johan-manssonjayway-com/) (1)
Johan Nordenswan (https://blog.jayway.com/author/johannordenswan/) (3)
Johan Olsson (https://blog.jayway.com/author/johanolsson/) (10)
Johan Rask (https://blog.jayway.com/author/johanrask/) (4)
Johan Silfversparre (https://blog.jayway.com/author/johansilfversparre/) (13)
Karin Hofbauer (https://blog.jayway.com/author/karinhofbauer/) (1)

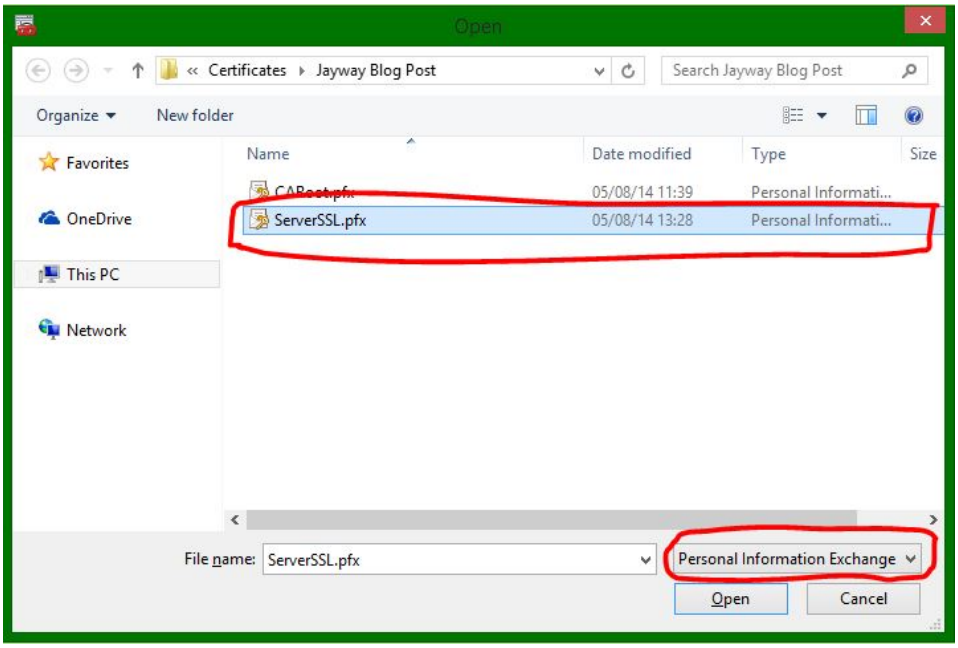


(http://blog.jayway.com/wp-content/uploads/2014/09/16.-ServerSSL-Certs.jpg)

If you didn't include the -sr and -ss parameters, import the Personal Information Exchange (pfx) certificate into your Personal Certificates in the Microsoft Management Console:
Open the Personal folder → right-click Certificates → Import...

Again the Certificate Import Wizard pops up → Go Next

This time you will Browse for the ServerSSL.pfx file

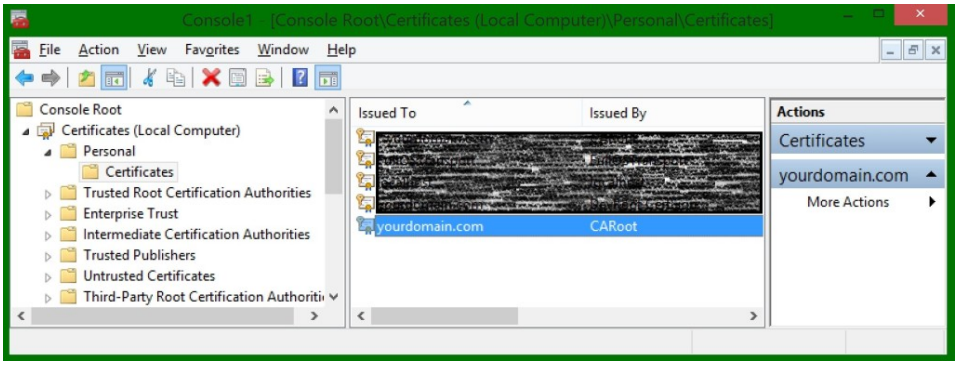


(http://blog.jayway.com/wp-content/uploads/2014/09/17.-MMCserver.jpg)

Karl Marhäll (https://blog.jayway.com/author/karl-marhalljayway-com/) (1)
Kenneth Andersson (https://blog.jayway.com/author/kennethandersson/) (1)
Khalid Afridi (https://blog.jayway.com/author/khalid-afridijayway-com/) (1)
Lars-Håkan Jönsson (https://blog.jayway.com/author/larshakanjonsson/) (2)
László Urszuly (https://blog.jayway.com/author/laszlourszuly/) (2)
Mads Enevoldsen (https://blog.jayway.com/author/madsenevoldsen/) (7)
Magnus Mårtensson (https://blog.jayway.com/author/magnusmartensson/) (9)
Magnus Palmér (https://blog.jayway.com/author/magnuspalmer/) (1)
Magnus Robertsson (https://blog.jayway.com/author/magnusrobertsson/) (3)
Magnus Rydin (https://blog.jayway.com/author/magnusrydin/) (1)
Mario Boikov (https://blog.jayway.com/au

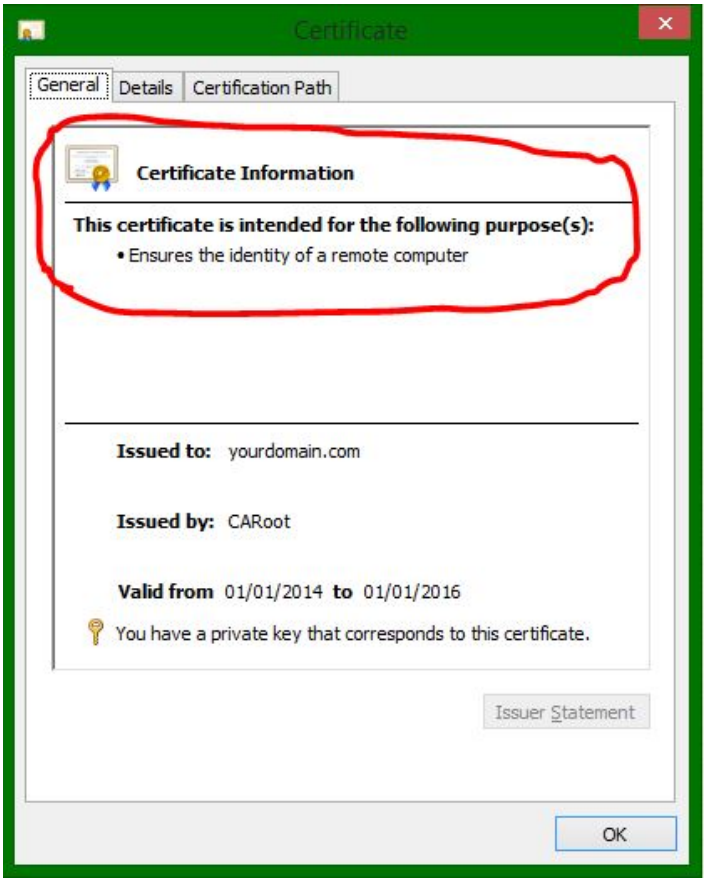
Go next → Type in the password for your pfx file *(The -po parameter from the batch file)* → Continue going next until finish and the message box with "The import was successful" appears.

