

BCP – Ejemplos criptografía

Proyectos de encriptación y desencriptación de configuración

Cliente:

BCP

Preparado por:

Gabriel Lopardo – Developer

4-Jun-18

Table of Contents

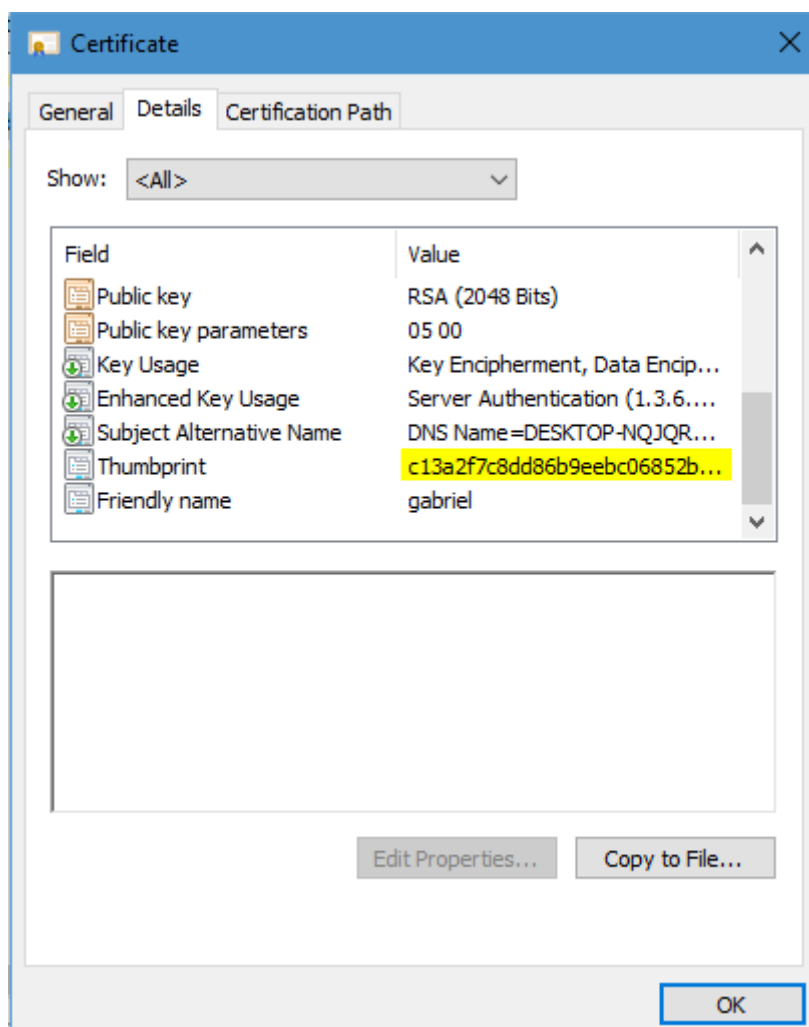
Encriptación y desencriptación de archivos de configuración .json con .ASP NET Core	3
1. Encriptación	3
a. ¿Qué hacer con la información encriptada?	4
2. Desencriptación	5
Encriptación y desencriptación de archivos de configuración web.config	5
1. Encriptación de una sección	6
2. Desencriptación de una sección	6

Encriptación y desencriptación de archivos de configuración .json con .ASP NET Core

En esta solución se pretende ilustrar un caso de encriptación de un archivo de configuración para una aplicación web en .ASP NET Core 2.0 con el agregado de un ConfigurationProvider custom para separar la configuración con datos sensibles en un archivo aparte que no se publica en producción

1. Encriptación

Se debe crear un server certificate (cualquier tipo de certificado) en IIS y copiar su thumbprint, la usaremos para identificar el certificado y posteriormente acceder a sus claves pública y privada.



Para la encriptación se utiliza una aplicación de consola que va a leer dos parámetros (de a uno por vez) para devolverlos en formato .txt con una estructura similar a la de un archivo de configuración .json para facilitar trasladar allí los datos.

El primer parámetro es el **id cliente** que es meramente informativo, ya que esta aplicación permite hacer un ingreso masivo de clientes.

El ingreso de un idCliente vacío finaliza la carga masiva.

El segundo parámetro es la información que queremos encriptar, que en este caso se ingresan 3 **connection strings**.

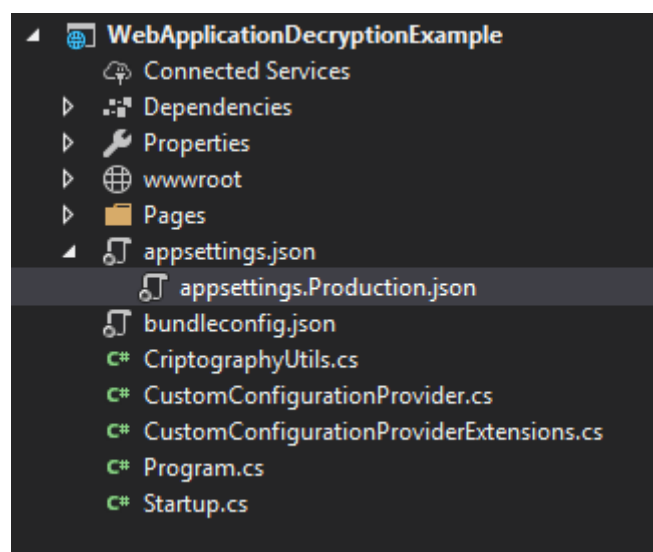
El resultado será un archivo con el siguiente formato:

```
"idCliente_1": "informacionEncriptada_1",
"idCliente_2": "informacionEncriptada_2",
...
"idCliente_n": "informaciónEncriptada_n"
```

Donde informacionEncriptada se representa como un string expresado en base 64, de la data ingresada como segundo parámetro, encriptada utilizando el algoritmo RSA y la clave pública del certificado creado en el primer paso.

a. ¿Qué hacer con la información encriptada?

