Lab: Extended Validation Zertifikat für Webserver:

Ziel: Installation eine EV-Zertifikates auf einem IIS und prüfen der „grünen“ Adressleiste

Voraussetzung:
- einstufige Zertifizierungsstelle unter 2008 R2 / Active Directory-Umgebung
- Webserver unter Windows Server 2008 oder höher
- Internet Explorer 7 oder höher

---

1. Vorbereiten der Zertifikatvorlage

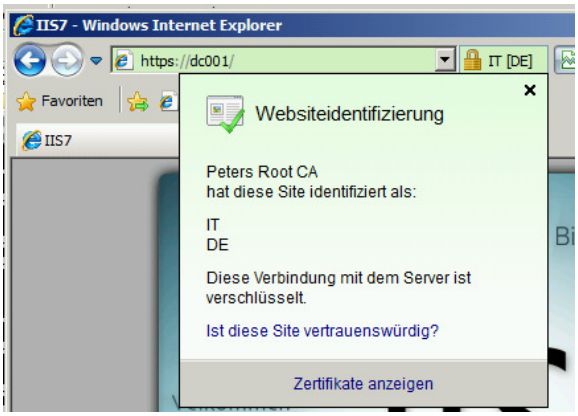
a. Wechsele auf die Zertifizierungsstelle und öffne die Zertifizierungsstellen-MMC
b. Rechtsklick auf Zertifikatvorlagen → Verwalten
c. Rechtsklick auf Webserver → Doppelte Vorlage → Windows Server 2003 Enterprise
d. Benenne die Vorlage (Extended Validation Webserver) und passe – wenn gewünscht – Laufzeit und weitere Parameter an (Sicherheit: Webserver → Lesen + Registrieren).
e. Wähle die Registerkarte Erweiterungen und klicke auf Ausstellungsrichtlinien → Bearbeiten
f. Klicke auf Hinzufügen → Neu
g. Gebe im Feld „Neue Ausstellungsrichtlinie“ einen Namen für die Objektkennung an (Contoso Extended Validation) und kopiere die Objektkennung in die Zwischenablage.
h. Klicke auf OK und nochmals auf OK
i. Prüfe, dass die Ausstellungsrichtlinie in der Liste „Ausstellungsrichtlinien“ aufgeführt ist.
j. Klicke zweimal auf OK, so dass die Eigenschaften der neuen Vorlage geschlossen wird.
k. Schließe die Konsole Zertifikatvorlagen
l. Wechsele wieder zur Zertifizierungsstellen-MMC → rechtsklick auf Zertifikatvorlagen →Neu → Auszustellende Zertifikatvorlagen → wähle die Vorlage aus Punkt 1.d aus.
m. Exportiere das CA-Zertifikat rechtklick auf CA → Eigenschaften → Allgemein → Zertifikat anzeigen → Details → In Datei kopieren → und speichere die Datei mit den Standardeinstellungen als .cer-Datei.

2. Verteilen der EV-OID

a. Öffne die Gruppenrichtlinienverwaltungskonsole
b. Erstelle eine GPO oder bearbeite die Default Domain Policy
c. Computerkonfiguration → Richtlinien → Windows-Einstellungen → Sicherheitseinstellungen → Richtlinien für öffentliche Schlüssel → Vertrauenswürdige Stammzertifizierungsstellen
d. Wird hier die Root-CA nicht gelistet installiere das Zertifikat, das unter 1.m exportiert wurde.
e. Rechtsklick auf dem Root-CA-Zertifikat in der Policy → Eigenschaften → Erweiterte Überprüfung
f. Füge nun die OID aus Punkt 1.g hinzu und klicke nach „OID hinzufügen“ auf OK.
g. Schließe die Gruppenrichtlinienverwaltungskonsole
h. Wechsele auf den Computer, von dem zugegriffen werden soll und führe ein gpupdate /force aus
i. Öffne die Zertifikat-MMC (certmgr.msc) und prüfe, ob die OID verteilt wurde (Vertrauenswürdige Zertifizierungsstellen → Zertifikate → Root-CA → rechte Maustaste → Eigenschaften → Erweiterte Überprüfung.
   Hinweis: Sollte die OID nicht per GPO verteilt werden, kann sie an dieser Stelle auf lokal eingetragen werden.

3. **Installation des Webserver-Zertifikates**
    a. Öffne auf dem Webserver eine MMC → Snap-In hinzufügen → Zertifikate → Computerkonto → lokaler Computer → OK
    b. Zertifikate → Eigene Zertifikate → rechte Maustaste auf Eigene Zertifikate → Alle Aufgaben → neues Zertifikat anfordern
    c. Klicke durch den Assistenten und wähle die Zertifikatvorlage aus 1 aus.
    d. Beachte den Hinweis, dass weitere Optionen benötigt werden. Klicke auf „Es werden zusätzliche ..:“
    e. Allgemeiner Name : Hostheader des IIS
    f. Land : DE
    g. Organisation : IT
    h. Klicke anschließend auf Registrieren und fordere das Zertifikat an.
    i. Öffne die IIS-Konsole → Sites → Website auswählen → rechtklick auf der Website → Bindungen bearbeiten
    j. Wenn keine https-Bindung vorhanden ist klicke auf Hinzufügen (ansonsten wähle die https-Bindung aus und wähle bearbeiten)
    k. Bindung → https → wähle als SSL-Zertifikat das unter 3.b angeforderte Zertifikat aus.
    l. Klicke auf OK und schließen.

4. **Prüfen des Clients**
    a. Wechsele nun auf einen Computer mit Internet Explorer (kann auch der Webserver sein)
    b. Starte den Internet Explorer und prüfe die Adressleiste.
    c. Wenn alles richtig konfiguriert wurde, wird die Adressleiste grün.
    d. Klicke auf das „Schloss“ und schau die die Extended Validation an.



5. Troubleshooting
    a. Die Adressleiste wird rot und es wird eine Zertifikatwarnung angezeigt
        i. Stimmt „Ausgestellt für“ mit der Adresse im IE überein?
        ii. Ist das Root-Zertifikat vertrauenswürdig?
    b. Die Adressleiste bleibt weiß
        i. Prüfe auf dem Computer mit IE, ob die OID im RootCA-Zertifikat eingetragen ist (2.i)