Erstellen sicherer ASP.NET-Anwendungen

Authentifizierung, Autorisierung und sichere Kommunikation

Auf der Orientierungsseite finden Sie einen Ausgangspunkt und eine vollständige Übersicht zum *Erstellen sicherer ASP.NET-Anwendungen*.

Zusammenfassung

Um die Integrität und Vertraulichkeit von Nachrichten zu garantieren, die an einen Webdienst übergeben und von diesem übertragen werden, kann SSL (Secure Sockets Layer) verwendet werden. In dieser Vorgehensweise wird erläutert, wie SSL in Verbindung mit Webdiensten verwendet wird.

Vorgehensweise: Aufrufen eines Webdienstes unter Verwendung von SSL

Sie können einen Webdienst so konfigurieren, dass SSL (Secure Sockets Layer) gefordert wird, um die vertraulichen Daten zu schützen, die zwischen einem Client und dem Dienst ausgetauscht werden. SSL bietet folgende Vorteile:

- **Integrität von Nachrichten –** Hiermit wird sichergestellt, dass Nachrichten bei der Übertragung nicht geändert werden.
- **Vertraulichkeit von Nachrichten –** Hiermit wird die Vertraulichkeit der Nachrichten während der Übertragung sichergestellt.

In dieser Vorgehensweise wird erläutert, wie ein Webdienst für die Verwendung von SSL konfiguriert und wie ein Webdienst von einer ASP.NET-Clientanwendung unter Verwendung des HTTPS-Protokolls aufgerufen wird.

Hinweis: Die Informationen in dieser Vorgehensweise gelten auch für Remoteobjekte, für die ASP.NET und IIS (unter Verwendung der .NET Remoting-Technologie) als Host fungieren. Informationen über die Erstellung einer Remotekomponente, für die IIS als Host fungiert, finden Sie in der Microsoft Knowledge Base im Artikel Q312107, "HOW TO: Host a Remote Object in Microsoft Internet Information Services" (US).

Anforderungen

Im Folgenden finden Sie eine Liste der empfohlenen Hardware und Software und eine Beschreibung der Netzwerkinfrastruktur, der Fähigkeiten und Kenntnisse sowie der Service Packs, die Sie benötigen:

- Microsoft® Windows® 2000 Server als Betriebssystem
- Microsoft Visual Studio® .NET als Entwicklungssystem
- Einen Webserver mit einem installierten Serverzertifikat
  Weitere Informationen über das Installieren von Webserverzertifikaten finden Sie unter "Vorgehensweise. Einrichten von SSL auf einem Webserver".

Die in dieser Vorgehensweise erläuterten Verfahren setzen zudem Kenntnisse der ASP.NET-Webentwicklung mit dem Entwicklungstool Microsoft Visual C#™ voraus.

Zusammenfassung

Diese Vorgehensweise enthält folgende Verfahren:

1. Erstellen eines einfachen Webdienstes
2. Konfigurieren des virtuellen Verzeichnisses des Webdienstes für die Verwendung von SSL
3. Testen des Webdienstes mit einem Browser
4. Installieren des Zertifikats der Zertifizierungsstelle auf dem Clientcomputer
5. Entwickeln einer Webanwendung zum Aufrufen der Serviced Component

1. Erstellen eines einfachen Webdienstes

▶ **So erstellen Sie einen einfachen Webdienst auf dem Webdienst-Hostcomputer**

1. Starten Sie Visual Studio .NET, und erstellen Sie mit C# eine neue ASP.NET-Webdienstanwendung mit Namen **SecureMath**.
2. Benennen Sie den Dienst **Service1.asmx** in **Math.asmx** um.
3. Öffnen Sie **Math.asmx.cs**, und benennen Sie die Klasse **Service1** in **math** um.
4. Fügen Sie der **math**-Klasse die folgende **Web**-Methode hinzu.

```
[WebMethod]
public long Add(long operand1, long operand2)
{
    return (operand1 + operand2);
}
```

5. Zum Erstellen des Webdienstes klicken Sie im Menü **Erstellen** auf **Projektmappe erstellen**.

2. Konfigurieren des virtuellen Verzeichnisses des Webdienstes für die Verwendung von SSL

Der Webdienst wird unter IIS (Internet-Informationsdienste) ausgeführt und setzt auf IIS auf, um SSL-Unterstützung bereitzustellen.

