

نام قوی (Strong Name یا به صورت مخفف SN) تکنولوژی‌ای است که با ورود دانت نت معرفی شده و امکانات متنوعی را در زمینه حفاظت از هویت اسمبلی فراهم کرده است. اما بسیاری از برنامه‌نویسان به اشتباه آن را به عنوان ابزاری برای فعال‌سازی امنیت می‌پندارند، در صورتی که «نام قوی» در واقع یک تکنولوژی تعیین «هویت منحصر به فرد» اسمبلی‌ها است. یک نام قوی حاوی مجموعه‌ای از مشخصات یک اسمبلی (شامل نام ساده، نسخه و داده‌های کالچر (culture) آن در صورت وجود) به همراه یک کلید عمومی و یک امضای دیجیتال است. در زیر یک نمونه از یک اسمبلی دارای نام قوی را مشاهده می‌کنید:

```
System.Web.Mvc, Version=3.0.0.0, Culture=neutral, PublicKeyToken=31BF3856AD364E35
```

این نام با استفاده از داده‌های موجود در فایل اصلی یک اسمبلی و نیز یک کلید خصوصی تولید می‌شود. (فایل اصلی اسمبلی فایلی است که حاوی مانیفست اسمبلی است که این مانیفست خود شامل عنوان و هش‌کدهای تمام فایل‌هایی است که اسمبلی را می‌سازند. دات نت از MultiFile Assembly پشتیبانی می‌کند. برای مدیریت این نوع از اسمبلی‌ها می‌توان از (Assembly Linker) استفاده کرد. البته در حال حاضر امکان توسعه این نوع از اسمبلی‌ها در ویژوال استودیو موجود نیست.) در sdkهای میکروسافت ابزارهایی برای تولید نام‌های قوی برای اسمبلی‌ها وجود دارد که در ادامه در مورد نحوه استفاده از یک مورد از آن‌ها توضیح داده خواهد شد.

اسمبلی‌هایی که نام‌های قوی یکسانی دارند همانند و یکسان هستند. با اختصاص دادن یک نام قوی به یک اسمبلی می‌توان اطمینان حاصل کرد که نام آن منحصر به فرد خواهد شد. به طور کلی نام‌های قوی نیازمندی‌های زیر را برطرف می‌کنند:

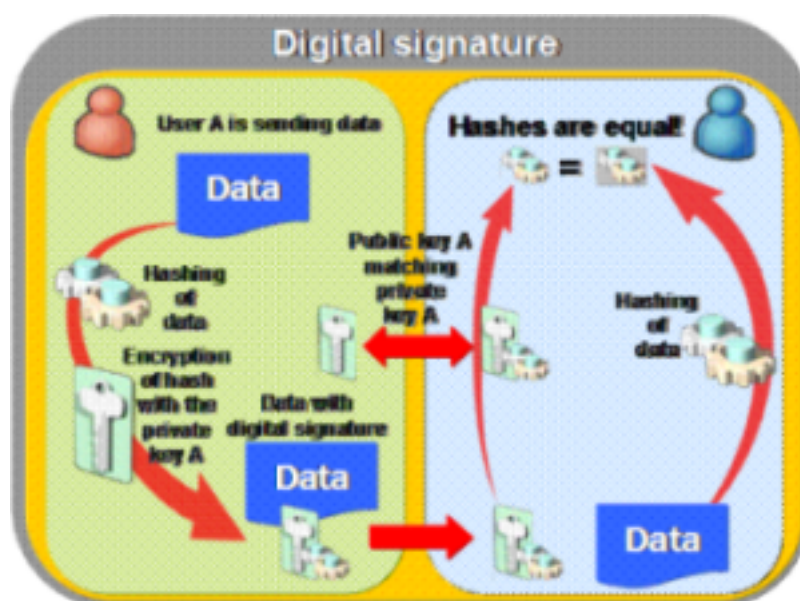
- نام‌های قوی منحصر به فرد بودن نام یک اسمبلی را براساس جفت‌کلیدهای یکتا فراهم می‌کنند. هیچ‌کس دیگری امکان تولید همان اسمبلی‌ای را که شما تولید کرده‌اید ندارد، زیرا اسمبلی‌ای که با یک کلید خصوصی تولید شده است نسبت به اسمبلی دیگری که با یک کلید خصوصی دیگر تولید شده است نام متفاوتی خواهد داشت چون کلید عمومی متناظر با این کلید خصوصی بخشی از نام قوی نهایی تولید شده خواهد بود.

- نام‌های قوی از خط تولید نسخه‌های یک اسمبلی محافظت می‌کنند. یک نام قوی اطمینان می‌دهد تا شخص دیگری نتواند نسخه دیگری از اسمبلی شما را تولید کند. مصرف‌کنندگان می‌توانند مطمئن باشند که نسخه‌ای از اسمبلی را که بارگذاری می‌کنند از همان توزیع‌کننده اسمبلی می‌آید که این نسخه از اسمبلی را تولید کرده است.

- نام‌های قوی بررسی هویت مستحکمی را فراهم می‌کنند. عبور از دروازه امنیتی دات نت فریمورک نشان‌دهنده این است که محتوای اسمبلی پس از تولید آن تغییر نکرده است.

هنگامی که به یک اسمبلی دارای نام قوی در اسمبلی دیگری ریفرنس داده می‌شود، تا زمانی که به اسمبلی مقصد نیز یک نام قوی داده نشود نمی‌توان در نهایت از مزایای یک نام قوی بهره برد. در واقع در دنیای دات نت به اسمبلی‌های دارای نام قوی تنها می‌توان اسمبلی‌هایی ریفرنس داد که خود نیز دارای نام قوی هستند.

نام قوی یک تکنولوژی براساس اصول کریپتوگرافی و امضاهای دیجیتال است که ایده پایه‌ای آن را می‌توان در تصویر زیر دید:



برای استفاده از این تکنولوژی ابتدا نیاز است تا یک جفت کلید عمومی/خصوصی (توسط ادمین، منبع گواهی‌نامه‌ها، یک بانک یا یک ابزار خاص) فراهم شود تا از آن برای اینکریپشن استفاده شود. سپس داده‌های موردنظر (هر داده کلی که قصد ارسال و توزیع آن را داریم مثل یک اسمبلی) با استفاده از یک الگوریتم هش کردن (مثل MD5، SHA یا ترکیبی از آن‌ها، هرچند MD5 توصیه نمی‌شود) پردازش شده و یک هش‌کد مخصوص تولید می‌شود. این هش‌کد با استفاده از کلید خصوصی در دسترس اینکریپت می‌شود و به عنوان یک امضای دیجیتال به همراه داده موردنظر ارسال یا توزیع می‌شود. در سمت مصرف کننده که با استفاده از یک روش خاص و امن به کلید عمومی دسترسی پیدا کرده است عملیات دیکریپت کردن این امضای دیجیتال با استفاده از کلید عمومی انجام شده و هش‌کد مربوطه بدست می‌آید. همچنین عملیات تولید هش‌کد با استفاده از داده‌ها در سمت مصرف کننده انجام شده و هش‌کد داده‌ها نیز دوباره با استفاده از همان الگوریتم استفاده شده در سمت توزیع کننده تولید می‌شود. سپس این دو مقدار محاسبه شده در سمت مصرف کننده با یکدیگر مقایسه شده و در صورت برابر بودن می‌توان اطمینان حاصل کرد همان داده‌ای که توزیع کننده در اصل ارسال کرده بدون تغییر به دست مصرف کننده رسیده است. درواقع ویژگی اینکریپت/دیکریپت کردن داده‌ها توسط جفت کلید این است که به صورت یکطرفه بوده و داده‌های اینکریپت شده با استفاده از یک کلید خصوصی را تنها با استفاده از کلید عمومی همان کلید خصوصی می‌توان بدرستی دیکریپت کرد.

1. تولید و مدیریت جفت کلیدهای قوی- نام‌گذاری شده (Strongly Named Key Pairs)

همان‌طور که در قسمت قبل اشاره شد برای نام‌گذاری قوی یک اسمبلی به یک کلید عمومی (public key) و یک کلید خصوصی (private key) که در مجموع به آن یک جفت کلید (key pair) می‌گویند، نیاز است. برای این کار می‌توان با استفاده از برنامه sn.exe (عنوان کامل آن Microsoft .Net Framework Strong Name Utility است) یک جفت کلید تولید کرده و آن را در یک فایل و یا در CSP (یا همان cryptographic service provider) ذخیره کرد. همچنین این کار را می‌توان توسط ویژوال استودیو نیز انجام داد. امکان موردنظر در فرم پراپرتی یک پروژه و در تب Signing آن وجود دارد.

نکته : یک CSP عنصری از API کریپتوگرافی ویندوز (Win32 CryptoAPI) است که سرویس‌هایی چون اینکریپشن، دیکریپشن، و تولید امضای دیجیتال را فراهم می‌کند. این پرووایدرها همچنین تسهیلاتی برای مخازن کلیدها فراهم می‌کنند که از اینکریپشن‌های قوی و ساختار امنیتی سیستم عامل (سیستم امنیتی و دسترسی کاربران ویندوز) برای محافظت از تمام کلیدهای کریپتوگرافی ذخیره شده در مخزن استفاده می‌کند. به‌طور خلاصه و مفید می‌شود اشاره کرد که می‌توان کلیدهای کریپتوگرافی را درون یک مخزن کلید CSP ذخیره کرد و تقریباً مطمئن بود که تا زمانی که هیچ‌کس کلمه عبور سیستم عامل را نداند، این کلیدها امن خواهند ماند. برای کسب اطلاعات بیشتر به داده‌های CryptoAPI در اسناد SDK سیستم عامل خود مراجعه کنید.

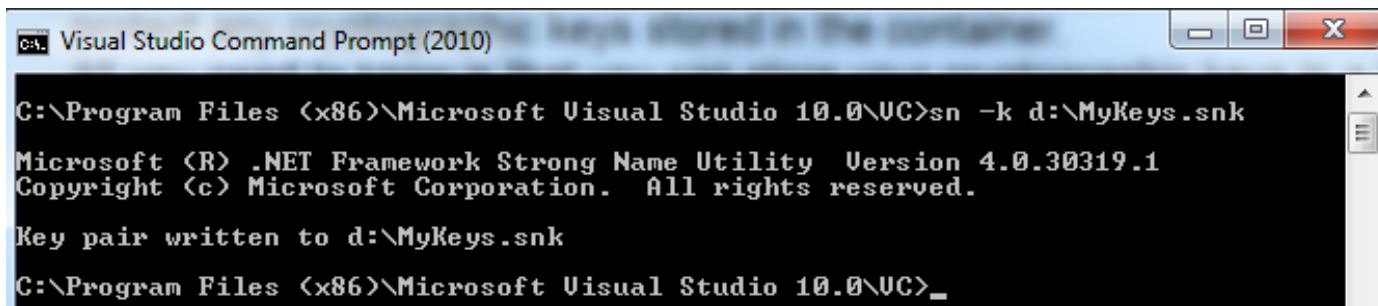
برنامه sn به همراه SDKهای ویندوز نصب می‌شود. البته با نصب ویژوال استودیو تمام SDKهای موردنیاز مطابق با نسخه‌های

موجود، نصب خواهد شد. مسیر نسخه 4 و 32 بیتی این برنامه در سیستم عامل Windows 7 به صورت زیر است:

```
C:\Program Files\Microsoft SDKs\Windows\v7.0A\Bin\NETFX 4.0 Tools\sn.exe
```

با استفاده از آرگومان k همانند دستور زیر یک جفت کلید جدید تولید شده و در فایل MyKeys.snk در ریشه درایو d: ذخیره می شود:

```
sn -k d:\MyKeys.snk
```



```
Visual Studio Command Prompt (2010)
C:\Program Files (x86)\Microsoft Visual Studio 10.0\UC>sn -k d:\MyKeys.snk
Microsoft (R) .NET Framework Strong Name Utility Version 4.0.30319.1
Copyright (c) Microsoft Corporation. All rights reserved.
Key pair written to d:\MyKeys.snk
C:\Program Files (x86)\Microsoft Visual Studio 10.0\UC>
```

نکته : به بزرگی و کوچکی حروف سوییچ های دستورات برنامه sn دقت کنید!