You should now see you newly imported certificate in your → Personal Certificates folder



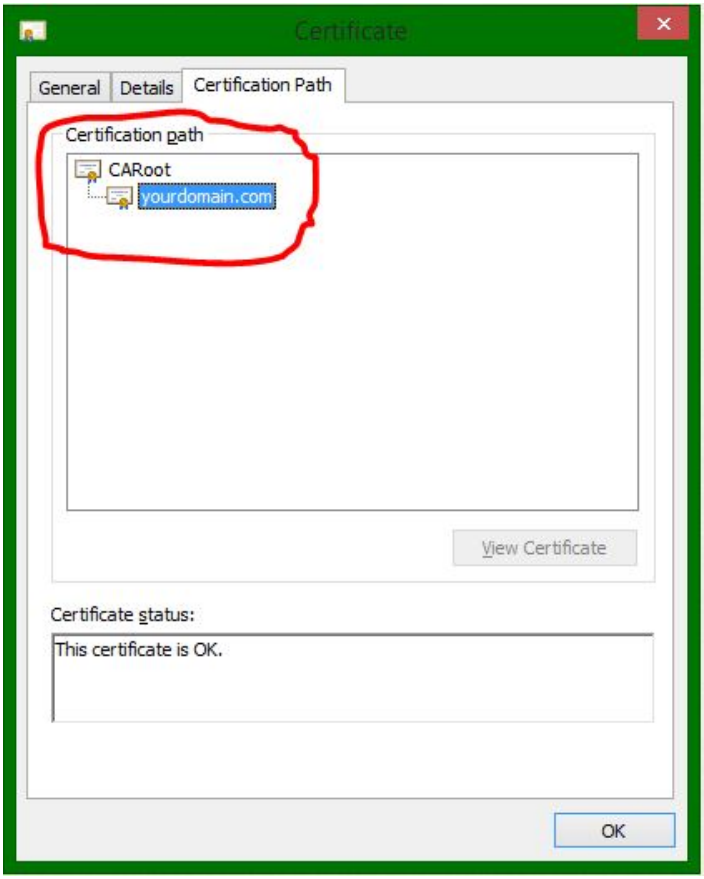
(http://blog.jayway.com/wp-content/uploads/2014/09/18.-MMCServer21.jpg)

It is trusted automatically because your CARoot that signed it is trusted and has a private key corresponding to this certificate.



thor/mario-boikov/) (3)
Mårten Österberg (https://blog.jayway.com/author/martenosterberg/) (1)
Mattias Ask (https://blog.jayway.com/author/mattiasask/) (8)
Mattias Hellborg Arthursson (https://blog.jayway.com/author/mattiasarthursson/) (12)
Mattias Lindskog (https://blog.jayway.com/author/mattiaslindskog/) (9)
Mattias Rosberg (https://blog.jayway.com/author/mattiasrosberg/) (3)
Mattias Severson (https://blog.jayway.com/author/mattiasseverson/) (39)
Mattias Sjögren (https://blog.jayway.com/author/mattias-sjogren/) (4)
Max Ringström (https://blog.jayway.com/author/max-ringstromjayway-com/) (1)
Michael Kober (https://blog.jayway.com/author/michaelkober/) (5)
Mikael Karlsson (https://blog.jayway.com/author/mikaelkarlsson/) (1)
Mina Ashna (https://blog.jayway.com/au

(http://blog.jayway.com/wp-content/uploads/2014/09/19.-TrustedServerCert1.jpg) (http://blog.jayway.com/wp-content/uploads/2014/09/20-TrustedServerCertPath.jpg)



(http://blog.jayway.com/wp-content/uploads/2014/09/20-TrustedServerCertPath1.jpg)

You can now configure your server to use this certificate.

Client Certificates

Last but not least we will create the client certificate which can be used for client certificate authentication. We will again create a command batch file, now with the following parameters:

thor/mina-ashnajayway-com/) (2)
Mohsan Khan (https://blog.jayway.com/author/mohsan-khanjayway-com/) (1)
Morten Faester (https://blog.jayway.com/author/mortenfaester/) (1)
Niklas Lundberg (https://blog.jayway.com/author/niklaslundberg/) (1)
Niklas Uhrberg (https://blog.jayway.com/author/niklasuhrberg/) (2)
Nino Martinez (https://blog.jayway.com/author/ninomartinez/) (1)
Oleksii Kulikov (https://blog.jayway.com/author/oleksii-kulikovjayway-com/) (1)
Olof Åkesson (https://blog.jayway.com/author/olofakesson/) (2)
Ondrej Bendo (https://blog.jayway.com/author/ondrej-bendojayway-com/) (1)
Oskar Wickström (https://blog.jayway.com/author/oskarwickstrom/) (3)
Paolo Longato (https://blog.jayway.com/author/paolo-longatojayway-com/) (2)

```
makecert.exe ^
-n "CN=%1" ^
-iv CARoot.pvk ^
-ic CARoot.cer ^
-pe ^
-a sha512 ^
-len 4096 ^
-b 01/01/2014 ^
-e 01/01/2016 ^
-sky exchange ^
-eku 1.3.6.1.5.5.7.3.2 ^
-sv %1.pvk ^
%1.cer

pvk2pfx.exe ^
-pvk %1.pvk ^
-spc %1.cer ^
-pfx %1.pfx ^
-po Test123
```

You may notice that this is almost identical to the server certificate parameters, all except:

- "CN=%1" ➜ This can be whichever name you like and will be what you type in after .cmd
  You can also add more than one in the -n parameter for example: "-n "CA=%1,O=My Organization,OU=Dev,C=Denmark" and so on.
  Reference:
  - CN = commonName (for example, "CN=My Root CA")
  - OU = organizationalUnitName (for example, "OU=Dev")
  - O = organizationName (for example, "O=Jayway")
  - L = localityName (for example, "L=San Francisco")
  - S = stateOrProvinceName (for example, "S=CA")

Pär Sikö (https://blog.jayway.com/author/parsiko/) (1)
Patrik Nordwall (https://blog.jayway.com/author/patriknordwall/) (1)
Per Böckman (https://blog.jayway.com/author/perbockman/) (4)
Per Ökvist (https://blog.jayway.com/author/perokvist/) (20)
Per Wendel (https://blog.jayway.com/author/perwendel/) (1)
Per-Erik Bergman (https://blog.jayway.com/author/pererikbergman/) (14)
Per-Olof Bondesson (https://blog.jayway.com/author/perolofbondesson/) (10)
Petar Mataic (https://blog.jayway.com/author/petar-mataic/) (5)
Peter Neubauer (https://blog.jayway.com/author/peterneubauer/) (7)
Peter von Lochow (https://blog.jayway.com/author/petervonlochow/) (18)
Peter Winzell (https://blog.jayway.com/author/peterwinzell/) (2)
Philip Nilsson (https://blog.jayway.com/au

- C = countryName (for example, “C=US”)

