ECOS Appliances

OCSP einrichten

Admin-Tutorial

Version: 2.0

Datum: 11/2022

IT-Security Solutions

Made in Germany

ECOS TECHNOLOGY GMBH | Sant' Ambrogio-Ring 13 a-b | D-55276 Oppenheim | Tel: +49 6133 939-0 | Fax: +49 6133 939-333

OCSP einrichten

ECOS Appliances können für die Prüfung von gesperrten Zertifikaten das Online Certificate Status Protocol (OCSP) anbieten. Dazu muss der dazugehörige Dienst auf der ECOS Appliance angelegt und konfiguriert werden.

1 Zertifikat erstellen

Für die Nutzung des OCSP wird ein Zertifikat benötigt.

Legen Sie dazu ein **X.509-Zertifikat** im **Container: Zertifikate** an. Möchten Sie mit dem OCSP-Dienst die Zertifikate von mehreren CAs prüfen, fassen Sie die OCSP-Zertifikate in einem eigenen Container zusammen. Beachten Sie auch, dass für jede CA ein eigenes OCSP-Zertifikat benötigt wird.

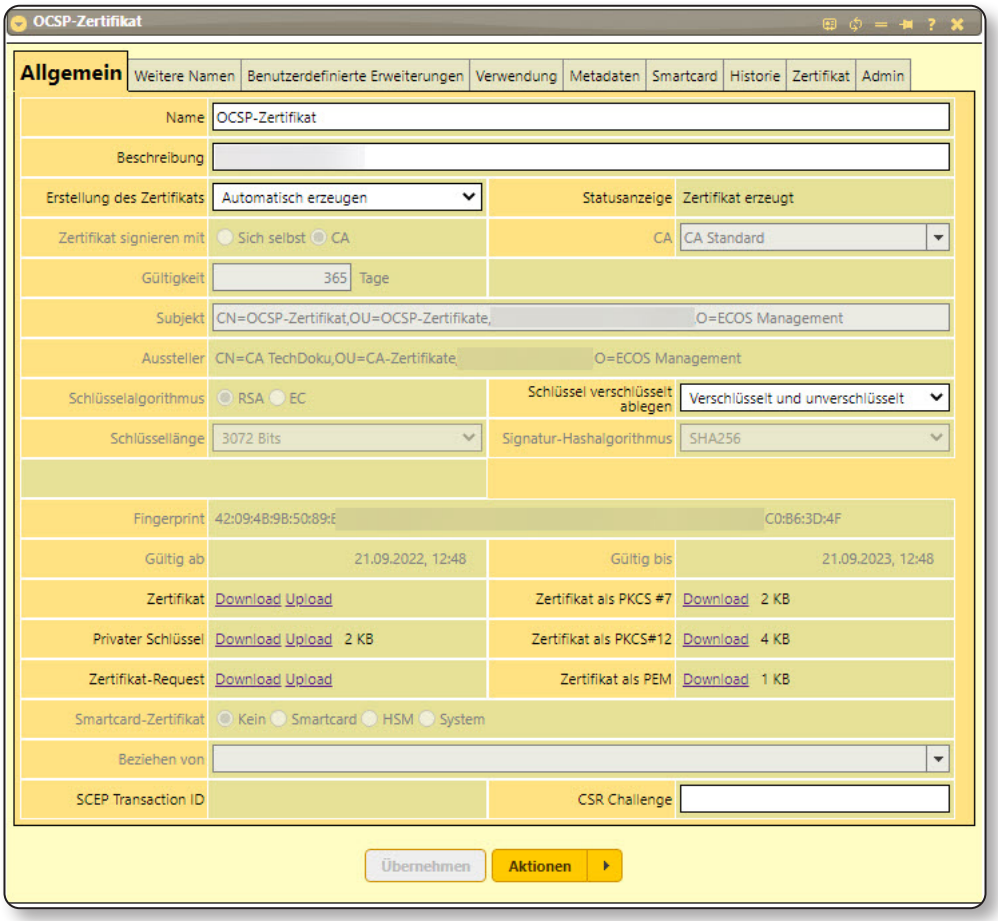

Abb. 1.01: *Einstellungen OCSP-Zertifikat - Reiter Allgemein*

Allgemein

- Name: Vergeben Sie einen aussagekräftigen Namen.
- Erstellung des Zertifikats: **Automatisch erzeugen**
- Zertifikat signieren mit: **CA**
- CA: Wählen Sie die CA aus.
- Schlüsselalgorithmus: **RSA**
- Schlüssellänge: **3072 Bits** (oder höher)

