ECOS TrustManagementAppliance®

ECOS TrustManagementAppliance®

Admin-Handbuch

Version: 1.0

Datum: 11/2026

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

© by ECOS Technology GmbH

Weitergabe sowie Vervielfältigung dieses Dokuments, Verwendung und Mitteilung seines Inhalts sind verboten, soweit nicht ausdrücklich von uns gestattet. Zuwiderhandlungen verpflichten zu Schadenersatz. Alle Rechte für den Fall der Patent- oder Gebrauchsmustereintragungen vorbehalten.

Inhalt

Einführung **11**
Verwendung des Handbuchs **11**
Die ECOS TrustManagementAppliance® 11
Sicherheitshinweise 12

Teil I - Inbetriebnahme **13**

1 Installation und Inbetriebnahme der Appliance **14**
1.1 Vorbereitungen für die Inbetriebnahme **14**
1.2 Installation auf der virtuellen Maschine 14
1.3 Anmeldung an der Administrationsoberfläche 16
1.4 Ersteinrichtung 16
1.4.1 Administratorkonto einrichten 16
1.4.2 Lizenzvereinbarung 17
1.4.3 Netzwerkkonfiguration 17
1.4.4 PKI-Dienste einrichten 18
1.4.4.1 Root-CA erstellen 18
1.4.4.2 Signer-CA erstellen 19
1.4.4.3 ACME-Dienst einrichten 20
1.4.4.4 CMP-Dienst einrichten 21
1.4.4.5 EST-Dienst einrichten 21
1.4.4.6 SCEP-Dienst einrichten 22
1.4.4.7 OCSP-Dienst einrichten 23
1.4.4.8 Einrichtung abschließen 23
1.5 Smartcard-Zugriff für Admin-Benutzer im VS-NfD-Umfeld 24

2 Aufbau der Administrationsoberfläche - Standardansicht **25**
2.1 Header 26
2.1.1 Suche 27
2.2 Sitemap 28
2.3 Seitenmenü 28
2.4 Container-Menü 29
2.5 Seite 30
2.5.1 Tabellen 30
2.5.2 Kontextmenü 31
2.5.3 Assistent und Dialogfenster 32

3 Aufbau der Expertenansicht **33**
3.1 Wechsel in die Expertenansicht **33**
3.2 Menüleiste 33
3.3 Navigationsbaum 34
3.3.1 Funktionsleiste 34
3.3.2 Baum 34
3.3.3 Kontextmenü 35
3.4 Konfigurationsbereich 1 & 2 36
3.4.1 Konfigurationsobjekte 36

3.4.1.1 Neues Objekt anlegen 36
3.4.1.2 Namensleiste 37
3.4.1.3 Kontextmenü 38
3.4.1.4 Konfigurationsformular 38
3.4.1.5 Tabellen 39
3.4.1.6 Aktionsleiste 42
3.5 Informationsleiste 42
3.6 Werkzeuge des Systems 42
3.6.1 Reiter Admin 42
3.6.2 Reiter Log 43

Teil II - Standardansicht 44

4 Dashboards 45

5 CA-Management 46
5.1 CA-Zertifikate 46
5.1.1 Aufbau 47
5.1.1.1 Tabelle 47
5.1.1.2 Kontextmenü 48
5.1.2 Eigenes CA-Zertifikat erstellen 49
5.1.3 Externes CA-Zertifikat hochladen 53
5.1.4 CA-Hierarchie erstellen 56
5.2 CA-Zugangspunkte 57
5.3 Zertifikate 57
5.3.1 Aufbau 58
5.3.1.1 Tabelle 58
5.3.1.2 Kontextmenü 58
5.3.2 Eigenes Zertifikat erstellen 59
5.3.3 Externes Zertifikat hochladen 65
5.3.4 Zertifikat-Lifecycle-Management 68
5.3.4.1 Zertifikate verlängern 68
5.3.4.2 Zertifikate zurückziehen 68
5.3.4.3 Zertifikate vorübergehend ungültig setzen 69
5.4 Richtlinien 69
5.4.1 Eine neue Richtlinie erstellen 70

6 RA-Management 73
6.1 CSR-Inventar 73
6.1.1 Aufbau **73**
6.1.1.1 Tabelle 74
6.1.2 CSR genehmigen 74
6.1.3 CSR ablehnen 75

7 Benutzerverwaltung 77
7.1 Benutzer 77
7.1.1 Einen neuen Benutzer anlegen 78
7.1.2 Admin-Zugriff gewähren 79
7.1.3 Kennwort ändern 80

7.1.4 Benutzerkonto deaktivieren ... 80
7.2 Benutzerrollen ... 80
7.2.1 Eine neue Benutzerrolle anlegen ... 80
7.2.2 Eine Benutzerrolle zuweisen ... 81

8 PKI-Dienste ... 82
8.1 Zugangspunkte ... 82

9 Globale Einstellungen ... 83
9.1 Netzwerk ... 83
9.1.1 DNS-Server ... 83
9.1.2 NTP-Server ... 83
9.2 Organisation ... 84
9.3 Metadaten ... 84
9.3.1 Neue Metadatenschlüssel anlegen ... 84
9.3.2 Metadaten zu einem bereits erstellten Zertifikat hinzufügen ... 85
9.4 Lizenzinformationen ... 85

10 Dokumentation ... 86

11 Self-Service-Portal ... 87
11.1 Aufbau ... 88
11.1.1 Tabellen ... 88
11.1.2 Aufbau der Tabellen ... 88
11.2 Neues Zertifikat anfordern ... 89
11.3 CSR importieren ... 91

Teil III - Expertenansicht ... 92

12 Das ECOS Appliance-Objekt ... 93
12.1 Das Konfigurationsobjekt ... 93
12.1.1 Reiter Allgemein ... 93
12.1.2 Reiter Netzwerk ... 94
12.1.3 Reiter Abhängigkeiten ... 94
12.1.4 Reiter Softwarelizenzen ... 94
12.1.5 Reiter Aktionen ... 94
12.1.5.1 Netzwerktools ... 94
12.1.5.2 Update ... 97
12.1.5.3 Konfigurationsexport ... 98
12.1.5.4 Restart System/Dienste ... 98
12.1.5.5 Uhrzeit einstellen ... 99
12.1.5.6 Backup ... 99
12.1.6 Reiter Info ... 100
12.2 Das ECOS Appliance-Objekt als Container ... 100
12.2.1 Dienst-Objekte ... 100
12.2.2 Netzwerk-Objekte ... 101
12.2.2.1 Netzwerk-Interface ... 101
12.2.2.2 Routing ... 101

13 Netzwerkkonfiguration 102
13.1 Netzwerk-Interfaces definieren 102
13.2 Host-Namen definieren 102
13.3 Ports definieren 103
13.4 Netzwerke definieren 104

14 Grundlegende Dienste 105
14.1 Dienst: HTTPS-Administration 105
14.2 Dienst: Backup 107
14.2.1 Erzeugen und Sichern des Backup-Schlüssels 107
14.2.2 Ausführen von Backups 108
14.2.3 Bereitstellen von Backups 108
14.2.4 Log 109
14.3 Dienst: Wartung 109
14.4 Dienst: Smartcard-Enrollment 110
14.5 Software-Updates 111
14.5.1 Software-Update über die Software-Update-Server von ECOS 111
14.5.1.1 Automatische Updates 111
14.5.1.2 Manuelles Update 112
14.5.2 Software-Update über die ECOS Appliance 112
14.5.2.1 Software-Image bereitstellen 112
14.5.2.2 Update-Quelle definieren 113
14.5.2.3 Dienst: Software-Update-Server einrichten 114
14.5.2.4 Dienst: Software-Update einrichten 114

15 Benutzerverwaltung (Experte) 115
15.1 Benutzer und Rollen 115
15.2 Authentisierung 116

16 Zertifikate 118
16.1 Wichtige Zertifikatparameter 118
16.1.1 Gemeinsame Zertifikatparameter 118
16.1.2 CA-Zertifikat-spezifische Parameter 120
16.1.3 Zertifikat-spezifische Parameter 121
16.2 Zertifikatsperrliste (CRL) 123
16.2.1 Gültigkeit der CRL 123
16.3 Im- und Export 124
16.3.1 Import von Zertifikaten und Dateien 124
16.3.2 Export von Zertifikaten und Dateien 125
16.4 Externe Speicherung für Zertifikate und Schlüssel 125
16.4.1 Speicherung auf der Smartcard 125
16.4.2 Speicherung auf einem HSM 126
16.4.2.1 Anbinden eines HSM 127

17 Zertifikat-Enrollment mit Standardprotokollen 128
17.1 Die TMA als Zertifizierungsstelle 128
17.1.1 Vorbereitungen 129
17.1.1.1 CA-Zertifikat zum Signieren der Client-Zertifikate 129
17.1.1.2 TLS-Server-Zertifikat für den Server-Dienst 129

17.1.1.3 Container: Abonnentengruppe anlegen ... 130
17.1.1.4 Zielcontainer für Zertifikate anlegen ... 130
17.1.1.5 CA-Abonnentenverknüpfung ... 130
17.1.2 Zertifikat-Enrollment mit ACME ... 131
17.1.2.1 Dienst: ACME-Server anlegen ... 131
17.1.2.2 ACME-Abonnentenkonto anlegen ... 132
17.1.3 Zertifikat-Enrollment mit CMP ... 134
17.1.3.1 Dienst: CMP-Server anlegen ... 134
17.1.3.2 CMP-Abonnentenkonto anlegen ... 135
17.1.4 Zertifikat-Enrollment mit EST ... 136
17.1.4.1 Dienst: EST-Server anlegen ... 136
17.1.4.2 EST-Abonnentenkonto anlegen ... 137
17.1.5 Zertifikat-Enrollment mit SCEP ... 138
17.1.5.1 Dienst: SCEP-Server anlegen ... 138
17.1.5.2 SCEP-Abonnentenkonto anlegen ... 139
17.2 Die TMA als Client für andere Zertifizierungsstellen ... 141
17.2.1 Vorbereitungen ... 141
17.2.1.1 Registrierung beim Provider ... 141
17.2.1.2 Externes CA-Zertifikat zum Signieren der Client-Zertifikate ... 141
17.2.2 Zertifikat-Enrollment mit ACME ... 142
17.2.3 Zertifikat-Enrollment mit CMP ... 144

18 Zertifikat-Enrollment mit dem Certificate Enrollment Agent ... 146
18.1 Vorbereitungen ... 147
18.1.1 Dienst: Certifcate Enrollment Agent anlegen ... 147
18.1.2 Abonnentenkonto für Agent anlegen ... 148
18.2 Installation auf dem Zielsystem (Pull-Modus) ... 151
18.2.1 Voraussetzungen ... 151
18.2.2 Automatische Installation unter Linux ... 151
18.2.2.1 Reinstallation ... 153
18.2.3 Manuelle Installation unter Linux ... 153
18.2.4 Installation unter Windows ... 153
18.2.5 Unattended Installation unter Windows ... 154
18.3 Registrierung und Authentisierung ... 155
18.3.1 Registrierung im Pull-Modus ... 155
18.3.1.1 Ablauf der Registrierung ... 155
18.3.1.2 Automatische Erneuerung des Authentisierungszertifikats ... 156
18.3.2 Authentisierung im Push-Modus ... 156
18.4 Zertifikat-Enrollment ... 157
18.4.1 Zertifikate erstellen ... 157
18.4.1.1 Zertifikatplan für Agent anlegen ... 157
18.4.1.2 Mehrere Zertifikatpläne nutzen ... 158
18.4.2 Zertifikate ausrollen ... 158
18.4.2.1 Deploymentinfo für Agent anlegen ... 158
18.4.2.2 Deployment-Methoden ... 160
18.4.3 Ablauf der Zertifikatverteilung ... 165
18.4.4 Zertifikate verlängern ... 165

19 Verzeichnissynchronisation 166
19.1 Verzeichnisdienst konfigurieren 166
19.2 Verzeichnis-Map konfigurieren 167
19.3 Verzeichnissynchronisation konfigurieren 167

20 Hochverfügbarkeit 169
20.1 Voraussetzungen für High Availability (HA) 169
20.1.1 Master-Appliance einrichten 170
20.1.2 Vollsynchronisierte Slave-Appliance einrichten 171
20.2 Vereinfachung der Konfiguration durch Vererbung 171
20.2.1 Basis-Konfiguration erstellen 172
20.2.2 Vererbung konfigurieren 172
20.3 Konfiguration bei Ausfall umschwenken 172
20.3.1 HA-Konfiguration einrichten 173
20.3.1.1 HA-Konfiguration zu Appliance-Objekten hinzufügen 173
20.4 Synchronisation aufbauen 173
20.4.1 Übertragung der Konfiguration vom Master zum Slave 173
20.4.2 Privater Schlüssel der CA übertragen 174
20.4.3 Systeme prüfen 174

21 Abfragen 175
21.1 Reiter Allgemein 175
21.2 Reiter Abfrage 175
21.2.1 Auswahl des Objekttyps 175
21.2.2 Erstellen von Vergleichen der Attribute 175
21.2.3 Keine automatische Suche 177
21.3 Reiter Felder 177
21.3.1 Felder selbst definieren 177
21.4 Reiter Hervorhebungen 178
21.5 Beispiel: Abfrage mit Aktion zum automatischen Verlängern von Zertifikaten und CRLs 179

22 Berechtigungen 180
22.1 Rollen zu Gruppen zusammenfassen 180
22.2 Gruppen Berechtigungen zuweisen 180
22.3 Rechtearten 181
22.4 Sonderfälle bei Berechtigungen 182
22.4.1 Eine Rolle wird mehreren Gruppen zugeordnet 182
22.4.2 Unterschiedliche Rechte für Eltern und untergeordnete Objekte 182

Teil IV - Anhänge 183

23 Fehlerbeseitigung 184

24 Schlüsselverwendungszwecke 187
24.1 Voreingestellte Schlüsselverwendungszwecke 187
24.2 Schlüsselverwendungen 188
24.3 Erweiterte Schlüsselverwendungen 188

25 DocExpressions 190
25.1 DocExpressions Anwendungen 190

25.1.1 Validierung ... 190
25.1.2 Vorbelegung ... 190
25.2 Konfigurationsobjekt DocExpression Debugger ... 190
25.2.1 Reiter Allgemein ... 191
25.2.2 Reiter Metadaten ... 191
25.2.3 Reiter Funktionen ... 191
25.3 Syntax ... 191
25.3.1 Konstanten ... 192
25.3.1.1 Zahlen ... 192
25.3.1.2 Zeichenketten ... 192
25.3.2 Attribute ... 192
25.3.2.1 Array-Attribute ... 192
25.3.2.2 Hash-Attribute ... 192
25.3.2.3 Datasource-Attribute ... 192
25.3.3 Operatoren ... 193
25.3.4 Funktionen ... 193
25.3.4.1 Liste der verfügbaren Funktionen ... 194
25.4 Beispiel ... 196

26 Certificate Enrollment Agent - Anhänge ... 197
26.1 Kommandozeilenoptionen ... 197
26.2 Template-Variablen ... 198
26.2.1 Hilfsfunktionen ... 198
26.2.2 Verzeichnisse und Bezeichnung ... 198
26.2.3 Zertifikatidentität ... 199
26.2.4 Subject/Distinguished Name ... 200
26.2.5 Schlüsseltyp ... 201
26.2.6 Zertifikatdaten ... 201
26.2.7 CA-Zertifikate ... 203
26.2.8 CRL ... 204
26.2.9 Privater Schlüssel ... 204
26.2.10 Serververbindung (TMA-Abruf) ... 205
26.2.11 Remote-Dateizugriff (Push-Modus) ... 206
26.2.12 Systeminformationen ... 207
26.2.13 Benutzerdefinierte Eigenschaften ... 207
26.2.14 Vollständiges Template-Beispiel ... 208
26.2.15 Beispielwerte ... 209
26.3 Fehlersuche und Logging ... 210

27 Support ... 211
27.1 Technischer Support ... 211
27.2 Störungsannahme ... 211
27.3 Bearbeitungszeiten von Supportfällen ... 211
27.4 Hardware-Tests ... 211
27.5 Meldung von Security-Vorfällen ... 211
27.6 Updates ... 211

28 Abbildungen ... 212

Einführung

Verwendung des Handbuchs

Dieses Handbuch erklärt die wesentlichen Abläufe und Konfigurationen der ECOS **TrustManagementAppliance®**. Für eine ausführliche Erklärung jedes einzelnen Konfigurationsobjekts und seiner Felder ziehen Sie die Online-Hilfe der Trust Management Appliance (TMA) zu Rate.

Es ist in mehrere Teile unterteilt. **Teil I – Inbetriebnahme** umfasst alle notwendigen Vorbereitungen, Einstellungen und Konfigurationen, die für eine erfolgreiche Installation und Inbetriebnahme der Trust Management Appliance (TMA) notwendig sind. In **Teil II – Standardansicht** werden alle Einstellungen erklärt, die in der Standardansicht konfigurierbar sind. Die Einstellungen der Expertenansicht werden in **Teil III – Expertenansicht** erklärt.

Die Objekte in diesem Handbuch werden nach ihrem Objekttyp benannt, wie er im Reiter Admin des Objekts und in der Online-Hilfe angegeben ist. Der tatsächliche Name kann abweichen und ist durch die Eingabe im jeweiligen Konfigurationsobjekt bestimmt.

Die ECOS TrustManagementAppliance®

Die ECOS **TrustManagementAppliance®**, kurz TMA, ist eine PKI- und Key-Management-Lösung zur Absicherung von mobilen Geräten, PCs, Servern, Prozessen und sonstigen Geräten im Bereich (I)IoT.

Die TMA verfügt über eine Standard- und eine Expertenansicht. In der Standardansicht stehen die wichtigsten Funktionen für ein zuverlässiges PKI- und Zertifikatmanagement zur Verfügung, während in der Expertenansicht die gesamten Funktionen konfigurierbar sind.

Sicherheitshinweise

Auf der ECOS TrustManagementAppliance® werden sensible Informationen administriert und gespeichert. Sie sind für den sicheren Betrieb im Netzwerk von zentraler Bedeutung. Diese Informationen müssen daher besonders geschützt werden.

Die folgenden Sicherheitsmaßnahmen müssen für einen sicheren Betrieb der Appliance ungesetzt werden:

1. Die Appliance muss in einem abgesicherten Netzwerk betrieben werden.
2. Der administrative Zugriff darf ausschließlich durch autorisiertes und geschultes Personal erfolgen, das über die erforderlichen Kenntnisse der Netzwerkinfrastruktur sowie der eingesetzten technischen Sicherheitsmechanismen verfügt.
3. Für administrative Zugriffe im mobilen Einsatz muss ein sicherer Zugang (z.B. über VPN) eingerichtet werden.
4. Es wird empfohlen, regelmäßig Backups der Appliance zu erstellen. Backups müssen sicher gespeichert werden und dürfen nur autorisiertem Personal zugänglich sein.
5. Bei Ersteinrichtung der Appliance muss für den Standardbenutzer **admin** das initiale Kennwort geändert und ein neues Kennwort gesetzt werden (**7.1.3 Kennwort ändern**). In VS-NfD-Umgebungen muss das initiale Administratorkonto nach der Ersteinrichtung und vor Aufnahme des Regelbetriebs deaktiviert werden.
6. Für jeden Administrator muss ein eigenes Benutzerkonto angelegt werden, um eine eindeutige Nachvollziehbarkeit sicherzustellen.
7. Bei Einrichtung der grundlegenden Dienste muss im Dienst: Wartung ein individuelles Kennwort für den lokalen Wartungszugang gesetzt werden (siehe **14.3 Dienst: Wartung**).
8. Für VS-NfD-Umgebungen wird für den Schutz von CA-Schlüsseln der Einsatz eines geeigneten Hardware Security Moduls (HSM) empfohlen (siehe **16.4 Externe Speicherung für Zertifikate und Schlüssel**).

⚠ **Hinweis für VS-NfD:** Zusätzliche Anforderungen für den zugelassenen Betrieb in VS-NfD-Umgebungen sind im Dokument **ECOS TrustManagementAppliance: Hinweise zum zugelassenen Betrieb** beschrieben.



Teil I - Inbetriebnahme

1 Installation und Inbetriebnahme der Appliance

1.1 Vorbereitungen für die Inbetriebnahme

Die ECOS **TrustManagementAppliance®** wird i.d.R. auf einer virtuellen Maschine (VM) installiert. Es werden die Virtualisierungsumgebungen Citrix, XenServer, Hyper-V, VMware und Proxmox unterstützt. Die virtuelle Maschine benötigt folgende Mindestanforderungen:

- CPU: 4 Kerne
- RAM: 8 GB
- Festplattenspeicher: 120 GB
- Netzwerkschnittstellen: 1x Ethernet
- Mit BIOS statt UEFI anlegen
- Secure Boot muss deaktiviert sein

Je nach Anforderungen empfiehlt es sich, diese Werte zu erhöhen.

⚠ **Hinweis:** Im VS-NfD-Umfeld benötigt der Linux-Kernel 6.x eine zuverlässige Entropiequelle, die über eine an die VM durchgereichte Smartcard bereitgestellt wird. Hyper-V unterstützt keinen Smartcard-Passthrough. Für VMware ESXi, XenServer, Proxmox und HPE Morpheus stehen entsprechende Passthrough-Verfahren zur Verfügung.

Der Betrieb der Trust Management Appliance erfordert eine infrastrukturseitige Freischaltung der folgenden Ports durch den Betreiber:

Port	Verwendung	
543/TCP	HTTPS-Dienst	Management
53/UDP	DNS-Dienst	System-Infrastruktur
123/UDP	NTP-Dienst	System-Infrastruktur

⚠ **Hinweis:** Alle weiteren Ports, z.B. für Protokoll-Dienste, soweit diese verwendet werden (SCEP, ACME, EST etc.), unterliegen der infrastrukturseitigen Policy des Betreibers.

1.2 Installation auf der virtuellen Maschine

Für die Installation benötigen Sie eine ISO-Datei. Diese erhalten Sie über den ECOS Support.

⚠ **Hinweis:** Vor Installationen im ESXi muss ggf. der Dateiname der ISO umbenannt werden, da in manchen Fällen Dateinamen mit einem enthaltenen +-Zeichen nicht als Installationsmedium verwendet werden können.

Booten Sie die ISO-Datei von der VM aus. Wählen Sie die Sprache für die Installation aus. Es besteht die Auswahl zwischen Deutsch und Englisch.

Wählen Sie anschließend die Festplatte aus, auf der die TMA installiert werden soll, indem Sie die angegebene Nummer vor der Festplatte eingeben. Bestätigen Sie dies mit ENTER. Die Installation beginnt. Starten Sie das System nach Abschluss der Installation neu.

Anschließend öffnet sich ein Konsolenfenster und es werden die Netzwerkdaten abgefragt. Geben Sie eine IP-Adresse mit der Subnetzmaske im Format **nnn.nnn.nnn.nnn/mm** und das Standard-Gateway der Appliance im Format **nnn.nnn.nnn.nnn** ein.

Die TMA bootet vollständig. Sie erhalten eine Übersicht über die Hardware, Software und Netzwerkeinstellungen, inkl. der URL zur webbasierten Administrationsoberfläche. Alle weiteren Konfigurationen werden über die Weboberfläche durchgeführt.

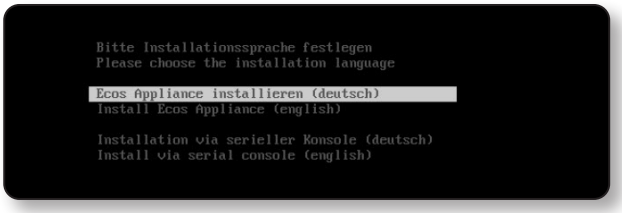


Abb. 1.01: *Start der Installation*



Abb. 1.02: *Auswahl der Festplatte*

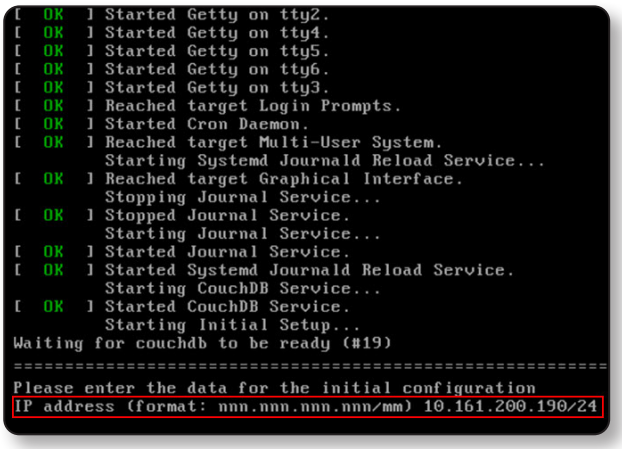


Abb. 1.03: *Angabe der IP-Adresse*

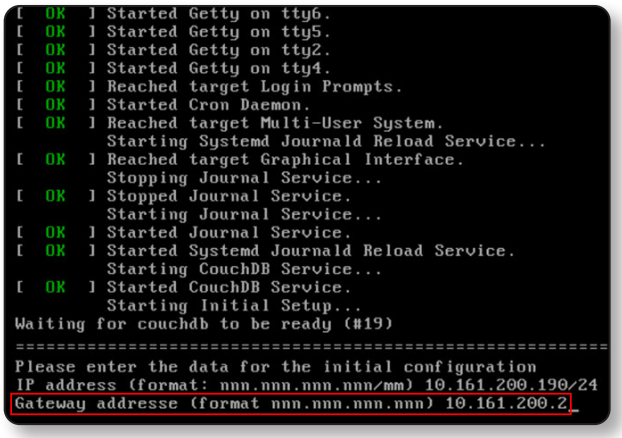


Abb. 1.04: *Angabe der Gateway-Adresse*

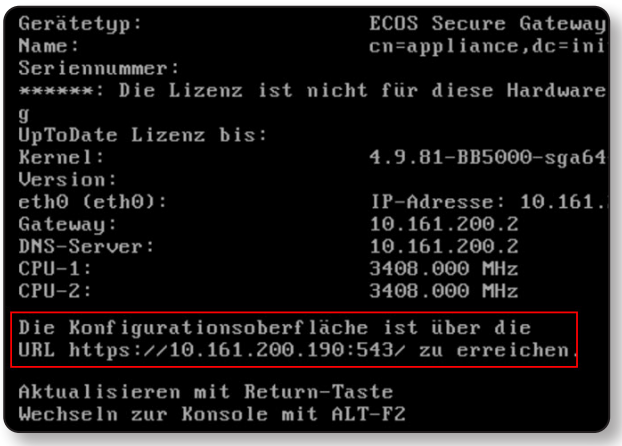


Abb. 1.05: *Die Installation ist abgeschlossen*

1.3 Anmeldung an der Administrationsoberfläche

Der Zugriff auf die Administrationsoberfläche der TMA erfolgt über einen Webbrowser. Der Zugriff erfolgt über die bei der Installation vergebene IP-Adresse. Ist Port 80 erreichbar, reicht die Eingabe der IP-Adresse im Browser. Die Weiterleitung auf den korrekten HTTPS-Port erfolgt automatisch. Alternativ kann über Port 543 direkt via HTTPS auf die Administrationsoberfläche zugegriffen werden.