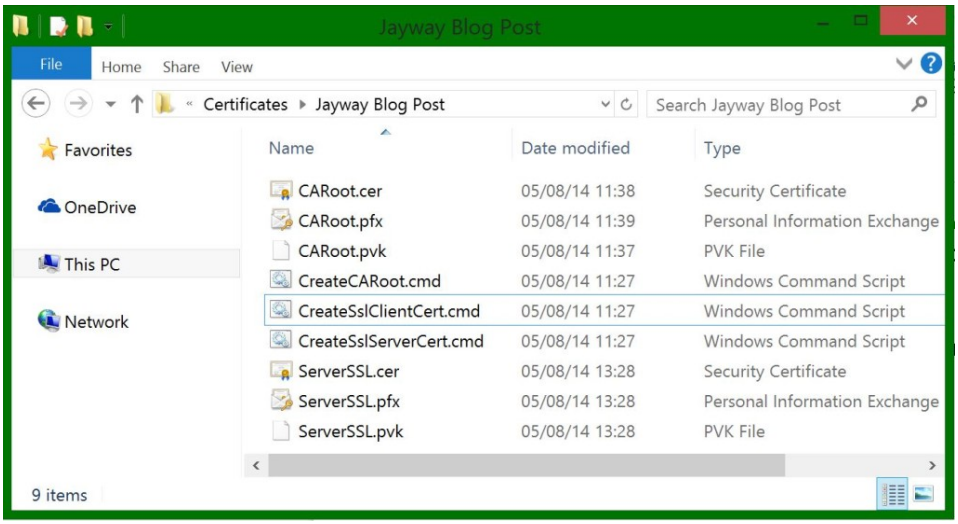
- -eku 1.3.6.1.5.5.7.3.2 → The client authentication OID (Object Identifier).

Optional: install client certificate directly into the CurrentUser Personal certificate store

NOTE: This will only install the .cer file into the MMC, in order to import the .pfx file you will have to do it manually.

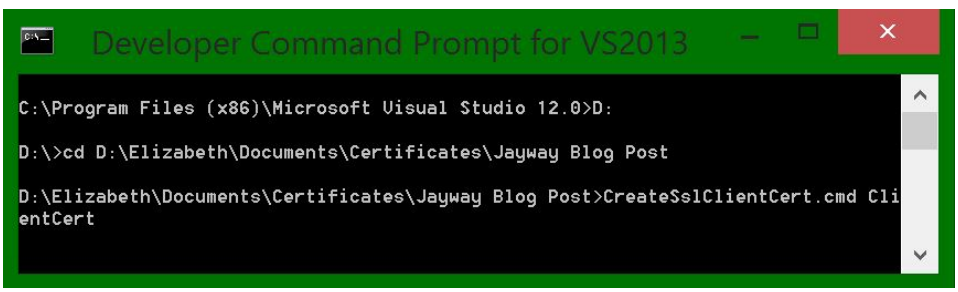
- -sr CurrentUser → The subject’s certificate store location
- -ss My → The certificate store name

Your batch command will create a SSL certificate to use on your client and will be signed by your CARoot authority.



(http://blog.jayway.com/wp-content/uploads/2014/09/21.-ClientCertCmd.jpg)

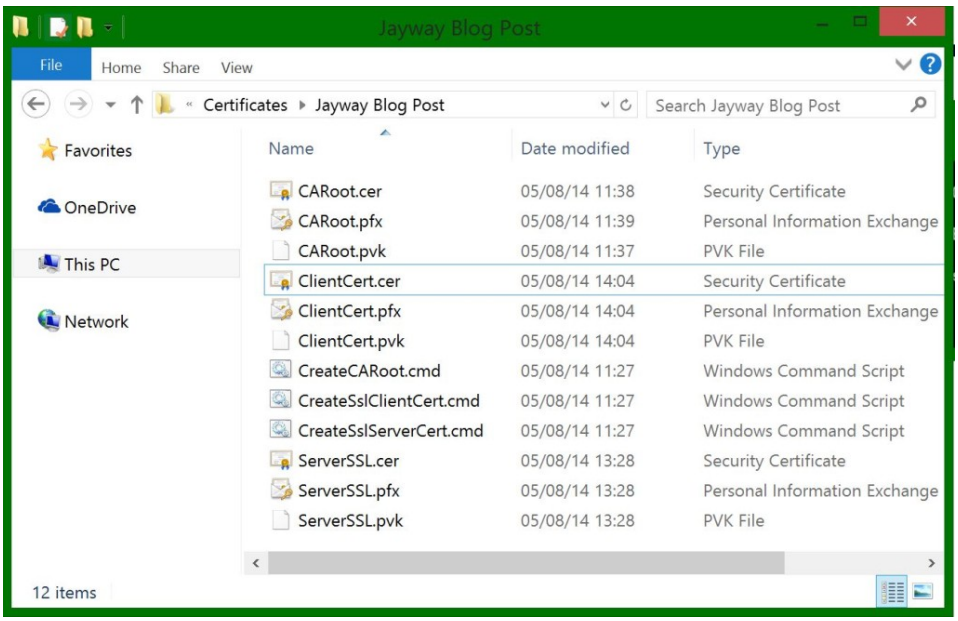
Execute the command batch file in the Developer Command Prompt, again with a name after the cmd. (Mine will be: CreateSslClientCert.cmd ClientCert)



thor/philipnilsson/) (2)
Renas Reda (https://blog.jayway.com/author/renasreda/) (4)
Rickard Nilsson (https://blog.jayway.com/author/rickardnilsson/) (2)
Rickard Öberg (https://blog.jayway.com/author/rickardoberg/) (7)
Rikard Ottosson (https://blog.jayway.com/author/rikardottosson/) (2)
Robert Hedgate (https://blog.jayway.com/author/roberthedgate/) (21)
Sebastian Potter (https://blog.jayway.com/author/sebastian-potterjayway-com/) (1)
Sergii Nezdolii (https://blog.jayway.com/author/sergiinezdolii/) (1)
Sigurdur Birgisson (https://blog.jayway.com/author/sigurdurbirgisson/) (11)
Silvia Man (https://blog.jayway.com/author/silvia-manjayway-com/) (3)
Sladjan Trajkovic (https://blog.jayway.com/author/sladan-trajkovic/) (1)
Stefan Li (https://blog.jayway.com/author/stefanli/) (1)

(http://blog.jayway.com/wp-content/uploads/2014/09/22.-PromptClientCert.jpg)

Enter the passwords in the same pattern as the server certificate and you now have your client certificate.