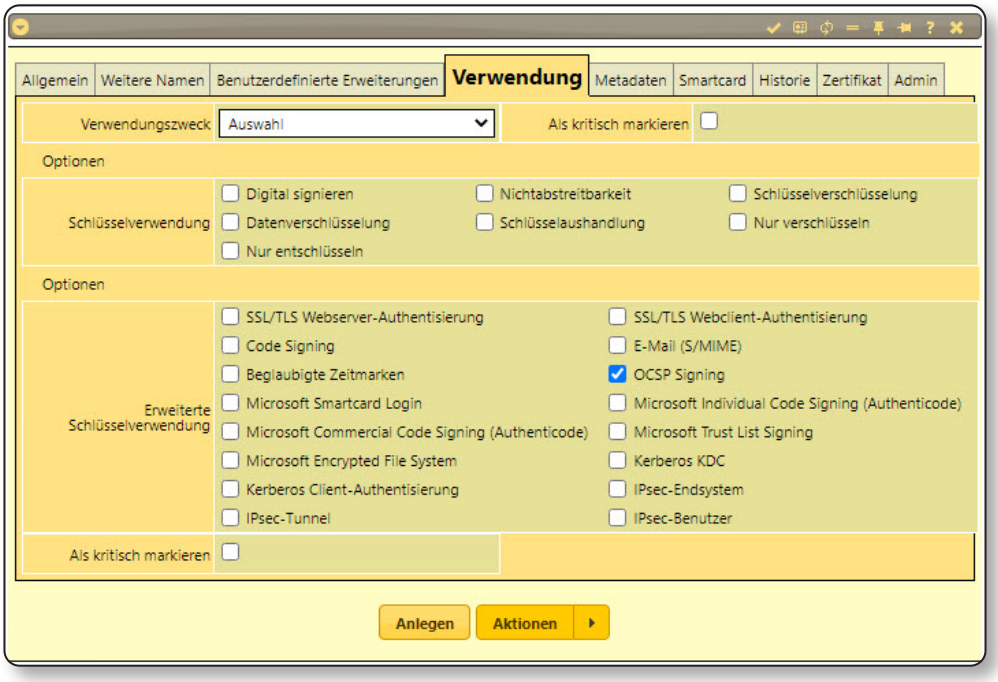

Abb. 1.02: *Einstellungen OCSP-Zertifikat - Reiter Verwendung*

Verwendung

- Verwendungszweck: **Auswahl**
- Erweiterte Schlüsselverwendung:
  - OCSP-Signing: Aktivieren Sie die Checkbox.

Erzeugen Sie das Zertifikat über den Button **Anlegen**. Laden Sie anschließend das Zertifikat als PEM herunter.

2 Dienst: OCSP-Server einrichten

Navigieren Sie im Navigationsbaum der ECOS Appliance zum **Container: Dienste** und dort zu **Dienst: OCSP-Server**. Sollte der Dienst noch nicht vorhanden sein, legen Sie ihn neu an.