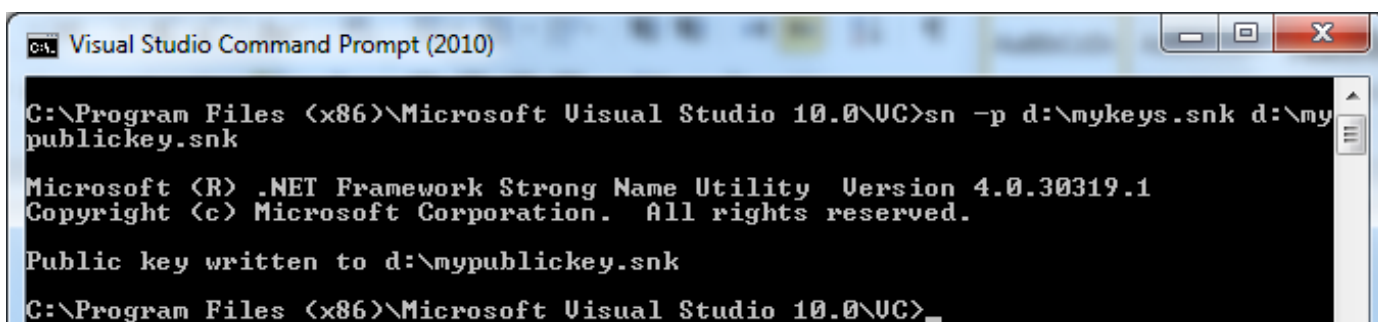
این کار یک جفت کلید کریپتوگرافی 1024 بیتی به صورت تصادفی تولید می کند. این دستور را باید در خط فرمانی (Command Prompt) اجرا نمود که مسیر فایل sn.exe را بداند. برای راحتی کار می توان از خط فرمان ویژوال استودیو (Visual Studio Command Prompt) استفاده کرد.

نکته : اجرای عملیات فوق در یک شرکت یا قسمت توسعه یک شرکت، تنها یک بار نیاز است زیرا تمام اسمبلی های تولیدی تا زمانی که عناوین ساده متمایزی دارند می توانند از یک جفت کلید مشترک استفاده کنند.

نکته : هر چند که می توان از پسوند های دیگری نیز برای نام فایل حاوی جفت کلید استفاده کرد، اما توصیه می شود از همین پسوند snk استفاده شود.

فایل تولید شده حاوی هر دو کلید «عمومی» و «خصوصی» است. می توان با استفاده از دستور زیر کلید عمومی موجود در فایل mykeys.snk را استخراج کرده و در فایل mypublickey.snk ذخیره کرد:

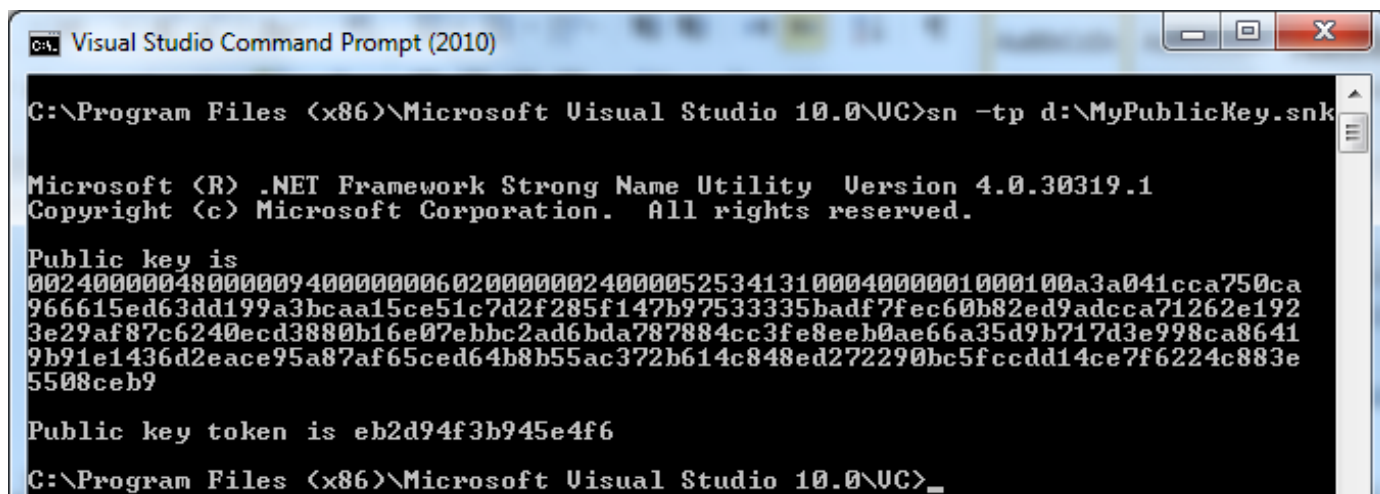
```
sn -p d:\mykeys.snk d:\mypublickey.snk
```



```
Visual Studio Command Prompt (2010)
C:\Program Files (x86)\Microsoft Visual Studio 10.0\UC>sn -p d:\mykeys.snk d:\mypublickey.snk
Microsoft (R) .NET Framework Strong Name Utility Version 4.0.30319.1
Copyright (c) Microsoft Corporation. All rights reserved.
Public key written to d:\mypublickey.snk
C:\Program Files (x86)\Microsoft Visual Studio 10.0\UC>
```

با استفاده از فایل حاوی کلید عمومی می‌توان با استفاده از دستور زیر کلید عمومی موجود در آن را بدست آورد:

```
sn -tp MyPublicKey.snk
```



```

C:\Program Files (x86)\Microsoft Visual Studio 10.0\VC>sn -tp d:\MyPublicKey.snk

Microsoft (R) .NET Framework Strong Name Utility Version 4.0.30319.1
Copyright (c) Microsoft Corporation. All rights reserved.

Public key is
00240000048000009400000006020000002400000525341310004000001000100a3a041cca750ca
966615ed63dd199a3bcaa15ce51c7d2f285f147b9753335badf7fec60b82ed9adcca71262e192
3e29af87c6240ecd3880b16e07ebbc2ad6bda787884cc3fe8eeb0ae66a35d9b717d3e998ca8641
9b91e1436d2eace95a87af65ced64b8b55ac372b614c848ed272290bc5fccdd14ce7f6224c883e
5508ceb9

Public key token is eb2d94f3b945e4f6
C:\Program Files (x86)\Microsoft Visual Studio 10.0\VC>_

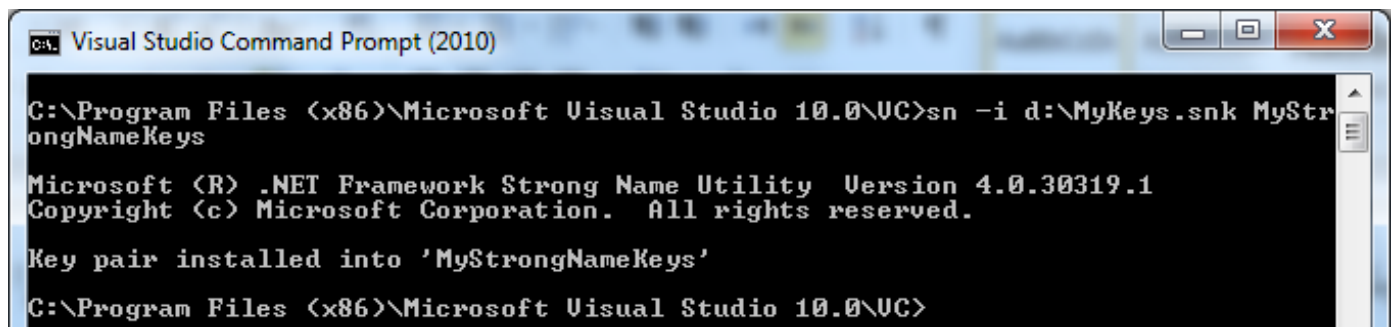
```

مقدار نمایش داده در انتهای تصویر فوق به‌عنوان «توکن کلید عمومی» (Public key Token) در واقع 8 بایت پایانی کد هش شده کریپتوگرافی محاسبه شده از کلید عمومی است. چون خود کلید عمومی همان‌طور که مشاهده می‌شود بسیار طولانی است، دات‌نت فریمورک معمولاً از این توکن برای نمایش آن و ریفرنس دادن اسمبلی‌ها استفاده می‌کند. نیازی نیست تا راز این کلیدها توسط توسعه‌دهنده حفظ شود! پس از نام‌گذاری قوی اسمبلی (که در ادامه توضیح داده می‌شود) کامپایلر با استفاده از کلید خصوصی فراهم شده یک امضای دیجیتالی (یک کد اینکریپت شده) با استفاده از داده‌های «مانیفست اسمبلی» تولید می‌کند. در ادامه کامپایلر این «امضای دیجیتال» و «کلید عمومی» را درون اسمبلی قرار می‌دهد تا مصرف‌کننده‌های اسمبلی بتوانند این امضای دیجیتال را تایید کنند. حفظ کردن «کلید خصوصی» بسیار مهم است! اگر کسی به کلید خصوصی اسمبلی دست یابد می‌تواند با استفاده از آن نسخه‌ای تغییر یافته از اسمبلی را امضا کرده و در اختیار مصرف‌کنندگان قرار دهد. مصرف‌کنندگان نیز بدون اینکه متوجه شوند می‌توانند از این نسخه تغییر یافته با همان توکن کلید عمومی که در اختیار دارند استفاده کنند. در حال حاضر روشی برای فهمیدن این تغییر وجود ندارد. اگر کلید خصوصی لو رفت، باید یک جفت کلید دیگر تولید و با استفاده از کلید خصوصی جدید اسمبلی را دوباره امضا کرد و در اختیار مصرف‌کنندگان قرار داد. همچنین باید مشتریان اسمبلی را از این تغییر آگاه ساخت و کلید عمومی مورد اطمینان را در اختیار آن‌ها قرار داد.