Primero se debe crear un archivo de configuración en la solución con el nombre appsettings.ENVIRONMENT.json donde ENVIRONMENT va a ser el ambiente correspondiente (development, staging, production) definido en las propiedades del proyecto en la variable de entorno ASPNETCORE_ENVIRONMENT.



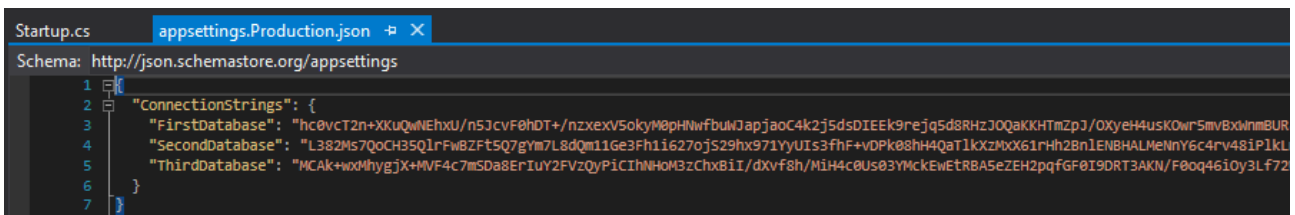
Una vez agregado el archivo (en este caso appsettings.production.json) el mismo se anidará a appsettings.json.

En el constructor de la clase Startup al instanciar un nuevo ConfigurationBuilder se deberá llamar al método custom (AddCustomProvider) que devuelve una instancia de CustomConfigurationBuilder y luego al método de extensión AddJsonFiles que se le pasa como parámetro el nombre del archivo de configuración que vamos a agregar.

```
public Startup(IHostingEnvironment env)
{
    var builder = new ConfigurationBuilder()
        .SetBasePath(env.ContentRootPath)
        .AddJsonFile("appsettings.json", true, true)
        .AddCustomProvider()
        .AddJsonFile($"appsettings.{env.EnvironmentName}.json", true, true);

    _configuration = builder.Build();
}
```

Luego podemos copiar la información que encriptamos con la aplicación (siguiendo el formato correspondiente).



2. Desenscriptación

Se sigue el proceso inverso, esta vez utilizando la clave privada del certificado mencionado anteriormente, se lee el archivo de configuración con la data encriptada, la convertimos en una cadena de bytes y se la pasamos como parámetro al método Decrypt() de la clase CryptographyUtils, quien también nos retorna una cadena de bytes que podremos pasar a un string si así lo deseáramos.

```
var decryptedConnStr1 = Encoding.UTF8.GetString(CryptographyUtils.Decrypt(Convert.FromBase64String(connStr1), _configuration["CertificateThumbPrint"]));
var decryptedConnStr2 = Encoding.UTF8.GetString(CryptographyUtils.Decrypt(Convert.FromBase64String(connStr2), _configuration["CertificateThumbPrint"]));
var decryptedConnStr3 = Encoding.UTF8.GetString(CryptographyUtils.Decrypt(Convert.FromBase64String(connStr3), _configuration["CertificateThumbPrint"]));
```

Encriptación y desenscriptación de archivos de configuración web.config

Para encriptar y desenscriptar un archivo de configuración web.config se debe utilizar la herramienta Aspnet_regiis.exe ubicada en la ruta %windows%\Microsoft.NET\Framework\versionNumber

1. Encriptación de una sección

Se debe ejecutar la aplicación mencionada enviando los siguientes parámetros:

- pe** y el nombre de la sección que se quiere encriptar, por ejemplo *-pe "connectionStrings"*
- app** y el identificador de la aplicación a la que corresponde el web.config a encriptar, por ejemplo *-app "/SampleApplication"*
- site** y el nombre del sitio del cual la aplicación es parte, por ejemplo *-site "2"*.

El numero identificador del sitio se extrae de la metabase de IIS, se encuentra en la variable "INSTANCE_META_PATH" en la colección de variables ServerVariables. Por ejemplo, cuando se instala IIS, se crea automáticamente el sitio "Default Web Site" con el identificador "1" (uno).

- prov** y el nombre del ProtectedConfigurationProvider que va a realizar la encriptación y desencriptación, por ejemplo *-prov "RsaProtectedConfigurationProvider"*

Un comando completo de encriptación para un archivo de configuración Web.config para la aplicación SampleApplication del sitio con el id = "2" usando RsaProtectedConfigurationProvider quedaría como:

```
aspnet_regiis -pe "connectionStrings" -app "/SampleApplication" -site "2" -prov "RsaProtectedConfigurationProvider"
```

Esto genera un Web.config Nuevo con la sección encriptada, el cual hay que copiar reemplazando el Web.config viejo.

2. Desencriptación de una sección

Para desencriptar un archive de configuración Web.config también se utiliza la aplicación aspnet_regiis con los siguientes parámetros

- pd** y el nombre de la sección a desencriptar, por ejemplo *-pd "connectionStrings"*
- app** igual que en la encriptación.
- site** igual que en la encriptación

En este caso no es necesario el parámetro -prov ya que éste lo lee de la sección configProtectionProvider.

Un comando completo de desencriptación para el archivo encriptado en el paso anterior quedaría:

```
aspnet_regiis -pd "connectionString" -app "/SampleApplication" -site "2"
```

Fuente: <https://msdn.microsoft.com/en-us/library/zhddkxy.aspx>