IT Services IT

Zertifizierung von Hochschulservern

Die Serverzertifikate werden von einer vertrauenswürdigen Instanz ausgestellt, die es Benutzern ermöglicht die Authentizität der Server zu verifizieren.

Für den Prozeß der Beantragung wenden Sie sich zwecks Unterstützung an Ihre Fachbereichs-IT. Handelt es sich um zentrale Server kann auch das Rechenzentrum unterstützen.

Der Prozeß zum Erhalt eines Server - Zertifikats sieht wie folgt aus:

1. Zertifikats - Signierungsanfrage (CSR) erstellen
2. Zertifikat beantragen
3. RA im Rechenzentrum prüft den Antrag
4. RA im Rechenzentrum genehmigt den Antrag
5. Zertifikat wird an den Antragsteller per E-Mail versendet
6. Antragsteller installiert Zertifikat im Server

Voraussetzung für die Ausstellung von Serverzertifikaten ist die Domainvalidierung. Die Domain th-brandenburg.de ist validiert. Sollen Serverzertifikate für anderer Domains der THB beantragt werden, so muss zunächst die Domain validiert werden. Eine Domain, die noch nicht validiert ist, verursacht bei der Zertifikats - Antragstellung einen Fehler. Bitte beantragen Sie vor der Antragsstellung die Domainvaldierung und senden uns dazu eine E-Mail.

Sie als Antragsteller und Inhaber eines Zertifikates akzeptieren die Nutzungsbedingungen und verpflichten sich zur Einhaltung.

Nutzungsbedingungen TCS Sectigo

Verfahren Sie nun laut Prozeß wie folgt:

1. Zertifikats - Signierungsanfrage (CSR) erstellen

Sie erstellen einen Certificate Signing Request (CSR). Bei dem Vorgang wird der private Schlüssel generiert, den Sie am Ende zusammen mit dem signierten öffentlichen Schlüssel für die Installation benötigen. Desweiteren wird der CSR erstellt. Dieser wird für den folgenden eigentlichen Zertifikatsantrag benötigt.

Die Erstellung eines CSR erfolgt mit openssl. Laden Sie sich dazu folgende vorbereitete

Konfigurationsdatei thb-ca.cnf herunter. Diese Datei enthält schon Festlegungen für unsere Organisation, die nicht mehr von Ihnen eingetragen werden müssen.

Soll das Zertifkat nur einen Namen enthalten, kann die datei ohne Anpassung verwendet werden. Sind zustätzliche Namen notwendig, öffnen und editieren Sie die Datei wie folgt:

1. Kommentarzeichen (#) vor subjectAltName entfernen
2. DNS.1, DNS.2 usw. die zusätzlichen Namen eintragen
3. Datei speichern

Das erstellen des CSR erfolgt mit dem Kommando openssl. Als Parameter werden die Konfigurationsdatei und Dateinamen für den privaten Schlüssel und den eigentlichen Request für die Antragsstellung benötigt. Nach dem Aufruf des Programmes können alle Fragen bis auf die Eingabe eines Common Name und eines Passwortes für den Schutz des privaten Schlüssels, welches Sie sich bestenfalls in einem KeePass hinterlegen, mit ENTER bestätigt werden. Der Aufruf könnte exemplarisch wie folgt sein:

openssl req -config thb-ca.cnf -new -keyout server-key.pem -out server-req.pem

Sie können den erstellten CSR mit folgenden Kommando überprüfen und bei falschen Einträgen mit dem obigen Kommando jederzeit neu genieren. Entscheinend ist, dass Sie den erzeugten privaten Schlüssel und das Passwort sichern und gut aufbewahren um später das Zertifkat zu installieren.

openssl req -text -noout -verify -in server-req.pem -inform PEM

Die Datei server-req.pem ist die Datei, die Sie nun für "Zertifikat beantragen" benötigen.

2. Zertifikat beantragen

Übergeben Sie das CSR Ihrer zuständigen IT - Abteilung bzw. benutzen entsprechend Ihrer Berechtigung das folgende Online - Formular:

THB Zertifikatsantrag

Es sind einige Punkte bei der Bearbeitung zu beachten.

1. Obiger Link öffnet ein neues Fenster. Wählen Sie "Your Institution" und geben "Brandenburg" ein. Unter den Treffern wählen Sie th-brandenburg.de aus.
2. Es erfolgt eine Weiterleitung zum IdP der THB. Dort melden Sie sich an und werden weitergeleitet zum "Sectigo Certificate Manager". Der Aufbau der Seite dauert einen Moment! Nicht die Geduld verlieren.
3. Wählen Sie unter "Select Enrollment Account" den Eintrag "THB" aus und klicken "Next".
4. Organization, Department und Email sind vorausgefüllt. Certifikate Profile "OV Multi Domain" wählen. Nichts anderes! Certifikate Term ist 1 Jahr. Über "Upload CSR" laden Sie Ihren Request hoch.
5. Common Name wird aus dem CSR automatisch gelesen. Subject Alternative Names werden auch aus dem CSR ausgelesen und können aber auch noch ergänzt/verändert

werden. External Requester tragen Sie gerne eine weitere Email ein, die zusätzlich zur oben erwähnten Email, die Zertifikatsinformationen erhalten soll. Dies betrifft auch Erinnerungs-E-Mails vor Ablauf des Zertifikates. Unter Comments können Sie Kommentare für das RA-Team hinterlassen.

6. Klick auf "Submit" versendet den Antrag, erstellt eine Übersicht und generiert eine E-Mail mit dem Betreff "Awaiting Approval". Mit der E-Mail wird die Übermittlung und warten auf Bearbeitung zusätzlich bestätigt.

3. RA im Rechenzentrum prüft den Antrag

Es werden die Angaben und die Berechtigung überprüft.

4. RA im Rechenzentrum genehmigt den Antrag

Der Antrag wird bei positiver Prüfung genehmigt. Anderfalls erfolgt eine Rückmeldung an den Antragsteller.

5. Zertifikat wird an den Antragsteller per E-Mail versendet

Die E-mail enthält Links zum Download für verschiedene Zertifkats-Formate. Es kann mehrfach und auch verschiedene oder alle Formate heruntergeladen werden. Die E-Mail kommt unsigniert von Sectigo!

6. Antragsteller installiert Zertifikat im Server

Je nach Servertyp sind die Zertifkate entsprechend zu installieren. Die notwendigen Wurzel- und CA-Zertifkate von TCS finden Sie hier.