نکته : معمولاً گروه کوچکی از افراد مورد اطمینان (که دسترسی امضای اسمبلی را دارند: signing authority) مسئولیت کلیدهای نامگذاری قوی یک شرکت را بر عهده دارند و برای امضای تمام اسمبلی‌ها قبل از ریلیز نهایی آن‌ها مسئول هستند. قابلیت امضای تاخیری اسمبلی (که در ادامه بحث می‌شود) تسهیلاتی را برای بهره‌برداری راحت‌تر از این روش و جلوگیری از توزیع کلیدهای خصوصی میان تمام توسعه‌دهندگان را فراهم می‌کند. یکی از روش‌هایی که sn برای افزایش امنیت کلیدها ارائه می‌دهد، استفاده از مخزن کلید CSP است. پس از تولید فایل حاوی جفت کلید، می‌توان با استفاده از دستور زیر این کلیدها را درون CSP با نام MyStrongNameKeys ذخیره کرد:

```
sn -i MyKeys.snk MyStrongNameKeys
```

سپس می‌توان فایل حاوی جفت کلید را حذف کرد.



```

C:\Program Files (x86)\Microsoft Visual Studio 10.0\VC>sn -i d:\MyKeys.snk MyStrongNameKeys

Microsoft (R) .NET Framework Strong Name Utility Version 4.0.30319.1
Copyright (c) Microsoft Corporation. All rights reserved.

Key pair installed into 'MyStrongNameKeys'

C:\Program Files (x86)\Microsoft Visual Studio 10.0\VC>

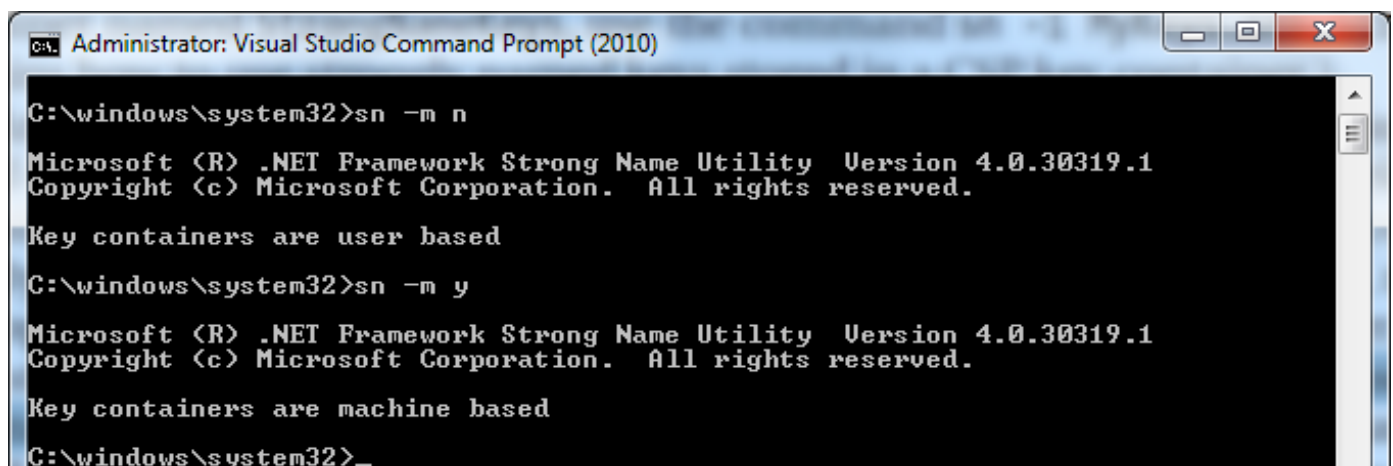
```

نکته مهمی که درباره مخازن کلید CSP باید بدان اشاره کرد این است که این مخازن شامل مخازن تعریف شده توسط «کاربر» و نیز مخازن «سیستمی» است. سیستم امنیتی ویندوز به کاربران اجازه دسترسی به مخازنی غیر از مخازن خودشان و مخازن سیستمی را نمی‌دهد. برنامه sn به صورت پیش فرض کلیدها را درون مخازن سیستمی ذخیره می‌کند. بنابراین هر کسی که بتواند به سیستم لاگین کند و نیز از نام مخزن مربوطه آگاه باشد، به راحتی می‌تواند اسمبلی شما را امضا کند! برای اینکه ابزار sn کلیدها را در مخازن کاربری ذخیره کند باید از دستور زیر استفاده کرد:

```
sn -m n
```

برای برگرداندن تنظیم به مخازن سیستمی نیز باید از دستور زیر استفاده کرد:

```
sn -m y
```



```

C:\windows\system32>sn -m n

Microsoft (R) .NET Framework Strong Name Utility Version 4.0.30319.1
Copyright (c) Microsoft Corporation. All rights reserved.

Key containers are user based

C:\windows\system32>sn -m y

Microsoft (R) .NET Framework Strong Name Utility Version 4.0.30319.1
Copyright (c) Microsoft Corporation. All rights reserved.

Key containers are machine based

C:\windows\system32>_

```

برای حذف کلیدها از مخزن می‌توان از دستور زیر استفاده کرد:

```
sn -d MyStrongNameKeys
```

```

Administrator: Visual Studio Command Prompt (2010)

C:\windows\system32>sn -d MyStrongNameKeys

Microsoft (R) .NET Framework Strong Name Utility Version 4.0.30319.1
Copyright (c) Microsoft Corporation. All rights reserved.

Container 'MyStrongNameKeys' deleted

C:\windows\system32>_

```

2. نام‌گذاری قوی یک اسمبلی

نام‌گذاری قوی یک اسمبلی به دلایل زیادی انجام می‌شود:

- برای اینکه اسمبلی شناسه‌ای منحصر به فرد داشته باشد، تا کاربران بتوانند مجوزهای ویژه‌ای را در حین تنظیم سیاست‌های امنیتی دسترسی به کد اعمال کنند.
- تا اسمبلی را نتوان تغییر داده و سپس به عنوان اسمبلی اصلی توزیع نمود.
- تا اسمبلی بتواند نسخه‌گذاری (Versioning) و سیاست‌های نسخه‌گذاری را پشتیبانی کند.
- تا بتوان اسمبلی را در GAC (همان Global Assembly Cache که در مسیر %windir%\assembly% قرار دارد) ذخیره کرده و آن را بین چند اپلیکیشن به اشتراک گذاشت.
- برای نام‌گذاری قوی اسمبلی با استفاده از خط فرمان کامپایلر C# باید از سوییچهای /keyfile و /keycontainer استفاده کنید.

```

Administrator: Visual Studio Command Prompt (2010)

C:\windows\system32>csc /?
Microsoft (R) Visual C# 2010 Compiler version 4.0.30319.1
Copyright (C) Microsoft Corporation. All rights reserved.

Visual C# 2010 Compiler Options

- OUTPUT FILES -
/out:<file>          Specify output file name (default: base name of
                    file with main class or first file)
/target:exe         Build a console executable (default) (Short form:
                    /t:exe)
/target:winexe      Build a Windows executable (Short form:
                    /t:winexe)
/target:library     Build a library (Short form: /t:library)
/target:module      Build a module that can be added to another
                    assembly (Short form: /t:module)
/delay:sign[+!-]   Delay-sign the assembly using only the public
                    portion of the strong name key
/doc:<file>         XML Documentation file to generate
/keyfile:<file>     Specify a strong name key file
/keycontainer:<string> Specify a strong name key container
/platform:<string>  Limit which platforms this code can run on: x86,
                    Itanium, x64, or anycpu. The default is anycpu.

- INPUT FILES -

```

"csc /keyfile:d:\mykeys.snk /out:"C:\Projects\ClassLibrary1\Class1.exe" "C:\Projects\ClassLibrary1\Class1.cs"

نکته : برای استفاده از این ویژگی در ویژوال استودیو، باید در تب Signing در تنظیمات پروژه گزینه Sign the Assembly را انتخاب کرد. سپس می‌توان فایل حاوی جفت کلیدهای تولیدشده را انتخاب یا فایل جدیدی تولید کرد. البته ویژوال استودیو تا نسخه 2010 امکانی جهت استفاده از مخازن CSP را ندارد.

☒ Sign the assembly

Choose a strong name key file:

<New...>

<Browse...>

When delay signed, the project will not run or be debuggable.

Reference Paths

Signing*

Security

Publish

Code Analysis

Timestamp server URL:

☒ Sign the assembly

Choose a strong name key file:

☐ Delay sign only

When delay signed, the project will not run or be debuggable.

روش ساده دیگر استفاده از attribute های سطح اسمبلی است:

```
[assembly:AssemblyKeyFileAttribute("MyKeys.snk")]
```

3. بررسی اینکه آیا یک اسمبلی قوی-نام گذاری شده تغییر یافته یا خیر

زمانی که CLR در زمان اجرا یک اسمبلی قوی-نام گذاری شده را بارگذاری می کند:

-ابتدا با استفاده از کلید عمومی (که در خود اسمبلی ذخیره شده است) هش کد اینکریپت شده که در زمان کامپایل محاسبه شده (یا همان امضای دیجیتال که این نیز درون خود اسمبلی ذخیره شده است) را دیکریپت می کند. (هش کد زمان کامپایل)

-پس از آن هش کد اسمبلی را با استفاده از داده های مانیفست اسمبلی محاسبه می کند. (هش کد زمان اجرا)

-سپس این دو مقدار بدست آمده (هش کد زمان کامپایل و هش کد زمان اجرا) را با یکدیگر مقایسه می کند. این عملیات مقایسه و تایید مشخص می کند که آیا اسمبلی پس از امضا دچار تغییر شده است یا خیر!

اگر یک اسمبلی نتواند عملیات تایید نام قوی را پشت سر بگذارد، CLR پیغام خطایی به نمایش خواهد گذاشت. این خطا یک اکسپشن از نوع System.IO.FileLoadException با پیغام Strong name validation failed خواهد بود. با استفاده از ابزار sn نیز می توان یک اسمبلی قوی-نام گذاری شده را تایید کرد. برای مثال برای تایید اسمبلی MyAsm.exe می توان از دستور زیر استفاده کرد:

```
sn -vf MyAsm.exe
```

```

Administrator: Visual Studio Command Prompt (2010)

C:\windows\system32>sn -vf "C:\Users\Saleh\Documents\Visual Studio 2010\Projects\
\ConsoleApplication1\ClassLibrary1\Class1.exe"

Microsoft (R) .NET Framework Strong Name Utility Version 4.0.30319.1
Copyright (c) Microsoft Corporation. All rights reserved.

Assembly 'C:\Users\Saleh\Documents\Visual Studio 2010\Projects\ConsoleApplication1\ClassLibrary1\Class1.exe' is valid

C:\windows\system32>_