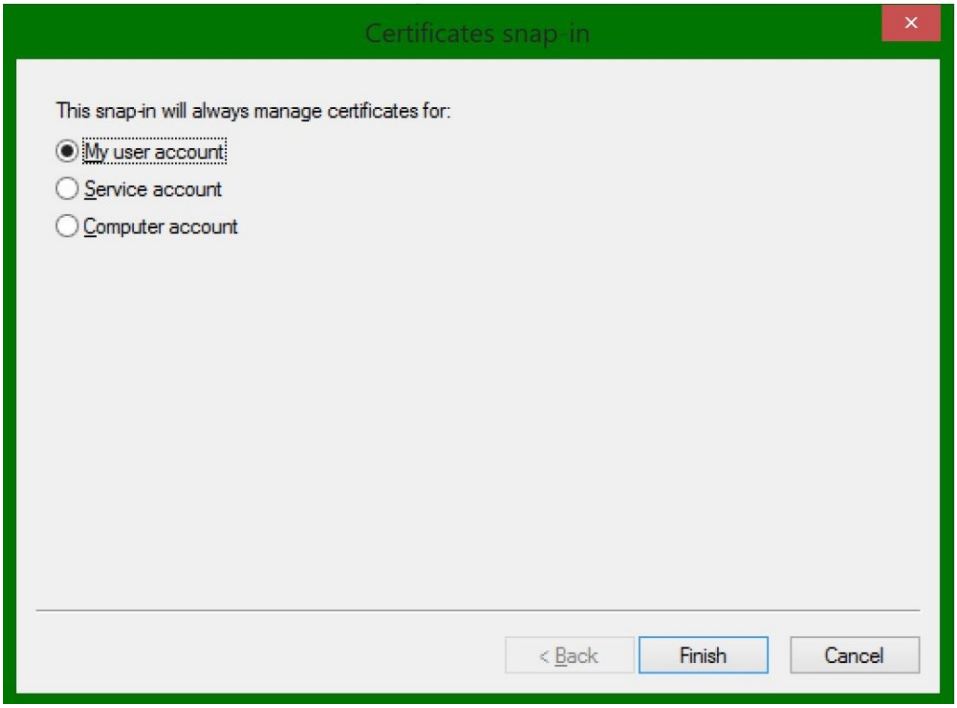


(http://blog.jayway.com/wp-content/uploads/2014/09/23.-ClientCert.jpg)

You can now add it to your Current User Personal Certificate store:
In the Microsoft Management Console, click File → Add/Remove Snap-in

Double-click Certificates again, but this time choose My user account

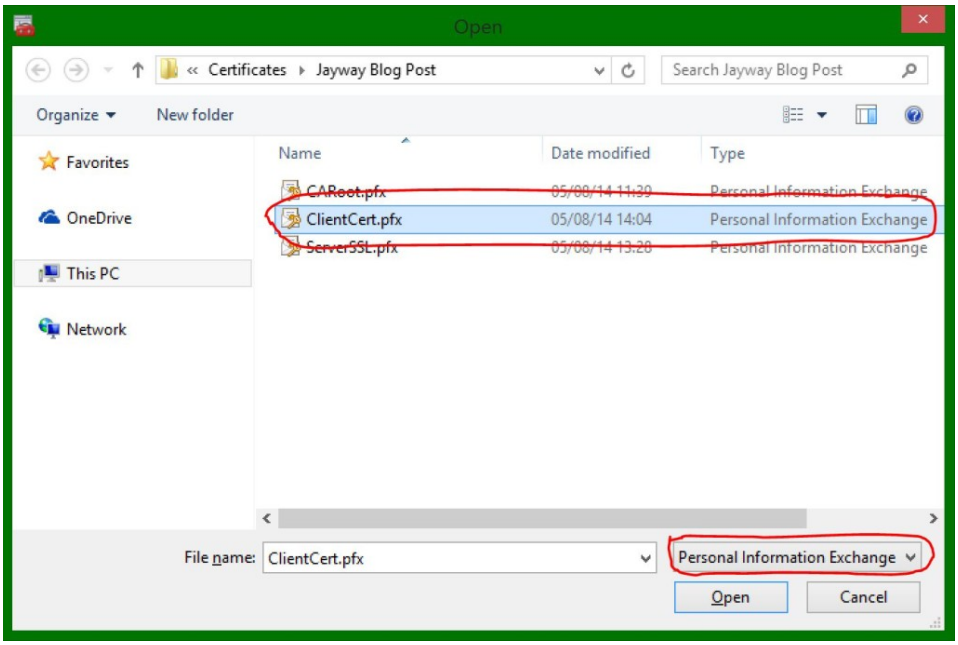
Stefan Severin (https://blog.jayway.com/author/stefanseverin/) (2)
Steve Widinghoff (https://blog.jayway.com/author/steve-widinghoffjayway-com/) (6)
Stuart Mcculloch (https://blog.jayway.com/author/stuartmcculloch/) (1)
Sune Simonsen (https://blog.jayway.com/author/sunesimonsen/) (1)
Thomas Hansson (https://blog.jayway.com/author/thomas-hanssonjayway-com/) (2)
Tobias Södergren (https://blog.jayway.com/author/tobiassodergren/) (17)
Tomas Aschan (https://blog.jayway.com/author/tomas-aschanjayway-com/) (9)
Tomas Nilsson (https://blog.jayway.com/author/tomasnilsson/) (10)
Ulrik Sandberg (https://blog.jayway.com/author/ulriksandberg/) (30)
Uzi Landsmann (https://blog.jayway.com/author/uzilandsmann/) (1)
Vlado Palczynski (https://blog.jayway.com/author/vladopalczynski/) (1)



(http://blog.jayway.com/wp-content/uploads/2014/09/24.-MMC-client.jpg)

Open the Personal folder → Right-click Certificates → Import...

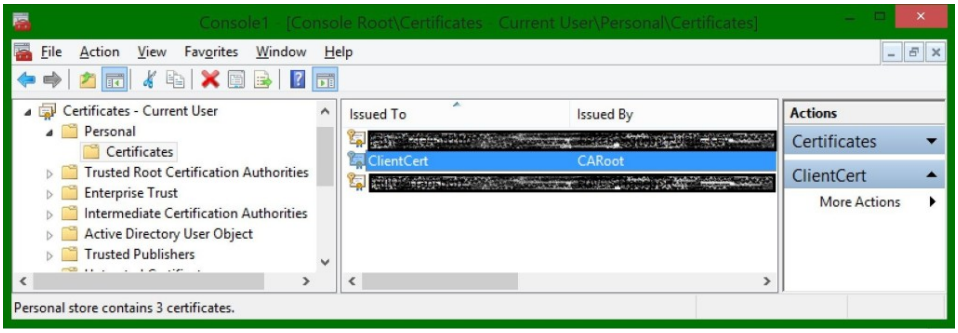
Browse for your ClientCert.pfx file



(http://blog.jayway.com/wp-content/uploads/2014/09/25.-MMC-client-2.jpg)

Go next → Type in the password to your pfx file (-po parameter from the batch file) → Continue going next until finish and "The import was successful" message box appears.

You should now see you newly imported certificate in your Personal → Certificates folder



(http://blog.jayway.com/wp-content/uploads/2014/09/26.-MMC-Client3.jpg)

Again the certificate is trusted because the CARoot is trusted by Windows.

(http://blog.jayway.com/wp-content/uploads/2014/09/27.-

TrustedClient.jpg)

(http://blog.jayway.com/wp-content/uploads/2014/09/28.-TrustedClientPath.jpg)

You can now configure your client to use this certificate.

