Creating and Exporting an RSA Key Container

خلاصه:

ابتدا باید یک کلید خصوصی ایجاد کنیم و آن کلید را خروجی بگیریم و فایل کلید خصوصی را به سرور دیگر انتقال دهیم و به عنوان کلید وارد کنیم که بتوانیم در سرور دوم هم encrypt و هم decrypt انجام شود.

ابتدا باید کلید را ایجاد کنیم.

برای این کار با cmd وارد دایرکتوری فریمورک می شویم تا از aspnet_regiis.exe استفاده کنیم.

با استفاده از این دستور

```
cd \WINDOWS\Microsoft.Net\Framework\v2.0.*
```

با استفاده از دسور زیر کلید را ایجاد میکنیم که:

- بعد از pc- نام کلید می آید(key pair Container)
- exp- قابلیت خروجی گرفتن می دهد (Exportable)

```
aspnet_regiis -pc "MyKeys" -exp
```

سپس اجازه دسترسی به کلید را به کاربر NETWORK SERVICE می دهیم.

```
aspnet_regiis -pa "MyKeys" "NT AUTHORITY\NETWORK SERVICE"
```

سپس در وب کانفیک بالای ConnectionStrings اطلاعات کانفیگ را در بالای آن قرار می دهیم.

```
<configuration>
   <configProtectedData>
      <providers>
         <add name="MyProvider"
              type="System.Configuration.RsaProtectedConfigurationProvider,
System.Configuration, Version=2.0.0.0,
                   Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a,
                   processorArchitecture=MSIL"
              keyContainerName="MyKeys"
              useMachineContainer="true" />
      </providers>
   </configProtectedData>

   <connectionStrings>
      <add name="SqlServices" connectionString="Data Source=localhost;Integrated
Security=SSPI;Initial Catalog=Northwind;" />
   </connectionStrings>
</configuration>
```

سپس با دستور زیر WEBCONFIG را Encrypt می کنیم.

- بعد از pe- نام بخشی از وب کانفیگ که می خواهیم Encrypt شود را می نویسیم.
- با استفاده از pef- بعد از نام بخش آدس فیزیکی فولدر وب کانفیگ را وارد می کنیم.
- با استفاده از prov- نامی که در بخش وب کانفیگ وارد کردیم وارد می کنیم

```
aspnet_regiis -pef "connectionStrings"
"C:\Users\Administrator\source\repos\TestEncryptWebConfig\TestEncryptWebConfig" -prov
"MyProvider"
```

بعد از مشاهده پیغام زیر، بخش مربوطه Encrypt شده است.

```
Encrypting configuration section...
Succeeded!
```

برای اینکه در یک سرور دیگر بتوانیم فایل را Encrypt یا Decrypt کنیم باید فایل مربوط به کلید خصوصی را به سرور دیگر انتقال دهیم.

برای دریافت فایل کلید دستور زیر را اجرا می کنیم.

- بعد از px– نام کلید
- مسیر و نامی که فایل اتقال بیابد
- pri- به معنی اینکه کلید خصوصی را هم در فایل قرار بده

```
aspnet_regiis -px "MyKeys" "c:\keys.xml" -pri
```

فایل ایجاد شده را به سرور دیگر انتقال می دهیم.

دوباره به دایرکتوری میرویم

```
cd \WINDOWS\Microsoft.Net\Framework\v2.0.*
```

و دستور زیر را اجرا میکنیم.

- pi- برای import کردن فایل key استفاده می شود.

```
aspnet_regiis -pi "MyKeys" "c:\keys.xml"
```

دسترسی را دوباره ایجاد میکنیم.

```
aspnet_regiis -pa "MyKeys" "NT AUTHORITY\NETWORK SERVICE"
```

سپس با دستور زیر می توانیم فایل را Decrypt کنیم.

```
aspnet_regiis -pdf "connectionStrings"
"C:\Users\Administrator\source\repos\TestEncryptWebConfig\TestEncryptWebConfig"
```

نکته:

حتما فایل xml. را در سرور ها پاک کنیم.