```

سوییچ v موجب تایید نام قوی اسمبلی شده و سوییچ f برنامه را مجبور به بررسی صحت نام قوی اسمبلی می‌کند، حتی اگر این امکان قبلاً برای اسمبلی غیرفعال شده باشد. (با استفاده از سوییچ Vn مثل دستور sn -Vn MyAsm.exe می‌توان عملیات تایید نام قوی یک اسمبلی خاص را غیرفعال کرد). اگر اسمبلی تغییر کرده باشد و نتواند آزمون فوق را پشت سر بگذارد خطایی به شکل زیر نمایش داده می‌شود:

```

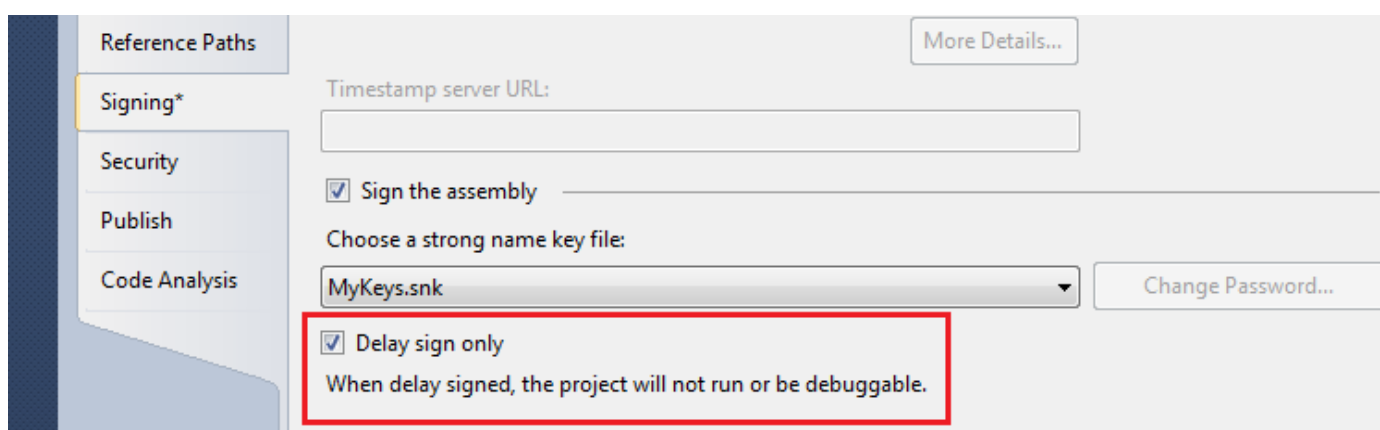
Microsoft (R) .NET Framework Strong Name Utility Version 2.0.50727.42
Copyright (C) Microsoft Corporation. All rights reserved.
Failed to verify assembly --
Strong name validation failed for assembly MyAsm.exe'.

```

4. امضای تأخیری (Delay Sign) یک اسمبلی

در صورتی که بخواهیم یک اسمبلی را امضا کنیم اما نخواهیم تمام اعضای تیم توسعه به کلید خصوصی مربوطه دسترسی داشته باشند باید از تکنیک امضای با تأخیر اسمبلی استفاده کنیم. ابتدا باید کلید عمومی تولید شده برای اسمبلی را استخراج کرده و آنرا توزیع کنیم. با توجه به توضیحات داده شده در بخش اول، به اسمبلی خود یک نام قوی اختصاص دهید. همچنین اسمبلی خود را با استفاده از سوییچ /delaysign باید کامپایل کنید. سپس با استفاده از سوییچ Vn برنامه sn عملیات تایید اسمبلی خود را غیرفعال کنید.

نکته : برای استفاده از این امکان در ویژوال استودیو باید گزینه Delay sign only را در تب Signing از پراپرتی پروژه انتخاب کرد.



اسمبلی‌هایی که ریفرنسی به اسمبلی‌های نام‌گذاری قوی شده دارند، حاوی توکن کلید عمومی آن اسمبلی‌ها نیز هستند. این بدین معنی است که این گونه اسمبلی‌ها بایستی قبل از ریفرنس داده شدن امضا شده باشند. در یک محیط توسعه که اسمبلی‌ها مرتباً کامپایل می‌شوند نیاز است تا تمام توسعه دهندگان و آزمایش‌کنندگان به جفت‌کلیدهای موجود دسترسی داشته باشند (یک ریسک امنیتی بزرگ). به جای توزیع کلید خصوصی، دات‌نت فریمورک مکانیزمی به نام امضای تأخیری (delay-signing) فراهم کرده است، که به شما اجازه می‌دهد تا یک اسمبلی را به‌صورت ناکامل (ناقص) امضا کنید. اسمبلی «ناقص-نام‌گذاری قوی شده»! حاوی

کلید عمومی و توکن کلید عمومی است که برای ریفرنس دادن اسمبلی نیاز است، اما تنها حاوی مکان خالی امضای دیجیتالی است که توسط کلید خصوصی تولید می‌شود. پس از کامل شدن توسعه برنامه، فرد مسئول امضای اسمبلی‌ها (signing authority - شخصی که مسئول امنیت و حفظ جفت‌کلیدهاست) اسمبلی‌های حاوی امضای تأخیری را دوباره امضا می‌کند، تا نام‌گذاری قوی آن اسمبلی کامل شود. برای امضای تأخیری یک اسمبلی تنها نیاز به کلید عمومی آن است، که هیچ ریسک امنیتی‌ای برای آن وجود ندارد. برای استخراج کلید عمومی یک جفت کلید همان‌طور که قبلاً اشاره شده است، می‌توان از دستورات زیر استفاده کرد:

```
sn -p d:\MyKeys.snk d:\MyPublicKey.snk
sn -pc MyKeysContainer d:\MyPublicKey.snk
```

با داشتن فایل حاوی کلید عمومی، و با استفاده از دستور کامپایل زیر می‌توان اسمبلی را امضای تأخیری کرد:

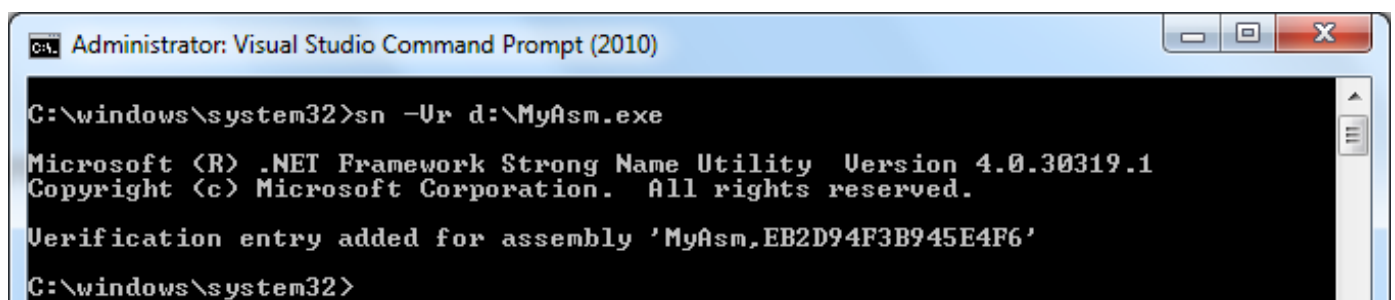
```
csc.exe /delaysign /keyfile:d:\MyPublicKey.snk /out:d:\MyAsm.exe d:\Class1.cs
```

نکته : برای امضای اسمبلی‌های چندفایلی (multifile assembly) باید از Assembly Linker (نام فایل اجرایی آن al.exe است) استفاده کرد. این ابزار نیز مانند ابزار sn.exe در sdkهای ویندوز یافت می‌شود. دستوری که باید برای امضای این نوع اسمبلی‌ها به‌کار برد به‌صورت زیر است:

```
al /out:<assembly name> <module name> /keyfile:<file name>
```

از آنجاکه در هنگام بارگذاری اسمبلی، CLR اسمبلی را به عنوان یک اسمبلی قوی نام‌گذاری شده در نظر می‌گیرد، همان‌طور که قبلاً اشاره شده، سعی می‌کند تا صحت آن را بررسی و تأیید کند. اما چون اسمبلی با امضای تأخیری هنوز امضا نشده است، باید CLR را جوری تنظیم کنید تا تأیید اعتبار این اسمبلی را در کامپیوتر جاری انجام ندهد. این کار را همان‌طور که در بالا توضیح داده شد، می‌توان با دستور زیر انجام داد:

```
sn -Vr d:\MyAsm.exe
```

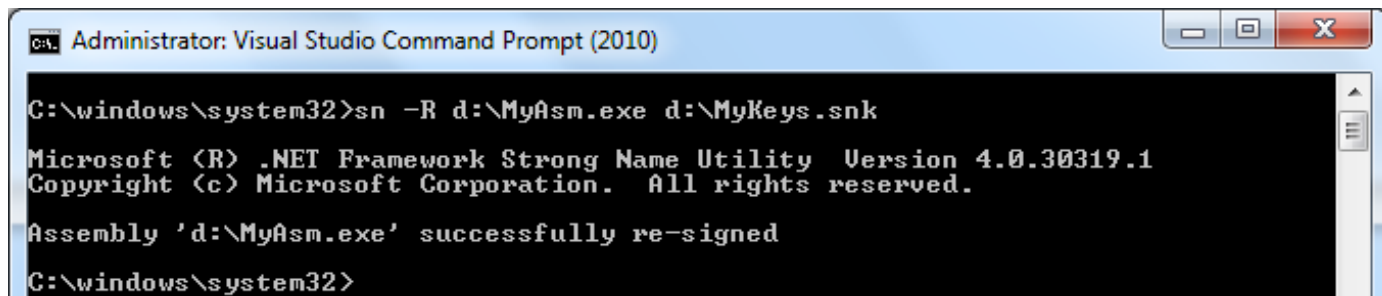


از لحاظ فنی این دستور اسمبلی موردنظر را در لیست «صرف‌نظر از تأیید اسمبلی» ثبت (register) می‌کند. دقت کنید که دستور فوق را باید در تمام سیستم‌هایی که قرار است به نحوی با این اسمبلی سروکار داشته باشند اجرا کنید!

نکته : تا زمانی که با استفاده از دستور فوق عملیات تأیید اعتبار اسمبلی‌های امضای تأخیری شده را غیرفعال نکنید امکان اجرا یا بارگذاری آن اسمبلی‌ها و نیز دیباگ سورس‌کدهای آن را نخواهید داشت! پس از تکمیل فاز توسعه باید اسمبلی را دوباره امضا کنید تا نام‌گذاری قوی کامل شود. برنامه sn به شما این امکان را می‌دهد تا بدون تغییر سورس‌کد اسمبلی خود یا کامپایل دوباره آن عملیات امضای دوباره آنرا انجام دهید. اما برای این کار شما باید به کلید خصوصی آن (در واقع به فایل حاوی جفت‌کلید مربوطه) دسترسی داشته باشید. برای امضای دوباره می‌توان از دستورات زیر استفاده کرد:

```
sn -R d:\MyAsm.exe MyKeys.snk
```

```
sn -R d:\MyAsm.exe MyKeysContainer
```



```
Administrator: Visual Studio Command Prompt (2010)

C:\windows\system32>sn -R d:\MyAsm.exe d:\MyKeys.snk

Microsoft (R) .NET Framework Strong Name Utility Version 4.0.30319.1
Copyright (c) Microsoft Corporation. All rights reserved.

Assembly 'd:\MyAsm.exe' successfully re-signed

C:\windows\system32>
```

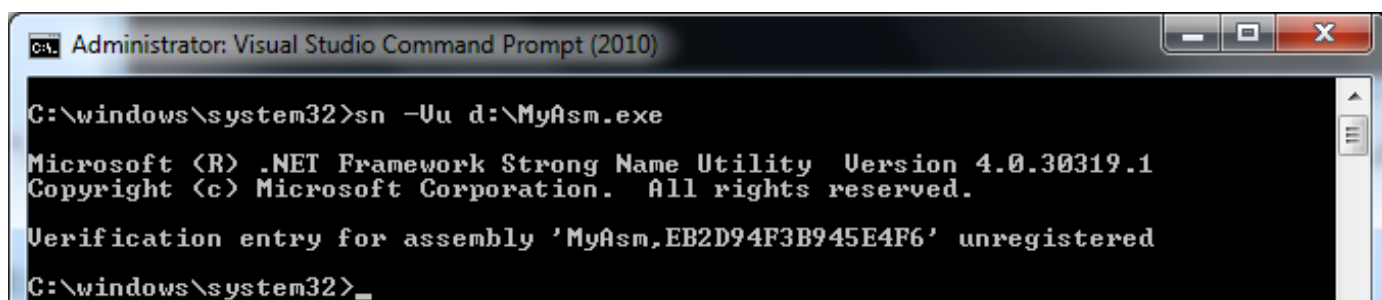
با استفاده از این دستور برنامه sn شروع به محاسبه هش کد زمان کامپایل می‌کند و در نهایت مقدار اینکریپت‌شده را درون اسمبلی ذخیره می‌کند.

