**Сертификат для подписи кода**

Если вы используете следующие версии Windows или более поздние: Windows Server 2012, Windows Server 2012 R2 или Windows 8.1, то MakeCert теперь устарел, и Корпорация Майкрософт рекомендует использовать [команду PowerShell New-SelfSignedCertificate](https://docs.microsoft.com/en-us/powershell/module/pkiclient/new-selfsignedcertificate)

Если вы используете более старую версию, такую как Windows 7, вам нужно будет придерживаться MakeCert или другого решения. Некоторые люди предлагают использовать модуль инфраструктуры открытых ключей Powershell (PSPKI).

Хотя вы можете создать самозаверяющий сертификат подписи кода (SPC- Software Publisher Certificate) за один раз, я предпочитаю делать следующее:

**Создание самозаверяющего центра сертификации (CA)**

makecert -r -pe -n "CN=My CA" -ss CA -sr CurrentUser ^

-a sha256 -cy authority -sky signature -sv MyCA.pvk MyCA.cer

(^ = разрешить пакетной командной строке обернуть строку)

Это создает самозаверяющий сертификат (-r) с экспортируемым закрытым ключом (-pe). Он называется "Мой CA" и должен быть помещен в хранилище CA для текущего пользователя. Мы используем алгоритм SHA-256. Ключ предназначен для подписи (- sky).

Закрытый ключ должен храниться в файле MyCA.pvk, а сертификат-в файле MyCA.cer.

**Импорт сертификата CA**

Поскольку нет смысла иметь сертификат CA, если вы ему не доверяете, вам нужно будет импортировать его в хранилище сертификатов Windows. Вы *можете* использовать оснастку Certificates MMC, но из командной строки:

certutil -user -addstore Root MyCA.cer

**Создание сертификата подписи кода (SPC)**

makecert -pe -n "CN=My SPC" -a sha256 -cy end ^

-sky signature ^

-ic MyCA.cer -iv MyCA.pvk ^

-sv MySPC.pvk MySPC.cer

Это почти то же самое, что и выше, но мы предоставляем ключ эмитента и сертификат (коммутаторы -ic и -iv).

Мы также хотим преобразовать сертификат и ключ в файл PFX:

pvk2pfx -pvk MySPC.pvk -spc MySPC.cer -pfx MySPC.pfx

Если вы хотите защитить файл PFX, добавьте переключатель -po, иначе PVK2PFX создаст файл PFX без парольной фразы.

**Использование сертификата для подписи кода**

signtool sign /v /f MySPC.pfx ^

/t http://timestamp.url MyExecutable.exe

Если вы хотите импортировать файл PFX в хранилище сертификатов, воспользуйтесь командой:

certutil -user -addstore spc MySPC.cer

Вы также можете использовать PVKIMPRT или MMC snapin. Чтобы подписать код, используйте команду:

signtool sign /v /n "Me" /s SPC ^

/t http://timestamp.url MyExecutable.exe

Некоторые возможные timestamp URLs для signtool /t:

* http://timestamp.verisign.com/scripts/timstamp.dll
* http://timestamp.globalsign.com/scripts/timstamp.dll
* http://timestamp.comodoca.com/authenticode