Das Verfahren setzt voraus, dass auf dem Webserver ein gültiges Serverzertifikat installiert ist. Weitere Informationen über das Installieren von Webserverzertifikaten finden Sie unter "Vorgehensweise. Einrichten von SSL auf einem Webserver".

▶ **So konfigurieren Sie das virtuelle Verzeichnis des Webdienstes mit IIS für SSL**

1. Starten Sie IIS auf dem Webdienst-Hostcomputer.
2. Wechseln Sie zum virtuellen Verzeichnis **SecureMath**.
3. Klicken Sie mit der rechten Maustaste auf **SecureMath**, und klicken Sie dann auf **Eigenschaften**.
4. Klicken Sie auf die Registerkarte **Verzeichnissicherheit**.

5. Klicken Sie unter **Sichere Kommunikation** auf **Bearbeiten**.
   Wenn der Befehl **Bearbeiten** nicht zur Verfügung steht, ist wahrscheinlich kein Webserverzertifikat installiert.
6. Aktivieren Sie das Kontrollkästchen **Sicheren Kanal verlangen (SSL)**.
7. Klicken Sie auf **OK** und dann noch einmal auf **OK**.
8. Klicken Sie im Dialogfeld **Vererbungsüberschreibungen** auf **Alles auswählen**, und klicken Sie dann auf **OK**, um das Eigenschaftendialogfeld von **SecureMath** zu schließen.
   Hiermit werden die neuen Sicherheitseinstellungen allen Unterverzeichnissen im virtuellen Stammverzeichnis zugewiesen.

3. Testen des Webdienstes mit einem Browser

Mit diesem Verfahren vergewissern Sie sich, dass das Webserverzertifikat gültig ist und von einer Zertifizierungsstelle (Certification Authority, CA) ausgegeben wurde, die seitens des Clientcomputers als vertrauenswürdig eingestuft wird.

▶ **So rufen Sie den Webdienst unter Verwendung von SSL in Internet Explorer auf**

1. Starten Sie Internet Explorer auf dem Clientcomputer, und navigieren Sie (unter Verwendung von HTTPS) zum Webdienst. Beispiel:

   ```
   https://WebServer/securemath/math.asmx
   ```

   Die Webdienst-Testseite sollte im Browser angezeigt werden.
2. Wenn die Webdienst-Testseite erfolgreich angezeigt wurde, schließen Sie Internet Explorer und fahren mit Verfahren 5, "Entwickeln einer Webanwendung zum Aufrufen der Serviced Component", fort.
3. Wenn das in Abbildung 1 dargestellte Dialogfeld **Sicherheitshinweis** angezeigt wird, klicken Sie auf **Zertifikat anzeigen**, um die Identität der ausgebenden Zertifizierungsstelle des Webserverzertifikats anzuzeigen. Sie müssen das Zertifizierungsstellenzertifikat auf dem Clientcomputer installieren. Die entsprechende Vorgehensweise ist in Verfahren 4, "Installieren des Zertifizierungsstellenzertifikats auf dem Clientcomputer", erläutert.
4. Schließen Sie Internet Explorer.

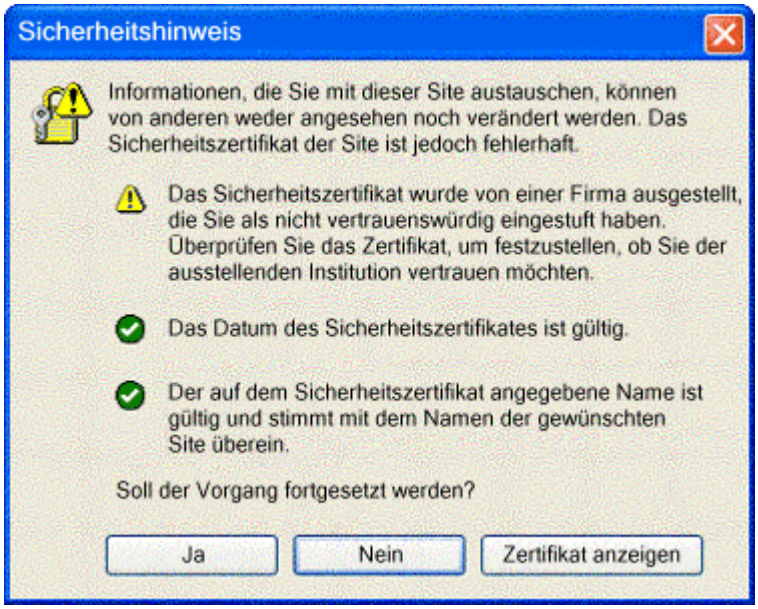

Abbildung 1
Dialogfeld "Security Alert" (Sicherheitshinweis)