نکته : هنگام استفاده از اسمبلی‌های با امضای تأخیری، امکان مقایسه بیلدهای مختلف یک اسمبلی خاص برای اطمینان از اینکه تنها در امضای دیجیتال با هم فرق دارند، معمولاً مفید است. این مقایسه تنها وقتی امکان‌پذیر است که اسمبلی موردنظر با استفاده از سویچ R دوباره امضا شود. برای مقایسه دو اسمبلی می‌توان از سویچ D استفاده کرد:

```
sn -D assembly1 assembly2
```

پس از امضای دوباره اسمبلی می‌توان عملیات تایید آنرا که قبلاً غیرفعال شده است، با استفاده از دستور زیر دوباره فعال کرد:

```
sn -Vu d:\MyAsm.exe
```



```
Administrator: Visual Studio Command Prompt (2010)

C:\windows\system32>sn -Vu d:\MyAsm.exe

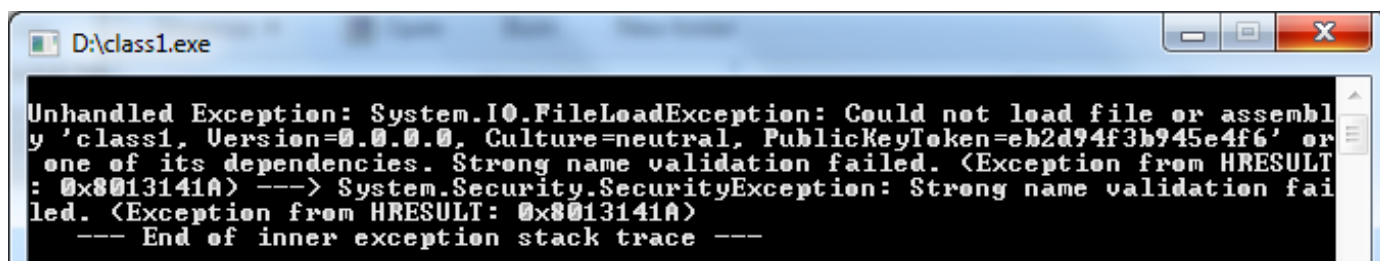
Microsoft (R) .NET Framework Strong Name Utility Version 4.0.30319.1
Copyright (c) Microsoft Corporation. All rights reserved.

Verification entry for assembly 'MyAsm.EB2D94F3B945E4F6' unregistered

C:\windows\system32>_
```

دستور فوق اسمبلی موردنظر را از لیست «صرفنظر از تایید اسمبلی» حذف (Unregister) می‌کند.

نکته : در صورتی که بخواهید یک اسمبلی را قبل از امضای دوباره (و یا در حالت کلی، قبل از اینکه اسمبلی دارای یک نام قوی کامل شده باشد) اجرا یا از آن به عنوان یک ریفرنس استفاده کنید، بدون اینکه آن را به لیست «صرفنظر از تایید اسمبلی» اضافی کنید، با خطای زیر مواجه خواهید شد:



برای فعال‌سازی تایید اسمبلی برای تمامی اسمبلی‌هایی که این ویژگی برای آنان غیرفعال شده است، می‌توانید از دستور زیر استفاده کنید:

```
sn -Vx
```

برای لیست کردن اسمبلی‌هایی که تایید آنان غیرفعال شده است، می‌توانید از دستور زیر استفاده کنید:

```
sn -Vl
```

نکته : در دات‌نت 1.0 و 1.1 کامپایلر C# فاقد سویچ `delaysign` است. برای استفاده از امکان امضای تأخیری اسمبلی می‌توان از attribute سطح اسمبلی `System.Reflection.AssemblyDelaySignAttribute` استفاده کرد. همچنین می‌شود از ابزار لینکر اسمبلی (`al.exe`) که از این سویچ پشتیبانی می‌کند استفاده کرد.

نکته : ابزارهای obfuscating که برای پیچیده‌کردن کد IL اسمبلی تولیدی به‌منظور جلوگیری از عملیات تولید دوباره کد (مثل کاری که برنامه Reflector انجام می‌دهد) به‌کار می‌روند، به دلیل تغییراتی که در محتوای اسمبلی ایجاد می‌کنند، در صورتیکه برای اسمبلی‌های دارای نام قوی استفاده شوند موجب از کار افتادن آن‌ها می‌شوند. بنابراین یا باید آن‌ها را در سیستم‌هایی استفاده کرد که آن اسمبلی موردنظر در لیست صرفنظر از تایید اسمبلی ثبت شده باشد یا اینکه اسمبلی مربوطه را دوباره با استفاده از روش‌های توضیح داده‌شده (مثلاً با استفاده از دستور `sn -R myAsm.dll MyKeys.snk` برای تخصیص نام قوی جدید امضا کرد). الگوی معمولی که برای استفاده از obfuscating برای اسمبلی‌های دارای نام قوی استفاده می‌شود به‌صورت زیر است:

- ساخت اسمبلی با امضای تأخیری
- افزودن اسمبلی به لیست صرفنظر از تایید اسمبلی (`sn -Vr`)
- دیباگ و تست اسمبلی
- obfuscate کردن اسمبلی
- دیباگ و تست اسمبلی obfuscate شده
- امضای دوباره اسمبلی (`sn -R`)
- الگوی ساده‌تر دیگری نیز برای این منظور استفاده می‌شود که به‌صورت زیر است:
- تولید اسمبلی بدون استفاده از تنظیمات امضای تأخیری
- دیباگ و تست اسمبلی
- obfuscate اسمبلی
- امضای دوباره اسمبلی (`sn -R`)
- دیباگ و تست دوباره نسخه obfuscate شده

5. مدیریت کش عمومی اسمبلی‌ها (Global Assembly Cache)

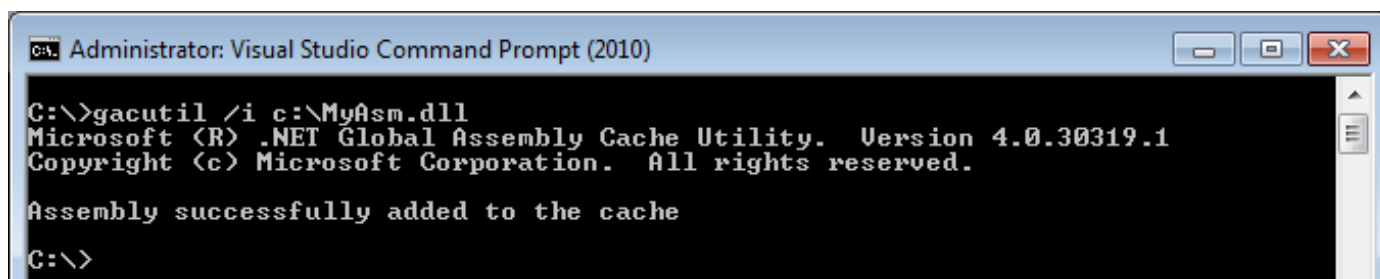
با استفاده از توضیحات این بخش می‌توان اسمبلی‌ها را به GAC اضافه و یا از درون آن حذف کرد. این کار با استفاده از برنامه `gacutil.exe` انجام می‌شود. مسیر نسخه 4 و 32 بیتی این برنامه به‌صورت زیر است:

```
C:\Program Files\Microsoft SDKs\Windows\v7.0A\Bin\NETFX 4.0 Tools\gacutil.exe
```

این برنامه به‌همراه SDK ویندوز و یا به‌همراه ویژوال استودیو در مسیری مشابه نشانی بالا نصب می‌شود. همانند توضیحات

داده شده در مورد برنامه sn.exe، برای راحتی کار می‌توانید از خط فرمان ویژه‌ای که ویژوال استودیو در اختیار شما قرار می‌دهد استفاده کنید. البته قبل از اجرای هر دستوری مطمئن شوید که خط فرمان شما با استفاده از مجوز مدیریتی (Administrator) اجرا شده است! تنها اسمبلی‌های دارای نام قوی می‌توانند در GAC نصب شوند. بنابراین قبل افزودن یک اسمبلی به GAC باید طبق راهنمایی‌های موجود در قسمت‌های قبلی آن را به صورت قوی نام‌گذاری کرد. برای افزودن یک اسمبلی با نام MyAsm.dll می‌توان از دستور زیر استفاده کرد:

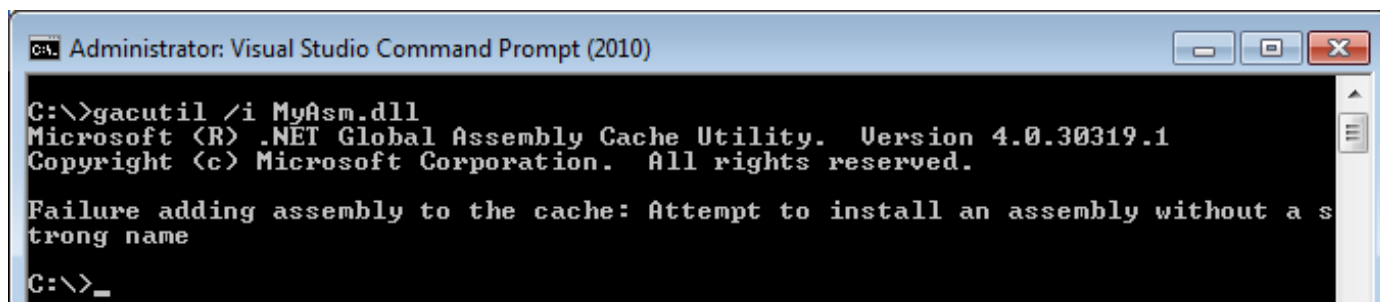
```
gacutil /i c:\MyAsm.dll
```



```
Administrator: Visual Studio Command Prompt (2010)
C:\>gacutil /i c:\MyAsm.dll
Microsoft (R) .NET Global Assembly Cache Utility. Version 4.0.30319.1
Copyright (c) Microsoft Corporation. All rights reserved.

Assembly successfully added to the cache
C:\>
```

در صورتی که اسمبلی مورد نظر دارای نام قوی نباشد، خطایی به صورت زیر نمایش داده خواهد شد:



