**17 Comments**

[**Grigoryan, Armenak**](https://confluence.it.ubc.ca/display/~armenak)

Thanks, Luca. Much needed. This instruction is the example how documentation should be done!

* + [Poyser, John](https://confluence.it.ubc.ca/display/~jpoyser) likes this
  + [Sep 17, 2015](https://confluence.it.ubc.ca/display/ITSecurity/how+to+obtain%2C+deploy+and+verify+an+X.509+certificate?focusedCommentId=75236541#comment-75236541)

[**Filipozzi, Luca**](https://confluence.it.ubc.ca/display/~lucaf)

For DNS-based domain control validation (updated per John's comment on 28 Jul 2017), use the following steps.

**Step 1: Generate the "MD5 hash":**

|  |
| --- |
| openssl req -in www.obfuscate.xzy.csr -outform der | openssl dgst -md5 |

**Step 2: Generate the "split SHA256 hash" (64-character string split into two 32-character string separated by a dot):**

|  |
| --- |
| openssl req -in www.obfuscate.xzy.csr -outform der | openssl dgst -sha256  -r | awk '{printf "%s.%s\n",substr($1,1,32),substr($1,33,32)}' |

**Step 3: Create CNAME record:**

|  |
| --- |
| \_«MD5 hash».www.obfuscate.xyz. IN CNAME «split SHA256 hash».comodoca.com. |

 Note the underscore in front of the the «MD5 hash».

* + [Jul 28, 2017](https://confluence.it.ubc.ca/display/ITSecurity/how+to+obtain%2C+deploy+and+verify+an+X.509+certificate?focusedCommentId=112888065#comment-112888065)

[**Bratlien, John**](https://confluence.it.ubc.ca/display/~johnbrat)

Comodo has updated the DNS-based DCV scheme to use SHA-256 and a slightly different format:

|  |
| --- |
| \_<MD5 hash>.www.obfuscate.xyz. CNAME <SHA-256 hash>.comodoca.com |

Note that a "hex (base-16) encoded SHA-256 hash will not fit in a single DNS label because it is too long. The SHA-256 hash should therefore be split into two labels, each 32 characters long."   
  
For more detail see 'DNS CNAME-based'  
<https://support.comodo.com/index.php?/comodo/Knowledgebase/Article/View/791/0/>

* + - [Jul 31, 2017](https://confluence.it.ubc.ca/display/ITSecurity/how+to+obtain%2C+deploy+and+verify+an+X.509+certificate?focusedCommentId=131503731#comment-131503731)

[**Filipozzi, Luca**](https://confluence.it.ubc.ca/display/~lucaf)

Thanks. I've updated the instructions.

* + - * [Jul 28, 2017](https://confluence.it.ubc.ca/display/ITSecurity/how+to+obtain%2C+deploy+and+verify+an+X.509+certificate?focusedCommentId=131503825#comment-131503825)

[**Filipozzi, Luca**](https://confluence.it.ubc.ca/display/~lucaf)

I have added example openssl configuration files for multi-domain and wildcard certificates.

* + [Mar 26, 2018](https://confluence.it.ubc.ca/display/ITSecurity/how+to+obtain%2C+deploy+and+verify+an+X.509+certificate?focusedCommentId=149063646#comment-149063646)

[**Filipozzi, Luca**](https://confluence.it.ubc.ca/display/~lucaf)

Some users complain that their operating system, browser or Java application (Tomcat, JBoss, Oracle Wallet or other) does not trust the end-entity certificate issued by Gandi.

This is neither a Gandi nor a Comodo issue (Gandi resells Comodo certificates). This is a trust store issue.

Typically, the trust store is provided by the operating system vendor or by the browser vendor. Each vendor (Apple for macOS/iOS/Safari, Microsoft for Windows/IE, Google for Android/Chrome, Oracle for Java) has their own policies / procedures for adding/removing the CA certificates from their respective trust stores. Most GNU/Linux distributions incorporate Mozilla's trust store as the operating system trust store.

Comodo’s responsibility is to work with vendors to ensure that the Comodo root certificates are included in each vendor’s master trust store.