I hope the whole self signed certificate creation together with the makecert.exe generation tool feels more understandable and that you can use this knowledge for your development process. For a walk-through on setting up IIS to use your self-signed certificates check out my next blog post: http://blog.jayway.com/2014/10/27/configure-iis-to-use-your-self-signed-certificates-with-your-application/ (http://blog.jayway.com/2014/10/27/configure-iis-to-use-your-self-signed-certificates-with-your-application/)

Check out my blog post for getting self signed certificates to work with a Windows Azure cloud service: http://blog.jayway.com/2015/04/21/configure-a-windows-azure-cloud-service-to-use-your-self-signed-certificates-for-iis-client-certificate-mapping-authentication/

(http://blog.jayway.com/2015/04/21/configure-a-windows-azure-cloud-service-to-use-your-self-signed-certificates-for-iis-client-certificate-mapping-authentication/)

Take care! =)

TAGS: .NET (HTTPS://BLOG.JAYWAY.COM/TAG/NET/), GUIDE (HTTPS://BLOG.JAYWAY.COM/TAG/GUIDE/), MAKECERT.EXE (HTTPS://BLOG.JAYWAY.COM/TAG/MAKECERT-EXE/), MMC (HTTPS://BLOG.JAYWAY.COM/TAG/MMC/), PROGRAMMING (HTTPS://BLOG.JAYWAY.COM/TAG/PROGRAMMING/), PVK2PFX.EXE (HTTPS://BLOG.JAYWAY.COM/TAG/PVK2PFX-EXE/), SELF SIGNED CERTIFICATES (HTTPS://BLOG.JAYWAY.COM/TAG/SELF-SIGNED-CERTIFICATES-2/), SSL (HTTPS://BLOG.JAYWAY.COM/TAG/SSL/), TOOLS (HTTPS://BLOG.JAYWAY.COM/TAG/TOOLS/), TUTORIAL (HTTPS://BLOG.JAYWAY.COM/TAG/TUTORIAL/), WALK-THROUGH (HTTPS://BLOG.JAYWAY.COM/TAG/WALK-THROUGH/)

← Previous Post
Jay Librarian – Jayway's Book Management System (https://blog.jayway.com/2014/08/29/jay-librarian-jayways-book-management-system/)

Next Post →
Display map content in Windows Phone 8.1 (https://blog.jayway.com/2014/10/23/display-map-content-in-windows-phone-8-1/)

THIS POST HAS 101 COMMENTS

Anders Poulsen

5 SEP 2014 REPLY

Just used your guide this morning, thanks. The only thing missing, I think, is "How do I set up my IIS to actually USE this selv signed certificate".

Elizabeth Andrews

5 SEP 2014 REPLY

Great to hear that you found it useful.

I'm actually writing my next blog post as we "speak", on how to configure Windows IIS and application to use these self signed certificates, so keep posted ;-)

Adriaan Booysen

3 OCT 2014 REPLY

Nice article, was clear and simple.
Just a further note would be to use a chained root CA to issue the server and client SSL's and therefore you don't have to expose the Root CA.
makecert -n "CN=CARoot Sub" -iv CARoot.pvk -ic CARoot.cer -pe -a sha512 -len 4096 -cy authority -sv SCARoot.pvk SCARoot.cer
-sr LocalMachine -ss Root ****Optional parameters
pvk2pfx -pvk SCARoot.pvk -spc SCARoot.cer -pfx SCARoot.pfx
Then change the ServerSSL and ClientSSL batch to use the chained CA.
The same will apply for those people using Active Directory Certificate Services (ADCS)
Regards

Napoleon Tan

15 OCT 2014 REPLY

I was able to use the said step for creating the certificate. It was very helpful step by step especially for people who do not know the ins and out of the SSL protocol. Good job.

Prabhu

16 OCT 2014 REPLY

How are you getting that ServerSSL in the MMC console for the server certificate i am getting the domain name there. I replaced the %1 with the ServerSSL and i got all the 3 files .cer,.pfx and the .pvk file with the

name as ServerSSL, but in my mmc i am getting my domain name when i import the certificate.

Elizabeth Andrews

21 OCT 2014 REPLY

I understand you got confused there Prabhu, I have changed the pictures for the server certificate to correctly display the CN name (your domain name) in both the certificate and in the MMC after import. The %1 parameter only defines the file name of the certificates (.cer, .pvk and .pfx), in this case we put in ServerSSL. The MMC doesn't display the file name, it displays the CN name (what you wrote in your CN="yourdomain.com" parameter). In the old pictures I had generated a certificate with the CN parameter set to "CN=ServerSSL" which is why it was displayed like so in the MMC. I apologize for the outdated pictures, please read the Server Certificate part again and hopefully it becomes clear. It sounds like you imported the certificate correctly.

Prabhu

23 OCT 2014 REPLY

Thanks Elizabeth for the reply.
I had to do a mutual SSL authentication for peer-peer communication not localhost. I am doing this using Microsoft.Net using socket communication class.
For this i have created self-signed certificates comprising of one root certificate a server certificate and a client certificate. Below are the commands i am using for generating the same.
Root
→makecert.exe -n "CN=abc.com" -r -pe -a sha512 -len 4096 -cy authority -sv RootCert.pvk RootCert.cer

→pvk2pfx -pvk RootCert.pvk -spc RootCert.cer -pfx RootCert.pfx -po test123

Server

→makecert.exe -pe -n “CN=abc.com” -a sha512 -sky exchange -eku 1.3.6.1.5.5.7.3.1 -ic RootCert.cer -iv RootCert.pvk -sp “Microsoft RSA SChannel Cryptographic Provider” -sy 12 -sv ServerCert.pvk ServerCert.cer

→pvk2pfx -pvk ServerCert.pvk -spc ServerCert.cer -pfx ServerCert.pfx -po test123

Client

→makecert.exe -pe -n “CN=abc.com” -a sha512 -sky exchange -eku 1.3.6.1.5.5.7.3.2 -ic RootCert.cer -iv RootCert.pvk -sp “Microsoft RSA SChannel Cryptographic Provider” -sy 12 -sv ClientCert.pvk ClientCert.cer

→pvk2pfx -pvk ClientCert.pvk -spc ClientCert.cer -pfx ClientCert.pfx -po test123

After generating all the required certificates i am adding them to mmc console as you have explained above.

To check for mutual authentication i am using X509Certificate2 class, while doing this in SslPolicyErrors i am encountering error stating RemoteCertificate name mismatch

I know this is a long shot but can anyone give me any pointers on the same.

Alif

24 OCT 2014 REPLY

Hi Prabhu,

We are also facing the same issue while testing the client and server application on two different machines.

Please let me us know any more information how to resolve the issue.

Thanks in Advance

Alif

Phil

25 OCT 2014 REPLY

Thanks Elizabeth.

I was looking for your follow up post on how to configure your Local IIS, but couldn't find it. Any chance that's still coming?

Cheers

:phil

Elizabeth Andrews

27 OCT 2014 REPLY

Hi Phil

Yes, as a matter of fact I just published it today! :D

Here's the link: http://blog.jayway.com/2014/10/27/configuring-iis-on-windows-to-use-your-self-signed-certificates-with-your-application/ (http://blog.jayway.com/2014/10/27/configuring-iis-on-windows-to-use-your-self-signed-certificates-with-your-application/)

Hope you find it useful

Ben

25 OCT 2014 REPLY

I've just gone through all this but Chrome is still moaning at me about my SSL certificate. NET::ERR_CERT_COMMON_NAME_INVALID. I'm trying to find out why now but just thought I'd ask here and see if anyone has any hints. Thanks

Ben

30 OCT 2014 REPLY

It's because I'd tried to use the same port binding on more than one site and IIS got all confused and switched my cert to not match the domain.