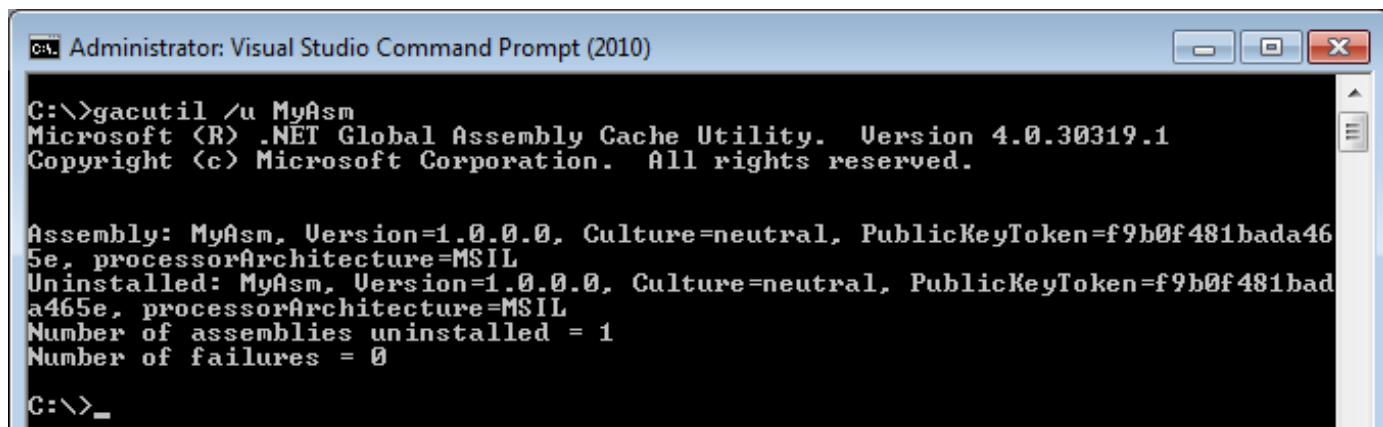
```
Administrator: Visual Studio Command Prompt (2010)
C:\>gacutil /i MyAsm.dll
Microsoft (R) .NET Global Assembly Cache Utility. Version 4.0.30319.1
Copyright (c) Microsoft Corporation. All rights reserved.

Failure adding assembly to the cache: Attempt to install an assembly without a strong name
C:\>_
```

می‌توان نسخه‌های متفاوتی از یک اسمبلی (با نام یکسان) را با استفاده از این ابزار در GAC رجیستر کرد و آن‌ها را در کنار یکدیگر برای استفاده در نرم‌افزارهای گوناگون در اختیار داشت. برای حذف یک اسمبلی از GAC و یا به اصطلاح uninstall کردن آن می‌توان از دستور زیر استفاده کرد:

```
gacutil /u MyAsm
```

نکته : دقت کنید که در این دستور تنها از نام اسمبلی استفاده شده است و نه نام فایل حاوی آن!



```

Administrator: Visual Studio Command Prompt (2010)

C:\>gacutil /u MyAsm
Microsoft (R) .NET Global Assembly Cache Utility. Version 4.0.30319.1
Copyright (c) Microsoft Corporation. All rights reserved.

Assembly: MyAsm, Version=1.0.0.0, Culture=neutral, PublicKeyToken=f9b0f481bada465e, processorArchitecture=MSIL
Uninstalled: MyAsm, Version=1.0.0.0, Culture=neutral, PublicKeyToken=f9b0f481bada465e, processorArchitecture=MSIL
Number of assemblies uninstalled = 1
Number of failures = 0

C:\>_

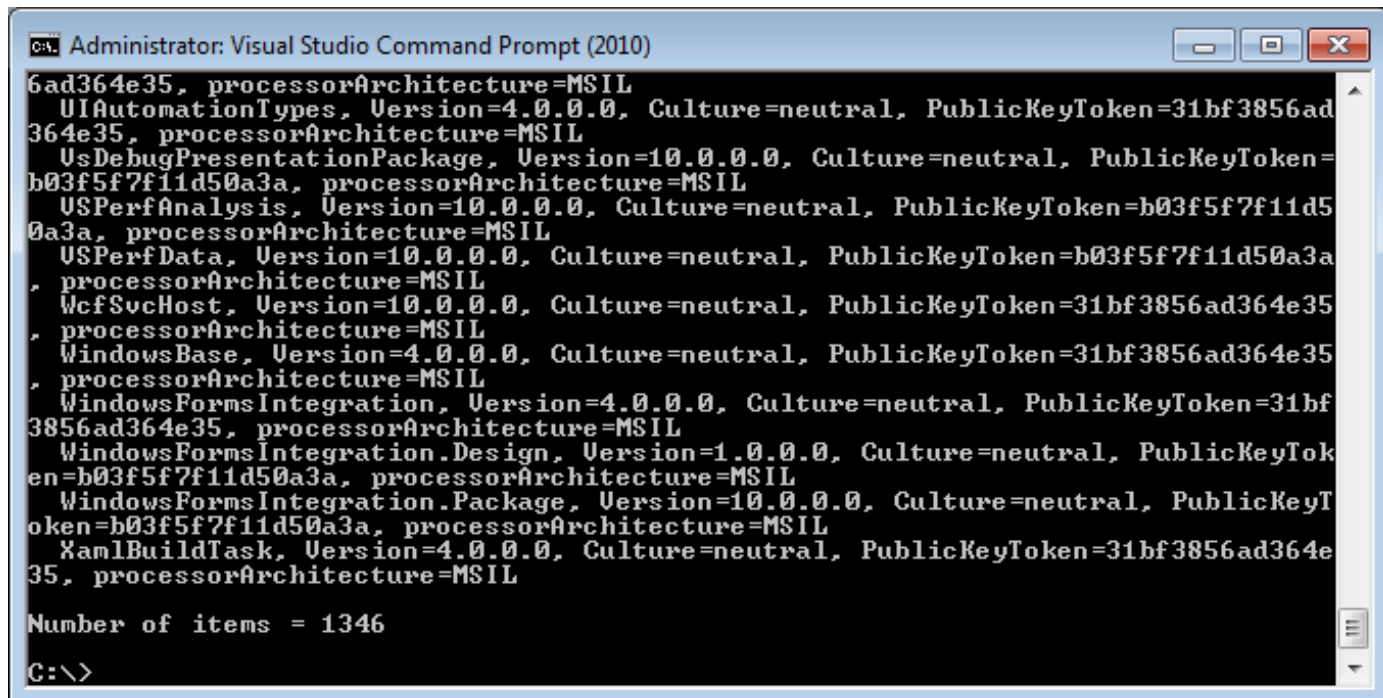
```

دستور فوق تمام نسخه‌های اسمبلی MyAsm موجود در GAC را حذف خواهد کرد. برای حذف نسخه‌ای خاص باید از دستوری مشابه زیر استفاده کرد:

```
gacutil /u MyAsm,Version=1.3.0.5
```

برای مشاهده تمام اسمبلی‌های نصب شده در GAC می‌توان از دستور زیر استفاده کرد:

```
gacutil /l
```



```

Administrator: Visual Studio Command Prompt (2010)

6ad364e35, processorArchitecture=MSIL
  UIAutomationTypes, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35, processorArchitecture=MSIL
  UsDebugPresentationPackage, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a, processorArchitecture=MSIL
  USPerfAnalysis, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a, processorArchitecture=MSIL
  USPerfData, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a, processorArchitecture=MSIL
  WcfSvcHost, Version=10.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35, processorArchitecture=MSIL
  WindowsBase, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35, processorArchitecture=MSIL
  WindowsFormsIntegration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35, processorArchitecture=MSIL
  WindowsFormsIntegration.Design, Version=1.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a, processorArchitecture=MSIL
  WindowsFormsIntegration.Package, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a, processorArchitecture=MSIL
  XamlBuildTask, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35, processorArchitecture=MSIL

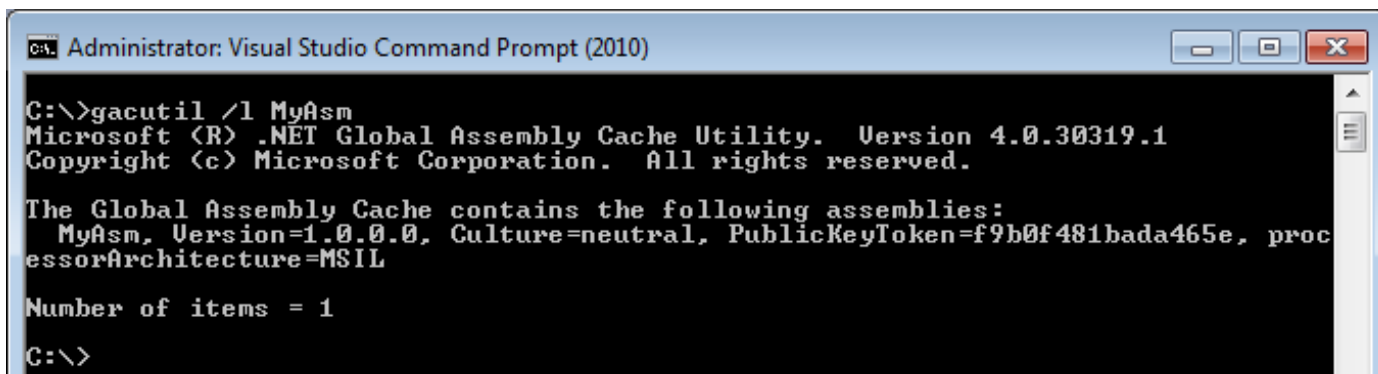
Number of items = 1346

C:\>

```

همان‌طور که مشاهده می‌کنید دستور فوق فهرستی بسیار طولانی از تمام اسمبلی‌های نصب شده در GAC را به همراه لیست اسمبلی‌هایی که در کش ngen به فرم باینری پیش‌کامپایل (Precompiled) شده‌اند، نمایش می‌دهد. برای تعیین اینکه آیا اسمبلی موردنظر در GAC نصب شده است می‌توان از دستور زیر استفاده کرد:

```
gacutil /l MyAsm
```



```

Administrator: Visual Studio Command Prompt (2010)

C:\>gacutil /l MyAsm
Microsoft (R) .NET Global Assembly Cache Utility. Version 4.0.30319.1
Copyright (c) Microsoft Corporation. All rights reserved.

The Global Assembly Cache contains the following assemblies:
  MyAsm, Version=1.0.0.0, Culture=neutral, PublicKeyToken=f9b0f481bada465e, processorArchitecture=MSIL

Number of items = 1

C:\>

```

نکته : دات نت از GAC تنها در زمان اجرا استفاده می کند. بنابراین کامپایلر C# به صورت خودکار درون GAC را برای یافتن ریفرنس های یک اسمبلی جستجو نخواهد کرد. در زمان توسعه، کامپایلر C# به یک نسخه لوکال از ریفرنس های مذکور نیاز خواهد داشت. برای حل این مشکل می توان یک نسخه از این ریفرنس ها را به مسیر اسمبلی کپی کرد (در ویژوال استودیو می توان از خاصیت Copy Local ریفرنس ها استفاده کرد) یا با استفاده از سوییچ /lib کامپایلر، مسیری را که می تواند این ریفرنس ها را در آن بیابد معرفی کرد (کاری که ویژوال استودیو به صورت خودکار انجام می دهد).