The vendors' responsibility is to manage their master trust store so that it **does** **include** the root certificates from trusted CAs and **does not include** the root certificates from untrusted CAs. CAs become untrusted when their operations are determined to be in contravention of the CA/B Forum’s Baseline Requirements: recent examples include Symantec and StartCom/WoSign. Since each vendor has different policies/procedures, there are differences between the vendors’ trust stores.

**The users' responsibility is to keep her local copy of the trust stores up-to-date. It does no good for Comodo to work with vendors, nor for the vendors to actively manage their master trust store if users never refresh their local trust stores from the vendor master trust store.**

Typically, users accomplish this local trust store update by patching their operating systems or updating their browsers to the latest version.

Where this breaks, frequently, is when an application embeds a trust store, such as with Java Runtime Environments. System administrators may remember to update the operating system's trust store but often forget/neglect to update the JRE's trust store.

**Rule of Thumb: keep your systems up to date, kids.**

* + [Poyser, John](https://confluence.it.ubc.ca/display/~jpoyser) likes this
  + [Mar 27, 2018](https://confluence.it.ubc.ca/display/ITSecurity/how+to+obtain%2C+deploy+and+verify+an+X.509+certificate?focusedCommentId=149064287#comment-149064287)

[**Poyser, John**](https://confluence.it.ubc.ca/display/~jpoyser)

UBC IT needs an annual award for Best KB submission.  This gets my vote.

* + [Jun 28, 2018](https://confluence.it.ubc.ca/display/ITSecurity/how+to+obtain%2C+deploy+and+verify+an+X.509+certificate?focusedCommentId=156537076#comment-156537076)

[**Heck, Aaron**](https://confluence.it.ubc.ca/display/~aheck)

We've had a question come up with regards to the SHA1 certification path going EOL in 2020.  I’ve added a small “alert” section in the pathing area to let people know the timeline of the deprecation of the SHA1 path, and the impact for users.

* + [Nov 28, 2018](https://confluence.it.ubc.ca/display/ITSecurity/how+to+obtain%2C+deploy+and+verify+an+X.509+certificate?focusedCommentId=164139258#comment-164139258)

[**Heck, Aaron**](https://confluence.it.ubc.ca/display/~aheck)

In Step 5, when performing the wget, the response from Gandi will be a redirect to a different location.

Gandi is using a 302 (Temporary) redirect, instead of a 301 (Permanent) redirect to point to the new location.  Assuming that Gandi knows their stuff, and is following the [standards defined in the RFC](https://tools.ietf.org/html/rfc7231#page-56):

* + If the redirect is a 301, then “…any future references to this resource ought to use one of the enclosed URIs”.  In other words, update your links and documentation.
  + If the redirect is a 302, then “…the client ought to continue to use the effective request URI for future requests”.  In other words, no documentation change.

The documentation is intentionally not being updated to reflect this new URL.

* + [Jun 13, 2019](https://confluence.it.ubc.ca/display/ITSecurity/how+to+obtain%2C+deploy+and+verify+an+X.509+certificate?focusedCommentId=178601702#comment-178601702)

[**Heck, Aaron**](https://confluence.it.ubc.ca/display/~aheck)

[Bratlien, John](https://confluence.it.ubc.ca/display/~johnbrat) Pointed out that the intermediate cert he fetched from Gandi today no longer contains the SHA1 intermediate cert.  Will update the page accordingly.

* + [Oct 09, 2019](https://confluence.it.ubc.ca/display/ITSecurity/how+to+obtain%2C+deploy+and+verify+an+X.509+certificate?focusedCommentId=187516715#comment-187516715)

[**Sherrington, Ryan**](https://confluence.it.ubc.ca/display/~sherri3)

The Tomcat docs for version 7 [say that PKCS12 is supported](https://tomcat.apache.org/tomcat-7.0-doc/ssl-howto.html#Prepare_the_Certificate_Keystore). As well, the JDK 8 version of keytool throws a warning when I try and use jks:

|  |
| --- |
| Warning:  The JKS keystore uses a proprietary format. It is recommended to migrate to PKCS12 which is an industry standard format using "keytool ...-deststoretype pkcs12". |

Should I use pkcs12 instead of jks as the confluence instructions say?