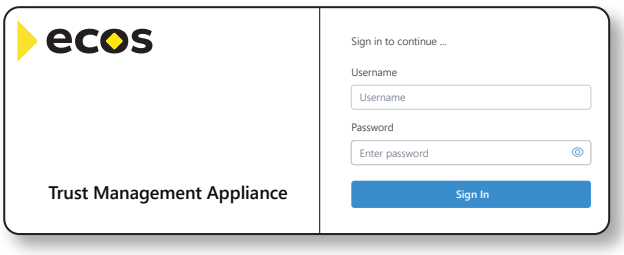


Abb. 1.06: *Anmeldung an der Administrationsoberfläche*

Beispiel:

Wurde die TMA mit der IP-Adresse **192.168.1.5** installiert, ist die Administrationsoberfläche über die URL **https://192.168.1.5:543** erreichbar.

Im Auslieferungszustand erfolgt die Authentifizierung mit folgenden initialen Zugangsdaten:

Benutzername: **admin**
Kennwort: **bb5000**

Nach erfolgreicher Authentifizierung öffnet sich die Administrationsoberfläche.

1.4 Ersteinrichtung

Bei der ersten Anmeldung an der Administrationsoberfläche startet der Ersteinrichtungsassistent. Er unterstützt bei der Einrichtung eines Administratorkontos, dem Einspielen der Lizenzen, der Netzwerkkonfiguration, der Einrichtung der ersten CA-Zertifikate und, je nach Lizenz, bei der Einrichtung verschiedener PKI-Dienste.

1.4.1 Administratorkonto einrichten

Das initiale Kennwort für den Benutzer **admin** muss geändert und ein neues Kennwort gesetzt werden.

Login: Vergeben Sie einen Loginnamen, mit dem Sie sich zukünftig an der Administrationsoberfläche anmelden. Der Login kann später geändert werden.

Kennwort: Vergeben Sie ein Kennwort für das Administratorkonto.

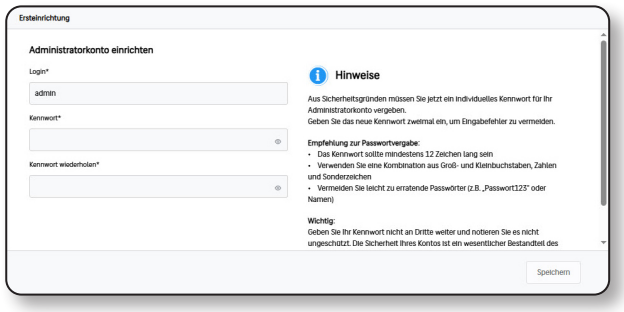


Abb. 1.07: *Ersteinrichtung - Administratorkonto einrichten*

Kennwort wiederholen: Wiederholen Sie das Kennwort für das Administratorkonto.

Nach dem Speichern der Zugangsdaten werden Sie ausgeloggt und müssen sich mit den neuen Zugangsdaten einloggen.

⚠ Hinweis für VS-NfD: Nach Abschluss der Ersteinrichtung muss für jeden Benutzer mit administrativen Rechten ein eigenes Benutzerkonto angelegt werden, um die Nachvollziehbarkeit administrativer Zugriffe sicherzustellen.
Nach Einrichtung der erforderlichen Administratorkonten, spätestens vor Aufnahme des Regelbetriebs, muss das initiale Administratorkonto deaktiviert werden (siehe **7.1.4 Benutzerkonto deaktivieren**).

1.4.2 Lizenzvereinbarung

Nach der erneuten Anmeldung müssen Sie der Lizenzvereinbarung zustimmen und anschließend die Lizenzdatei hochladen, die Sie zusammen mit der TMA erhalten haben.

Die Übersicht zeigt Ihnen, welche Features in Ihrer Lizenz enthalten sind.

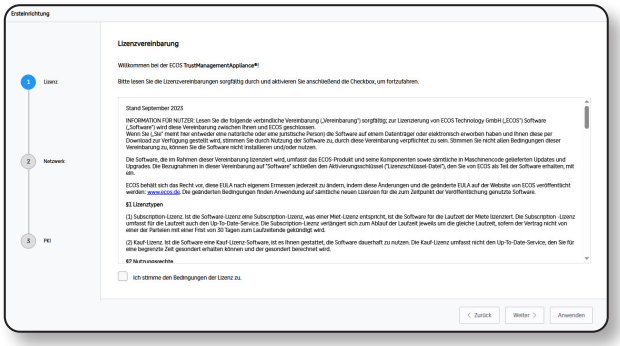


Abb. 1.08: *Ersteinrichtung - Lizenzvereinbarung*

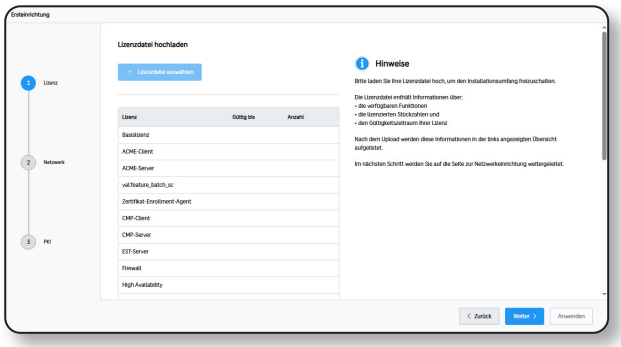


Abb. 1.09: *Ersteinrichtung - Lizenz einspielen*

1.4.3 Netzwerkkonfiguration

Im nächsten Schritt müssen Sie die grundlegenden Netzwerk- und NTP-Server-Einstellungen konfigurieren.

Organisationsname: Vergeben Sie einen aussagekräftigen Namen für die Organisation. Der Name ist Bestandteil aller ausgestellten Zertifikate.

IPv4-Adresse: Hier wird die IP-Adresse angezeigt, die während der Installation der TMA konfiguriert wurde. Sie lässt sich im Assistenten nicht ändern.

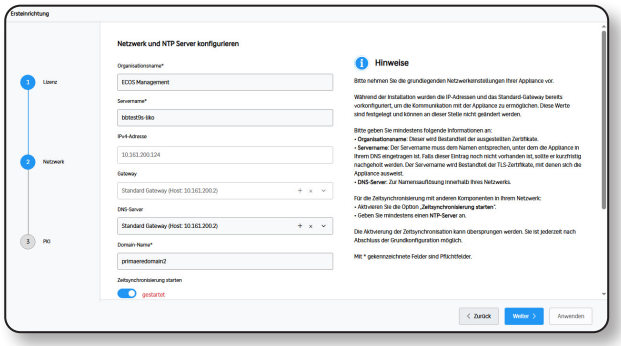


Abb. 1.10: *Ersteinrichtung - Netzwerkeinrichtung*

Gateway: Hier wird das Gateway angezeigt, das während der Installation der TMA konfiguriert wurde. Es lässt sich im Assistenten nicht ändern.

DNS-Server: Wählen Sie hier den DNS-Server aus. Er dient zur Namensauflösung innerhalb Ihres Netzwerks. Über das + können Sie ein neues Host-Objekt anlegen. Den DNS-Server können Sie später jederzeit ändern (siehe **9.1.1 DNS-Server**).

Zeitsynchronisierung starten: Aktivieren Sie diese Option, um die Zeitsynchronisation mit einem der angegebenen NTP-Servern zu starten.

NTP-Server: Geben Sie hier einen NTP-Server an. Über das + können Sie ein neues Host-Objekt anlegen. Sie können bis zu drei NTP-Server angeben. Eine Liste mit öffentlichen Zeitservern findet sich unter: http://support.ntp.org/bin/view/Servers/StratumOneTimeServers. Die NTP-Server können Sie später jederzeit ändern (siehe **9.1.2 NTP-Server**).

1.4.4 PKI-Dienste einrichten

Nach der Netzwerkkonfiguration wählen Sie die PKI-Dienste aus, die Sie mit dem Einrichtungsassistenten konfigurieren wollen. Es stehen nur die Dienste zur Auswahl, die in Ihrer Lizenz enthalten sind.

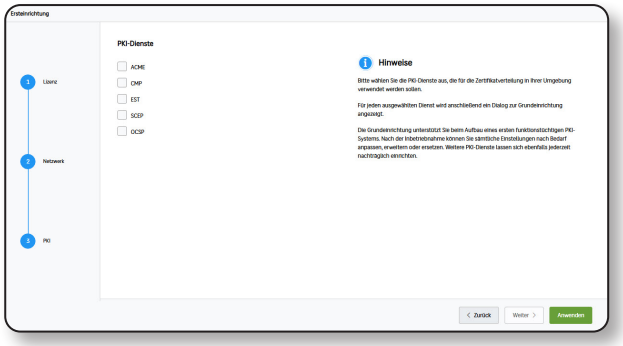


Abb. 1.11: *Ersteinrichtung - PKI-Dienste auswählen*

1.4.4.1 Root-CA erstellen

Als erstes muss eine Root-CA angelegt werden. Bei einer Root-CA handelt es sich um die oberste Zertifizierungsstelle, die Zertifikate und untergeordnete Sub-CAs signiert.

Name: Vergeben Sie einen aussagekräftigen Namen. Standardmäßig wird der Name **ECOS Management ROOT CA G1** vorgeschlagen.

Gültigkeitsdauer (Tage): Geben Sie die Gültigkeit in Tagen an. Standardmäßig wird eine Gültigkeit von **3650 Tagen** vorgeschlagen. Dies entspricht 10 Jahre. Das ist die empfohlene Laufzeit für Root-CAs.

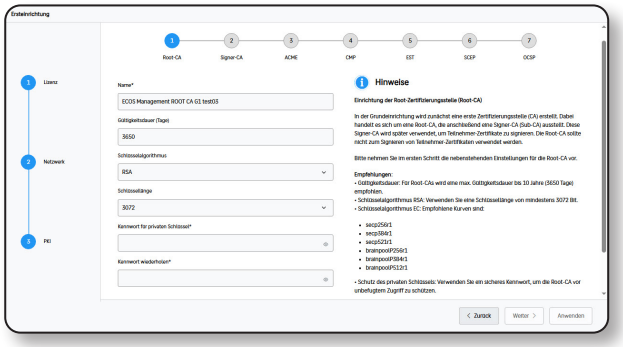


Abb. 1.12: *Ersteinrichtung - Root-CA konfigurieren*

Schlüsselalgorithmus: Wählen Sie einen Schlüsselalgorithmus aus. Mit dem Schlüsselalgorithmus wird das kryptografische Schlüsselpaar des Zertifikats erzeugt. Zur Auswahl stehen **RSA** und **Elliptische Kurven**.

> RSA: Das RSA-Verfahren berechnet das Schlüsselpaar mithilfe einer modularen Potenzierung großer Primzahlen. Für dieses Verfahren müssen Sie zusätzlich eine Schlüssellänge festlegen.

Elliptische Kurven: Das EC-Verfahren berechnet das Schlüsselpaar mithilfe mathematischer Operationen auf Elliptischen Kurven (engl. Elliptic Curves). Für dieses müssen Sie eine Elliptische Kurve auswählen.

Schlüssellänge: Wählen Sie die Schlüssellänge für das RSA-Verfahren aus. Standardmäßig sind **3072 Bit** voreingestellt. Diese Einstellung entspricht den aktuellen Anforderungen und Empfehlungen des BSI für den Einsatz von RSA-Schlüsseln in VS-NfD-Umgebungen. Außerhalb von VS-NfD-Umgebungen können abweichende Schlüssellängen je nach Einsatzszenario und Kompatibilität der eingesetzten Systeme oder Hardwarekomponenten erforderlich sein.

Elliptische Kurve: Hier wählen Sie elliptische Kurve für das ECC-Verfahren aus. Standardmäßig ist **prime256v1** eingestellt. Diese Einstellung entspricht den aktuellen Anforderungen und Empfehlungen des BSI für den Einsatz von EC-Schlüsseln in VS-NfD-Umgebungen. Außerhalb von VS-NfD-Umgebungen können abweichende elliptische Kurven je nach Einsatzszenario und Kompatibilität der eingesetzten Systeme oder Hardwarekomponenten erforderlich sein.

Kennwort für privaten Schlüssel: Geben Sie hier das Kennwort für den privaten Schlüssel des CA-Zertifikats an. Verwenden Sie ein sicheres Kennwort und legen Sie es sicher ab, um es vor unbefugten Zugriff von Dritten zu schützen.

Kennwort wiederholen: Wiederholen Sie das oben gewählte Kennwort.

1.4.4.2 Signer-CA erstellen

Nach der Root-CA muss eine Signer-CA erzeugt werden. Dabei handelt es sich um eine Sub-CA, die von der Root-CA signiert ist und für die Signierung von Zertifikaten genutzt wird.

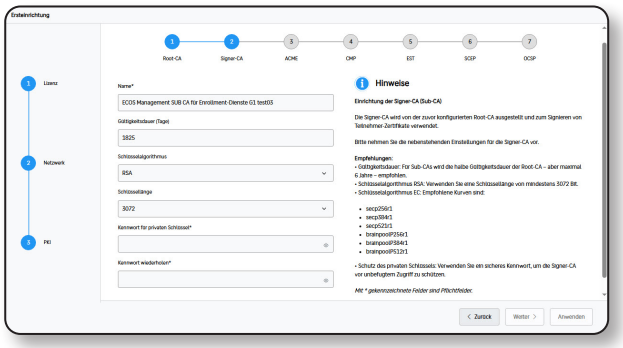


Abb. 1.13: *Ersteinrichtung - Sub-CA konfigurieren*

Name: Vergeben Sie einen aussagekräftigen Namen. Standardmäßig wird der Name **ECOS Management SUB CA für Enrollment-Dienste G1** vorgeschlagen.

Gültigkeitsdauer (Tage): Geben Sie die Gültigkeit in Tagen an. Standardmäßig wird eine Gültigkeit von **1825 Tagen** vorgeschlagen. Dies entspricht 5 Jahre. Für Sub-CAs wird die halbe Laufzeit der signierenden Root-CA empfohlen, maximal aber 6 Jahre.

Schlüsselalgorithmus: Wählen Sie einen Schlüsselalgorithmus aus. Mit dem Schlüsselalgorithmus wird das kryptografische Schlüsselpaar des Zertifikats erzeugt. Zur Auswahl stehen **RSA** und **Elliptische Kurven**.

RSA: Das RSA-Verfahren berechnet das Schlüsselpaar mithilfe einer modularen Potenzierung großer Primzahlen. Für dieses Verfahren müssen Sie zusätzlich eine Schlüssellänge festlegen.

Elliptische Kurven: Das EC-Verfahren berechnet das Schlüsselpaar mithilfe mathematischer Operationen auf Elliptischen Kurven (engl. Elliptic Curves). Für dieses müssen Sie eine Elliptische Kurve auswählen.

Schlüssellänge: Hier wählen Sie die Schlüssellänge für das RSA-Verfahren aus. Standardmäßig sind **3072 Bit** voreingestellt. Diese Einstellung entspricht den aktuellen Anforderungen und Empfehlungen des BSI für den Einsatz von RSA-Schlüsseln in VS-NfD-Umgebungen. Außerhalb von VS-NfD-Umgebungen können abweichende Schlüssellängen je nach Einsatzszenario und Kompatibilität der eingesetzten Systeme oder Hardwarekomponenten erforderlich sein.

Elliptische Kurve: Hier wählen Sie elliptische Kurve für das ECC-Verfahren aus. Standardmäßig ist **prime256v1** eingestellt. Diese Einstellung entspricht den aktuellen Anforderungen und Empfehlungen des BSI für den Einsatz von EC-Schlüsseln in VS-NfD-Umgebungen. Außerhalb von VS-NfD-Umgebungen können abweichende elliptische Kurven je nach Einsatzszenario und Kompatibilität der eingesetzten Systeme oder Hardwarekomponenten erforderlich sein.

Kennwort für privaten Schlüssel: Geben Sie hier das Kennwort für den privaten Schlüssel des CA-Zertifikats an. Verwenden Sie ein sicheres Kennwort und legen Sie es sicher ab, um es vor unbefugten Zugriff von Dritten zu schützen.

Kennwort wiederholen: Wiederholen Sie das oben gewählte Kennwort.

1.4.4.3 ACME-Dienst einrichten

ACME steht für Automated Certificate Management Environment. Der Dienst ermöglicht die automatisierte Verteilung von Zertifikaten über das ACME-Protokoll. Für Informationen zum ACME-Protokoll (siehe **17.1.2 Zertifikat-Enrollment mit ACME** und **17.2.2 Zertifikat-Enrollment mit ACME**).

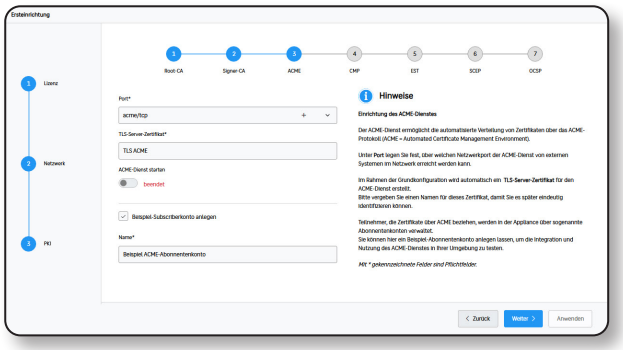


Abb. 1.14: *Ersteinrichtung - ACME-Dienst einrichten*

Port: Wählen Sie hier den Netzwerkport aus, über den der ACME-Dienst von externen Systemen erreichbar ist. Es muss ein Port verwendet werden, an dem keine andere Instanzen der ECOS Appliance lauschen. Über das + können Sie ein neues Port-Objekt anlegen.

TLS-Server-Zertifikat: Vergeben Sie einen aussagekräftigen Namen für das TLS-Server-Zertifikat. Es wird automatisch für den ACME-Dienst erstellt.

ACME-Dienst starten: Aktivieren Sie diese Option, um den ACME-Dienst zu starten.

Beispiel-Abonnentenkonto anlegen: Aktivieren Sie diese Checkbox, um ein Beispiel-Abonnentenkonto anzulegen. Damit können Sie die Integration und Nutzung des ACME-Diensts in Ihrer Umgebung testen.

Name: Vergeben Sie einen aussagekräftigen Namen für das Beispiel-Abonnentenkonto. Standardmäßig wird der Name **Beispiel ACME-Abonnentenkonto** vorgeschlagen.

1.4.4.4 CMP-Dienst einrichten

CMP steht für Certificate Management Protocol. Der Dienst ermöglicht die automatisierte Verteilung von Zertifikaten über das CMP-Protokoll (siehe **17.1.3 Zertifikat-Enrollment mit CMP** und **17.2.3 Zertifikat-Enrollment mit CMP**).

Port: Wählen Sie hier den Netzwerkport aus, über den der CMP-Dienst von externen Systemen erreichbar ist. Es muss ein Port verwendet werden, an dem keine andere Instanzen der ECOS Appliance lauschen. Über das + können Sie ein neues Port-Objekt anlegen.

TLS-Server-Zertifikat: Vergeben Sie einen aussagekräftigen Namen für das TLS-Server-Zertifikat. Es wird automatisch für den CMP-Dienst erstellt.

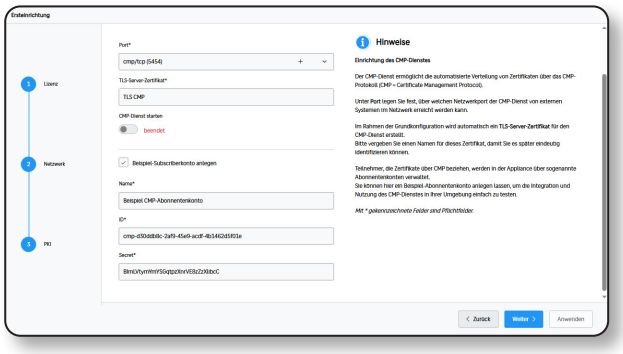


Abb. 1.15: *Ersteinrichtung - CMP-Dienst einrichten*

CMP-Dienst starten: Aktivieren Sie diese Option, um den CMP-Dienst zu starten.

Beispiel-Abonnentenkonto anlegen: Aktivieren Sie diese Checkbox, um ein Beispiel-Abonnentenkonto anzulegen. Damit können Sie die Integration und Nutzung des CMP-Diensts in Ihrer Umgebung testen.

Name: Vergeben Sie einen aussagekräftigen Namen für das Beispiel-Abonnentenkonto. Standardmäßig wird der Name **Beispiel CMP-Abonnentenkonto** vorgeschlagen.

ID: Vergeben Sie eine ID für das Beispiel-Abonnentenkonto. Standardmäßig wird eine zufällig generierte ID vergeben.

Secret: Geben Sie hier das Secret für das Beispiel-Abonnentenkonto an. Standardmäßig wird ein zufällig generiertes Secret vergeben.

1.4.4.5 EST-Dienst einrichten

EST steht für Enrollment over Secure Transport. Der Dienst ermöglicht die automatisierte Verteilung von Zertifikaten über das EST-Protokoll (siehe **17.1.4 Zertifikat-Enrollment mit EST**).

Port: Wählen Sie hier den Netzwerkport aus, über den der EST-Dienst von externen Systemen erreichbar ist. Es muss ein Port verwendet werden,

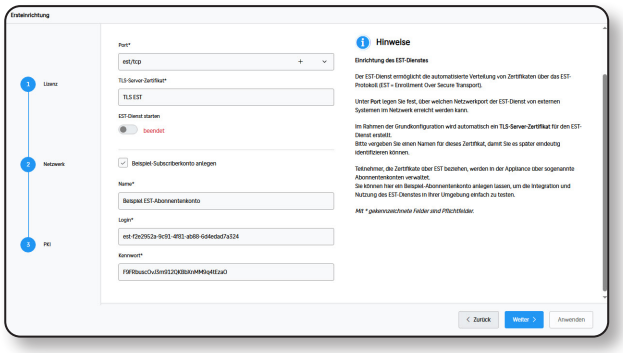


Abb. 1.16: *Ersteinrichtung - EST-Dienst einrichten*

an dem keine andere Instanzen der ECOS Appliance lauschen. Über das + können Sie ein neues Port-Objekt anlegen.

TLS-Server-Zertifikat: Vergeben Sie einen aussagekräftigen Namen für das TLS-Server-Zertifikat. Es wird automatisch für den EST-Dienst erstellt.

EST-Dienst starten: Aktivieren Sie diese Option, um den EST-Dienst zu starten.

Beispiel-Abonnentenkonto anlegen: Aktivieren Sie diese Checkbox, um ein Beispiel-Abonnentenkonto anzulegen. Damit können Sie die Integration und Nutzung des EST-Diensts in Ihrer Umgebung testen.

Name: Vergeben Sie einen aussagekräftigen Namen für das Beispiel-Abonnentenkonto. Standardmäßig wird der Name **Beispiel EST-Abonnentenkonto** vorgeschlagen.

Login: Vergeben Sie einen Login-Namen für das Beispiel-Abonnentenkonto. Standardmäßig wird ein zufällig generierte Login-Name vergeben.

Kennwort: Geben Sie hier das Kennwort für das Beispiel-Abonnentenkonto an. Standardmäßig wird ein zufällig generiertes Kennwort vergeben.

1.4.4.6 SCEP-Dienst einrichten

SCEP steht für Simple Certificate Enrollment Protocol. Der Dienst ermöglicht die automatisierte Verteilung von Zertifikaten über das SCEP-Protokoll. Für Informationen zum SCEP-Protokoll (siehe **17.1.5 Zertifikat-Enrollment mit SCEP**).

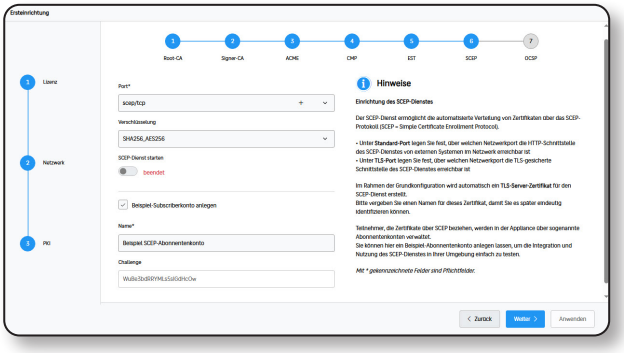


Abb. 1.17: *Ersteinrichtung - SCEP-Dienst einrichten*

Port: Wählen Sie hier den Netzwerkport aus, über den der SCEP-Dienst von externen Systemen erreichbar ist. Es muss ein Port verwendet werden, an dem keine andere Instanzen der ECOS Appliance lauschen. Über das + können Sie ein neues Port-Objekt anlegen.

TLS-Server-Zertifikat: Vergeben Sie einen aussagekräftigen Namen für das TLS-Server-Zertifikat. Es wird automatisch für den SCEP-Dienst erstellt.