نکته : نکته ای که در پایان باید اشاره کرد این است که تکنولوژی نام قوی برای بحث امنیت کد اسمبلی (مثلا برای جلوگیری از مهندسی معکوس IL و تغییر آن) بوجود نیامده است زیرا حذف این نام های قوی کار سختی نیست. بلکه هدف اصلی این تکنولوژی جلوگیری از تغییرات مخفی خرابکارانه و محرمانه اسمبلی توزیع شده و توزیع این نسخه های دستکاری شده به جای نسخه اصلی است. در زیر ابزارها و روش هایی که می توانند برای حذف کامل نام قوی یک اسمبلی به کار روند آورده شده است. [SNRemove](#)
[v1.00 Removing Strong-Signing from assemblies at file level \(byte patching\) Remove strong name from assembly while de serialize using regular expressions](#)

البته باید به این نکته اشاره کرد که در صورت حذف نام قوی یک اسمبلی (یا همان حذف امضای دیجیتال درون آن) تمامی اسمبلی هایی که قبل از حذف نام قوی به آن ریفرنس داشتند از کار خواهند افتاد. یعنی درواقع تمامی آن اسمبلی ها برای ریفرنس دادن به این اسمبلی با نام جدید (نامی که دیگر قوی نیست) باید آپدیت شوند. همچنین در صورتی که اسمبلی هایی که قبل از حذف نام قوی به اسمبلی مورد نظر ما ریفرنس داشتند، خود نام قوی داشته باشند با حذف نام قوی، آنها از کار خواهند افتاد. چون اسمبلی های دارای نام قوی تنها می توانند از اسمبلی های دارای نام قوی ریفرنس داشته باشند. بنابراین برای کارکردن برنامه مورد نظر باید نام قوی تمامی اسمبلی های درگیر را حذف کرد!

منابع استفاده شده در تهیه این مطلب: [Strong Names Explained](#)

[Giving a .NET Assembly a Strong Name](#)

[How to: Sign an Assembly with a Strong Name](#)

[Strong-Named Assemblies](#)

نظرات خوانندگان

نویسنده: مجید
تاریخ: ۲۲:۱ ۱۳۹۱/۰۸/۲۹

فقط می‌تونم بگم عالیه
ممنون

نویسنده: یوسف نژاد
تاریخ: ۱۶:۳۹ ۱۳۹۲/۰۲/۰۹

برای مشاهده Public Key Token یک اسمبلی با استفاده از فایل آن نیز میتوان از دستور زیر استفاده کرد:

sn -T MyAssembly.dll

پارامتر T حتما باید با حرف بزرگ وارد شود.

نحوه ایجاد یک External Tools در VS2012 جهت تهیه Public Key Token

عنوان:

نویسنده: محمد باقر سیف اللهی

تاریخ:

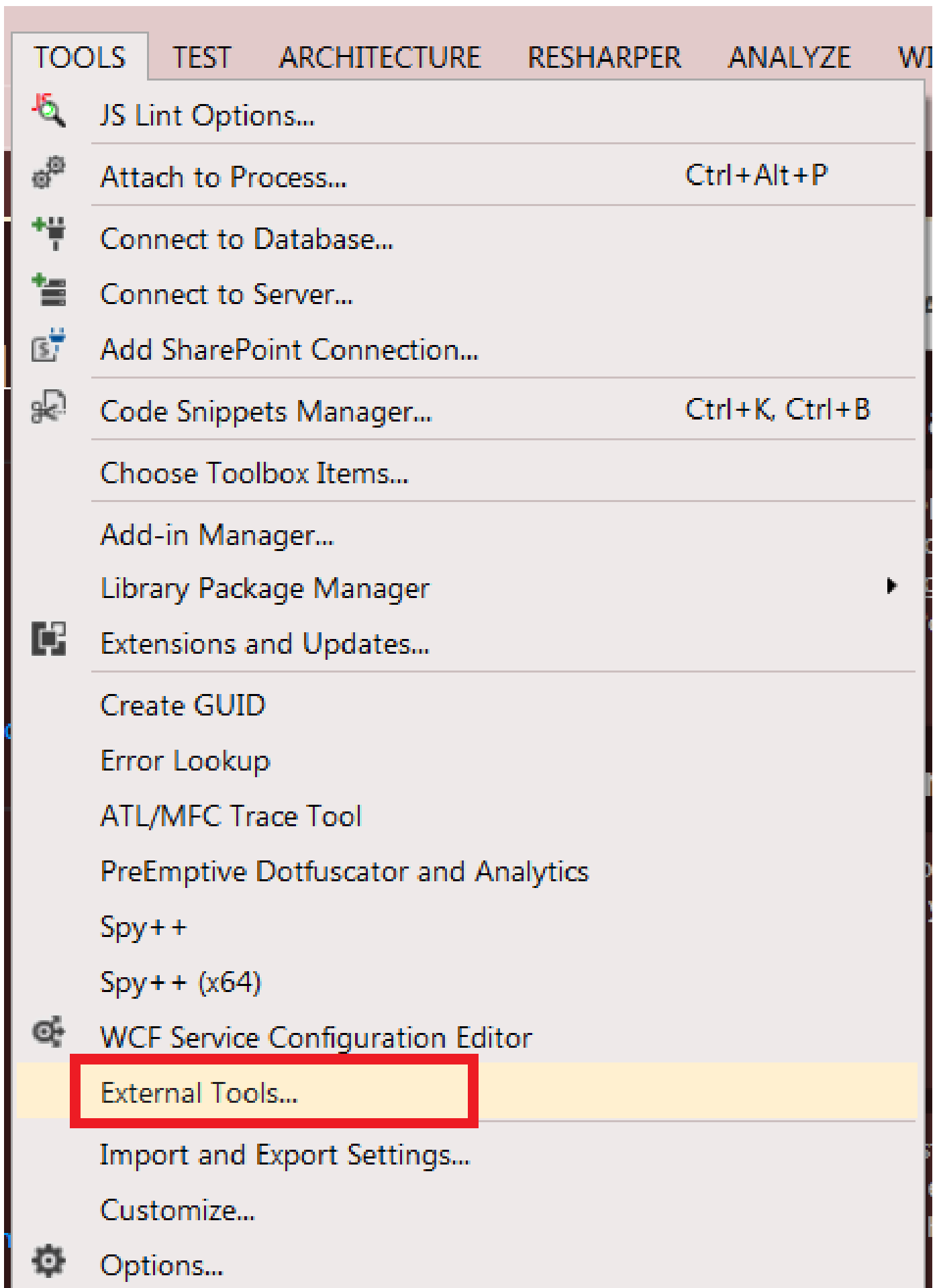
۱۱:۳۵ ۱۳۹۱/۱۰/۱۴

آدرس:

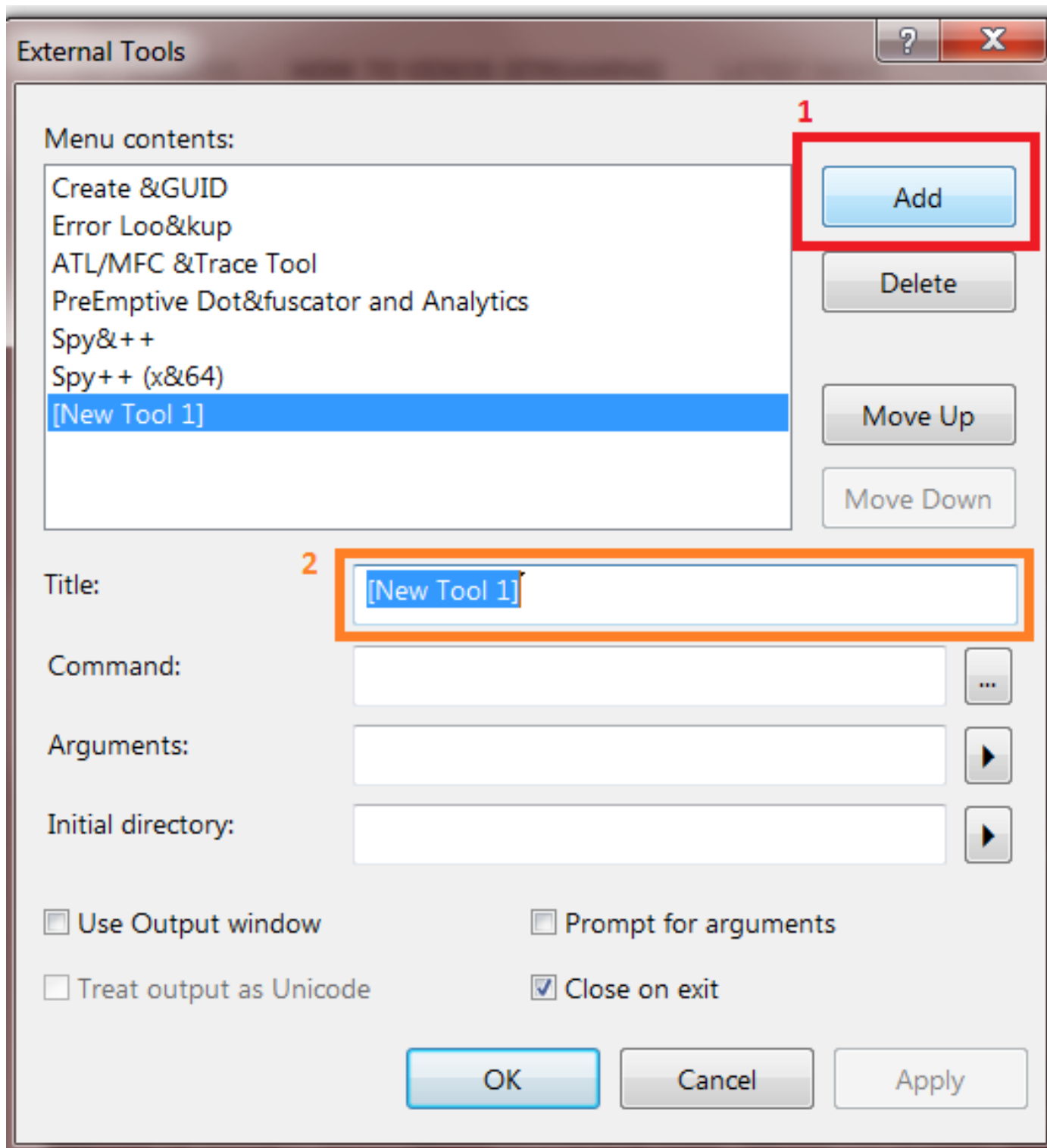
www.dotnettips.info

برچسب‌ها: Tools, VisualStudio.NET, .NET, Visual Studio, Strong Name

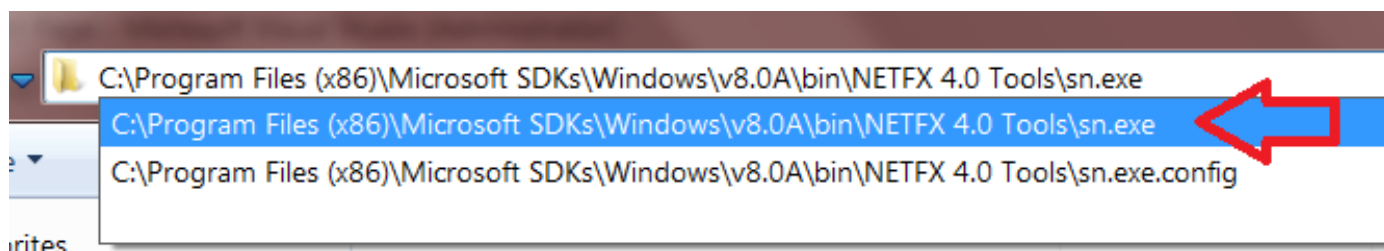
ایجاد Strong Name به اسمبلی برای داشتن یک هویت منحصر به فرد برای آن اسمبلی کمک می‌کند و یکی از پارامترهای آن داشتن Public Key Token برای اسمبلی است ([بیشتر](#)). در این پست قصد دارم به کمک ابزارهای جانبی Visual Studio 2012 که البته در 2010 نیز امکان پذیر است روشی برای تهیه آسان‌تر این Key ارائه کنم .
برای آغاز نرم افزار VS2012 را باز می‌کنیم و به منوی Tools رفته و گزینه External Tools را انتخاب می‌کنیم :