Prabhu

10 NOV 2014 REPLY

After about 10 days of all possible permutations and combinations have created a link with our team which maybe helpful for some of you people.
https://social.msdn.microsoft.com/Forums/en-US/51149679-106b-47ac-9898-3ba9467a08aa/sslstream-mutual-authentication-client-certificate-is-null-at-server?forum=netfxbcl (https://social.msdn.microsoft.com/Forums/en-US/51149679-106b-47ac-9898-3ba9467a08aa/sslstream-mutual-authentication-client-certificate-is-null-at-server?forum=netfxbcl)

Pingback: itemprop="name">Creating self signed certificates with makecert.exe for development | Jayway | Jackie Chan Focus Daily (http://jackiechanfocus.azurewebsites.net/?p=511)

Ali

4 DEC 2014 REPLY

I spent hours trying to solve my WCF security error and tried every single solution on the web. None is any close to this detailed and clear explanation. You are the best.
Thanks

Orlando

10 DEC 2014 REPLY

Wanted to thank you for this very informative article. Best regards

César Cruz

20 DEC 2014 REPLY

Thanks. Fine

Henk Brink

14 JAN 2015 REPLY

Literally saved me hours this morning. Extremely well documented and clear explanation. Won't soon forget. Thanks a ton Elizabeth.

Harman Gill

15 JAN 2015 REPLY

Great article, very well done! Just wanted to add that it will be good to add that you can export the certificate in Base64 encoding after importing it into Trusted Certification Authorities. This plain text/readable CER file is useful where X509 certificate is an element of a XML configuration file like in SAML Single Sign On applications.

Gerard

17 JAN 2015 REPLY

Dear Elizabeth,
This is a "Wow!" post. Thank you soooooo much.
I do have some tiny remarks (aka things i had to solve)
1. "You can add these two parameters: -sr LocalMachine ^ and -ss Root ^ to the upcoming command batch file" = add to the MAKECERT command in the .CMD file (not to the end of the file)
2. In your CMD files you have " -po Test123" . But during the process we enter our own passwords... (so i deleted that line)

3. At first i got the impression that i could invent my own ” -eku” identifier. I soon learned this is not the case. The OID says something about the use of the certificate:

Encrypting File System (1.3.6.1.4.1.311.10.3.4)

Code Signing (1.3.6.1.5.5.7.3.3)

Secure Email (1.3.6.1.5.5.7.3.4)

Smart Card Logon (1.3.6.1.4.1.311.20.2.2)

Client Authentication (1.3.6.1.5.5.7.3.2)

Server Authentication (1.3.6.1.5.5.7.3.1)

IP security IKE intermediate (1.3.6.1.5.5.8.2.2)

But YOU brought me 99% to the finishline.

Again: great many thanks!!

Mohsan Hassan

4 FEB 2015 REPLY

It is very detailed walk through. really helped me in understanding CA, Server and Client Certificates.

Very good article

Amit Manchanda

10 FEB 2015 REPLY

Hi Elizabeth, You wrote very well, as i am new to ssl, i was facing so much issues based on ssl certificates. but your post finally make me feel better. But it works fine on my local machine. but now i want to use it on my live server still it is not working well on live server. i am using ssl certificates with windows service .

Please suggest me how to use ssl certificate to authenticate my server to clients and please tell me if i want to authenticate my server to clients then should i have to provide my server certificates to clients who will interact with my windows service to match

Joel Sam

26 FEB 2015 REPLY

can't wait for the post for getting self signed certificates to work with a Windows Azure cloud service

Sheng Jiang

20 APR 2015 REPLY

Very good article which helps me setting an IIS environment which requires client certificate!

Leandros

9 MAY 2015 REPLY

Excellent article! I would only add that if Visual Studio is not available you have to install "Windows Software Development Kit (SDK) for Windows 8.1", or similar. Then, add the SDK folder to the system PATH, for example "C:\Program Files (x86)\Windows Kits\8.1\bin\x64". And then, simply use the Windows Command Prompt (as opposed to Visual Studio Developer Command Prompt).

Ashok Kumar

14 MAY 2015 REPLY

Hi,
I am using this concept and applied to one of my site this is working to chrome and IE but getting issue with Firefox as
Secure Connection Failed
The connection to http://www.abc.com (http://www.abc.com) was interrupted while the page was loading.

The page you are trying to view cannot be shown because the authenticity of the received data could not be verified.
Please contact the website owners to inform them of this problem.
can any one help me.

Raifel

27 MAY 2015 REPLY

How can we generate intermediate certificate from root certificte?

Justin Andrews

29 MAY 2015 REPLY

I am struggling with this process and would appreciate a bit of guidance. I have followed the guide for creating self signed certificates and am now trying to get my local IIS environment configured to use them. I am running IIS8 on a windows 8 machine.
The domain I am using is 'angularjsauthenticationweb.com' and I have modified the hosts file according to the sample. The non-https urls return as expected.
In IE both the angularjsauthenticationweb.com and http://www.angularjsauthenticationweb.com (http://www.angularjsauthenticationweb.com) sites return with HTTPS. However, the lock does not appear in the URL bar until I press F5 to refresh the page. Once the page has been refreshed the locks appear and the cert appears to be correct (issued by CARoot and issued to matches my URL).
In Chrome I see some different behavior. https://angularjsauthenticationweb.com/ (https://angularjsauthenticationweb.com/) opens up correctly with a nice green lock. However, when I add www to make the URL https://www.angularjsauthenticationweb.com

(https://www.angularjsauthenticationweb.com) I still see the green lock in the corner but the page does not return correctly and instead I receive an error message indicating:
'Your client certificate is either not trusted or is invalid.'
When I view the certificate it indicates it is issued by 'CARoot' and issued to the correct url 'www.angularjsauthenticationweb.com'
I also followed the instructions to add the CARoot cert to firefox:
Firefox Settings ➜ Options ➜ Advanced ➜ View Certificates ➜ Authorities ➜ import your CARoot.cer file
However, when I try to open the secure URL's from firefox on my local PC where the site is hosted I receive the 'Secure Connection Failed' error with either the angularjsauthenticationweb.com or http://www.angularjsauthenticationweb.com (http://www.angularjsauthenticationweb.com) URL's.
I have been through the examples several times and have been unable to resolve the issues. I must be missing something here and could really use a nudge in the right direction. Thanks!

Kevin Snow

11 JUN 2015 REPLY

I also just wanted to throw in that this was a really helpful article. While I was doing a lot of these things I didn't have the level of understanding that this article provided, this really helped put things together for me. Many thanks!