Verschlüsselung: Wählen Sie hier die Verschlüsselung aus. Standardmäßig ist die Verschlüsselung SHA256_AES256 ausgewählt. Dies entspricht der aktuell sichersten Verschlüsselung.

SCEP-Dienst starten: Aktivieren Sie diese Option, um den SCEP-Dienst zu starten.

Beispiel-Abonnentenkonto anlegen: Aktivieren Sie diese Checkbox, um ein Beispiel-Abonnentenkonto anzulegen. Damit können Sie die Integration und Nutzung des SCEP-Diensts in Ihrer Umgebung testen.

Name: Vergeben Sie einen aussagekräftigen Namen für das Beispiel-Abonnentenkonto. Standardmäßig wird der Name **Beispiel SCEP-Abonnentenkonto** vorgeschlagen.

Challenge: Hier wird die Challenge für das Beispiel-Abonnentenkonto angezeigt. Standardmäßig wird ein zufällig generierte Challenge vergeben. Sie können die Challenge in dieser Einrichtung nicht ändern.

1.4.4.7 OCSP-Dienst einrichten

OCSP steht für Online Certificate Status Protocol. Der OCSP-Dienst ermöglicht die Online-Prüfung des Gültigkeitsstatus von Zertifikaten.

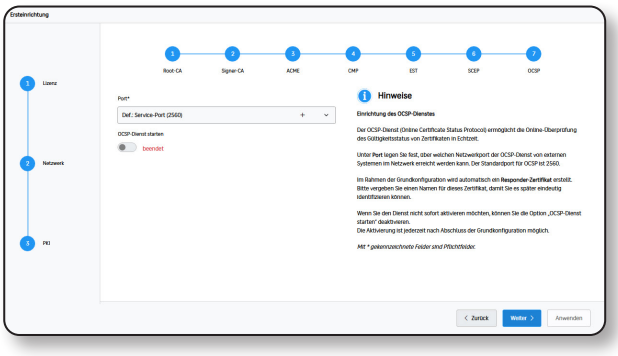


Abb. 1.18: *Ersteinrichtung - OCSP-Dienst einrichten*

Port: Wählen Sie hier den Netzwerkport aus, über den der OCSP-Dienst von externen Systemen erreichbar ist. Der Standardport für OCSP ist 2560. Über das + können Sie ein neues Port-Objekt anlegen.

Responder-Zertifikate: Vergeben Sie einen Namen für das Responder-Zertifikat. Dieses Zertifikat besitzt die erweiterte Schlüsselverwendung OCSP-Signing. Mit diesem Zertifikat kann der Responder seine Antworten signieren. Für jede CA, die über den OCSP-Dienst die Gültigkeit ihrer ausgestellten Zertifikate prüfen lassen will, wird ein eigenes Responder-Zertifikat benötigt. Standardmäßig wird der Name **Responder-Zertifikat OCSP** vergeben.

OCSP-Dienst starten: Aktivieren Sie diese Option, um den OCSP-Dienst zu starten.

1.4.4.8 Einrichtung abschließen

Nach Abschluss der Einrichtung wird Ihnen eine Übersicht der vorgenommenen Einstellungen angezeigt. Speichern Sie die Einstellungen mit **Anwenden**. Anschließend werden Sie auf das Dashboard weitergeleitet. Die im Einrichtungsassistenten vorgenommen Einstellungen für können Sie jederzeit im Expertenmodus ändern.

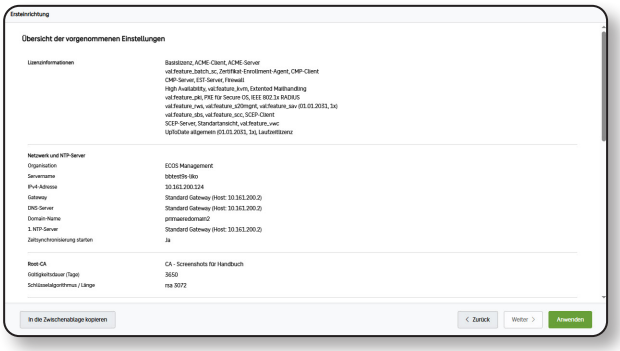


Abb. 1.19: *Ersteinrichtung - Übersicht der Ersteinrichtung*

1.5 Smartcard-Zugriff für Admin-Benutzer im VS-NfD-Umfeld

Im VS-NfD-Umfeld muss für die Anmeldung an der Administrationsoberfläche eine Smartcard als zusätzlicher Sicherheitsfaktor verwendet werden. Außerhalb des VS-NfD-Umfelds kann eine Smartcard als zusätzlicher Sicherheitsfaktor genutzt werden.

Jeder Benutzer mit administrativem Zugriff muss ein gültiges Zertifikat besitzen. Dazu muss eine CA angelegt werden, die die Benutzerzertifikate signiert. Im Anschluss wird ein Zertifikat für den Benutzer erstellt, dessen privater Schlüssel auf der Smartcard gespeichert werden muss. Der CN des Zertifikats muss zeichengenau dem Namen des Benutzers entsprechen. Dazu wird am einfachsten der Benutzername des Benutzer-Objekts als Name des Zertifikats gesetzt.

Um die Anmeldung per Smartcard zu aktivieren, navigieren Sie zu **Globale Einstellungen → Admin UI Zugriff**.

Im Feld Admin-Anmeldung muss **Kennwort & Zertifikat mit CN** ausgewählt werden. Außerdem muss die CA, die die Benutzerzertifikate ausstellt, im Feld CA für Zertifikatanmeldung ausgewählt sein.

Im VS-NfD-Umfeld muss das Benutzerzertifikat außerdem auf einer Smartcard gespeichert werden. Hierzu müssen im Zertifikat-Objekt folgende Einstellungen für das vorgenommen werden:

Reiter **Allgemein**

- Zertifikat auf Smartcard HSM speichern: Option Smartcard wählen.

Reiter **Smartcard**

- Privater Schlüssel: Option Smartcard/HSM wählen, sodass der private Schlüssel auf der Smartcard erzeugt und gespeichert wird.

Siehe **5.1.2 Eigenes CA-Zertifikat erstellen** und **5.3.2 Eigenes Zertifikat erstellen**.

⚠ **Hinweis:** Sobald diese Änderungen gespeichert sind, ist für die Anmeldung am Admin-UI zwingend ein Zertifikat notwendig. Entspricht der CN des Zertifikats nicht dem Benutzernamen oder ist das Zertifikat nicht von der eingestellten CA ausgestellt, ist eine Anmeldung nicht mehr möglich.

2 Aufbau der Administrationsoberfläche - Standardansicht

Die TMA verfügt über eine Standard- und eine Expertenansicht. In der Standardansicht stehen die wichtigsten Funktionen für ein zuverlässiges PKI- und Zertifikatmanagement zur Verfügung, während in der Expertenansicht die gesamten Funktionen konfigurierbar sind.

Nach der Anmeldung öffnet sich das Dashboard der TMA. Dieses zeigt einen Überblick über den aktuellen Zustand der TMA.

Die Administrationsoberfläche ist in mehrere Bereiche aufgeteilt, die der Navigation dienen. Die Bereiche sind im Folgenden beschrieben.

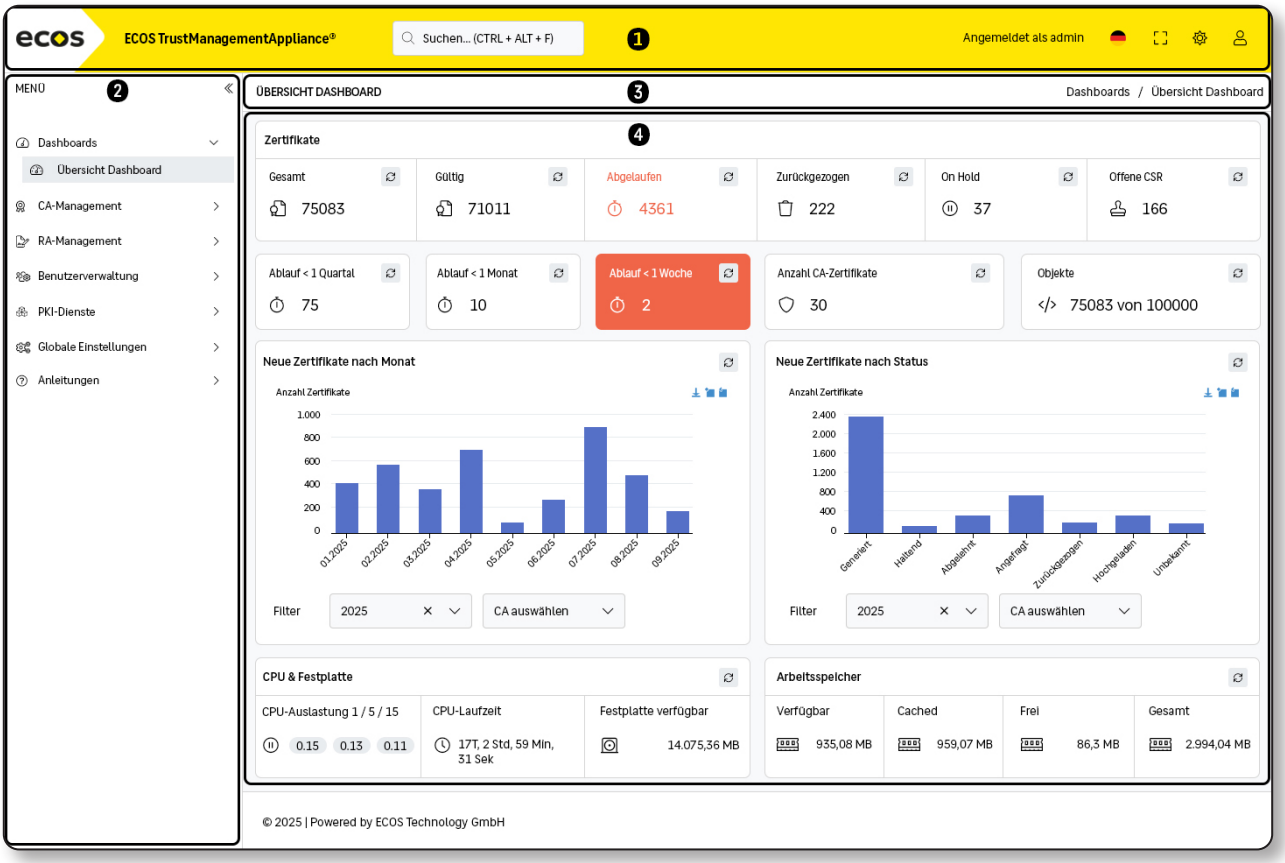


Abb. 2.01: *Hauptansicht der Administrationsoberfläche*

❶ Header
❷ Seitenmenü
❸ Sitemap
❹ Inhalt

2.1 Header

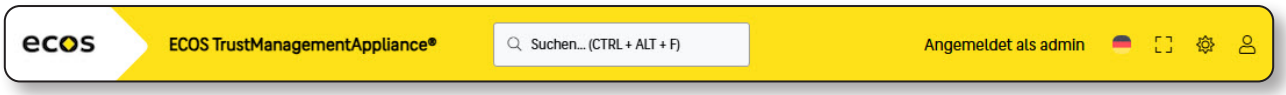


Abb. 2.02: *Header-Menü der Administrationsoberfläche*

ECOS-Logo: Über das Logo öffnet sich das Dashboard.

Menü: Über dieses Symbol wird das Seitenmenü eingeblendet. Ist das Menü eingeblendet, wird das Symbol nicht angezeigt.

Suche: Über die Suche werden CA-Zertifikate, Zertifikate, Benutzer und Menüpunkte gesucht (siehe **2.1.1 Suche**).

Angemeldet als: Hier wird angezeigt, welches Benutzerkonto eingeloggt ist.

Sprache: Über dieses Symbol wird die Anzeigesprache der Administrationsoberfläche geändert. Aktuell stehen die Sprachen Englisch und Deutsch zur Verfügung.

Vollbildschirm: Über dieses Symbol wird der Vollbildschirm aktiviert und deaktiviert.Im Vollbildschirm verschwinden die Menü- und Adressleisten des Browsers.

Hell-/Dunkelmodus: Über dieses Symbol wird zwischen einem hellen und einem dunklen Design gewechselt.

Benutzer: Über dieses Symbol öffnet sich eine Dropdown-Liste, in dem benutzerspezifische Einstellungen vorgenommen werden können.

Kontoeinstellungen: Es werden Informationen zum eingeloggten Account aufgerufen. Es können z.B. Logindaten, inkl. Kennwort oder persönliche Informationen geändert werden.

Expertenansicht: Es wird in den Expertenmodus gewechselt.

Self-Service-Portal: Es wird zum Self-Service-Portal gewechselt, über das Zertifikatanfragen gestellt werden können.

Abmelden: Der Benutzer wird von der Trust Management Appliance abgemeldet.

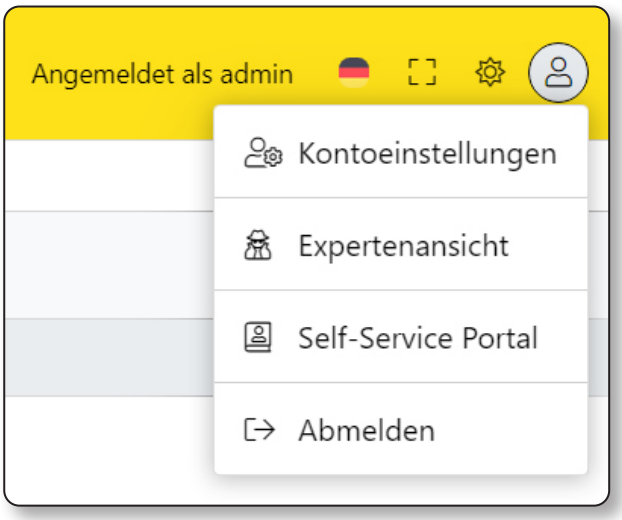


Abb. 2.03: *Untermenü Benutzer*

2.1.1 Suche

Über das Suchfeld können verschiedene Objekte innerhalb der TMA gesucht werden. Dazu zählen CA-Zertifikate, Zertifikate, Benutzer und Menüpunkte.

Die Suche mit Wildcards * ist möglich. Das System setzt automatisch Wildcards vor und nach dem Suchbegriff, die allerdings nicht angezeigt werden.

Nach Eingabe von mindestens drei Zeichen erscheint ein Dropdownpanel, das die Suchergebnisse in den vier Kategorien Menü, CA-Zertifikate, Zertifikate und Benutzer auflistet.

Über dieses Panel können die Objekte direkt aufgerufen werden.

Werden mehr als 5 Einträge in einer Kategorie gefunden, können die weiteren Einträge über **Mehr anzeigen** (unterhalb der Liste oder in der Kategorieleiste) in einem neuen Fenster angezeigt werden.

Schließen: Das Panel mit den Suchergebnissen wird geschlossen und die Eingabe im Suchfeld wird gelöscht.

Alle Suchergebnisse: Es öffnet sich ein Fenster, in dem die Suchergebnisse angezeigt werden. Über das Suchfeld oben links kann der Suchbegriff angepasst oder geändert werden.

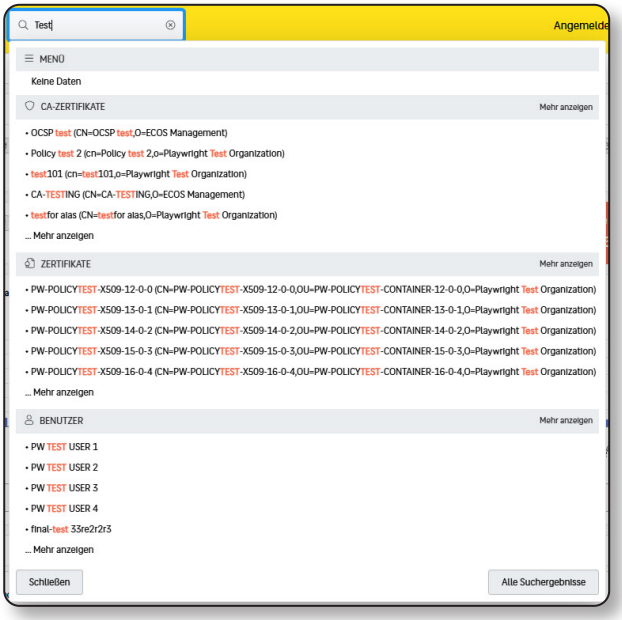


Abb. 2.04: *Anzeige der Suchergebnisse*

Die Suchergebnisse können über die Schaltflächen oben rechts gefiltert werden. Die Zahl hinter jedem Filterbutton gibt an, wie viele Suchergebnisse in dieser Kategorie vorhanden sind.

Alle: Es werden alle Suchergebnisse, die den Suchbegriff enthalten angezeigt.

CA-Zertifikate: Es werden nur die CA-Zertifikate angezeigt, die den Suchbegriff enthalten.

Zertifikate: Es werden nur die Zertifikate angezeigt, die den Suchbegriff enthalten.

Benutzer: Es werden nur Benutzer angezeigt, die den Suchbegriff enthalten.

Die Menüpunkte, die den Suchbegriff enthalten, werden in dem Übersichtfenster nicht angezeigt.

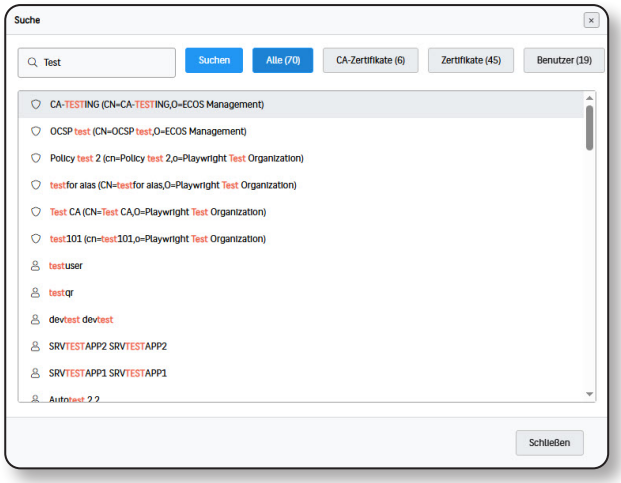


Abb. 2.05: *Übersicht der Suchergebnisse*

2.2 Sitemap

Unterhalb des Headers und oberhalb des Seiteninhalts befindet sich die Sitemap. Auf der linken Seite steht der Seitentitel. Rechts ist eine Navigationshilfe, die geöffnet werden kann. Es erscheint eine Übersicht des Bereichs mit seinen Unterkategorien.



Abb. 2.06: *Sitemap-Anzeige*

2.3 Seitenmenü

Das Seitenmenü unterstützt bei der Navigation der einzelnen Bereiche der Trust Management Appliance. Es stehen verschiedene Bereiche zur Verfügung, z.B. **Dashboards, CA-Management**, etc.



Doppelpfeil: Über dieses Symbol wird das Seitenmenü ausgeblendet. Im Header erscheint das Menü-Symbol neben dem Logo, um das Seitenmenü wieder einzublenden.

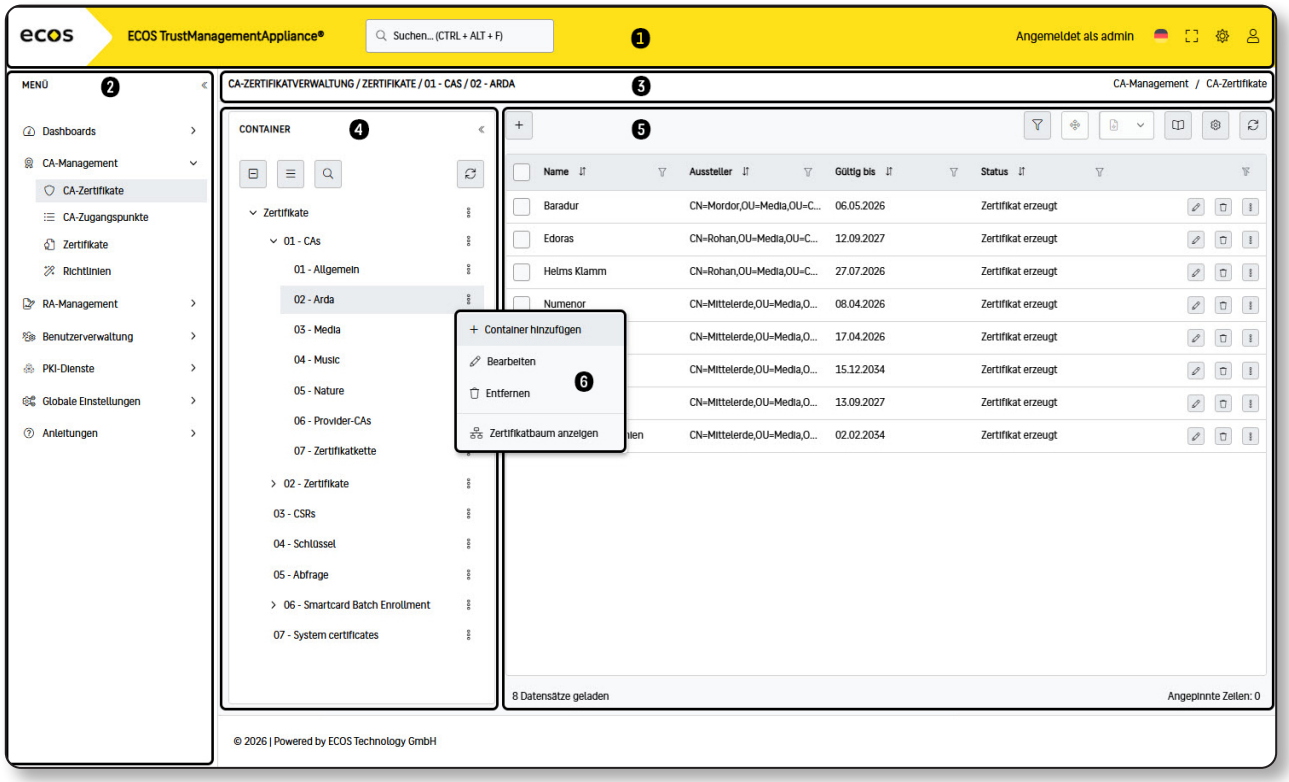


Abb. 2.07: *Containeransicht der Administrationsoberfläche*

1. Header
2. Seitenmenü
3. Sitemap
4. Containermenü
5. Inhalt
6. Kontextmenü

2.4 Container-Menü

Die verschiedenen Objekte der TMA werden in Containern gruppiert. Ein Container funktioniert dabei ähnlich einem Ordner in einem Dateisystem. Es gibt zum einen spezielle Container, die bestimmte Objekte zu einem Thema zusammenfassen, z.B. der Container: Benutzer, in dem alle Benutzer-Objekte zusammengefasst sind. In der Regel werden diese Container automatisch beim Erstellen eines der untergeordneten Objekte mit angelegt. Zum anderen können allgemeine Container angelegt werden, die mehrere Objekte des gleichen Typs zusammenfassen. Damit ist es z.B. möglich eine größere Gruppe von Objekten für eine bestimmte Funktion auszuwählen oder einen Speicherort für automatische angelegte Objekte zu bestimmen.

Das Container-Menü steht in den Bereichen **CA-Management** und **RA-Management** zur Verfügung. Es bildet die Ordnerstruktur für die CA-Zertifikate und Zertifikate sowie die CSRs ab.

Doppelpfeil: Über dieses Symbol wird das Container-Menü ausgeblendet. In der Seite erscheint ein Doppelpfeil-Symbol, um das Container-Menü wieder einzublenden.

Minimieren/Maximieren: Über dieses Symbol werden alle Container und Untercontainer eingeblendet bzw. wieder ausgeblendet.

Inhalte des Containers und seiner Untercontainer anzeigen: Über dieses Symbol werden auch die Inhalte aus den Untercontainern des ausgewählten Containers in der Tabelle angezeigt bzw. wieder ausgeblendet. Ist die Funktion aktiv, ist das Symbol je nach eingestelltem Farbschema farbig hinterlegt.

Suche: Über dieses Symbol wird das Suchfeld eingeblendet. Sie können nach Containern suchen. Ist die Funktion aktiv, ist das Symbol je nach eingestelltem Farbschema farbig hinterlegt.

Aktualisieren: Über dieses Symbol wird das Container-Menü neugeladen.

Weitere Optionen: Über dieses Symbol öffnen sich weitere Funktionen für den jeweiligen Container.

Container hinzufügen: Über dieses Symbol wird ein neuer Container bzw. Untercontainer hinzugefügt. Es öffnet sich ein Fenster zur Konfiguration des Containers.

Bearbeiten: Über dieses Symbol wird der ausgewählten Container bearbeitet. Es öffnet sich ein Fenster zur Konfiguration des Containers.

Entfernen: Über dieses Symbol wird der ausgewählte Container gelöscht. Alle Inhalte dieses Containers werden mitgelöscht.

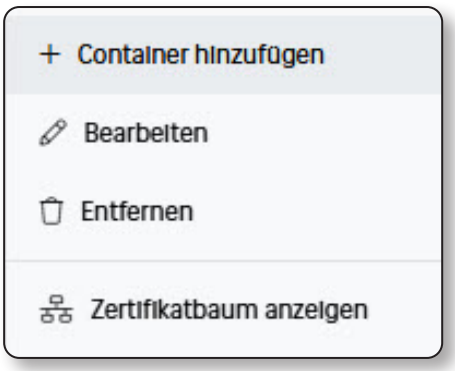


Abb. 2.08: *Weitere Optionen für Container*

Zertifikatbaum anzeigen: Über dieses Symbol wird der Zertifikatbaum der im Container befindlichen CA-Zertifikaten mit dem Container als Wurzel angezeigt. Zusätzlich wird ein Bericht zu den Zertifikaten erstellt.

Vertikaler Schwarzer Balken: Mit diesem Balken lässt sich die Breite des Container-Menüs verändern.