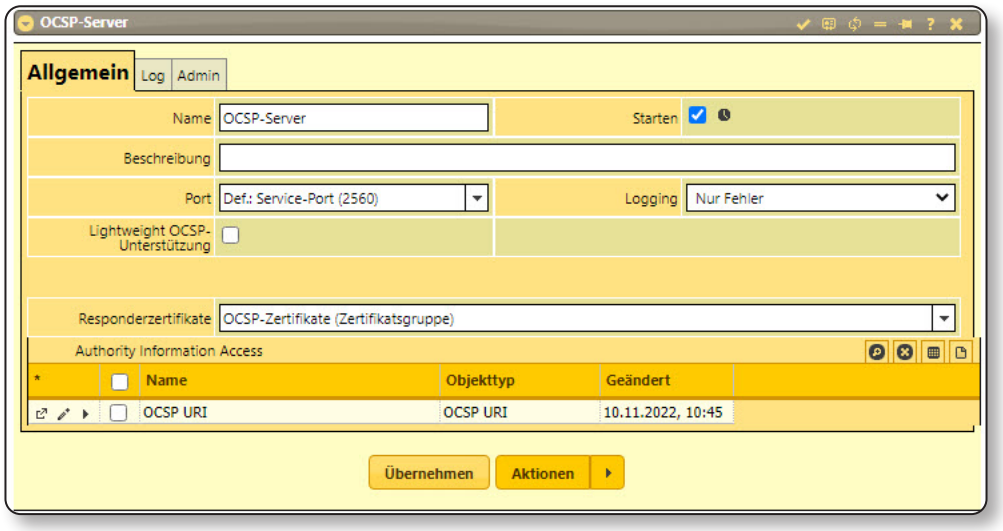

Abb. 1.03: *Einrichtung des Dienst: OCSP-Server*

Allgemein

- NAME: Vergeben Sie einen aussagekräftigen Namen.
- STARTEN: Aktivieren Sie die Checkbox.
- PORT: Tragen Sie den Port ein. Der Standard-Port ist **2560**.
- RESPONDERZERTIFIKAT: Wählen Sie in der Dropdown-Liste das unter Punkt ❶ erstellte Zertifikat oder die Zertifikatgruppe, in der das erstellte Zertifikat enthalten ist, aus.

Speichern Sie die Änderungen mit **Übernehmen** oder **Anlegen**.

3 OCSP URI-Objekt für die CA einrichten

Für die Nutzung von OCSP wird ein **OCSP URI**-Objekt benötigt, das einer oder mehreren CAs zugewiesen werden kann.

Legen Sie ein **OCSP URI**-Objekt an. Sie finden es mit Rechtsklick auf das Organisationsobjekt ganz oben im Navigationsbaum unter **Container: PKI-Einstellungen**.

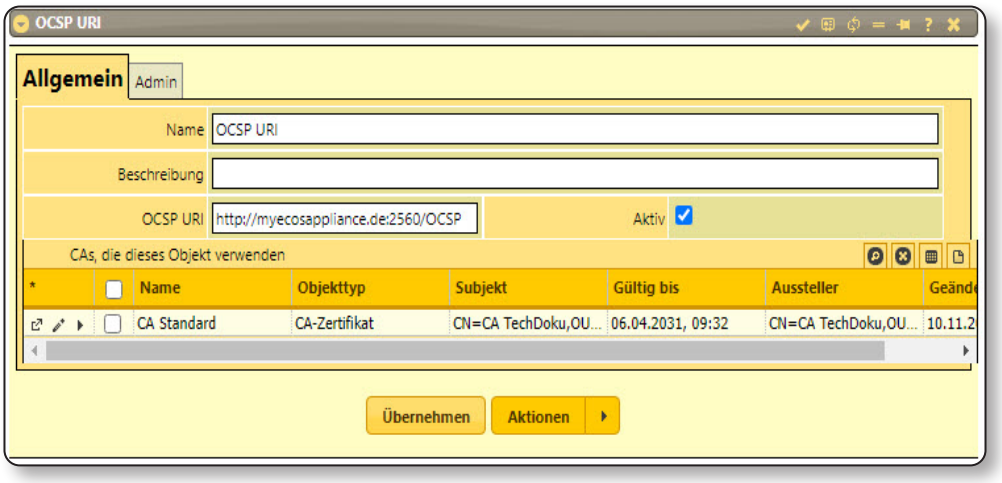

Abb. 1.04: *Einstellungen im OCSP URI-Objekt*

Allgemein

- NAME: Vergeben Sie einen aussagekräftigen Namen.
- OCSP URI: Geben Sie hier die URI an unter der die Informationen für den OCSP abgerufen werden können. Die URI setzt sich aus der HTTP-Adresse der ECOS Appliance (IP-Adresse oder FQDN, wenn der Speicherort öffentlich erreichbar sein soll), dem Port, der im **Dienst: OCSP-Server**-Objekt angegeben wurde, und einem beliebigen String zusammen.

  Beispiel: http://myecosappliance.de:2560/OCSP
- AKTIV: Aktivieren Sie die Checkbox, um den Zugriff auf die URI von außen zu erlauben.

Speichern Sie die Änderungen mit **Übernehmen** oder **Anlegen**.

4 Signierende CA anpassen

In der signierenden CA des unter Punkt ❶ angelegten OCSP-Zertifikats muss die OCSP-Information eingetragen werden. Sollen die OCSP-Informationen für mehrere CAs zur Verfügung gestellt werden, muss das **OCSP URI**-Objekt in jeder dieser CAs eingetragen werden.