4. Installieren des Zertifizierungsstellenzertifikats auf dem Clientcomputer

Mit diesem Verfahren wird das Zertifikat der ausgebenden Zertifizierungsstelle als vertrauter Stammzertifizierungsstelle auf dem lokalen Computer installiert wird. Der Clientcomputer muss der ausgebenden Zertifizierungsstelle vertrauen, damit das Serverzertifikat akzeptiert und das Dialogfeld **Sicherheitshinweis** nicht angezeigt wird.

▶ **Wenn Sie die Microsoft Zertifikatdienste als Zertifizierungsstelle in der Windows-Domäne verwenden**

Führen Sie dieses Verfahren nur durch, wenn das Webserverzertifikat von einer Microsoft Zertifikatdienste-Zertifizierungsstelle ausgegeben wurde. Sofern Sie andernfalls über die CER-Datei der Zertifizierungsstelle verfügen, fahren Sie mit Schritt 8 fort.

1. Starten Sie Internet Explorer, und navigieren Sie zu **http://***Hostname***/certsrv**, wobei *Hostname* für den Namen des Computers steht, auf dem sich die Microsoft Zertifikatdienste befinden, die das Serverzertifikat ausgegeben haben.
2. Klicken Sie auf **Zertifizierungsstellenzertifikat oder Zertifikatsperrliste abrufen**, und klicken Sie dann auf **Weiter**.
3. Klicken Sie auf **Diesen Zertifizierungsstellen-Zertifikatspfad installieren**.
4. Klicken Sie im Dialogfeld **Stammzertifikatspeicher** auf **Ja**.
5. Navigieren Sie unter Verwendung von HTTPS zum Webdienst. Beispiel:

   ```
   https://WebServer/securemath/math.asmx
   ```

   Die Webdienst-Testseite sollte nun korrekt und ohne Anzeige des Dialogfeldes **Security Alert** (**Sicherheitshinweis**) im Browser angezeigt werden.

   Sie haben nun das Zertifizierungsstellenzertifikat in Ihrem persönlichen Speicher für vertrauenswürdige Stammzertifikate installiert. Um den Webdienst von einer ASP.NET-Seite erfolgreich aufrufen zu können, müssen Sie das Zertifizierungsstellenzertifikat auch im Speicher für vertrauenswürdige Stammzertifikate des Computers installieren.
6. Wiederholen Sie die Schritte 1 und 2, klicken Sie auf **Download des Zertifizierungsstellenzertifikats**, und speichern Sie es in einer Datei auf dem lokalen Computer.
7. Führen Sie nun die noch verbleibenden Schritte durch.

Wenn Sie über die CER-Zertifikatdatei der Zertifizierungsstelle verfügen

8. Klicken Sie auf der Taskleiste auf **Start** und dann auf **Ausführen**.
9. Geben Sie **mmc** ein, und klicken Sie auf **OK**.
10. Klicken Sie im Menü **Datei** auf **Snap-In hinzufügen/entfernen**.
11. Klicken Sie auf **Hinzufügen**.
12. Klicken Sie auf **Zertifikate** und dann auf **Hinzufügen**.
13. Klicken Sie auf **Computerkonto** und dann auf **Weiter**.
14. Klicken Sie auf **Lokaler Computer (Computer, auf dem diese Konsole ausgeführt wird)** und dann auf **Fertig stellen**.
15. Klicken Sie auf **Schließen** und dann auf **OK**.
16. Erweitern Sie im linken Fensterbereich des MMC-Snap-Ins den Eintrag **Zertifikate (Lokaler Computer)**.
17. Erweitern Sie **Vertrauenswürdige Stammzertifizierungsstellen**.
18. Klicken Sie mit der rechten Maustaste auf **Zertifikate**, zeigen Sie auf **Alle Tasks**, und klicken Sie auf **Importieren**.
19. Klicken Sie auf **Weiter**, um den Begrüßungsdialog des Zertifikatimport-Assistenten zu schließen.
20. Geben Sie den Pfad und den Dateinamen der CER-Datei der Zertifizierungsstelle ein.