2.5 Seite

Auf der Seite wird der eigentliche Inhalt der Bereiche und Container angezeigt, i.d.R. in Tabellenform. Je nach Inhalt stehen verschiedene Funktionen und Filter zur Verfügung.

2.5.1 Tabellen

Tabellen listen die Inhalte der Bereiche und Container auf, z.B. die CA-Zertifikate, Benutzerkonten oder die Zertifikatrequests (CSR).

Über der Tabelle befinden sich je nach Bereich verschiedene Buttons zur Bearbeitung der Tabellen. Die bereichsspezifischen Buttons werden im jeweiligen Abschnitt erklärt.

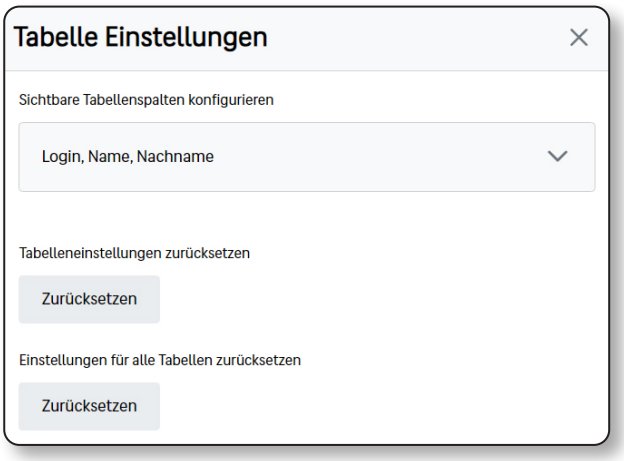


Abb. 2.09: *Tabelleneinstellungen*

Hinzufügen: Über dieses Symbol werden neue Objekte hinzugefügt. Es öffnet sich ein Fenster bzw. ein Assistent zur Konfiguration des neuen Objekts.

Dokumentation: Über dieses Symbol wird in einem neuen Fenster eine ausführliche Anleitung zu dem jeweiligen Bereich angezeigt.

Tabelleneinstellungen: Über dieses Symbol öffnen sich die Tabelleneinstellungen in einem neuen Fenster. Die angezeigten Spalten können über die Dropdown-Liste angepasst, neue ausgewählt oder vorhandene ausgeblendet werden. Ebenso können die Einstellungen wieder zurückgesetzt werden.

Aktualisieren: Über dieses Symbol wird die Tabelle neugeladen.

Aufbau der Tabellen

Die Tabellen haben voreingestellte Spalten, die sich je nach Bereich unterscheiden. Über die Tabelleneinstellungen oberhalb der Tabelle können die angezeigten Spalten angepasst werden.

Jede Spalte kann über den Tabellenkopf alphabetisch auf- bzw. absteigend sortiert werden. Über den Filter neben der Spaltenbezeichnung können individuelle Filter eingestellt werden. Es öffnet sich ein Dialog, in dem verschiedene Bedingungen und Regeln konfiguriert und miteinander verknüpft werden können.

In der letzten Spalte sind Buttons zur Bearbeitung vorhanden. Die Spalte kann nicht ausgeblendet werden und besitzt keine Filterfunktionen.

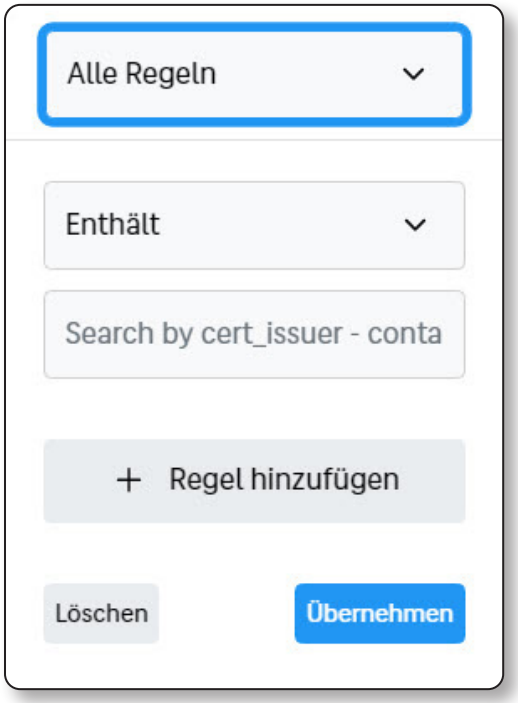


Abb. 2.10: *Filtereinstellungen*

Bearbeiten: Über dieses Symbol öffnet sich das Objekt zur Ansicht und Bearbeitung in einem neuen Fenster.

Löschen: Über dieses Symbol wird das Objekt gelöscht.

Weitere Optionen: Über dieses Symbol sind weitere Optionen verfügbar. Sie richten sich nach dem jeweiligen Bereich und stimmen mit dem Kontextmenü überein.

Unterhalb der Tabellen befindet sich die Anzahl der angezeigten Objekte. Sind weitere Objekte vorhanden erscheint der Hinweis **(weitere vorhanden)**. Durch Scrollen werden weitere Objekte angezeigt.

2.5.2 Kontextmenü

Jedes Objekt besitzt ein Kontextmenü, dass mit einem Rechtsklick geöffnet wird. Je nach Objekttyp stehen verschiedene Optionen zur Verfügung.

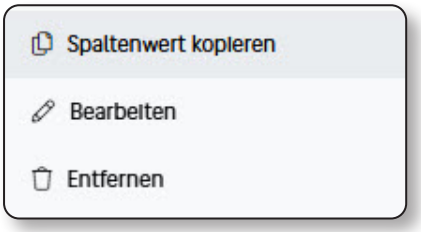


Abb. 2.11: *Kontextmenü in Tabellen*

Spaltenwert kopieren: Der Wert, der in dieser Spalte steht, wird in die Zwischenablage kopiert.

Bearbeiten: Das Objekt öffnet sich zur Ansicht und Bearbeitung.

Entfernen: Das Objekt wird gelöscht.

2.5.3 Assistent und Dialogfenster

Um neue Objekte zu erstellen, öffnet sich i.d.R. ein Assistent mit mehreren Seiten, die je nach Objekttyp unterschiedliche Informationen abfragen und anzeigen.

Allen Assistenten gemein ist der Aufbau: Links befinden sich die Konfigurationsfelder und rechts eine Hilfe zu den angezeigten Einstellungen.

Für die richtige Funktionsweise erforderliche Konfigurationen sind mit einem Sternchen gekennzeichnet.

Über die Buttons **Weiter** und **Zurück** oder über die Seitenzahlen oberhalb der Konfigurationsfelder wird zwischen den Seiten des Assistenten geblättert.

Rechts in der Kopfzeile von Assistenten und Dialogfenstern stehen einige Funktionen zur Verfügung.



Aktualisieren: Das Fenster des Assistenten oder Dialogs wird neugeladen.



Dokumentation: Es öffnet sich ein Fenster mit dem entsprechenden Kapitel in den Anleitungen. Diese Option steht bei Assistenten zur Verfügung.



Vollbild: Das Fenster wird im gesamten Browserfenster angezeigt.



Schließen: Der Assistent oder der Dialog wird geschlossen.

Der spezifische Aufbau wird im jeweiligen Bereich erklärt.

3 Aufbau der Expertenansicht

3.1 Wechsel in die Expertenansicht

Nachdem die Lizenzen der TMA eingespielt sind, öffnet sich nach der Anmeldung die Standardansicht. Um in die Expertenansicht zu wechseln, öffnen Sie das Menü unterhalb des Benutzersymbols rechts im Header der Standardansicht. Mit einem Klick auf die Option Expertenansicht wechselt die Ansicht der Administrationsoberfläche.

Die Administrationsoberfläche in der Expertenansicht besteht aus verschiedenen Bereichen:

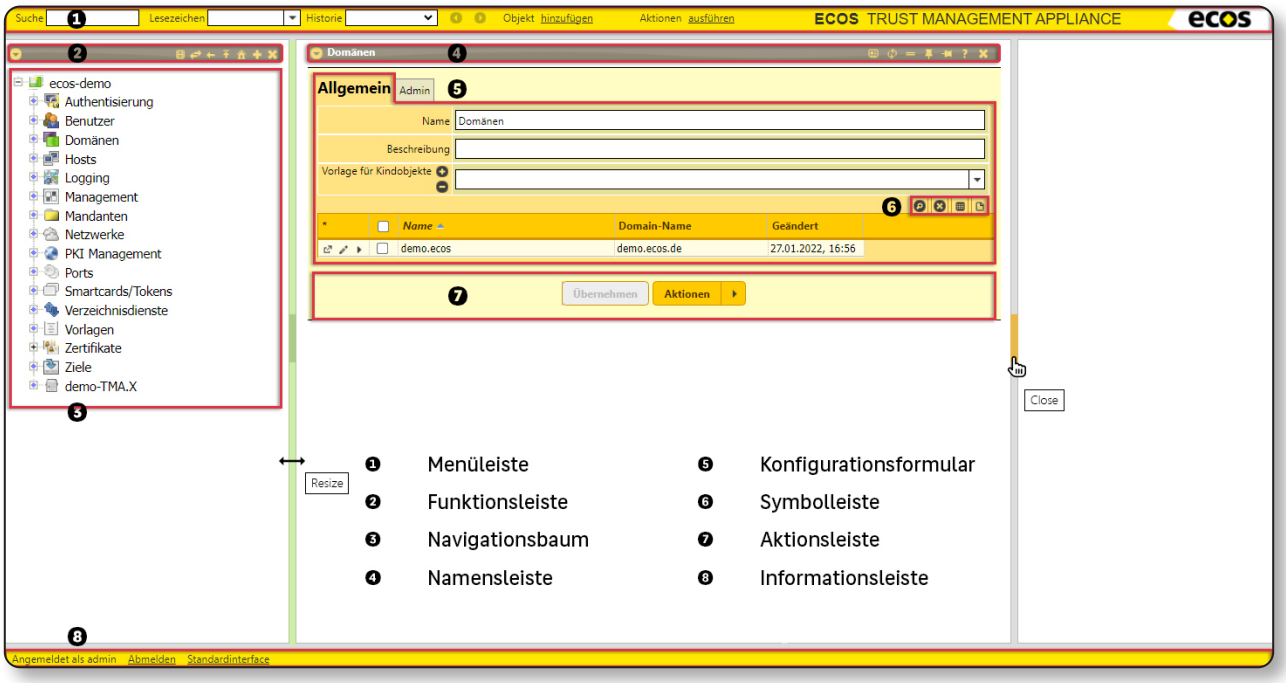


Abb. 3.01: *Aufbau der Administrationsoberfläche in der Expertenansicht*

3.2 Menüleiste

Suche: Über das Suchfeld kann nach einem bestimmten angelegten Konfigurationsobjekt gesucht werden.

Lesezeichen: Über die Dropdown-Liste kann ein Lesezeichen ausgewählt werden.

Historie: Über die Dropdown-Liste wird eine Übersicht der letzten geöffneten Objekte angezeigt. Mit den Pfeiltasten kann zwischen den Objekten gewählt werden.

Objekt hinzufügen: Es öffnet sich ein Fenster mit einer Übersicht über alle anzulegenden Objekte.

Auf der rechten Seite befindet sich der Namen der Software sowie das Herstellerlogo der ECOS Technology GmbH.

3.3 Navigationsbaum

Der Navigationsbaum dient zum Navigieren und hierarchischen Ordnen der einzelnen Konfigurationsobjekte. Oberhalb des Baums befindet sich die Funktionsleiste.

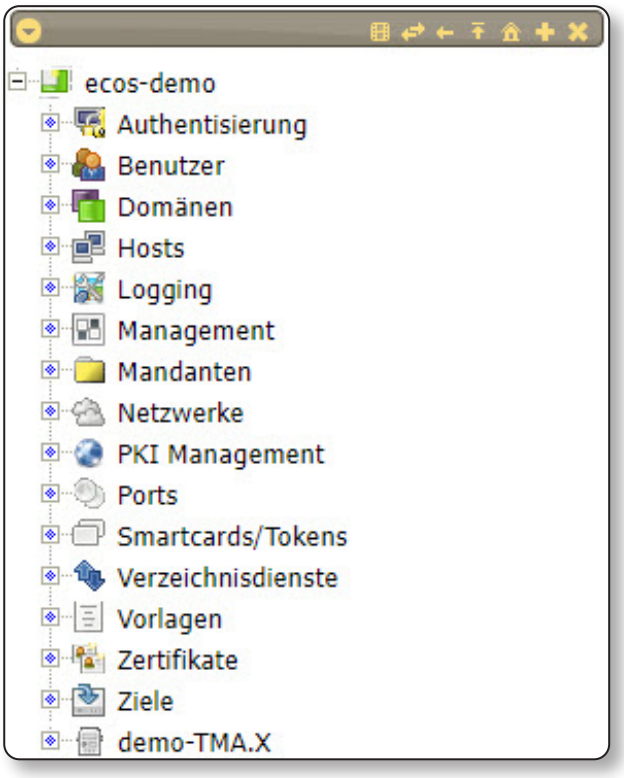


Abb. 3.02: *Navigationsbaum*

3.3.1 Funktionsleiste

Verstecken/Anzeigen: Über dieses Symbol wird die Baumstruktur aus- bzw. eingeklappt. Standardmäßig ist der Baum ausgeklappt.

Checkbox zum Verschieben umschalten: Über dieses Symbol erscheinen Checkboxen vor den einzelnen Objekten im Baum, die mit einem Klick aktiviert werden können. Dadurch lassen sich mehrere Objekte gleichzeitig verschieben.

Synchronisation mit aktuellem Objekt an/aus: Über dieses Symbol wird die Synchronisation mit dem aktuell geöffneten Konfigurationsobjekt aktiviert. Ist die Synchronisation aktiv, wird das Symbol fett formatiert.

Jetzt mit aktuellem Objekt synchronisieren: Über dieses Symbol wird die Synchronisation manuell angestoßen.

Baum ab aktuellem Objekt: Über dieses Symbol wird der Baum auf den Bereich unter dem geöffneten Objekt reduziert.

Gesamten Baum anzeigen: Über dieses Symbol wird der gesamte Baum wieder angezeigt.

Weiteren Baum anzeigen: Über dieses Symbol wird ein weiterer Baum unterhalb des aktuellen Baums angezeigt.

Baum schließen: Über dieses Symbol wird der Baum geschlossen. Dies ist nur möglich, wenn mehr als ein Baum angezeigt wird.

3.3.2 Baum

Der Baum ist hierarchisch aufgebaut. An oberster Stelle findet sich das Organisationsobjekt, dass den übergeordneten Namen festlegt.

Unterhalb befinden sich verschiedene Container, die alphabetisch sortiert sind und unterschiedliche Konfigurationsobjekte zusammenfassen. Über die Plus- und Minussymbole vor den Containern und

Objekten werden die untergeordneten Objekte angezeigt bzw. wieder ausgeblendet.

Die einzelnen Objekte können durch Gedrückthalten der Maus innerhalb des Baums verschoben werden, sofern das Objekt an der neuen Position angelegt werden kann.

Über das Kontextmenü können neue Objekte und Container angelegt werden.

3.3.3 Kontextmenü

Das Kontextmenü wird mit einem Rechtsklick auf eines der Konfigurationsobjekte oder Container geöffnet.

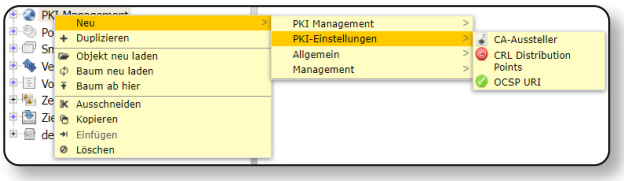


Abb. 3.03: *Navigationsbaum - Kontextmenü*

Neu: Es wird eine Liste mit allen Objekten oder Containern angezeigt, die sich unterhalb des ausgewählten Containers oder Objekts anlegen können. Dies variiert je nach ausgewähltem Container. Bestimmte Objekte und Container können nur einmal angelegt werden.

Duplizieren: Das ausgewählte Objekt wird dupliziert. Es öffnet sich ein Fenster, in der die Anzahl der Duplikate eingetragen wird. Die Duplikate werden im gleichen Pfad wie das Original angelegt und durchnummeriert.

Objekt neu laden: Das Objekt/der Container wird aktualisiert.

Baum neu laden: Der gesamte Baum wird aktualisiert.

Baum ab hier: Der Baum wird auf die Objekte/Container unterhalb des Objekts reduziert.

Ausschneiden: Das Objekt wird ausgeschnitten und kann an einer anderen Stelle im Baum eingefügt werden, sofern es unterhalb des neuen Containers angelegt werden kann. Ein Benutzerobjekt kann z.B. nicht in den Container: Zertifikate eingefügt werden.

Kopieren: Das Objekt wird kopiert und kann an kann an einer anderen Stelle im Baum eingefügt werden, sofern es unterhalb des neuen Containers angelegt werden kann. Ein Benutzerobjekt kann z.B. nicht in den Container: Zertifikate eingefügt werden.

Einfügen: Das zuvor kopierte oder ausgeschnittene Objekt wird eingefügt, sofern es unterhalb des neuen Containers angelegt werden kann. Ein Benutzerobjekt kann z.B. nicht in den Container: Zertifikate eingefügt werden.

Löschen: Das Objekt wird gelöscht.

3.4 Konfigurationsbereich 1 & 2

In den Konfigurationsbereichen werden die Objekte zum Anlegen oder Bearbeiten geöffnet. Mit den Trennlinien zwischen dem Navigationsbaum und den beiden Konfigurationsbereichen kann die Breite der drei Bereiche angepasst werden. Mit einem Klick auf den dunkleren Bereich der Trennlinien wird der Navigationsbaum (links) oder den Konfigurationsbereich 2 (rechts) aus bzw. wieder eingeblendet.

3.4.1 Konfigurationsobjekte

Das Konfigurationsobjekt dient zum Anlegen und Bearbeiten von Diensten, Benutzern, Objekten, Zertifikaten, etc. Das Konfigurationsobjekt besteht aus der Namensleiste, dem Konfigurationsformular und der Aktionsleiste.

3.4.1.1 Neues Objekt anlegen

Es gibt verschiedene Möglichkeiten neue Objekte in der TMA anzulegen. Legen Sie ein Objekt an, das unter einem bestimmten Container geordnet wird, wird der Container automatisch mit angelegt, wenn dieser noch nicht existiert. Einige Objekte können nur ein einziges Mal angelegt werden.

Über den Navigationsbaum

Eine Variante ist über das Kontextmenü eines Containers im Navigationsbaum. Mit einem Rechtsklick öffnet sich das Kontextmenü und es wird Ihnen unter dem Punkt Neu eine Auflistung der Objekte angezeigt, die Sie in dem Container anlegen können. Im Kontextmenü des Organisationsobjekts finden Sie alle Konfigurationsobjekte, die Sie in der TMA anlegen können, sortiert nach Kategorien.

Über Objekt hinzufügen

Über Objekt hinzufügen in der Menüleiste oder öffnet sich eine Auflistung aller Konfigurationsobjekte für die TMA. Sie sind nach ihrer jeweiligen Kategorie sortiert. Über **mehr** werden weitere Objekte angezeigt, die nur unterhalb des Objekts angelegt werden können.

Über ein Konfigurationsobjekt

In Konfigurationsobjekten, in denen andere Objekte referenziert werden, können Sie mit einem Rechtsklick in das entsprechende Feld ein neues Objekt anlegen. Handelt es sich um einen Container, gibt es oberhalb der Tabellen , in der die Objekte aufgelistet werden, einen Button **Objekt hinzufügen**, um ein neues Objekt anzulegen. Es öffnet sich ein Konfigurationsformular als schwebendes Fenster. Die notwendigen Daten werden eingegeben und mit **Übernehmen** wird das Objekt gespeichert. Das neu angelegte Objekt ist automatisch im Konfigurationsobjekt ausgewählt.

3.4.1.2 Namensleiste

Verstecken/Anzeigen: Über dieses Symbol kann die Baumstruktur aus- bzw. eingeklappt werden. Standardmäßig ist der Baum ausgeklappt.

Name: Es wird der vergebene Name des Konfigurationsobjekts/Containers angezeigt.

Übernehmen: Über dieses Symbol können die Änderungen im Objekt gespeichert werden. Es wird nur angezeigt, wenn Änderungen vorgenommen worden sind.

Ansicht: Über dieses Symbol öffnet sich ein Untermenü, in dem verschiedene Einstellungen in Bezug auf die Anzeige eingestellt werden können.

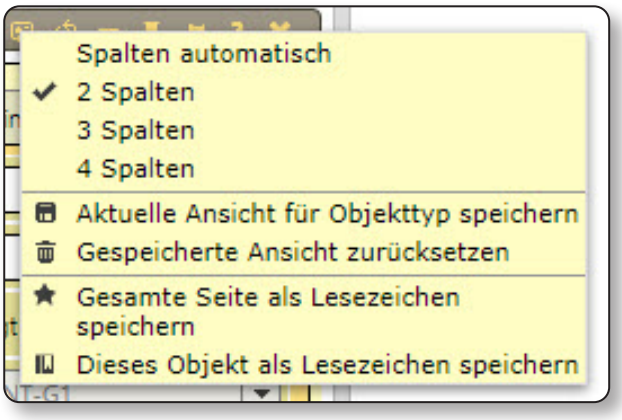


Abb. 3.04: *Konfigurationsobjekt - Ansicht*

Spalten automatisch: Die Anzahl der Spalten im Konfigurationsobjekt werden automatisch an die Breite des Konfigurationsbereichs angepasst. Es werden mindestens 2 Spalten angezeigt.

2 Spalten: Die Felder aller Konfigurationsobjekte werden in zwei Spalten angeordnet. Standardmäßig ist diese Auswahl aktiv.

3 Spalten: Die Felder aller Konfigurationsobjekte werden in drei Spalten angeordnet.

4 Spalten: Die Felder aller Konfigurationsobjekte werden in vier Spalten angeordnet.

Aktuelle Ansicht für Objekttyp speichern: Die aktuelle Spaltenanzahl wird für diesen Objekttyp gespeichert. Neue und andere Objekte des gleichen Typs werden mit der gleichen Anzahl der Spalten geöffnet.

Gespeicherte Ansicht zurücksetzen: Die Ansicht für diesen Objekttyp wird wieder auf den Standard (2 Spalten) zurückgesetzt.

Gesamte Seite als Lesezeichen speichern: Alle geöffneten Objekte werden als Lesezeichen gespeichert, die über die Menüleiste anschließend zur Auswahl stehen.

Dieses Objekt als Lesezeichen speichern: Es wird das einzelne Objekt als Lesezeichen gespeichert. Weitere geöffnete Objekte werden nicht mit im Lesezeichen gespeichert.

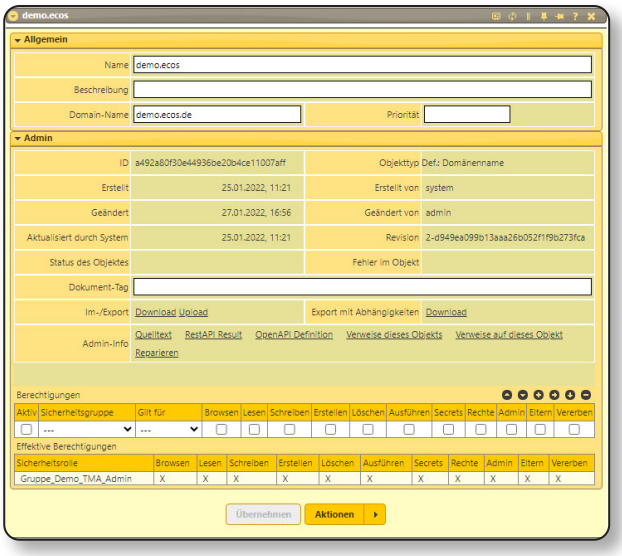


Abb. 3.05: *Konfigurationsobjekt - Untereinander anzeigen*

Objekt neu laden: Das Konfigurationsobjekt wird aktualisiert und neu geladen.

Untereinander/Nebeneinander anzeigen: Die Reiter des Konfigurationsobjekts werden untereinander bzw. wieder nebeneinander angezeigt.

Im Hauptfenster anpinnen: Das Objekt wird im Konfigurationsbereich 1 angepinnt und schließt sich nicht, wenn ein weiteres Objekt geöffnet wird. Das Symbol verschwindet, wenn das Objekt angepinnt ist.

Im rechten Fenster festpinnen: Das Objekt wird in den Konfigurationsbereich 2 verschoben und dort angepinnt. Mit der Option Im Hauptfenster anpinnen wird es wieder in den Konfigurationsbereich 1 verschoben.

Hilfe: Die Onlinehilfe für diesen Objekttyp wird im Konfigurationsbereich 2 geöffnet. Dort finden Sie ausführliche Erklärungen zu dem jeweiligen Objekttyp und jedem einzelnen Konfigurationsfeld.

Schließen: Das Objekt wird geschlossen. Haben Sie ungespeicherte Änderungen vorgenommen, öffnet sich ein Fenster, das Sie darauf hinweist. Sie können die Änderungen speichern, verwerfen oder das Schließen abbrechen.

3.4.1.3 Kontextmenü

Über die Namensleiste wird das Kontextmenü des Objekts aufgerufen. Es werden die Funktionen der Namensleiste und des Kontextmenüs im Navigationsbaum angezeigt.

Gleiches Objekt erstellen: Es öffnet sich ein neues Konfigurationsobjekt des gleichen Typs, das den gleichen Namen schon vorkonfiguriert hat. Die Einstellungen können geändert werden.