* + [Jul 17, 2020](https://confluence.it.ubc.ca/display/ITSecurity/how+to+obtain%2C+deploy+and+verify+an+X.509+certificate?focusedCommentId=210144798#comment-210144798)

[**Heck, Aaron**](https://confluence.it.ubc.ca/display/~aheck)

I don't see any security considerations to be concerned about in a move from jks to pkcs12.  I would agree moving to pkcs12 is a better option.  JKS can be a real pain and I would recommend getting away from it wherever possible.

* + - [Jul 17, 2020](https://confluence.it.ubc.ca/display/ITSecurity/how+to+obtain%2C+deploy+and+verify+an+X.509+certificate?focusedCommentId=210144991#comment-210144991)

[**Rolland, Stuart**](https://confluence.it.ubc.ca/display/~srolland)

Can I do this in windows or is it Linux only?

I found this on the gandi website so I guess that answers my question

[**What You Need**](https://docs.gandi.net/en/ssl/common_operations/csr.html#contents)[**¶**](https://docs.gandi.net/en/ssl/common_operations/csr.html#what-you-need)

To generate the CSR you will need access to a unix terminal on a machine with OpenSSL, or an equivalent, installed. You do not need to use the machine where you will install the certificate to generate the CSR.

Some options may be:

* + Your regular computer, if you use Linux or OSx
  + A Gandi cloud server
  + A Gandi simple hosting instance (even if you intend to use the certificate outside of Gandi)
  + An accessible production server running on Linux or Unix
  + A Windows computer with OpenSSL for Windows installed

I suggest making this document more open so we can crowdsource the improvement on it - like wikipedia

* + [Jul 20, 2020](https://confluence.it.ubc.ca/display/ITSecurity/how+to+obtain%2C+deploy+and+verify+an+X.509+certificate?focusedCommentId=211714976#comment-211714976)

[**Heck, Aaron**](https://confluence.it.ubc.ca/display/~aheck)

Thanks, Stuart.  Added a requirements section to address this question.

* + - [Jul 20, 2020](https://confluence.it.ubc.ca/display/ITSecurity/how+to+obtain%2C+deploy+and+verify+an+X.509+certificate?focusedCommentId=211715041#comment-211715041)

[**Sherrington, Ryan**](https://confluence.it.ubc.ca/display/~sherri3)

[Rolland, Stuart](https://confluence.it.ubc.ca/display/~srolland) I did this in [MAS-3315](https://jira.it.ubc.ca/browse/MAS-3315?focusedCommentId=7156797&page=com.atlassian.jira.plugin.system.issuetabpanels%3Acomment-tabpanel#comment-7156797) which is Windows Server 2012 R2, but you can do it on any windows machine that allows local application installation. See [openssl.org binaries page](https://wiki.openssl.org/index.php/Binaries).

* + - [Jul 21, 2020](https://confluence.it.ubc.ca/display/ITSecurity/how+to+obtain%2C+deploy+and+verify+an+X.509+certificate?focusedCommentId=211715564#comment-211715564)

[**Rolland, Stuart**](https://confluence.it.ubc.ca/display/~srolland)

Might also be worth including a link to this <https://docs.gandi.net/en/ssl/common_operations/csr.html>

* + [Jul 20, 2020](https://confluence.it.ubc.ca/display/ITSecurity/how+to+obtain%2C+deploy+and+verify+an+X.509+certificate?focusedCommentId=211715007#comment-211715007)

[**Heck, Aaron**](https://confluence.it.ubc.ca/display/~aheck)

Thanks, Stuart.  The document is carefully crafted to support the UBC centralized certificate service, so changes are currently curated and don't include links to vendor-specific guides that might not align with our practices or expectations.  To be fair, at the end of the day sysadmins are free to generate their CSRs any way they see fit and we will process them.  We provide the guide in an attempt to help with consistency and alignment with standards.

* + - [Jul 20, 2020](https://confluence.it.ubc.ca/display/ITSecurity/how+to+obtain%2C+deploy+and+verify+an+X.509+certificate?focusedCommentId=211715015#comment-211715015)
* ols and cipher suites.

.