21. Klicken Sie auf **Weiter**.
22. Wählen Sie **Alle Zertifikate in folgendem Speicher speichern**, und klicken Sie dann auf **Weiter**.
23. Wählen Sie **Physikalischen Speicher anzeigen**.
24. Erweitern Sie in der Liste den Eintrag **Vertrauenswürdige Stammzertifizierungsstellen**, und wählen Sie dann **Lokaler Computer**.
25. Klicken Sie auf **OK**, klicken Sie auf **Weiter**, und klicken Sie dann auf **Fertig stellen**.
26. Klicken Sie auf **OK**, um das Bestätigungsdialogfeld zu schließen.
27. Aktualisieren Sie die Ansicht des Ordners **Zertifikate** im MMC-Snap-In, und vergewissern Sie sich, dass das Zertifizierungsstellenzertifikat in der Liste aufgeführt wird.
28. Schließen Sie das MMC-Snap-In.

5. Entwickeln einer Webanwendung zum Aufrufen des Webdienstes

Mit diesem Verfahren wird eine einfache ASP.NET-Webanwendung erstellt. Sie verwenden diese ASP.NET-Webanwendung als Clientanwendung zum Aufrufen des Webdienstes.

▶ **So erstellen Sie eine einfache ASP.NET-Webanwendung**

1. Erstellen Sie auf dem Webdienst-Clientcomputer mit C# eine neue ASP.NET-Webanwendung mit Namen **SecureMathClient**.
2. Fügen Sie dem Webdienst einen Webverweis (unter Verwendung von HTTPS) hinzu.
   a. Klicken Sie im Projektmappen-Explorer mit der rechten Maustaste auf den Knoten **Verweise**, und klicken Sie dann auf **Webverweis hinzufügen**.
   b. Geben Sie im Dialogfeld **Webverweis hinzufügen** den URL Ihres Webdienstes ein. Verwenden Sie unbedingt einen HTTPS-URL.

   Hinweis: Wenn Sie bereits einen Webverweis auf einen Webdienst ohne Verwendung von HTTPS erstellt haben, können Sie die hiermit erzeugte Proxyklassendatei manuell bearbeiten und in der entsprechenden Codezeile die **Url**-Eigenschaft von einem HTTP-URL in einen HTTPS-URL ändern.

   c. Klicken Sie auf **Verweis hinzufügen**.
3. Öffnen Sie **WebForm1.aspx.cs**, und fügen Sie unterhalb der vorhandenen **using**-Anweisungen die folgende **using**-Anweisung hinzu.

```
using SecureMathClient.WebReference1;
```

4. Zeigen Sie **WebForm1.aspx** im Entwurfsmodus an, und erstellen Sie ein Formular ähnlich des in Abbildung 2 gezeigten unter Verwendung der folgenden IDs:
   - operand1
   - operand2
   - result
   - add

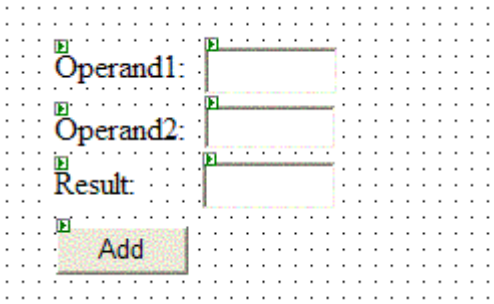

Abbildung 2
Formular "WebForm1.aspx"

5 Doppelklicken Sie auf die Schaltfläche **Add**, um einen Ereignishandler für das Klickereignis der Schaltfläche zu erstellen.

6. Fügen Sie dem Ereignishandler den folgenden Code hinzu.

```
private void add_Click(object sender, System.EventArgs e)
{
  math mathService = new math();
  int addResult = (int) mathService.Add( Int32.Parse(operand1.Text),
                                         Int32.Parse(operand2.Text));
  result.Text = addResult.ToString();
}
```

7. Klicken Sie im Menü **Erstellen** auf **Projektmappe erstellen**.
8. Führen Sie die Anwendung aus. Geben Sie zwei Zahlen ein, die addiert werden sollen, und klicken Sie dann auf die Schaltfläche **Add**.
   Die Webanwendung ruft nun den Webdienst unter Verwendung von SSL auf.

Weitere Ressourcen

- "Q312107 "HOW TO: Host a Remote Object in Microsoft Internet Information Services" in der Microsoft Knowledge Base"
- "Vorgehensweise: Einrichten von SSL auf einem Webserver"
- "Vorgehensweise: Aufrufen eines Webdienstes mit Clientzertifikaten von ASP.NET"