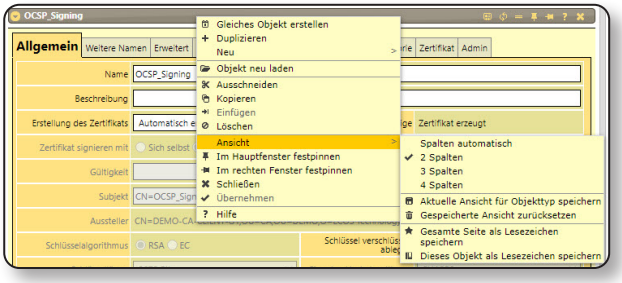


Abb. 3.06: *Kontextmenü eines Konfigurationsobjekts*

3.4.1.4 Konfigurationsformular

Im Konfigurationsobjekt können verschiedene Einstellungen vorgenommen werden. Die angezeigten Attribute und ihre Steuerelemente im Konfigurationsobjekt hängen sehr stark vom jeweiligen Objekttyp ab:

Steuerelement	Beschreibung
Reiter	Die Reiter teilen das Konfigurationsobjekt in verschiedene Kategorien auf.
Feld	Ein einzeiliges Textfeld zur manuellen Eingabe von Text oder Werten.
Dropdown-Liste	Eine ausklappbare Liste zur Auswahl vorgegebener Optionen.
Checkbox	Eine Box zum Aktivieren/Deaktivieren einer Option, Funktion oder eines Diensts.

Steuerelement	Beschreibung
Optionsfeld	Eine Anzahl von Radiobuttons zur Auswahl einer Option.
Button	Eine Schaltfläche zum Bestätigen oder Ausführen der zugeordneten Funktion.
Textfeld	Mehrzeiliges Textfeld zur manuellen Eingabe von Text, Werten oder Quelltext.
Symbolleiste	Werkzeugleiste zum Einfügen, Kopieren, Verschieben oder Löschen in einer Tabelle.
Tabelle	Eine Tabelle zur Auflistung von Ergebnissen oder der Verkettung von Funktionen.
Link	Ein Link zum Hoch- oder Herunterladen von Dateien.

Für einzelne Attribute kann die Hilfe angezeigt werden, indem auf die Bezeichnung des Attributs geklickt wird. Es öffnet sich ein kleines Fenster mit dem Hilfetext für dieses spezielle Attribut.

3.4.1.5 Tabellen

Einige Konfigurationsobjekte zeigen Ergebnistabellen an oder nutzen Tabellen zur Konfiguration und Verkettung von Funktionen.

Symbolleiste

Oberhalb der Tabelle befindet sich die Symbolleiste, die verschiedene Einstellungsmöglichkeiten und Operationen für die Tabelle bereitstellt.

Blättern: Zwischen den Seiten kann vor und zurück oder direkt zur ersten bzw. letzten Seite geblättert werden. Neben den Pfeilen zum Blättern wird die Anzahl der gesamten Seiten und Einträge in der Tabelle angezeigt.

Einträge anzeigen: Hier kann die Anzahl der Einträge, die pro Seite angezeigt werden sollen, bestimmt werden.

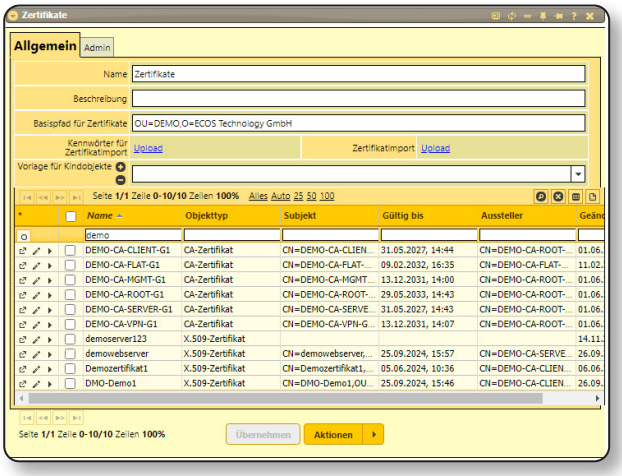


Abb. 3.07: *Tabellenfilter*

Filter anzeigen: Mithilfe der eingeblendeten Felder in jeder Spalte können die Einträge gefiltert und nach bestimmten Inhalten gesucht werden. Die Groß- und Kleinschreibung wird ignoriert. Es können Filter in mehreren Spalten verknüpft werden. Folgende Suchfilter stehen zur Verfügung:

Filter	Effekt
Wert	Es wird nach der angegebenen Zeichenfolge in dieser Spalte gesucht. Es kann nach Buchstaben, Zahlen und Sonderzeichen gefiltert werden.
Beispiel:	*Ergebnis*
ca	Einträge, die die Zeichenfolge **ca** enthalten

Filter	Effekt
< / > + *Wert* *Beispiel:* **>m**	Es werden nur Einträge mit Werten größer (>) oder kleiner (<) dem angegeben Wert angezeigt. *Ergebnis:* Einträge, die mit dem Buchstaben **M** und nachfolgenden Buchstaben anfangen
! + *Wert* *Beispiel:* **!ecos**	Es werden nur Einträge angezeigt, die den angegebenen Wert nicht besitzen. *Ergebnis:* Einträge, die das Wort **Ecos** besitzen, werde herausgefiltert
*****	Es werden nur Einträge angezeigt, die einen Wert in der Spalte haben, also nicht leer sind.
-	Es werden nur Einträge mit leeren Feldern in der Spalte angezeigt.
Wert1|*Wert2* *Beispiel:* **Ecos|ca**	Es werden nur Einträge angezeigt, die entweder den ersten Wert oder den zweiten Wert haben. *Ergebnis:* Einträge, die entweder die Werte **Ecos** oder **ca** in der Spalte besitzen
Wert1.**Wert2* *Beispiel:* **Ca.*ecos**	Es werden nur Einträge angezeigt, die den ersten Wert gefolgt von dem zweiten Wert beinhalten, unabhängig von der Zeichenfolge, die zwischen den beiden Werten liegen. *Ergebnis:* Einträge, die den Wert **ca** vor dem Wert **ecos** in der Spalte stehen haben (z.B. CA-Test-Ecos)

Filterwerte entfernen: Die Filter werden zurückgesetzt und die vollständige Ergebnistabelle wird angezeigt.

Dateiexport: Die Ergebnistabelle kann als CSV- oder XLSX-Datei heruntergeladen.

Objekt hinzufügen: Es wird ein neues Konfigurationsobjekt hinzugefügt. Diese Option steht nur bei Containern zur Verfügung. Eine Liste der Objekte, die angelegt werden können, wird durch einen Klick auf das Symbol angezeigt.

Bei Konfigurationstabellen stehen folgende Funktionen in der Symbolleiste zur Verfügung:

Zeile hoch: Die markierte Zeile wird um eine Stelle nach oben geschoben.

Zeile runter: Die markierte Zeile wird um eine Stelle nach unten geschoben.

Zeile hinzufügen: Es wird eine neue Zeile am Ende der Tabelle hinzugefügt.

Zeile einfügen: Es wird eine neue Zeile unterhalb der markierten Zeile hinzugefügt.

Zeile kopieren: Die markierte Zeile wird unterhalb der Zeile dupliziert.

Markierte Zeile löschen: Die markierte Zeile wird gelöscht.

Tabellenspalten

Die angezeigten Spalten können je nach Konfigurationsobjekt über eine Feldliste im Konfigurationsformular geändert werden. Containerobjekte haben feste Spalte, die sich nach dem untergeordneten Objekttyp richten.

Über den Spaltenkopf können die Einträge auf- bzw. absteigend sortiert und das Kontextmenü aufgerufen werden.

Sortieren ^: Die Einträge werden aufsteigend sortiert.

Sortieren v: Die Einträge werden absteigend sortiert.

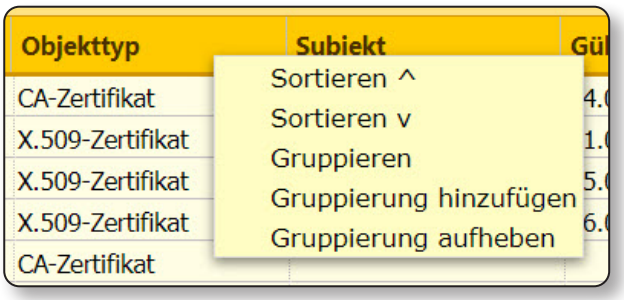


Abb. 3.08: *Tabellen - Kontextmenü einer Tabellenspalte*

Gruppieren: Die Einträge werden nach den verschiedenen Werten innerhalb der Spalte gruppiert.

Gruppierung hinzufügen: Es wird eine weitere Gruppierung zu einer bestehenden Gruppierung hinzugefügt.

Gruppierung aufheben: Alle vorhandenen Gruppierungen werden wieder aufgehoben.

Die ersten beiden Spalten sind in jeder Tabelle gleich. Sie besteht aus einer Aktionsspalte und einer Aktivierungsspalte.

Die Aktionsspalte stellt drei Aktionen zur Verfügung.

Gehe zu Objekt: Das Konfigurationsobjekt wird im Konfigurationsbereich 1 geöffnet.

Objekt editieren: Das Konfigurationsobjekt wird in einem schwebenden Fenster geöffnet.

Objekt öffnen: Das Konfigurationsobjekt wird ausgeklappt und die Einstellungen in der Tabelle angezeigt. Es können keine Änderungen vorgenommen werden.

Über das Kontextmenü dieser Spalte steht zusätzlich die Option Objekt löschen zur Verfügung.

In der Aktivierungsspalte können die Checkbox zur Auswahl des jeweiligen Objekts aktiviert werden. Es können mehrere Objekte ausgewählt werden. Wird die Checkbox im Kopf dieser Spalte ausgewählt, werden alle Objekte in der Tabelle ausgewählt.

Im Kontextmenü einer Spalte steht die Funktion Feld ändern zur Verfügung. Es öffnet sich ein schwebendes Fenster und es kann das spezielle Feld im Objekt bearbeitet werden.

3.4.1.6 Aktionsleiste

Unterhalb des Konfigurationsformular befindet sich die Aktionsleiste mit verschiedenen Buttons.

Anlegen: Das Objekt wird neu angelegt. Dieser Button steht nur bei neuen Objekten zur Verfügung.

Übernehmen: Die Änderungen im Konfigurationsobjekt werden gespeichert. Der Button ist ausgegraut, wenn keine Änderungen vorgenommen wurden.

Aktionen: Es stehen die Aktionen, die auch im Kontextmenü über die Namensleiste auswählbar sind, zur Verfügung.

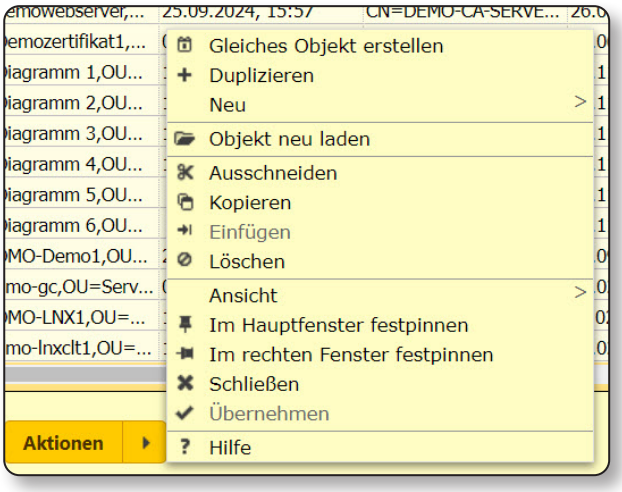


Abb. 3.09: *Aktionen der Aktionsleiste*

3.5 Informationsleiste

Die Informationsleiste schließt den Navigationsbaum und die Konfigurationsbereiche ab.

Angemeldet als: Hier wird angezeigt, welches Benutzerkonto eingeloggt ist.

Abmelden: Der Benutzer wird von der Trust Management Appliance abgemeldet.

Standardinterface: Es wird von der Expertenansicht in die Standardansicht zurückgewechselt.

3.6 Werkzeuge des Systems

Jedes Konfigurationsobjekt auf der TMA besitzt Reiter zur Konfiguration bestimmter Einstellungen. Ebenso gibt es Reiter, die Verwaltungsinformationen, Logs und Aktionen zur Verfügung stellen.

3.6.1 Reiter Admin

Der Reiter steht in jedem Konfigurationsobjekt zur Verfügung. Er fasst Verwaltungsinformationen zusammen.

Im oberen Bereich des Reiter befindet sich die eindeutige ID und der Objekttyp, wie er auch in der

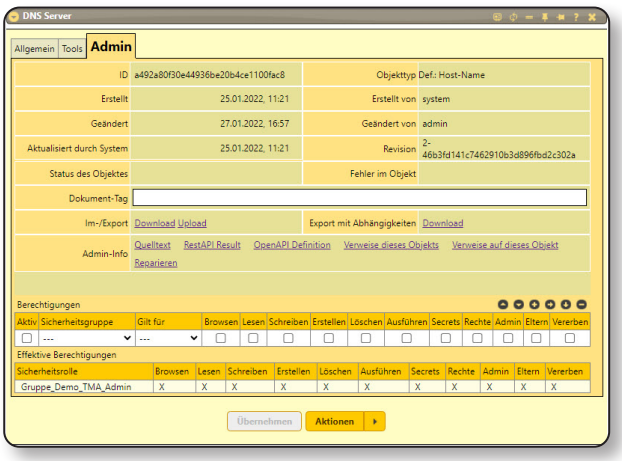


Abb. 3.10: *Reiter "Admin"*

Online-Hilfe angezeigt wird. Es werden Informationen angezeigt, wann das Objekt erstellt und zuletzt geändert wurde und von wem, welche Revision das Objekt hat, sowie den Status und die Fehler des Objekts.

Des Weiteren gibt es verschiedene Funktionen, die über den Reiter Admin ausgeführt werden können.

Im-/Export: Die Daten des Konfigurationsobjekts können mit allen untergeordneten Objekten in einer Datei herunterladen und auf einem anderen System wieder hochgeladen werden.

Export mit Abhängigkeiten: Die Daten des Konfigurationsobjekts können mit allen untergeordneten Objekten in einer Datei herunterladen. Dies schließt auch alle Objekte mit ein, auf die in diesem Konfigurationsobjekt verwiesen werden (z.B. Host-Objekte).

Admin-Info:

- Quelltext: Es wird die interne Repräsentation des Konfigurationsobjekts in der Datenbank in Quelltextform angezeigt.
- RestAPI Result: Es wird das Konfigurationsobjekt als RESTAPI-Ergebnis angezeigt.
- OpenAPI Definition: Es wird die OpenAPI Definition der ECOS REST API mit den Endpoints, Schemas, Request und Responses inkl. Beispielen für das Konfigurationsobjekt angezeigt.
- Verweise dieses Objekts: Es werden die Objekte angezeigt, die in diesem Konfigurationsobjekt referenziert werden.
- Verweise auf dieses Objekt: Es werden die Objekte angezeigt, in denen dieses Konfigurationsobjekt referenziert ist.
- Reparieren: Das Objekt wird geprüft und interne Fehler repariert.

Berechtigungen: Es können Berechtigungen für Benutzerrollen konfiguriert werden.

Effektive Berechtigungen: Die vergebenen Rechte werden in der Tabelle angezeigt.

3.6.2 Reiter Log

Der Reiter Log steht nur in ausgewählten Objekten zur Verfügung und bietet Informationen über das jeweilige Konfigurationsobjekt, z.B. das Appliance-Objekt oder ein Dienst. Über die Filtermöglichkeit oberhalb der Tabelle können die Einträge durchsucht werden.

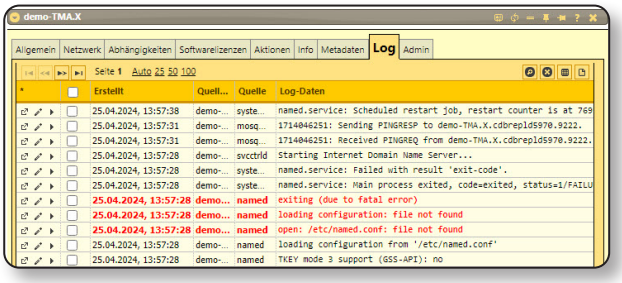


Abb. 3.11: *Reiter "Log"*



Teil II - Standardansicht

4 Dashboards

Nach der Anmeldung an der ECOS **TrustManagementAppliance®** gelangt der Benutzer auf das Dashboard der Standardansicht. Es zeigt eine voreingestellte Übersicht über den Zustand der TMA. Im oberen Bereich befinden sich Informationen zu Zertifikaten, ihrer Anzahl, ihrem Status (gültig, abgelaufen, zurückgezogen, etc.) sowie zur Anzahl offener Zertifikatrequests (CSR). Darunter werden ablaufende Zertifikate innerhalb der nächsten 3 Monate, innerhalb der nächsten 30 Tage und der nächsten 7 Tage angezeigt. Das rechte Panel zeigt die Anzahl der tatsächlich erstellten Objekte in Bezug zu den in der Lizenz enthaltenen Objekte. Dabei zählt jedes gültige Zertifikat, Geheimnis und Schlüssel als ein Objekt gewertet. Abgelaufene Objekte werden nicht berücksichtigt. Übersteigt die Zahl der angelegten Objekte die Zahl der lizensierten Objekte färbt sich das Panel rot und es erscheint eine Warnung, dass zu viele Objekte erstellt wurden und eine höhere Lizenz benötigt wird.

Zwei Diagramme stellen Abfragen zu neuen Client-Zertifikaten pro Monat und zu Client-Zertifikaten nach Status grafisch dar. Über die Filter können das Jahr und die CA beschränkt werden, für die die Diagramme dargestellt werden sollen.

Im unteren Bereich befindet sich eine Übersicht zur Hardware, auf der die TMA läuft. Sie zeigt Informationen zur CPU, des Speicherplatzes und dem Arbeitsspeicher.

Jedes Panel kann aktualisiert und aufgerufen werden, um detaillierte Informationen, z.B. zu den abgelaufenen Zertifikaten, zu erhalten.

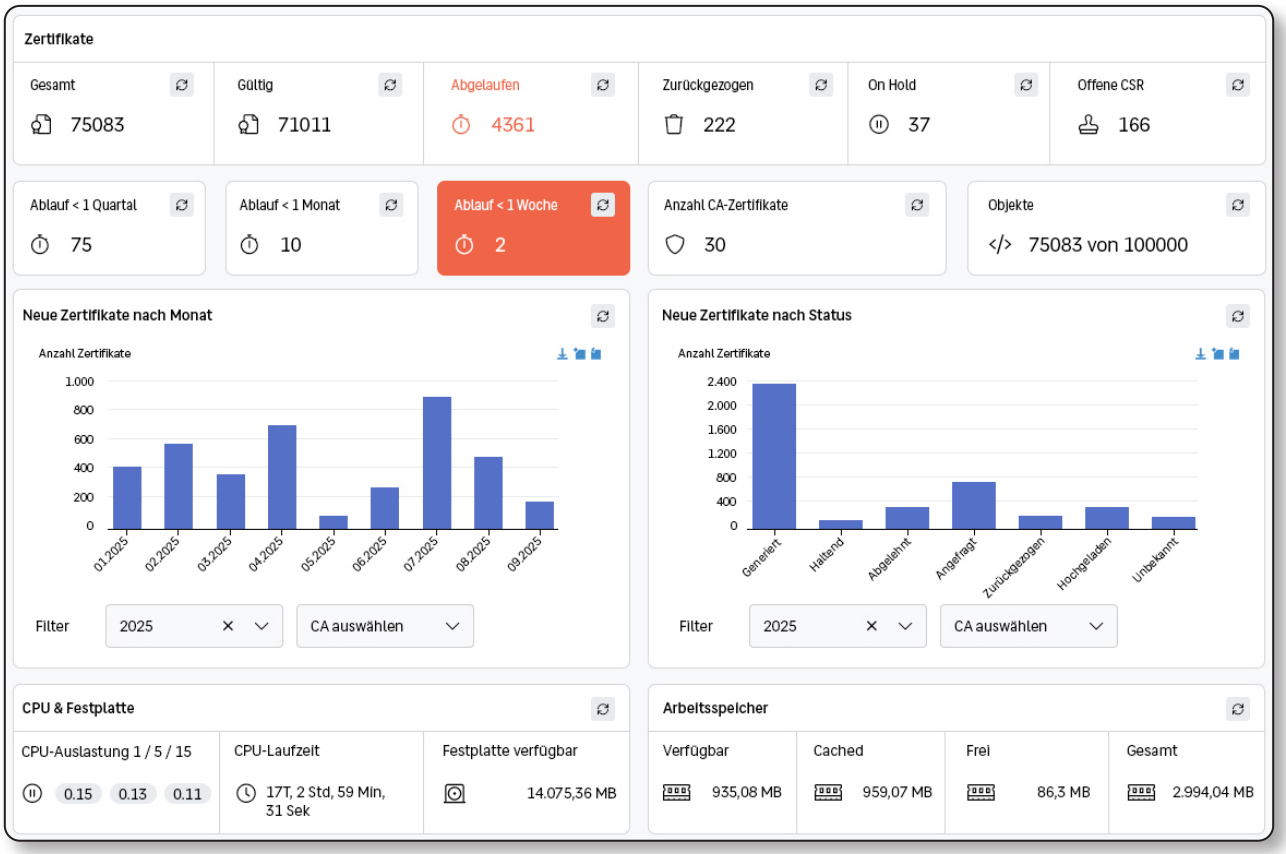


Abb. 4.01: *Dashboard der TMA*

5 CA-Management

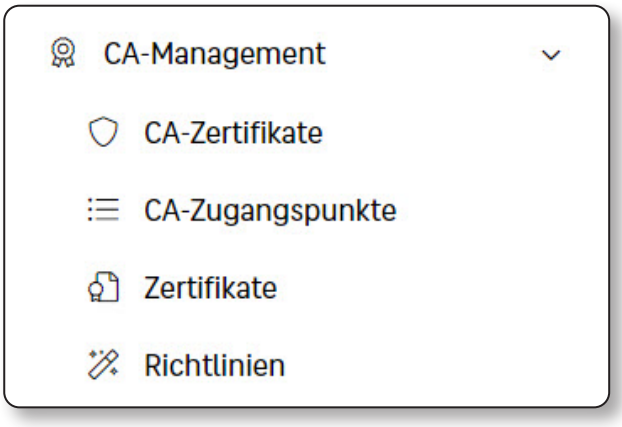


Abb. 5.01: *CA-Management im Seitenmenü*

Im CA-Management werden die CA-Zertifikate und Zertifikate verwaltet. Zertifikate bilden den Grundbaustein für IT-Sicherheit. Sie werden zur Identifikation und Authentifizierung von Benutzern, Maschinen, Diensten und Software genutzt, um eine sichere Kommunikation aufzubauen.

Die TMA unterscheidet zwischen zwei Zertifikat-Objekttypen. CA-Zertifikate umfassen alle Zertifikate, die zum Signieren von Zertifikaten und CSRs genutzt werden. Zertifikate umfassen alle Benutzer-, Client-, Server-, Geräte- und Softwarezertifikate, die nicht zum Signieren von anderen Zertifikaten genutzt werden.

Mit CA-Zertifikaten werden hierarchische und vertrauenswürdige Infrastrukturen aufgebaut. Mit ihrer Hilfe können anderen Benutzer, Maschinen und Dienste die Zertifikate ihrer Kommunikationspartner auf Echtheit prüfen.

Im CA-Management der TMA werden die Konfigurationsobjekte für CA-Zertifikate und Zertifikate sowie Richtlinien verwaltet .

5.1 CA-Zertifikate

Eine CA (engl. Certificate Authority) ist eine Zertifizierungsstelle für digitale Zertifikate. Sie signiert Zertifikate mit ihrem privaten Schlüssel. Andere Instanzen und Entitäten können das Zertifikat mithilfe des öffentlichen Schlüssels der CA auf ihre Echtheit prüfen, sofern sie der ausstellenden CA vertrauen.

CAs können in Hierarchien aufgebaut werden. Es gibt ein Stammzertifikat (Root-CA), das die abhängigen Sub-CAs signiert, die wiederum weitere Sub-CAs oder Zertifikate signieren. So können ganze Zertifikatketten aufgebaut werden.

Zu jeder CA gehört eine signierte Sperrliste (Certificate Revocation List, CRL), die alle Seriennummern zurückgezogener Zertifikate auflistet. Die CRLs haben i.d.R. eine Laufzeit von 30 Tagen und werden aktualisiert, wenn ein Zertifikat zurückgezogen wird. Die TMA kann zusätzlich einen OCSP-Dienst zur Verfügung stellen, der Zertifikate in Echtzeit auf ihre Gültigkeit prüft.

Die ECOS **TrustManagementAppliance®** unterstützt sowohl eigene CAs als auch externe CAs.