Dave Rubin

6 JUL 2015 REPLY

Very good article. I had no problem with the first part. But, I am having a difficult time creating the Server Certificates. When I run the .cmd file, it pops up with the 1st box and I enter the key twice. The next box, I enter

the key once. Then the 3rd box pops up and I enter the key again and after I hit click OK, I get an Error: Can't load the issuer certificate ('RDS-SERVER.cer'} Failed

Under that is shows another Error: File not found. (Error Code = 0x80070002). Here's my .cmd file: I tried changing the names, the dates, but still get the same error. Any help would be Greatly appreciated!

```
makecert.exe ^
-n "CN=phillytrans.homeip.net" ^
-iv RDS-SERVER.pvk ^
-ic RDS-SERVER.cer ^
-pe ^
-a sha512 ^
-len 4096 ^
-b 07/05/2015 ^
-e 07/05/2039 ^
-sky exchange ^
-eku 1.3.6.1.5.5.7.3.1 ^
-sv RDS-SERVER.pvk ^
RDS-SERVER.cer
pvk2pfx.exe ^
-pvk RDS-SERVER.pvk ^
-spc RDS-SERVER.cer ^
-pfx RDS-SERVER.pfx ^
-po Test123
```

Francis (http://simynazareth.blogspot.com) 14 JUL 2015 REPLY

Thank you for such a wonderful article! I was struggling with authenticating using client certificates until I found this article.

swapnil

23 JUL 2015 REPLY

Thanks it is realy very useful.

OutOfTouch6947

4 AUG 2015 REPLY

I did part 1 of what you have here but I keep getting this error on part 2 when trying to create the SSL cert

c:\Development\DevCerts>pvk2pfx.exe -pvk TestSSL.pvk -spc TestSSL.cer -pfx TestSSL.pfx -po IAmAPassword

ERROR: File not found.

(Error Code = 0x80070002).

> ### OutOfTouch6947
>
> 5 AUG 2015 REPLY
>
> My fault I was not putting in the correct password of my Issuer(RootCACert) to sign this new cert.
>
> I did part 1 of what you have here but I keep getting this error on part 2 when trying to create the SSL cert
>
> c:\Development\DevCerts>pvk2pfx.exe -pvk TestSSL.pvk -spc TestSSL.cer -pfx TestSSL.pfx -po IAmAPassword
>
> ERROR: File not found.
>
> (Error Code = 0x80070002).

Chris (http://dairymaster.com)

21 AUG 2015 REPLY

Hi this is a good guide, however I have a linux server and a windows host which I am trying to set up using SSL/TLS. I have created a CA on the server and generated the certs needed on this machine, I then added them to the ca-certs and copied the CA and cert to the client machine. I

converted the .pem cert file to .cer and added both the CA and .cer files to the trusted certs using mmc command. now when i run the server and fire up the client the handshake is not completed and the server just hangs until the connection is timed out , really struck so any advice would by appreciated.

Vijaykumar

17 SEP 2015 REPLY

Thank you very much for this blog…. It is very clear to understand the concept. Thanks again for this post.

Stephen Drew

19 SEP 2015 REPLY

Thanks Elizabeth – I have read many articles on this often infuriating subject, and yours is by far the clearest and most helpful!

---

liza

21 SEP 2015 REPLY

I find this article helpful for stand-alone servers, so I am wondering if there are topics on how to create SSL for a cluster environment? Help is appreciated

---

Kristina

22 SEP 2015 REPLY

Thank you very much madam.

Felix (http://skeena.net)

1 OCT 2015 REPLY

There is also a powershell cmdlet that does a similar thing to makecert.exe: New-SelfSignedCertificate

Stu

13 OCT 2015 REPLY

Thank you for the detailed article. I have one question which I am never able to answer no matter which process I find on the web to follow. It revolves around the passwords. Everyone says the same thing, just use the same password for all three (like you do at the top). But then later on there are more passwords to create. Are we literally supposed to use the exact same password in every single instance above throughout the entire article? For security, I want to use different passwords where possible, knowing that some of them need to be the same. I guess if I saw example passwords (such as pwd1, pwd1, pwd2) used in the example, it would ultra clear and finally answer that one nagging question I always have.
Thank you.

AmirReza

21 OCT 2015 REPLY

Thank you very very much.
your article is the best.
it is very simple and complete.

Marco Nardi

21 OCT 2015 REPLY

You Rock! Thank you for posting this, it was very helpful.

Pingback: itemprop="name">Client authentication using the pfx not working * Best Wordpress Themes - Reviews (http://wordpressthemes.review/client-authentication-using-the-pfx-not-working/)

Paul Kirk

13 NOV 2015 REPLY

Clear, concise and demystifies this process. Thank you!

Max

13 NOV 2015 REPLY

My company wants to use client certificates for clients on production. We have https certificate. As I understand we need CA root to create client certificate. Question: is it ok if I just create this CA root using makecert and install on web server only and will use it to create client certificates?

Pingback: itemprop="name">Connect Azure Virtual Machines on Company Network | ArunYadav_Blog (https://arunyadavblog.wordpress.com/2015/11/18/connect-azure-virtual-machines-on-company-network/)

Boris

27 NOV 2015 REPLY

Very good article, nicely explained. Helped me very quickly.
Thank you for writing it.

Pingback: itemprop="name">Creating Root and Client Certificate for Point-to-Site Azure VPN - Learning SharePoint (http://www.learningsharepoint.com/2016/01/03/creating-root-and-

client-certificate-for-point-to-site-azure-vpn/)

Joel 6 JAN 2016 REPLY

I've come back to this excellent post a couple of times now. (Because who can remember this stuff??)
Really well done, thanks.
Joel

Ahmed 11 JAN 2016 REPLY

Can I generate certificates on personal laptop and install the CA and Server certificate the web server and client certificate on user machines?

Ricardo Casquete 22 JAN 2016 REPLY

simply brilliant!!!
Thanks heaps

---

david 11 FEB 2016 REPLY

Thanks for your efforts, Elizabeth, this is very helpful.

Phuong Phan (http://www.logixsquare.com) 26 FEB 2016 REPLY

Hi Elizabeth, thank you so much. You really saved my life. By the way, I still do not understand why we need three certs, why we cannot use only one certificate for both server and client. I would very much appreciate it if you could give me your time to answer.

Edwig Huisman

21 MAR 2016 REPLY

Chapeau! The very first manual on creating development certificates and client ssl certificates I ever found AND could understand and use!! Very well done! Thank you!!

Pingback: itemprop="name">Custom domains, SSL and Azure | Coding Kram – Ideasyncline (http://codingkram.com/2016/03/28/custom-domains-ssl-and-azure/)

Philip Presser

30 MAR 2016 REPLY

Hi Elizabeth, can you create a wildcard certificate using the method you described above?

Cam

16 APR 2016 REPLY

Thank a lot, great help you are great.
But i should say, this is absolute madness!! There is a real need for a new, clean slate OS with no-nonsense paradigms…

Pingback: itemprop="name">Create and Sign Certificate in C# « TechAnswer (https://techanswer.xyz/2016/05/04/create-and-sign-certificate-in-c/)

Pingback: itemprop="name">How To Create Pvk File From Cer | How Give Money (http://howgivemoney.xyz/2016/06/06/how-to-create-pvk-file-from-cer/)

Amul Patel

29 JUN 2016 REPLY

Hii guyz,

i created certificate for self-sign,CA,code signing.

so when i am signing binary with this certificate and just checking certificate it's displayed "A certificate's basic constraint extension has not been observed. ".

Pls help me.

Silvio 22 JUL 2016 REPLY

Dear Elizabeth,

absolutely great! With your precise steps and detailed explanations I was able to setup SSL

certificates and code signing certificates as well. Very, very – very well done!

