

Re: RSACryptoServiceProvider Exception in DLL beim aufräumen durch GC

Source:

<http://www.tech-archive.net/Archive/German/Entwicklung/microsoft.public.de.german.entwickler.dotnet.csharp/2007>

- *From:* Thomas Östreich <no@xxxxxxxx>
 - *Date:* Mon, 15 Oct 2007 10:47:34 +0200
-

habe eine Problem mit dem RSACryptoServiceProvider. Sobald der GC Objekt aus dem Speicher entfernt wird so nach 10 min Inaktivität stürzt die Anwendung bzw irgend eine andere Security Anwendung (HP) ab.

Problem ist Stack Corruption von "OLEAUT32" (ACCESS_VIOLATION_OLEAUT32) beim entladen.

Konnte das Problem jetzt soweit ermitteln das der Fehler von RSACryptoServiceProvider kommt. Im SystemLog ".NET Runtime 2.0 Error"

Gehe davon aus das es an der HP-Software liegt, da sie sich in den Kontext reinhängt und sich nicht bei Zerstörung der Instanze bereinigt wahrscheinlich auf die Anwendung ein Hook hat (Erweitert Fenster welche Sicherheit benötigen um weiters System Icon auf der rechten Seite). Denn wenn ich die Funktion im MainThread ausführe, wo sie erst bei schließen der Anwendung vom GC entfernt wird läuft alles ohne Probleme.

[HP ProtectTools Security Manager]

Der RSACryptoServiceProvider läuft in einen Background Thread und sobald der Thread komplett bereinigt wird stürzt die Anwendung mit Speicher Fehler ab :(.

Der Code überprüft nur die Gültigkeit einer Signatur.

```
private bool IsValid()
{
    // Besitzt erweiterte Headerinformationen
    byte[] publicKeyAssembly =
    Assembly.GetExecutingAssembly().GetName().GetPublicKey();
    int size = publicKeyAssembly.Length - 12;
    // Key für CspProvider
    byte[] publicKey = new byte[size];
    Buffer.BlockCopy(publicKeyAssembly, 12, publicKey, 0, size);

    using (RSACryptoServiceProvider rsa = new RSACryptoServiceProvider())
    {
```

Re: RSACryptoServiceProvider Exception in DLL beim aufräumen durch GC

```
using (SHA1Managed sh1 = new SHA1Managed())  
{  
    rsa.ImportCspBlob(publicKey);  
    byte[] btHash = sh1.ComputeHash(MachineName);
```

Diese Zeile verursacht nach ca. 10 min nach Beendigung des Threads den Anwendungsabsturz:

```
bool ret = rsa.VerifyHash(btHash, CryptoConfig.MapNameToOID("SHA1"), _signHash);
```

```
    sh1.Clear();  
    rsa.Clear();  
    return ret;  
}  
}  
}
```