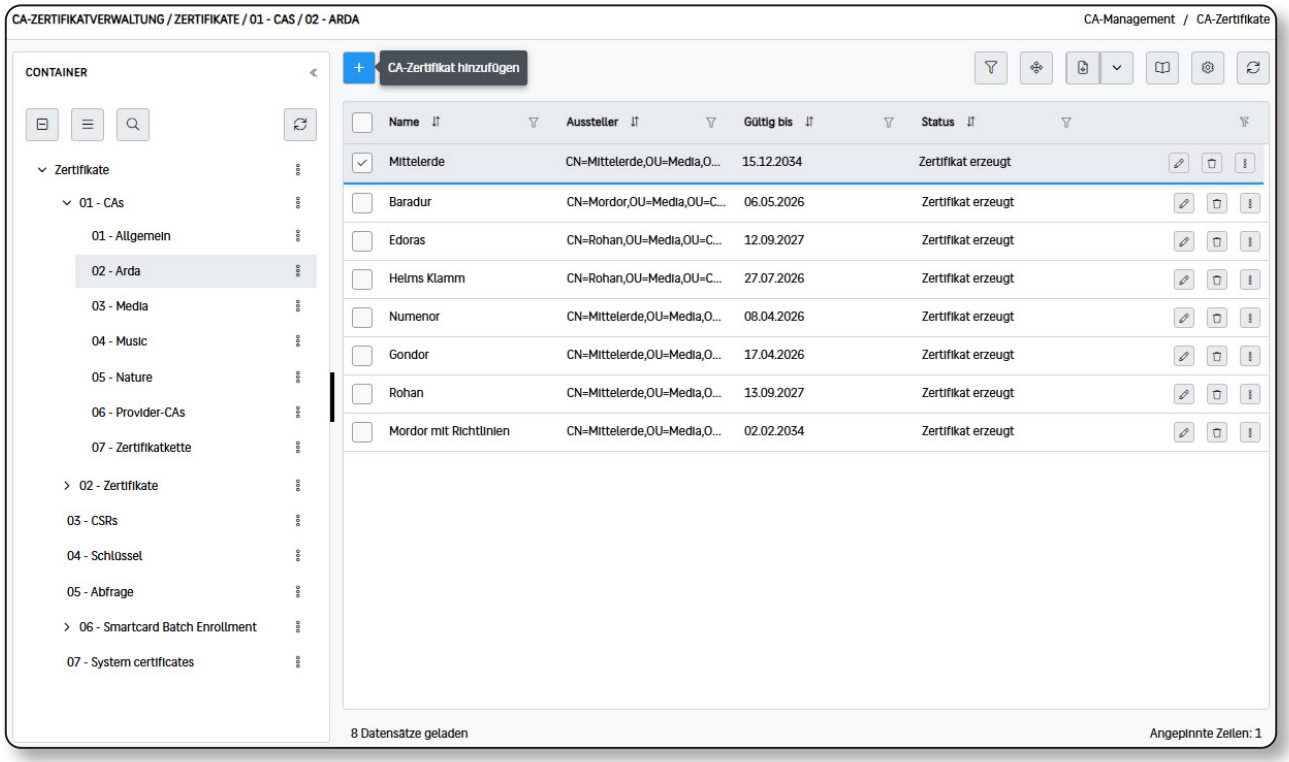


Abb. 5.02: *Übersicht CA-Zertifikate*

5.1.1 Aufbau

Rechts neben dem Seitenmenü wird das Container-Menü angezeigt. Neben den Menüs befindet sich eine tabellarische Übersicht über die vorhandenen CA-Zertifikate.

5.1.1.1 Tabelle

Oberhalb der Tabelle stehen neben den allgemeinen Tabellenfunktionen zusätzliche Symbole zur Verfügung.



Schnellfilter ein-/ausblenden: Über dieses Symbol werden Schnellfilter über der Tabelle angezeigt, um z.B. die Zertifikate nach Status, CA oder Schlüsselverwendung zu filtern. Der Filter wird durch ein erneutes Klicken auf den jeweiligen Button gelöscht. Zusätzlich lassen sich die Inhalte über die einzelnen Spalten filtern. Ist die Funktion aktiv, ist das Symbol je nach eingestelltem Farbschema farbig hinterlegt.



Verschieben: Über dieses Symbol können zuvor ausgewählte Zertifikate in einen anderen Container verschoben werden. Es öffnet sich ein Fenster, in dem die ausgewählten Zertifikate aufgelistet werden, die verschoben werden. Im Dropdown-Menü kann der neue Container ausgewählt werden. Der Vorgang wird mit Verschieben bestätigt. Anschließend erscheint eine Übersicht, ob und wie viele Zertifikate erfolgreich verschoben wurden.

Herunterladen: Über diesen Button können die ausgewählten CA-Zertifikate im Standardformat heruntergeladen werden. Über die integrierte Dropdown-Liste kann ein alternatives Dateiformat ausgewählt werden.

5.1.1.2 Kontextmenü

Die verschiedenen Aktionen für CA-Zertifikate stehen über das Kontextmenü zur Verfügung. Neben den allgemeinen Optionen zum Kopieren von Werten, Bearbeiten und Löschen der Objekte gibt es zusätzliche Aktionen , die vom Status des jeweiligen Zertifikats abhängig sind.

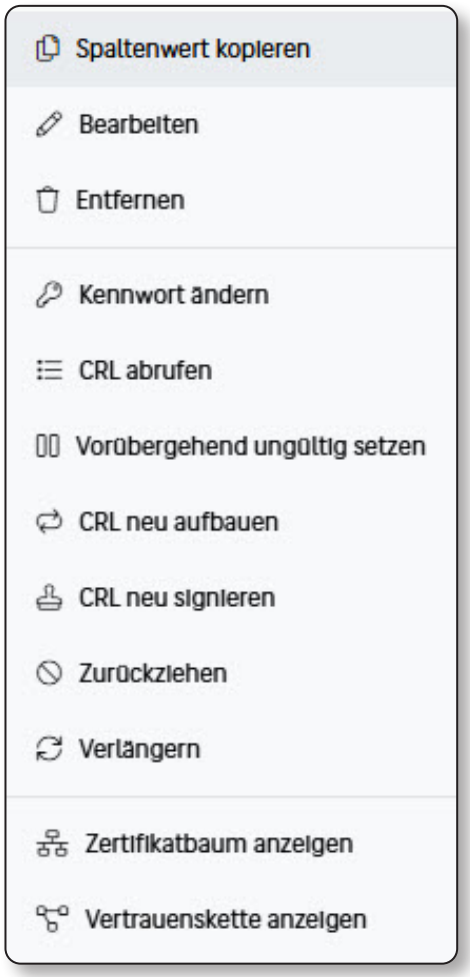


Abb. 5.03: *Kontextmenü für CA-Zertifikate*

Kennwort ändern: Es öffnet sich ein Dialog, um das Kennwort des CA-Zertifikats zu ändern.

Status löschen: Diese Option steht nur bei hochgeladenen CA-Zertifikaten zur Verfügung und löscht das CA-Zertifikat im Objekt. Das Objekt selbst bleibt erhalten.

Private Schlüssel endgültig löschen: Diese Option löscht den auf der TMA hinterlegten Privaten Schlüssel.

CRL abrufen: Die CRL für ein externes CA-Zertifikat wird durch die TMA heruntergeladen.

Vorübergehend ungültig setzen: Das CA-Zertifikat wird vorrübergehend für ungültig erklärt. Der Status ändert sich auf **On Hold**.

Wieder gültig setzen: Das CA-Zertifikat wird wieder gültig erklärt. Diese Option erscheint nur bei Zertifikaten, die den Status **On Hold** haben.

CRL neu aufbauen: Die CRL dieses CA-Zertifikats wird neu erzeugt. Dies ist normalerweise nicht notwendig, da die TMA die CRL automatisch aktuell hält.

CRL neu signieren: Die CRL dieses CA-Zertifikats wird erneut signiert. Dies ist notwendig, wenn die Gültigkeit der CRL abgelaufen ist. Das erneute Signieren, vor dem Ablauf der Gültigkeit, erfolgt normalerweise automatisch.

Zurückziehen: Das CA-Zertifikat wird zurückgezogen. Es werden auch alle von dieser CA signierten Zertifikate ungültig.

Verlängern: Das CA-Zertifikat wird verlängert.

Zertifikatbaum anzeigen: Es erscheint eine Grafik, die den Zertifikatbaum des ausgewählten CA-Zertifikats anzeigt. Neben dem Zertifikatbaum befindet sich ein Zertifikatbericht mit Informationen zu Root- und Sub-CAs sowie zu abhängigen Client-Zertifikaten und ihres jeweiligen Status. Die Grafik kann als Bild heruntergeladen werden.

Vertrauenskette anzeigen: Es erscheint eine Grafik, die die Vertrauenskette des ausgewählten Zertifikats anzeigt. Das ausgewählte Zertifikat erscheint grün. Die oberste CA ist rot hinterlegt. Zusätzlich zu den ausstellenden CAs werden auch weitere Sub-CAs, die von den CAs in der Zertifikatkette ausgestellt wurden. Es können weitere untergeordnete CAs angezeigt werden. Mit einem Klick auf ein Zertifikat wird dieses in einem neuen Fenster angezeigt. Die Grafik kann als Bild heruntergeladen werden.

5.1.2 Eigenes CA-Zertifikat erstellen

Navigieren Sie zum Bereich **CA-Management → CA-Zertifikate** und fügen Sie ein neues CA-Zertifikat hinzu. Es öffnet sich ein Wizard zum Erstellen eines neuen CA-Zertifikats.

1

Name: Vergeben Sie einen aussagekräftigen Namen.

Zielcontainer: Wählen Sie den Container aus, in dem das CA-Zertifikat gespeichert werden soll. Bitte beachten Sie, falls für den Container Richtlinien hinterlegt sind, können bestimmte Werte für das Zertifikat vorgegeben bzw. überschrieben werden. Die Abweichungen und Übereinstimmungen werden Ihnen in Schritt 8 angezeigt.

Manuell konfigurieren: Wählen Sie diese Option, um ein CA-Zertifikat manuell zu erstellen.

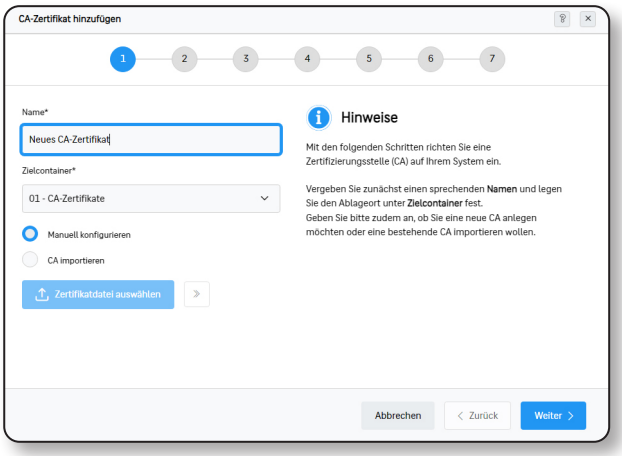


Abb. 5.04: *Neue CA: Wizard starten*

2

CA-Typ: Wählen Sie, ob es sich um eine Root-CA oder eine Sub-CA handelt.

Übergeordnete Zertifizierungsstelle: Handelt es sich bei dem Zertifikat um eine Sub-CA, geben Sie hier die übergeordnete, signierende CA an.

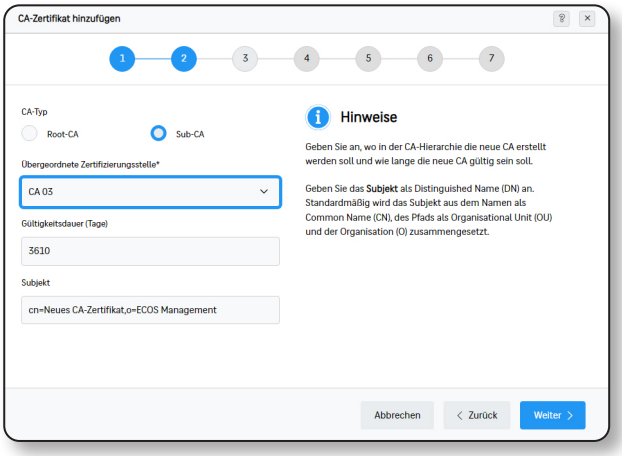


Abb. 5.05: *Übergeordnete Zertifizierungsstelle auswählen*

Gültigkeitsdauer (Tage): Geben Sie hier die Laufzeit des CA-Zertifikats in Tagen an. Standardmäßig sind hier **3650** Tage (10 Jahre) angegeben. Beachten Sie bitte, dass die Laufzeit bei einer Sub-CA nicht länger sein kann als die Laufzeit der signierenden CA.

Subjekt: Geben Sie das Subjekt als Distinguished Name (DN) an. Standardmäßig wird das Subjekt aus dem Namen als Common Name (CN), des Pfads als Organisational Unit (OU) und der Organisation (O) zusammengesetzt. Sie können das Subjekt ändern.

3

Schlüsselalgorithmus: Legen Sie den Schlüsselalgorithmus fest. Standardmäßig ist das **RSA**-Verfahren ausgewählt.

RSA: Das RSA-Verfahren berechnet Schlüssel mithilfe einer modularen Potenzierung großer Primzahlen.

EC: Das EC-Verfahren berechnet Schlüssel mithilfe mathematischer Operationen auf Elliptischen Kurven (engl. Elliptic Curves).

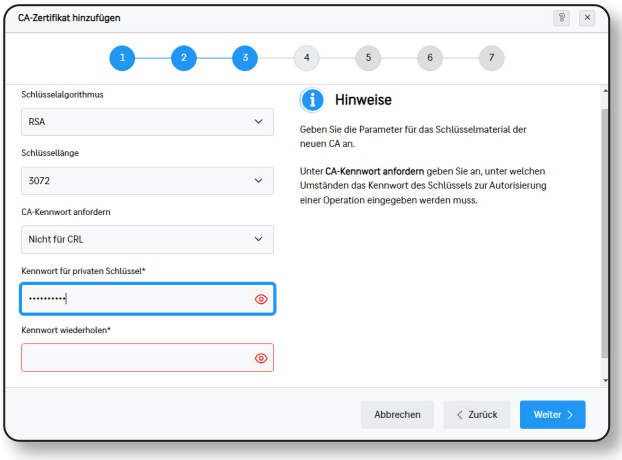


Abb. 5.06: *CA-Kennwort angeben*

Schlüssellänge: Haben Sie das RSA-Verfahren gewählt, legen Sie hier die Schlüssellänge fest. Standardmäßig sind **3072 bit** angegeben, dies entspricht der aktuellen BSI-Vorgabe für sichere RSA-Schlüssel. Beachten Sie, je größer der Schlüssel, desto rechenintensiver ist die Berechnung, was nicht jede Hardware leisten kann.

Elliptische Kurve: Haben Sie das EC-Verfahren gewählt, legen Sie hier die Elliptische Kurve fest, mit der die Schlüssel erzeugt werden sollen. Standardmäßig ist die Elliptische Kurve **prime256v1** ausgewählt.

CA-Kennwort anfordern: Legen Sie fest, wann das CA-Kennwort abgefragt werden soll. Standardmäßig ist **Immer** ausgewählt.

Immer: Das Kennwort wird bei jeder Aktion mit dieser CA abgefragt.

Nur beim Erstellen: Das Kennwort wird nur bei der Erstellung eines Zertifikats abgefragt.

Nie: Das Kennwort wird niemals abgefragt.

Nicht für CRL: Das Kennwort wird bei jeder Aktion außer bei der CRL abgefragt.

Kennwort für privaten Schlüssel: Geben Sie hier das CA-Kennwort ein.

Kennwort wiederholen: Wiederholen Sie das CA-Kennwort. Stimmen die Kennwörter nicht überein, wird Ihnen das direkt angezeigt.

4

Signatur-Hashalgorithmus: Wählen Sie hier den Hashalgorithmus, der zur Signatur des CA-Zertifikats verwendet wird, aus. Standardmäßig ist **sha256** ausgewählt.

Richtlinie: Sie können eine Richtlinie für das CA-Zertifikat auswählen oder neu erstellen. Diese findet bei den Zertifikaten Anwendung, die von dieser CA signiert werden (siehe **5.4 Richtlinien**).

Certification Practice Statement (CPS): Sie können den Verweis auf einen CPS hinzufügen.

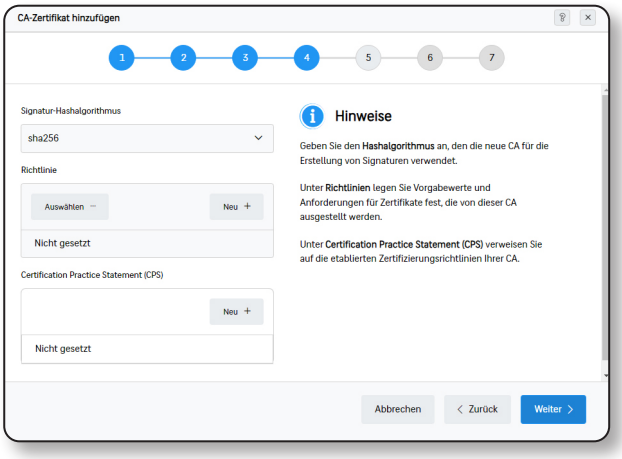


Abb. 5.07: *Policy & CPS*

5

CRL Distribution Points: Wählen Sie einen Distribution Point, über den die CRL abgerufen werden kann oder erstellen Sie einen neuen. Die URL für den CRL Distribution Point wird in alle Zertifikate, die von dieser CA ausgestellt werden, eingebettet.

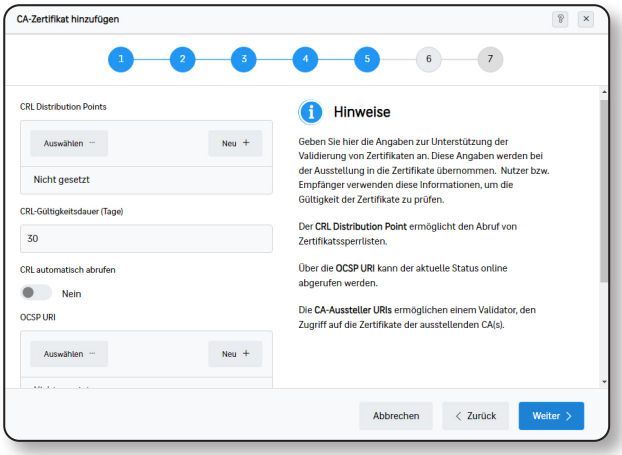


Abb. 5.08: *CDP, OCSP-URI & CA-Aussteller*

Name: Vergeben Sie einen aussagekräftigen Namen.

URL für CRL Distribution Point: Geben Sie die URL für den CRL Distribution Point ein. Die URL setzt sich aus der IP-Adresse oder dem FQDN der TMA sowie der Pfad-Komponente **crl** zusammen. Beim Ausstellen eines Zertifikats wird der URL-Präfix automatisch um den in der Subjektzeile der signierenden CA angegebenen Common Name (CN) ergänzt.

Beispiel: **http://1.2.3.4/crl/**

Alternativ kann auch eine andere URL angegeben werden. Es muss manuell sichergestellt sein, dass eine aktuelle CRL dort abrufbar ist.

CRL-Gültigkeitsdauer (Tage): Legen Sie hier die Gültigkeit in Tagen für die CRL fest. Standardmäßig sind hier 30 Tage angegeben.

CRL automatisch abrufen: Aktivieren Sie diese Option, wenn die CRL automatisch abgerufen werden soll. Für selbst erstellte Zertifikate ist die Aktivierung nicht notwendig.

OCSP URI: Sollen die Zertifikate in Echtzeit geprüft werden, wählen Sie hier die OCSP URI aus, die für die CA zuständig ist. Dazu muss ein OCSP-Server zuvor eingerichtet worden sein. Alternativ erstellen Sie eine neue URI.

Name: Vergeben Sie einen aussagekräftigen Namen.

OCSP URI: Geben Sie hier die URI des OCSP-Servers an.

Beispiel: **http://ocsp.meinserver.de**

CA-Aussteller: Wird das CA-Zertifikat extern zur Verfügung gestellt, können Sie hier eine URL auswählen bzw. neu erstellen, wo das CA-Zertifikat heruntergeladen werden kann.

Name: Vergeben Sie einen aussagekräftigen Namen.

CA Issuer URI: Geben Sie die URI des Speicherorts an, von dem das signierende CA-Zertifikat heruntergeladen werden kann. Wird der Speicherort für die TMA definiert, besteht die URI aus der IP-Adresse bzw. FQDN der TMA und der Pfad-Komponente **certs**. Beim Ausstellen eines Zertifikats wird der URI-Präfix automatisch um den in der Subjektzeile der CA angegebenen Common Namen (CN) ergänzt.

Beispiel: **http://1.2.3.4/certs/**

6

Metadaten: Legen Sie hier zusätzliche Informationen für das Zertifikat fest. Es öffnet sich ein Konfigurationsfenster. Wählen Sie einen Bezeichner aus der Dropdown-Liste aus und vergeben Sie einen Wert. Neue Bezeichner können unter **Globale Einstellungen → Metadaten** erstellt werden (siehe **9.3.1 Neue Metadatenschlüssel anlegen**).

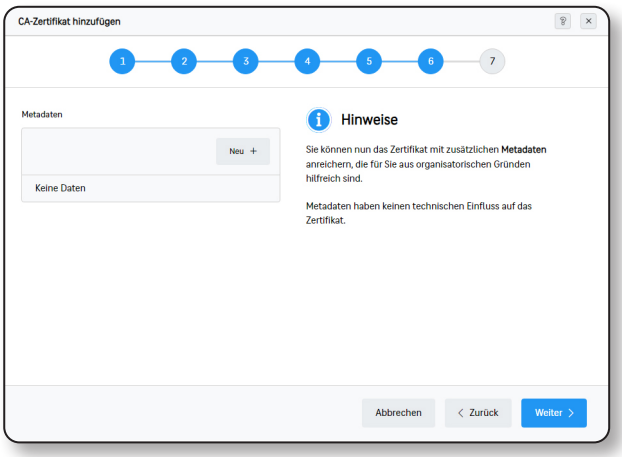


Abb. 5.09: *Metadaten hinzufügen*

7

Zertifikat auf Smartcard/HSM speichern: Wählen Sie hier den Speicherort für das Zertifikat aus. Standardmäßig ist **Nur intern** ausgewählt.

Nur intern: Das Zertifikat wird nur intern auf der TMA gespeichert.

HSM: Das Zertifikat wird auf einem Hardware Security Modul (HSM) gespeichert werden. Es öffnen sich weitere Konfigurationsfelder zur Auswahl des HSM.

HSM: Wählen Sie das HSM aus, auf dem das Zertifikat gespeichert werden soll.

Sind alle notwendigen Informationen für das CA-Zertifikat eingestellt, erstellen Sie die CA über den Button **Zertifikat ausstellen**.

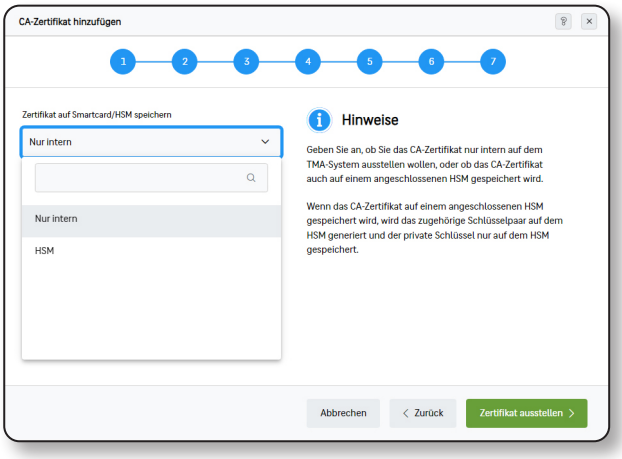


Abb. 5.10: *Speicherort festlegen*

8

Handelt es sich bei dem CA-Zertifikat um eine Sub-CA, werden Sie ggfs. nach dem Kennwort der signierenden CA gefragt. Geben Sie das Kennwort der ausstellenden CA ein.

Das Zertifikat wird erstellt. Anschließend erhalten Sie Informationen, ob die Erstellung erfolgreich war. Werden Ihnen Fehler angezeigt, z.B. weil Vorgaben durch Richtlinien nicht erfüllt werden, navigieren Sie zu der entsprechenden Seite und korrigieren Sie die Einstellung.

War die Erstellung erfolgreich, können Sie das CA-Zertifikat herunterladen oder ansehen.

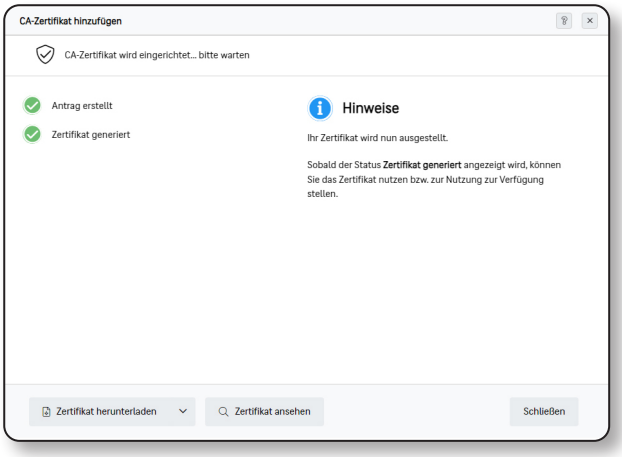


Abb. 5.11: *CA-Zertifikat wird ausgestellt*

Schließen Sie den Assistenten.

5.1.3 Externes CA-Zertifikat hochladen

\+

Navigieren Sie zum Bereich **CA-Management → CA-Zertifikate** und fügen Sie ein neues CA-Zertifikat hinzu. Es öffnet sich ein Assistent zum Erstellen eines neuen CA-Zertifikats.

1

Name: Vergeben Sie einen aussagekräftigen Namen.

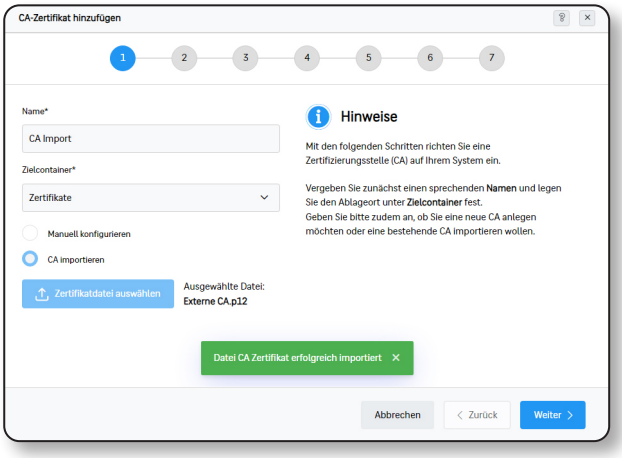


Abb. 5.12: *Upload erfolgreich*

Zielcontainer: Wählen Sie den Container aus, in dem das CA-Zertifikat gespeichert werden soll. Bitte beachten Sie, falls für den Container Richtlinien hinterlegt sind, können bestimmte Werte für das Zertifikat vorgegeben bzw. überschrieben werden. Die Abweichungen und Übereinstimmungen werden Ihnen in Schritt 8 angezeigt.

CA importieren: Wählen Sie diese Option, um ein externes CA-Zertifikat hochzuladen.

Zertifikatdatei auswählen: Es öffnet sich ein Auswahldialog. Wählen Sie das entsprechende CA-Zertifikat aus. Alternativ können Sie das base64-kodierte CA-Zertifikat über den Doppelpfeil in das erscheinende Eingabefeld einfügen und hochladen.