Sincerely Silvio

Pingback: itemprop="name">IIS Certificate import ► cannot be used as an SSL Certificate error | Tech (http://www.tech.ubuntutextbook.com/2016/09/05/iis_certificate_import__cannot_be_used_as_an_ssl_certificate_error/)

Prakash Sajwan 21 SEP 2016 REPLY

best article on this topic .Thanks :)

Andrew 17 NOV 2016 REPLY

Thank you!

You saved me from bureaucrats war in my company.

regards

AL

David 28 NOV 2016 REPLY

Would have been perfect except for “Open a Visual Studio Developer Command Prompt”.
You’re assuming we have Visual Studio.
I simply saved the cmd file and double clicked it in WindowsExplorer.
You might mentioned this in the instructions as an alternative.

Ben 26 JAN 2017 REPLY

Fantastic work. Thank you!

Tim Schmelter 14 FEB 2017 REPLY

Whoever got the “File not found” error. I guess you also changed the names but forgot to change the name of the file which is (in this example): CARoot.cer to f.e.: NewName.cer
It must match: -spc NewName.cer

Pavel Smirnov 23 FEB 2017 REPLY

Highly usable and clear! Thank you so much!

Pingback: itemprop="name">Creating self signed certificates with makecert.exe for development – Geek (G) of (T) Technology (https://gt8blog.wordpress.com/2017/03/31/creating-self-signed-

certificates-with-makecert-exe-for-development/)

Zeki 9 APR 2017 REPLY

Thank you very much!! A very good expression.

Jessica 10 MAY 2017 REPLY

Thank you so much! This helped me a lot.
I couldn't find another source where explains the complete information
Step by step...super clear!

Dwargh 24 MAY 2017 REPLY

Time o make new guide for Chrome 58+ with SAN

NiZelooer 25 JUL 2017 REPLY

Makecert doesn't have that option.
see: https://msdn.microsoft.com/en-us/library/bfsktky3(v=vs.80)
(https://msdn.microsoft.com/en-us/library/bfsktky3(v=vs.80)).aspx

Daniel 8 SEP 2017 REPLY

Thank you. Thank you. Thank you
remember folks to modify that expiry date!

Mentore 27 SEP 2017 REPLY

Clear as pure water. Thanks a lot, I was going through the struggle of creating certificates and I really couldn't find something really useful. Thanks, this is really good work!

Ranz 2 OCT 2017 REPLY

A very well done article to read, very comprehensive but I got a problem with my Server and Client certificates that these are not valid or expire.

Mohamed Emad (http://www.egyptitjobs.com) 26 OCT 2017 REPLY

Thank you. This was very helpful. I like the way you explain things.

Morton Lennox (http://bestcliponlensforsmartphone.xyz)

3 NOV 2017 REPLY

Came across your site, and I must say, it's interesting. Posts like this are what makes this blog awesome, Elizabeth. I really find this information very handy. Excited to see more similar contents from you in the future. More power!

Mike 1 JAN 2018 REPLY

Nice article !
I came across this free GUI tool to make signed and self-signed certificates. You can make any certificate with a few clicks...
Itiverba Self Signed Certificate Generator :
http://www.itiverba.com/en/software/itisscg.php
(http://www.itiverba.com/en/software/itisscg.php)

Emeka Vin

4 JAN 2018 REPLY

Thanks Elizabeth for this article!!

Pierre

7 JAN 2018 REPLY

Hi,

Here is a free alternative to the deprecated makecert :

http://www.itiverba.com/en/software/itisscg.php

(http://www.itiverba.com/en/software/itisscg.php).

It 's a GUI free tool for Windows and you can create self-signed certificate, CA certificate, view ASN format, eport to files, ...

Axel

28 MAR 2018 REPLY

Thank you for the tool ☺

The tool is very nice and usually easy to use, also to CA and Client (Software signing) or similar.

I created a CA and a Client certificate for software signing and it seems to work and Visual Studio 2017 like the certificate too 😀

PVK Lenght: 16384, SHA 512

What was your settings for CA and Client/Software or what are the best settings for CA and Software?

Nate

28 MAR 2018 REPLY

What is the purpose of the step where you are running pvk2pfx, while creating the root cert? I couldn't see where the resulting CAroot.pfx was ever used for anything.

Matt Duguid 27 APR 2018 REPLY

Great article, helped me quickly create some certificates for testing :)

Gabriel 20 MAY 2018 REPLY

Thank you. Any chances to generate EV SSL ones?

Helena Makarchuk 24 MAY 2018 REPLY

Thank you!

Chris Salem 25 JUN 2018 REPLY

Your're awesome. This article helped me so much. Thank you!

Brian Moseley 4 AUG 2018 REPLY

Thank you for taking the time to create a super detailed explanation. You are the greatest.

Trinto TA (http://NA) 14 AUG 2018 REPLY

Your're awesome. This article helped me so much. Thank you!

CJL

21 AUG 2018 REPLY

OMG. You are the greatest. Thank You!

jagadish

28 AUG 2018 REPLY

I was getting the following error:
pvk2pfx.exe -pvk CARoot.pvk -spc CARoot.cer -pfx CARoot.pfx -po Test123
'pvk2pfx.exe' is not recognized as an internal or external command, operable program or batch file.

Assoc.Prof. Michael Claudius (http://micl-easj.dk)

24 APR 2019 REPLY

The command is not recognized because either you are missing Windows SDK and set the properties of your folder correct.
http://micl-easj.dk/Cods/Administration/Weekly%20Plans.htm (http://micl-easj.dk/Cods/Administration/Weekly%20Plans.htm)
see week 17 CertificateX509 exercise

Arif Hossain

6 SEP 2018 REPLY

Great way to simply describe a complex issue pictorially. It was very helpful! Thank you.

Eric Lawrence (https://textslashplain.com/)

12 SEP 2018 REPLY

This is a great post, thanks for sharing it.
Anyone following these instructions should probably update the Expiration dates, and keep in mind that Chrome no longer accepts certificates without a SubjectAltName. Sadly, MakeCert cannot set that field. See https://github.com/FiloSottile/mkcert (https://github.com/FiloSottile/mkcert) for an alternative that works across platforms.

Milos Peric 24 DEC 2018 REPLY

Hey,
Thank you for this :) quick and easy explanation of makecert

Pingback: itemprop="name">Creating self-sign certificate – A developer's blog (https://danv74.wordpress.com/2019/04/17/creating-self-sign-certificate/)

Michael Claudius (http://micl-easj.dk) 24 APR 2019 REPLY

I like this explanation, good overview and enough details.
I have used this link as a reference in my teaching in IT-Security for the last three years.
Based on this I made 3 assignments to my students: CertificateX509 No.1 and No.2 plus a special SSL
assignment.
Assoc. Prof. Michael Claudius

Johannes 22 MAY 2019 REPLY

This was an amazing walkthrough, thanks it made my day.

Li Lin

6 FEB 2020 REPLY

Thank you for knowledge sharing, really helpful and time saver for any web development which requires HTTPS.

Vikas Chaturvedi

18 APR 2020 REPLY

Nice Blog for Create self signed certificate. Great Explanation.

Leave a Reply

Your Comment Here...

Name (required)

Email (required)

Website

Save my name, email, and website in this browser for the next time I comment.

POST COMMENT