Erweitert

- OCSP URI: Wählen Sie hier das unter Punkt ❸ angelegte **OCSP URI**-Objekt aus.

Speichern Sie die Änderungen mit **Übernehmen**. Sie können die OCSP-Informationen einer CA beliebig ändern oder weitere hinzufügen.

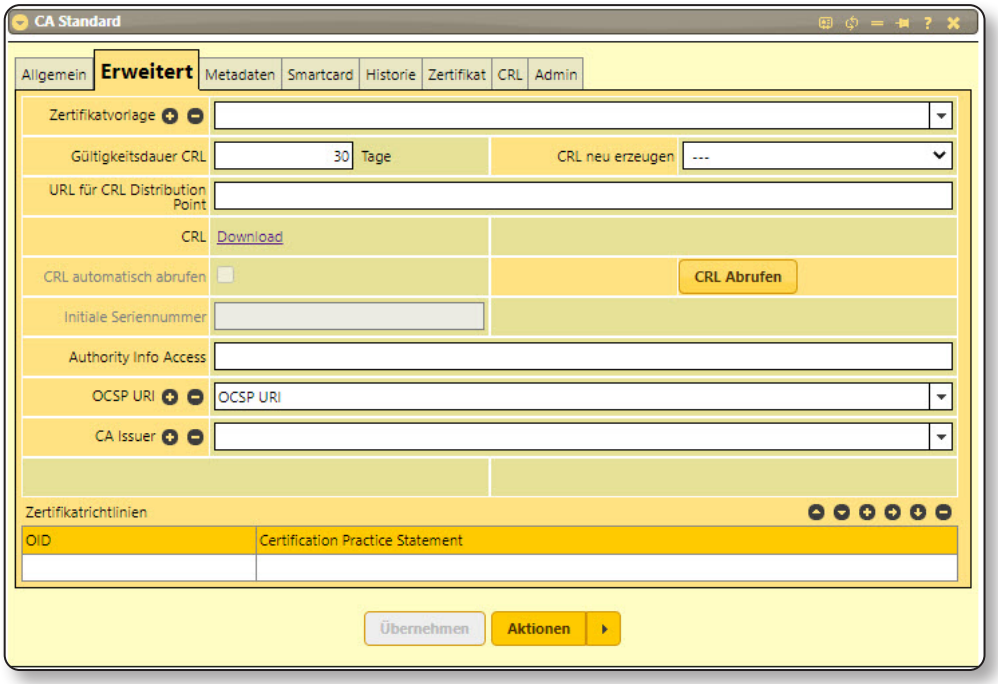

Abb. 1.07: *OCSP-Informationen in der signierenden CA eintragen*

5 Upload des Zertifikats auf der genuscreen & OCSP-Responder-URL konfigurieren

Das unter Punkt ❶ angelegte Zertifikat muss auf der genuscreen der genua GmbH hochgeladen werden und die OCSP-Responder-URL eingerichtet werden.

Navigieren Sie auf der genua genuscreen in der Menüleiste zu **VPN** und **IKEv2-Mobile-Einstellungen**.

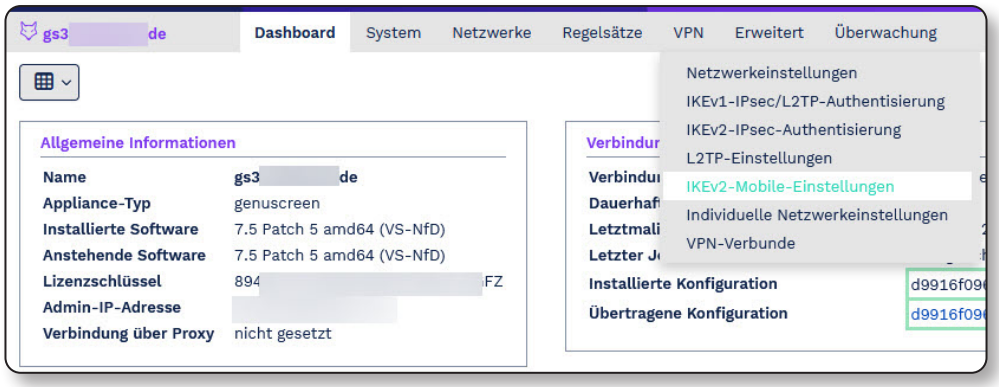

Abb. 1.05: *Navigation auf der genuscreen*

➡ Scrollen Sie zu AUTHENTISIERUNG/OCSP.