2

Ihnen wird die Art der CA (Root-CA oder Sub-CA), die Gültigkeit sowie das Subjekt angezeigt. Sie können die Einstellungen nicht ändern.

3

Ihnen werden Informationen zum Schlüsselpaar der CA angezeigt.

CA-Kennwort anfordern: Legen Sie fest, wann das CA-Kennwort abgefragt werden soll. Standardmäßig ist **Immer** ausgewählt.

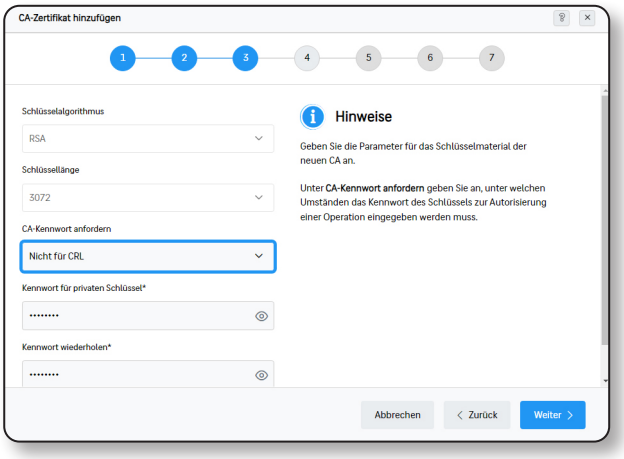


Abb. 5.13: *CA-Kennwortanforderung festlegen*

Immer: Das Kennwort wird bei jeder Aktion mit dieser CA abgefragt.

Beim Erstellen: Das Kennwort wird nur bei der Erstellung eines Zertifikats abgefragt.

Nie: Das Kennwort wird niemals abgefragt.

Nicht für CRL: Das Kennwort wird bei jeder Aktion außer beim Signieren der CRL abgefragt.

Kennwort für privaten Schlüssel: Geben Sie hier das CA-Kennwort ein.

Kennwort wiederholen: Wiederholen Sie das CA-Kennwort. Stimmen die Kennwörter nicht überein, wird Ihnen das direkt angezeigt.

4

Richtlinie: Sie können eine Richtlinie für das CA-Zertifikat auswählen oder neu erstellen. Diese findet bei den Zertifikaten Anwendung, die von dieser CA signiert werden. Siehe dazu **„5.4 Richtlinien“.**

Certification Practice Statement (CPS): Sie können den Verweis auf einen CPS hinzufügen.

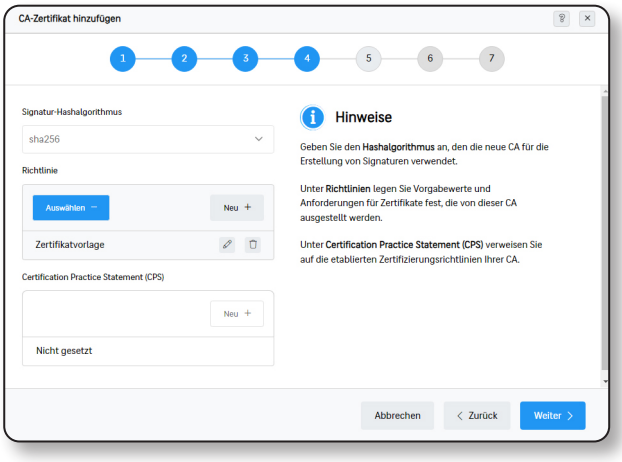


Abb. 5.14: *Policy auswählen oder erstellen*

5

CRL-Gültigkeitsdauer (Tage): Legen Sie hier die Gültigkeit in Tagen für die CRL fest. Standardmäßig sind hier 30 Tage angegeben.

CRL automatisch abrufen: Aktivieren Sie diese Option, wenn die CRL automatisch abgerufen werden soll.

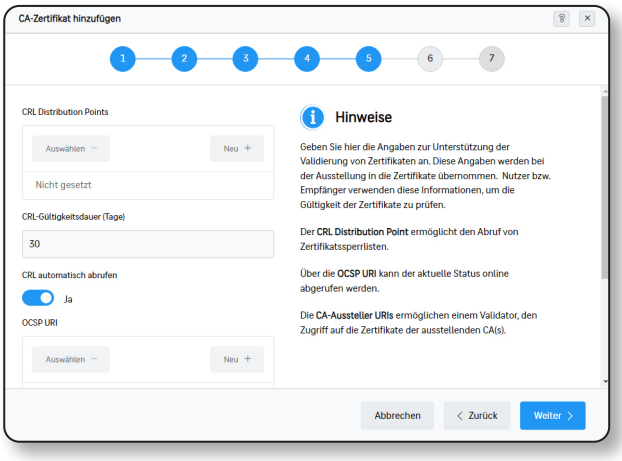


Abb. 5.15: *CRL Gültigkeitsdauer festlegen*

6

Metadaten: Legen Sie hier zusätzliche Informationen für das Zertifikat fest. Es öffnet sich ein Konfigurationsfenster. Wählen Sie einen Bezeichner aus der Dropdown-Liste aus und vergeben Sie einen Wert. Neue Bezeichner können unter **Globale Einstellungen → Metadaten** erstellt werden (siehe **9.3.1 Neue Metadatenschlüssel anlegen**).

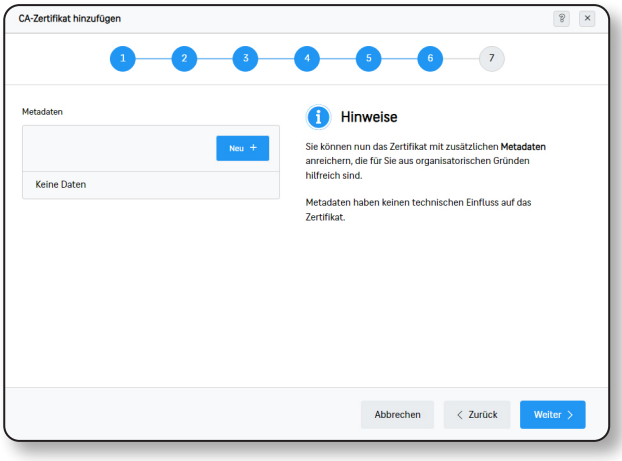


Abb. 5.16: *Metadaten*

7

Sie können keine Einstellungen auf dieser Seite des Assistenten ändern.

Sind alle notwendigen Informationen für das CA-Zertifikat eingestellt, importieren Sie die CA über den Button **CA importieren**.

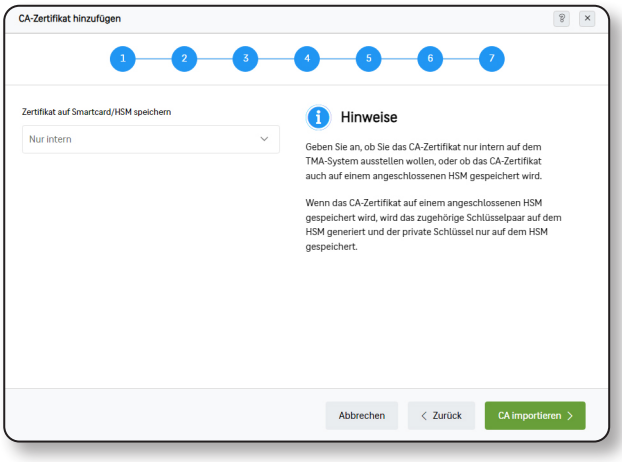


Abb. 5.17: *Smartcard-/HSM-Optionen*

8

Sie werden ggfs. nach dem Kennwort der importierten CA gefragt, falls die Datei mit einem Kennwort geschützt ist.

Sie erhalten Informationen zum erfolgreichen Import der CA. Werden Ihnen Fehler angezeigt, z.B. weil Vorgaben aus Richtlinien nicht erfüllt werden, navigieren Sie zu der entsprechenden Seite und korrigieren Sie die Einstellung.

War der Import erfolgreich können Sie das CA-Zertifikat herunterladen oder ansehen.

Schließen Sie den Assistenten.

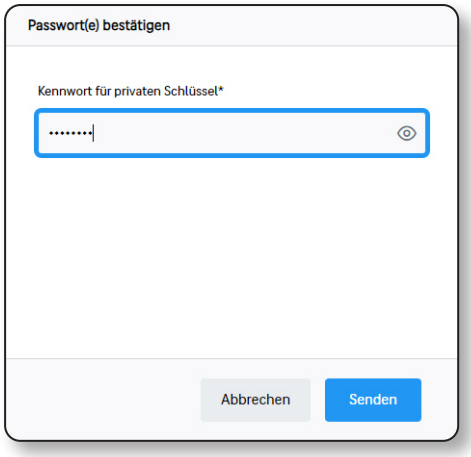


Abb. 5.18: *Angabe des CA-Kennworts*

5.1.4 CA-Hierarchie erstellen

Um eine mehrstufige CA-Hierarchie anzulegen, sollten vor dem Erstellen weiterer Zertifikate eine oder mehrere Sub-CAs genauso wie die Root-CA selbst erstellt werden, nur mit dem Unterschied, dass die Root-CA als übergeordnete CA ausgewählt wird. Danach können diese Sub-CAs zum Erstellen von Zertifikaten verwendet werden.

Da Zertifikate keine längere Laufzeit besitzen können als ihre ausstellende CA, empfiehlt es sich, vor dem Aufbau der CA-Hierarchie gründlich über die Laufzeiten der Root- und Sub-CAs nachzudenken, auch um rechtzeitig den Übergang von einer CA-Generation zur nächsten möglichst problemlos zu gestalten.

Beispiel: Root-CAs haben i.d.R. eine Laufzeit von 10 Jahren. Sie sind mit Datum und Uhrzeit versehen. Das bedeutet, eine abhängige Sub-CA, die 5 Minuten nach der Root-CA erstellt wird, kann keine Laufzeit von 10 Jahren mehr haben, da diese länger wäre als die Laufzeit der ausstellenden CA. Es hat sich daher bewährt, die Laufzeit von Sub-CAs um mindestens 2-3 Jahren zu verkürzen.

Die nächste Generation von Root- und Sub-CAs sollte jeweils nach Ablauf von ca. Zweidrittel der Laufzeit der ersten Generation angelegt werden. Bei einer Root-CA mit einer Laufzeit von 10 Jahren, also nach ca. 6-7 Jahren.

5.2 CA-Zugangspunkte

Es wird eine tabellarische Übersicht über die vorhandenen CAs mit ihren CRL Distribution Points, den OCSP URIs oder dem CA-Aussteller gezeigt.

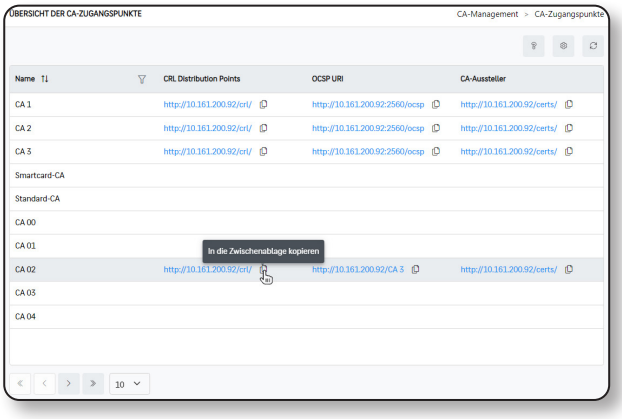


Abb. 5.19: *Übersicht der CA-Zugangspunkte*

5.3 Zertifikate

Digitale Zertifikate werden zur Identifizierung von Personen, Geräten und Diensten genutzt. Sie helfen, die Kommunikation zwischen Gesprächspartnern abzusichern. Jedes Zertifikat wird von einer Zertifizierungsstelle (CA) signiert. Vertraut ein Kommunikationspartner dieser CA, vertraut er automatisch auch dem Zertifikat und somit auch dem Besitzer dieses Zertifikats.

Die ECOS **TrustManagementAppliance®** unterstützt sowohl eigene Zertifikate als auch externe Zertifikate und CSRs (Certificate Signing Requests). Sie entsprechen dem X.509-Standard.

⚠ **Hinweis:** Für automatisierte Prozesse, wie z.B. die automatische Verlängerung von Zertifikaten, müssen Kryptooperationen mit dem privaten Schlüssel des Zertifikats ohne manuelle Kennworteingabe durchgeführt werden können. Der private Schlüssel muss dementsprechend „verschlüsselt und unverschlüsselt“ gespeichert werden.

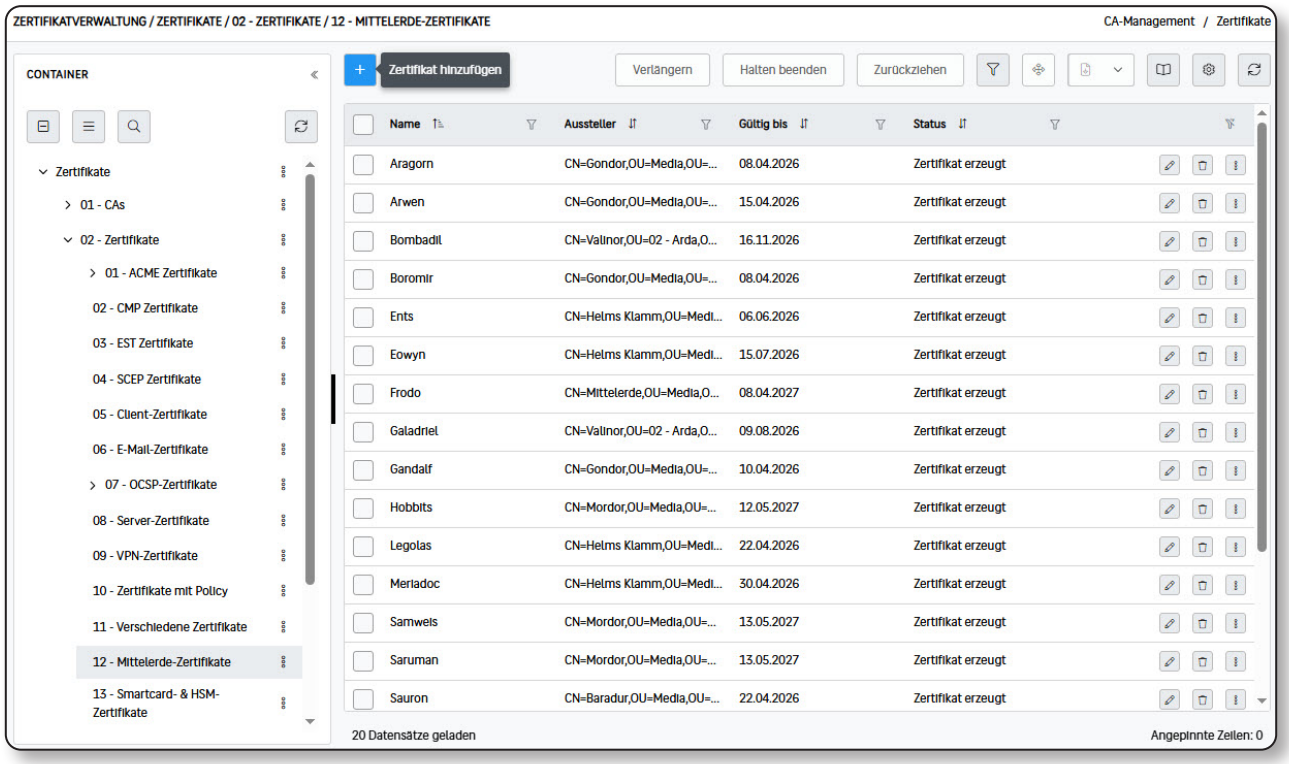


Abb. 5.20: *Übersicht der Zertifikate*

5.3.1 Aufbau

Rechts neben dem Seitenmenü wird das Container-Menü angezeigt. Neben den Menüs befindet sich eine tabellarische Übersicht über die vorhandenen Zertifikate.

5.3.1.1 Tabelle

Oberhalb der Tabelle stehen neben den allgemeinen Tabellenfunktionen zusätzliche Buttons zur Verfügung.

Verlängern: Über diesen Button können die ausgewählten Zertifikate verlängert werden.

Halten beenden: Über diesen Button können vorübergehend ungültige Zertifikate wieder gültig gesetzt werden.

Zurückziehen: Über diesen Button können die ausgewählten Zertifikate zurückgezogen werden.



Schnellfilter ein-/ausblenden: Über dieses Symbol werden Schnellfilter über der Tabelle angezeigt, um z.B. die Zertifikate nach Status, CA oder Schlüsselverwendung zu filtern. Der Filter wird durch ein erneutes Klicken auf den jeweiligen Button gelöscht. Zusätzlich lassen sich die Inhalte über die einzelnen Spalten filtern. Ist die Funktion aktiv, ist das Symbol je nach eingestelltem Farbschema farbig hinterlegt.



Verschieben: Über dieses Symbol können zuvor ausgewählte Zertifikate in einen anderen Container verschoben werden. Es öffnet sich ein Fenster, in dem die ausgewählten Zertifikate aufgelistet werden, die verschoben werden. Im Dropdown-Menü kann der neue Container ausgewählt werden. Der Vorgang wird mit Verschieben bestätigt. Anschließend erscheint eine Übersicht, ob und wie viele Zertifikate erfolgreich verschoben wurden.



Herunterladen: Über diesen Button können die ausgewählten CA-Zertifikate im Standardformat heruntergeladen werden. Über die integrierte Dropdown-Liste kann ein alternatives Dateiformat ausgewählt werden.

5.3.1.2 Kontextmenü

Die verschiedenen Aktionen für die CA-Zertifikate stehen über das Kontextmenü zur Verfügung. Neben den allgemeinen Optionen zum Kopieren von Werten, Bearbeiten und Löschen der Objekte gibt es zusätzliche Aktionen, die vom Status des jeweiigen Zertifikats abhänging sind.



Status löschen: Diese Option steht nur bei hochgeladenen Zertifikaten zur Verfügung und löscht das Zertifikat im Objekt. Das Objekt selbst bleibt erhalten.



Vorübergehend ungültig setzen: Das Zertifikat wird vorrübergehend für ungültig erklärt. Der Status ändert sich auf **On Hold**.

Wieder gültig setzen: Das Zertifikat wird wieder gültig erklärt. Diese Option erscheint nur bei Zertifikaten, die den Status **On Hold** haben.

Zurückziehen: Das Zertifikat wird zurückgezogen.

Verlängern: Das Zertifikat wird verlängert.

Zertifikat erzeugen: Mit dieser Option wird ein Zertifikat erzeugt. Je nach Einstellung im Konfigurationsobjekt ist die Eingabe eines Kennworts für den privaten Schlüssel und/oder die CA notwendig.

CSR erzeugen: Diese Option erzeugt einen CSR.

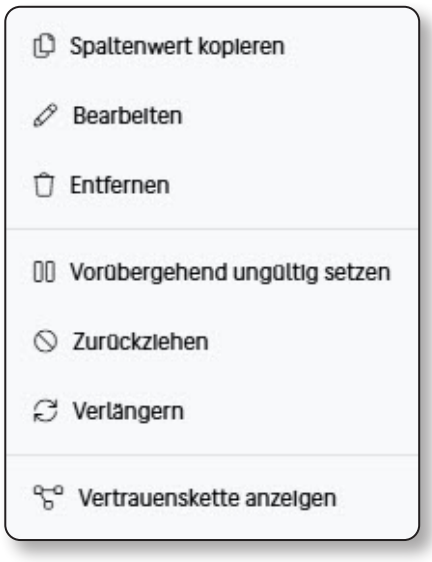


Abb. 5.21: *Kontextmenü der Zertifikate*

Private Schlüssel endgültig löschen: Diese Option löscht den auf der TMA hinterlegten Privaten Schlüssel

Vertrauenskette anzeigen: Es erscheint eine Grafik, die die Vertrauenskette des ausgewählten Zertifikats anzeigt. Das ausgewählte Zertifikat erscheint grün. Die oberste CA ist rot hinterlegt. Zusätzlich zu den ausstellenden CAs werden auch weitere Sub-CAs, die von den CAs in der Zertifikatkette ausgestellt wurden. Es können weitere untergeordnete CAs angezeigt werden. Mit einem Klick auf ein Zertifikat wird dieses in einem neuen Fenster angezeigt.

5.3.2 Eigenes Zertifikat erstellen

Navigieren Sie zum Bereich CA-Management → Zertifikate und fügen Sie ein neues Zertifikat hinzu. Es öffnet sich ein Assistent zum Erstellen eines neuen Zertifikats.

1

Name: Vergeben Sie einen aussagekräftigen Namen.

Zielcontainer: Wählen Sie den Container aus, in dem das Zertifikat gespeichert werden soll. Bitte beachten Sie, falls für den Container Richtlinien hinterlegt sind, können bestimmte Werte für das Zertifikat vorgegeben bzw. überschrieben werden. Die Abweichungen und Übereinstimmungen werden Ihnen in Schritt 8 angezeigt.

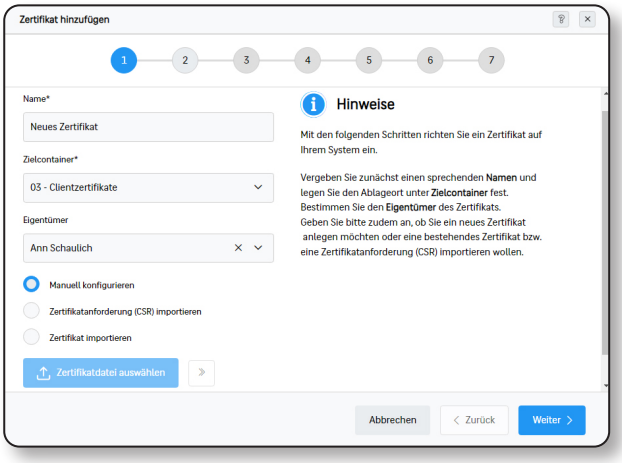


Abb. 5.22: *Start des Assistenten*

Eigentümer: Wählen Sie den Besitzer des Zertifikats aus.

Manuell konfigurieren: Wählen Sie diese Option, um ein CA-Zertifikat manuell zu erstellen.

2

Zertifizierungsstelle: Wählen Sie die CA aus, die das Zertifikat signieren soll.

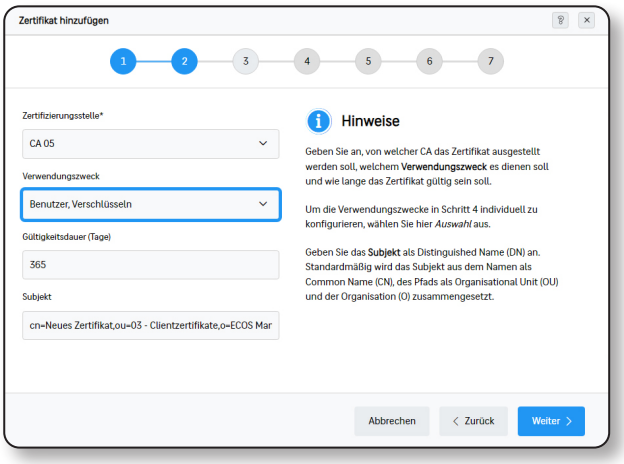


Abb. 5.23: *CA auswählen*

Verwendungszweck: Wählen Sie hier den Schlüsselverwendungszweck aus. Es stehen verschiedene voreingestellte Verwendungszwecke zur Verfügung. Über **Auswahl** können Sie bei Schritt 4 die Schlüsselverwendungen selbst bestimmen (siehe **24.1 Voreingestellte Schlüsselverwendungszwecke**).

Gültigkeitsdauer (Tage): Geben Sie hier die Laufzeit des Zertifikats in Tagen an. Standardmäßig sind hier **365** Tage (1 Jahr) angegeben. Beachten Sie bitte, dass die Laufzeit eines Zertifikats nicht länger sein kann als die Laufzeit der signierenden CA.

Subjekt: Geben Sie das Subjekt als Distinguished Name (DN) an. Standardmäßig wird das Subjekt aus dem Namen als Common Name (CN), des Pfads als Organisational Unit (OU) und der Organisation (O) zusammengesetzt. Sie können das Subjekt ändern.

3

Schlüsselalgorithmus: Legen Sie den Schlüsselalgorithmus fest. Standardmäßig ist das **RSA**-Verfahren ausgewählt.

RSA: Das RSA-Verfahren berechnet Schlüssel mithilfe einer modularen Potenzierung großer Primzahlen.

EC: Das EC-Verfahren berechnet Schlüssel mithilfe mathematischer Operationen auf Elliptischen Kurven (engl. Elliptic Curves).

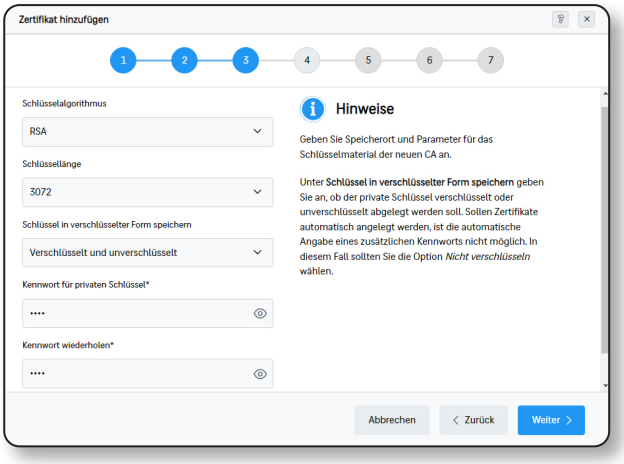


Abb. 5.24: *Schlüsseleinstellungen*

Schlüssellänge: Wählen Sie die Schlüssellänge für das RSA-Verfahren aus. Standardmäßig sind **3072 Bit** voreingestellt. Diese Einstellung entspricht den aktuellen Anforderungen und Empfehlungen des BSI für den Einsatz von RSA-Schlüsseln in VS-NfD-Umgebungen.