در پنجره‌ی پیش رو روی دکمه Add کلیک کنید و نامی برای Tools انتخاب کنید :



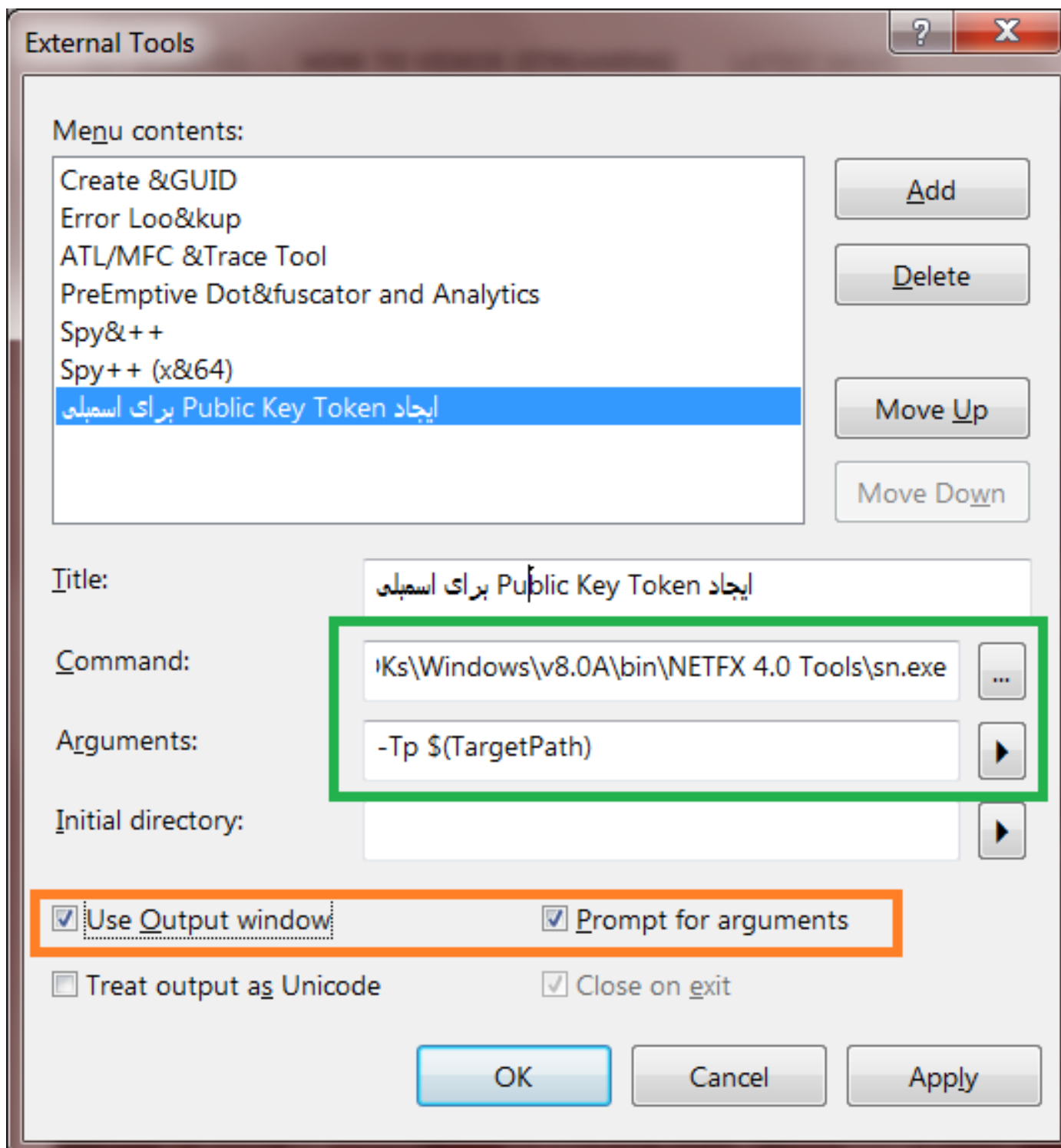
سپس مسیر فایل sn.exe را کپی کرده و در فیلد Command قرار دهید .



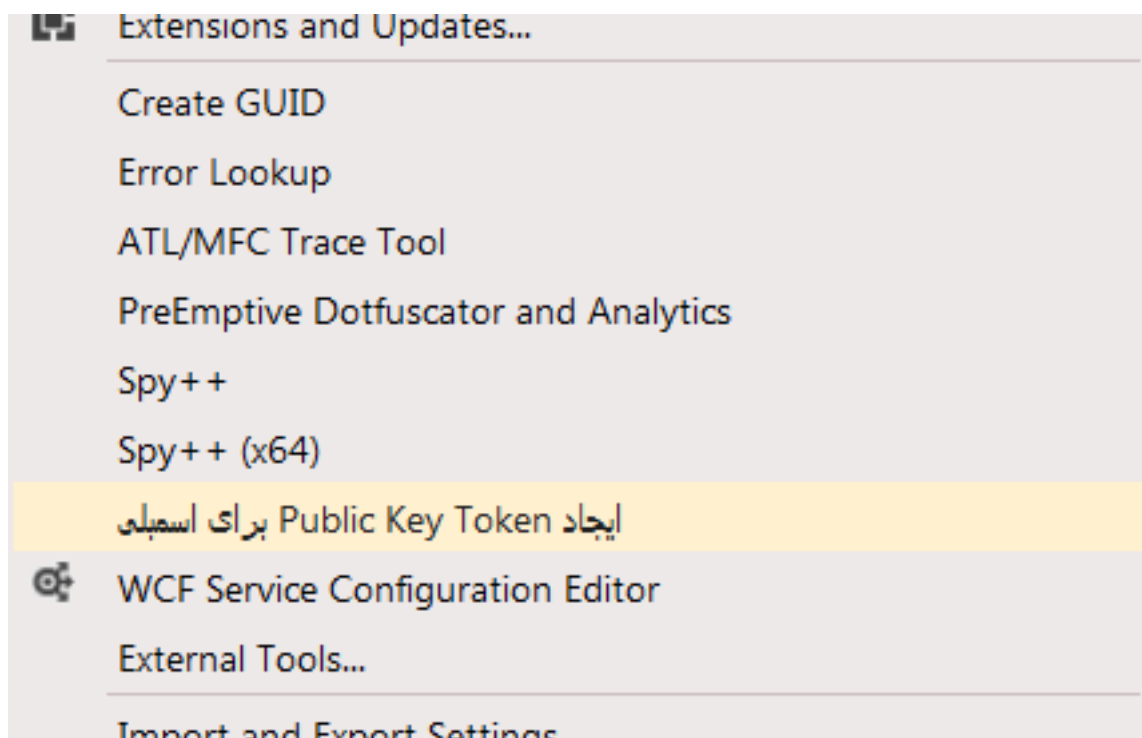
برای پارامتر از عبارت زیراستفاده کرده تا Public Key اسمبلی جاری را به شما بدهد . برای اطلاعات بیشتر در مورد آرگومانها به [اینجا](#) مراجعه کنید

```
-Tp $(TargetPath)
```

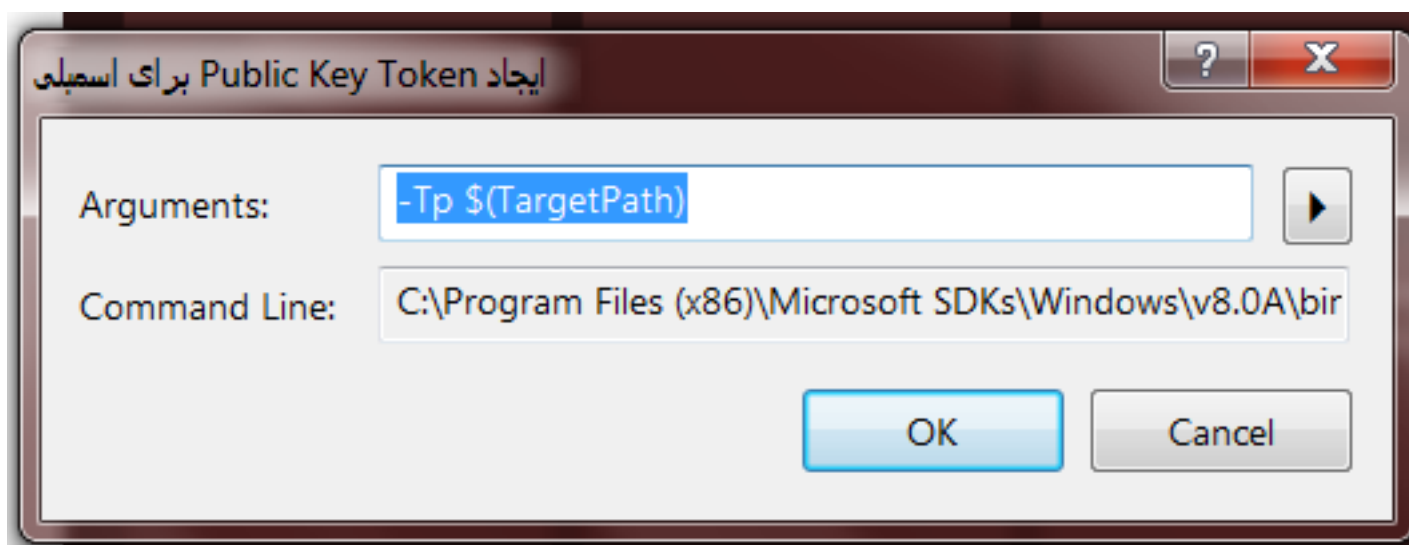
همچنین گزینه‌های Prompt for Arguments را برای دریافت آرگومان دلخواه شما (مثلا مواردی که مایلید برای یک اسمبلی دیگر key استخراج کنید) و Use Output window برای نمایش خروجی را علامت بزنید



روی OK کلیک کنید و به منوی Tools بازگردید :



حال روی نام پروژه خود در Solution Explorer کلیک کنید و روی Tools ساخته شده کلیک کنید :



و خروجی:

```
Output
Show output from: ایجاد Public Key Token برای اسمبلی
Microsoft (R) .NET Framework Strong Name Utility  Version 4.0.30319.17929
Copyright (c) Microsoft Corporation.  All rights reserved.

Public key (hash algorithm: sha1):
00240000048000000940000000060200000024000005253413100040000010001002dad9517360f66
c7e3968137a71d1c0fcfeb7264034b0ccb57528b66e557050568c78cce59087bfe25f4a012209a
d85c69657e823170306c46c2f99e2678e16f131dc865072165df730d2380b87a62e72dd3b2dde9
18c173785ebf08782cd457cf867822c5bb607bdf7c708ed6c1aab317262b951d54ea02167fc162
e4708aa8

Public key token is 25ce05e4457e7848
```

[موفق باشید](#)