➡ Laden Sie das Zertifikat über das + unter OCSP RESPONDER ZERTIFIKATE hoch.

- Geben Sie die OCSP-Responder-URL im http-Format an. Sie finden sie im unter Punkt ❸ angelegten **OCSP URI**-Objekt unter OCSP URI.

- Speichern Sie die Einstellungen und updaten Sie anschließend die genuscreen-Appliance.

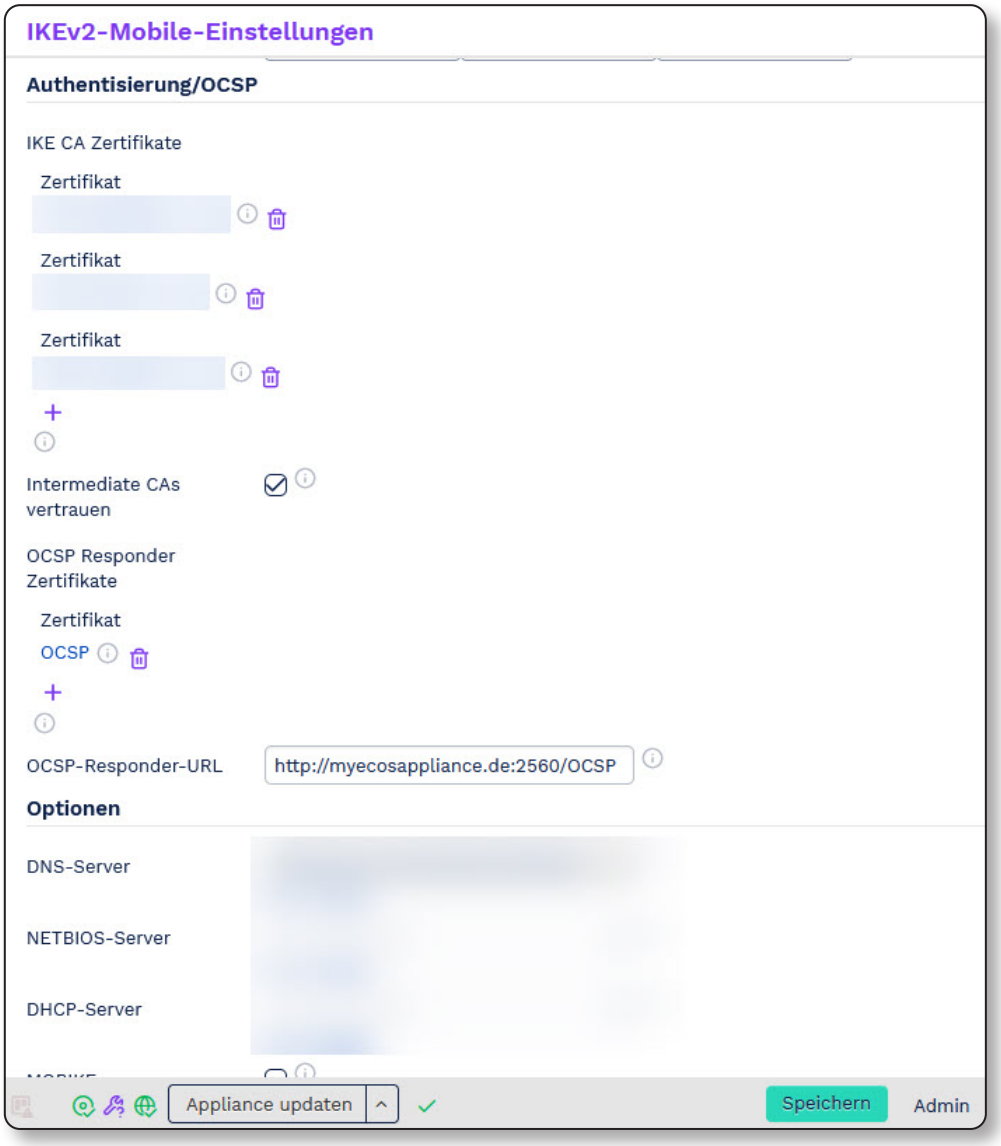

Abb. 1.06: *IKEv2-Mobile-Einstellungenen: OCSP Responder Zertifikate*