Außerhalb von VS-NfD-Umgebungen können abweichende Schlüssellängen je nach Einsatzszenario und Kompatibilität der eingesetzten Systeme oder Hardwarekomponenten erforderlich sein.

Elliptische Kurve: Wählen Sie die elliptische Kurve für das ECC-Verfahren aus. Standardmäßig ist **prime256v1** eingestellt. Diese Einstellung entspricht den aktuellen Anforderungen und Empfehlungen des BSI für den Einsatz von EC-Schlüsseln in VS-NfD-Umgebungen.

Außerhalb von VS-NfD-Umgebungen können abweichende elliptische Kurven je nach Einsatzszenario und Kompatibilität der eingesetzten Systeme oder Hardwarekomponenten erforderlich sein.

Schlüssel in verschlüsselter Form speichern: Legen Sie fest, ob der private Schlüssel verschlüsselt oder unverschlüsselt abgelegt werden soll. Der Schlüssel wird auf jeden Fall durch die allgemeinen Sicherheitsmechanismen geschützt und der Zugriff unterliegt den eingestellten Zugriffsrechten. Für den Zugriff auf einen verschlüsselten Schlüssel muss zusätzlich für jede Operation mit diesem Schlüssel, ein individuelles Kennwort eingegeben werden.

> Verschlüsselt und unverschlüsselt: Der private Schlüssel wird verschlüsselt und unverschlüsselt abgelegt. Für den Download steht die verschlüsselte Version bereit und der heruntergeladene Schlüssel kann nur mit dem individuellen Kennwort genutzt werden. Kryptooperationen für die automatische Verlängerung von Zertifikaten funktionieren ohne die Abfrage des Kennworts, da der private Schlüssel auch unverschlüsselt vorliegt.
>
> Nur verschlüsselt: Der private Schlüssel wird nur verschlüsselt abgelegt. Bei jeder Operation wird das individuelle Kennwort abgefragt.
>
> Nicht verschlüsseln: Der private Schlüssel wird nicht verschlüsselt abgelegt. Alle Operationen, die den privaten Schlüssel erfordern, werden ohne Abfrage eines individuellen Kennworts durchgeführt.

Kennwort für privaten Schlüssel: Geben Sie hier das Kennwort für den privaten Schlüssel ein. Haben Sie die Option **Nicht verschlüsseln** gewählt, ist dieses Feld inaktiv.

Kennwort wiederholen: Wiederholen Sie das Kennwort. Stimmen die Kennwörter nicht überein, wird Ihnen das direkt angezeigt. Haben Sie die Option **Nicht verschlüsseln** gewählt, ist dieses Feld ausgegraut.

4

Signatur-Hashalgorithmus: Wählen Sie hier den Hashalgorithmus, der zur Signatur des Zertifikats verwendet wird, aus. Standardmäßig ist **sha256** ausgewählt .

Schlüsselverwendung: Haben Sie in Schritt 2 die Option **Auswahl** gewählt, können Sie hier den Schlüsselverwendungszweck bestimmen. Andernfalls werden Ihnen die automatisch ausgewählten Verwendungszwecke angezeigt (siehe **24.2 Schlüsselverwendungen**).

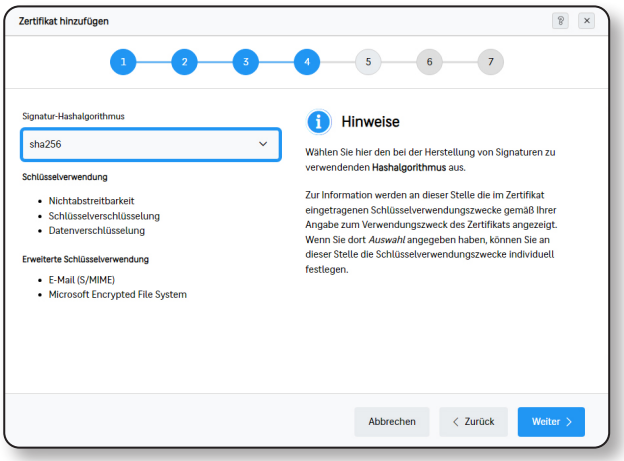


Abb. 5.25: *Signatureinstellungen*

Erweiterte Schlüsselverwendung: Sie können weitere Schlüsselverwendungszwecke bestimmen. Sie sind in Kategorien zusammengefasst (siehe **24.3 Erweiterte Schlüsselverwendungen**).

Als kritisch markieren: Sie können den Verwendungszweck als kritisch markieren. Ist der Verwendungszweck als kritisch markiert, darf das Zertifikat nur für den oder die angegebenen Zwecke verwendet werden. Ist der Verwendungszweck nicht als kritisch markiert, wird er als Hinweisfeld behandelt, das die Verwendung des Zertifikats nicht auf die angegebenen Zwecke beschränkt. Enthält ein Zertifikat sowohl einen als kritisch markierten Schlüsselverwendungszweck als auch einen als kritisch markierten erweiterten Schlüsselverwendungszweck, werden beide unabhängig voneinander verarbeitet. Das Zertifikat darf nur für einen Zweck verwendet werden, der mit beiden Werten übereinstimmt.

5

Alternative Namen: Sie können alternative Subjektnamen (Subject Alternative Names, SAN) für das Zertifikat angeben. Die Namen können zusätzlich oder anstelle der Identität im Subjektfeld des Zertifikats angegeben werden. Es öffnet sich ein Konfigurationsfenster. Wählen Sie einen Typ und vergeben Sie einen Wert. Sie können bspw. E-Mail-Adressen, DNS-Namen, IP-Adressen oder URIs angeben.

Benutzerdefinierte Erweiterungen: Sie können benutzerdefinierte Erweiterungen (OID) angeben. Es öffnet sich ein Konfigurationsfenster. Geben Sie eine OID und einen Wert ein.

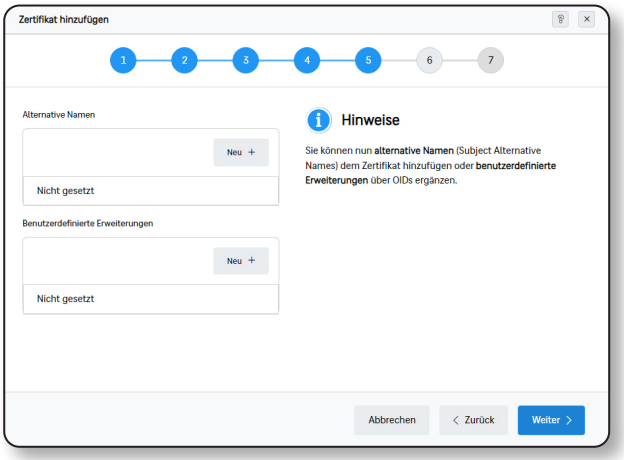


Abb. 5.26: *Alternative Namen angeben*

6

Metadaten: Legen Sie hier zusätzliche Informationen für das Zertifikat fest. Es öffnet sich ein Konfigurationsfenster. Wählen Sie einen Bezeichner aus der Dropdown-Liste aus und vergeben Sie einen Wert. Neue Bezeichner können unter **Globale Einstellungen → Metadaten** erstellt werden **(siehe 9.3.1 Neue Metadatenschlüssel anlegen)**.

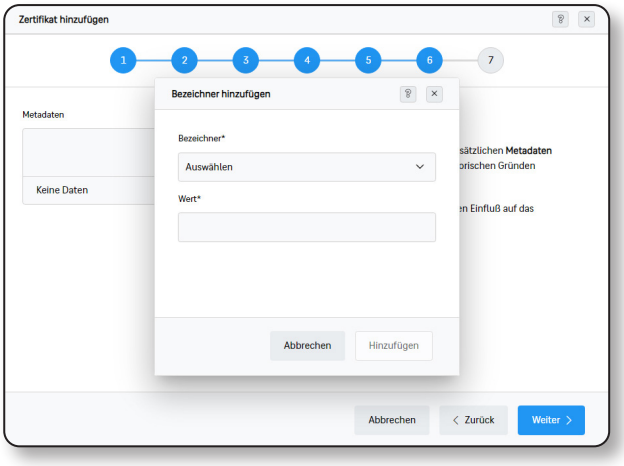


Abb. 5.27: *Metadaten hinzufügen*

7

Zertifikat auf Smartcard/HSM speichern: Wählen Sie hier den Speicherort für das Zertifikat aus. Standardmäßig ist **Nur intern** ausgewählt.

Nur intern: Das Zertifikat wird nur intern auf der TMA gespeichert.

Smartcard: Das Zertifikat wird auf einer Smartcard gespeichert. Für das Speichern auf einer Smartcard wird der Dienst: Smartcard-Enrollment benötigt. Dieser kann in der Expertenansicht angelegt und konfiguriert werden (siehe **14.4 Dienst: Smartcard-Enrollment**). Es öffnen sich weitere Konfigurationsfelder zur Auswahl der Smartcard.

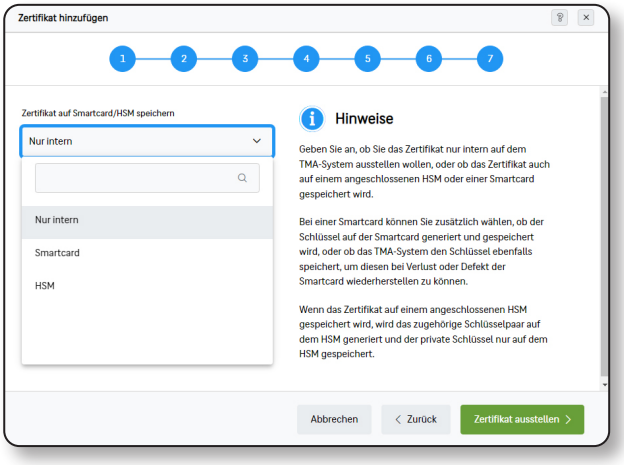


Abb. 5.28: *Speicherort für Schlüssel*

Zugeordnete Smartcard: Hier kann eine Smartcard ausgewählt werden, auf der das Zertifikat gespeichert werden soll. Im Normalfall sollte dieses Feld leer bleiben, dann wird das Zertifikat auf die aktuell eingesteckte Smartcard geschrieben.

Privater Schlüssel: Wählen Sie hier den Speicherort für den privaten Schlüssel aus.

Appliance: Der private Schlüssel wird zusätzlich auf der TMA erzeugt und gespeichert und danach auf die Smartcard kopiert. So existiert ein Backup des Schlüssels auf der TMA.

Smartcard/HSM: Der private Schlüssel wird direkt auf der Smartcard bzw. dem HSM erzeugt und auch nur dort gespeichert.

Smartcard-Initialisierung: Wählen Sie die Smartcard-Initialisierung aus. Eine Smartcard kann so neu initialisiert oder der Benutzer zur Eingabe einer neuen PIN aufgefordert werden, wenn das Smartcard-Enrollment-Tool ausgeführt wird.

Nein: Es werden keine Änderungen an der Smartcard oder der PIN durchgeführt. Bestehende Zertifikate und Schlüssel bleiben unverändert.

Formatieren: Die Smartcard wird formatiert. Bei einigen Modellen wird auch die Smartcard-Software aktualisiert. Alle zuvor installierten Zertifikate und Schlüssel werden von der Smartcard gelöscht. Der Vorgang erfordert die SO-PIN. Eine neue PIN wird vergeben.

Neue PIN: Vor dem Enrollment wird der Anwender nach einer neuen PIN gefragt. Bestehende Zertifikate und Schlüssel bleiben unverändert.

HSM: Das Zertifikat wird auf einem Hardware Security Modul (HSM) gespeichert. Es öffnen sich weitere Konfigurationsfelder zur Auswahl des HSM.

HSM: Wählen Sie das HSM aus, auf dem das Zertifikat gespeichert werden soll.

Sind alle notwendigen Informationen, eingestellt, erstellen Sie das Zertifikat über den Button **Zertifikat ausstellen**.

8

Geben Sie das Kennwort der ausstellenden CA ein, wenn Sie danach gefragt werden.

Das Zertifikat wird erstellt. Anschließend erhalten Sie Informationen, ob die Erstellung erfolgreich war. Werden Ihnen Fehler angezeigt, z.B. weil Vorgaben durch Richtlinien nicht erfüllt werden, navigieren Sie zu der entsprechenden Seite und korrigieren Sie die Einstellung.

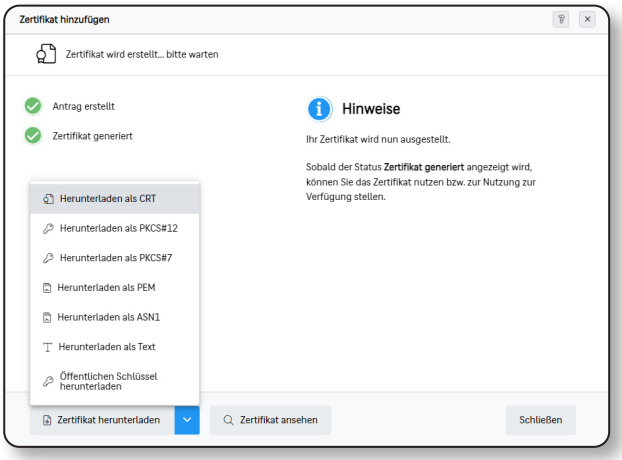


Abb. 5.29: *Zertifikatausstellung und Download*

Soll das Zertifikat auf einer Smartcard erzeugt werden, starten Sie das **Smartcard-Enrollment**-Tool. Wurde das Tool bereits auf dem Gerät installiert, von dem Sie auf die TMA zugreifen, können Sie die **Smartcard-Konfig herunterladen**, um die Zertifikate auf die Smartcard zu spielen. Dazu muss die Smartcard in einem angeschlossenen Smartcard-Reader eingesteckt sein.

War die Erstellung erfolgreich, können Sie das Zertifikat herunterladen oder ansehen.

Schließen Sie den Assistenten.

5.3.3 Externes Zertifikat hochladen

+ Navigieren Sie zum Bereich **CA-Management → Zertifikate** und fügen Sie ein neues Zertifikat hinzu. Es öffnet sich ein Assistent zum Erstellen eines neuen Zertifikats.

1

Name: Vergeben Sie einen aussagekräftigen Namen.

Zielcontainer: Wählen Sie den Container aus, in dem das Zertifikat gespeichert werden soll. Bitte beachten Sie, sind für den Container Richtlinien hinterlegt, können bestimmte Werte für das Zertifikat vorgegeben bzw. überschrieben werden. Die Abweichungen und Übereinstimmungen werden Ihnen erst in Schritt 8 angezeigt.

Eigentümer: Wählen Sie den Besitzer des Zertifikats aus.

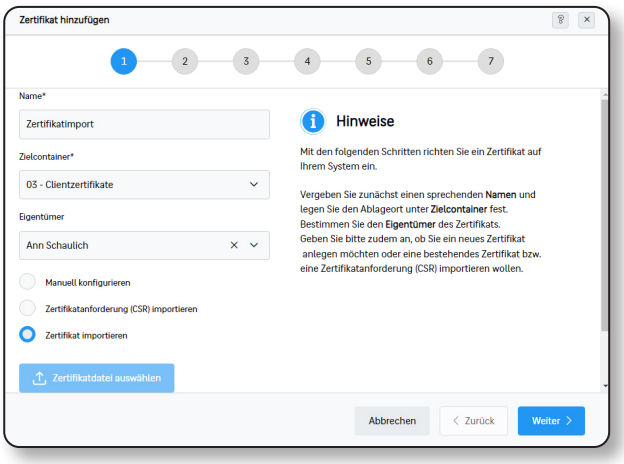


Abb. 5.30: *Start des Assistenten*

Zertifikat importieren: Wählen Sie diese Option, um ein externes Zertifikat hochzuladen.

Zertifikatdatei auswählen: Es öffnet sich ein Auswahldialog. Wählen Sie die entsprechende Zertifikatdatei aus. Alternativ können Sie das base64-kodierte Zertifikat über den Doppelpfeil in das erscheinende Eingabefeld einfügen und hochladen.

2

Zertifizierungsstelle: Wählen Sie die CA aus, die das Zertifikat signieren soll.

Die anderen Einstellungen können Sie nicht ändern.

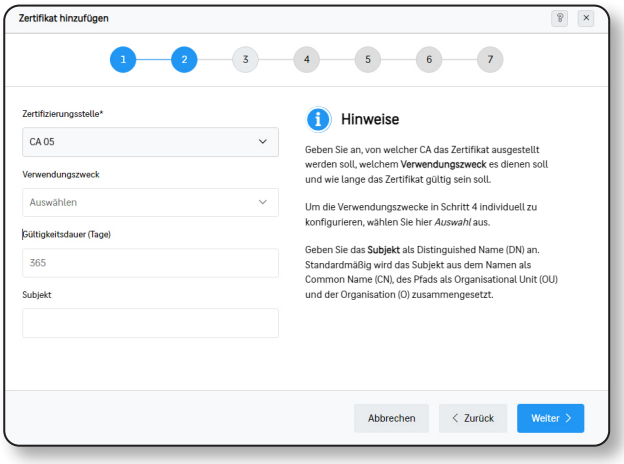


Abb. 5.31: *CA auswählen*

3

Sie erhalten Informationen zum Schlüsselmaterial des Zertifikats, die Sie nicht alle ändern bzw. einstellen können.

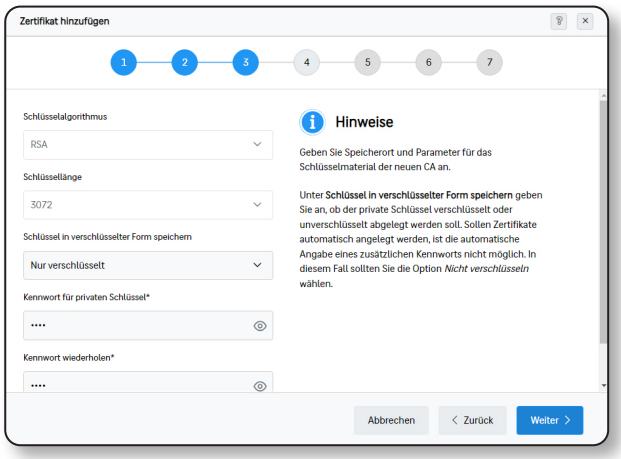


Abb. 5.32: *Schlüsseleinstellungen*

Schlüssel in verschlüsselter Form speichern: Legen Sie fest, ob der private Schlüssel verschlüsselt oder unverschlüsselt abgelegt werden soll. Der Schlüssel wird auf jeden Fall durch die allgemeinen Sicherheitsmechanismen geschützt und der Zugriff unterliegt den eingestellten Zugriffsrechten. Für den Zugriff auf einen verschlüsselten Schlüssel muss zusätzlich für jede Operation mit diesem Schlüssel, ein individuelles Kennwort eingegeben werden. Die Standardeinstellung ist **Nur verschlüsselt**.

Verschlüsselt und unverschlüsselt: Der private Schlüssel wird verschlüsselt und unverschlüsselt abgelegt. Für den Download steht die verschlüsselte Version bereit und der heruntergeladene Schlüssel kann nur mit dem individuellen Kennwort genutzt werden. Kryptooperationen für die automatische Verlängerung von Zertifikaten funktionieren hingegen ohne die Abfrage des Kennworts, da der private Schlüssel auch unverschlüsselt vorliegt.

Nur verschlüsselt: Der private Schlüssel wird nur verschlüsselt abgelegt. Bei jeder Operation wird das individuelle Kennwort abgefragt.

Nicht verschlüsseln: Der private Schlüssel wird nicht verschlüsselt abgelegt. Alle Operationen, die den privaten Schlüssel erfordern, werden ohne Abfrage eines individuellen Kennworts durchgeführt.

Kennwort für privaten Schlüssel: Geben Sie hier das Kennwort für den privaten Schlüssel ein. Haben Sie die Option **Nicht verschlüsseln** gewählt, ist dieses Feld ausgegraut.

Kennwort wiederholen: Wiederholen Sie das Kennwort. Stimmen die Kennwörter nicht überein, wird Ihnen das direkt angezeigt. Haben Sie die Option **Nicht verschlüsseln** gewählt, ist dieses Feld ausgegraut.

4

Sie erhalten Informationen zu Hashalgorithmus der Signatur und den Schlüsselverwendungszwecken, die Sie nicht ändern können.

5

Sie können keine Einstellungen auf dieser Seite des Assistenten ändern.

6

Metadaten: Legen Sie hier zusätzliche Informationen für das Zertifikat fest. Es öffnet sich ein Konfigurationsfenster. Wählen Sie einen Bezeichner aus der Dropdown-Liste aus und vergeben Sie einen Wert. Neue Bezeichner können unter **Globale Einstellungen** → **Metadaten** erstellt werden (siehe **9.3.1 Neue Metadatenschlüssel anlegen**).

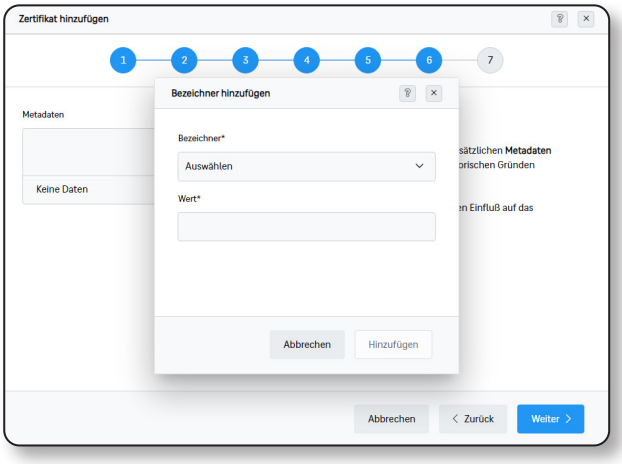


Abb. 5.33: *Metadaten festlegen*

7

Sie können keine Einstellungen auf dieser Seite des Assistenten ändern.

Sind alle notwendigen Informationen für das Zertifikat eingestellt, laden Sie das Zertifikat über den Button **Zertifikat ausstellen** hoch.

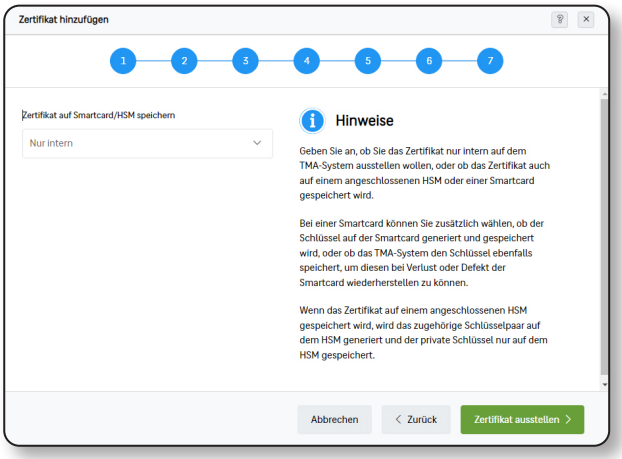


Abb. 5.34: *Speicherort für Schlüsselmaterial*

8

Geben Sie das Kennwort der ausstellenden CA ein, wenn Sie danach gefragt werden.

Das Zertifikat wird hochgeladen. Anschließend erhalten Sie Informationen zum Import des Zertifikats. Werden Ihnen Fehler angezeigt, z.B. weil Vorgaben durch Richtlinien nicht erfüllt werden, navigieren Sie zu der entsprechenden Seite und korrigieren Sie die Einstellung.

War der Import erfolgreich, können Sie das Zertifikat herunterladen oder ansehen.

Schließen Sie den Assistenten.

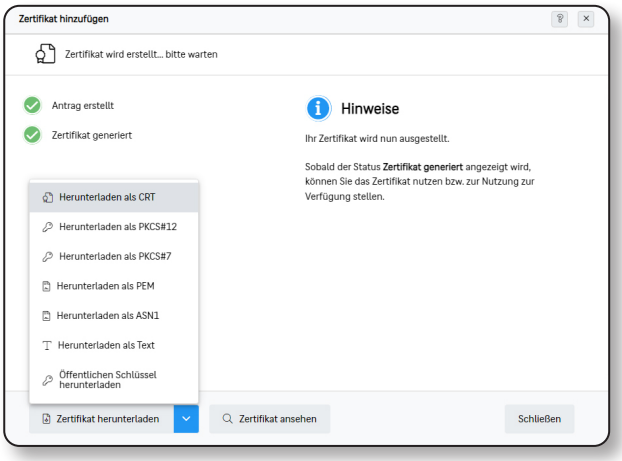


Abb. 5.35: *Zertifikat ausgestellt*

5.3.4 Zertifikat-Lifecycle-Management

Zertifikate besitzen einen Lebenszyklus. Sie durchlaufen fünf Phase:

- Erstellung: Ein Benutzer, Gerät oder Dienst fordert ein neues Zertifikat an. Der Antrag wird geprüft und genehmigt.
- Verteilung: Das angeforderte Zertifikat wird für den entsprechenden Benutzer, Dienst oder das Gerät bereitgestellt.
- Validierung: Während seiner Nutzungsphase wird das Zertifikat immer wieder geprüft und verifiziert, damit der Benutzer z.B. Zugriff zu bestimmten Diensten oder Dokumenten enthält.
- Verlängerung: Zum Ende seiner Gültigkeit werden Zertifikate verlängert, wenn sie weiterhin genutzt werden sollen. Dafür müssen sie neu verteilt werden.
- Zurücknahme/Sperrung: Wird ein Zertifikat nicht mehr gebraucht oder wurde es kompromittiert, wird es zurückgezogen oder gesperrt.

5.3.4.1 Zertifikate verlängern

Um ein auslaufendes Zertifikat zu verlängern, navigieren Sie zu **CA-Management → Zertifikate** und öffnen Sie mit einem Rechtsklick das Kontextmenü des Zertifikats. Wählen Sie die Option **Verlängern**. Geben Sie anschließend das Kennwort der CA, die das Zertifikat signiert hat, und das Kennwort für den privaten Schlüssel des Zertifikats ein, wenn Sie danach gefragt werden. War die Eingabe korrekt, erhalten Sie die Meldung, dass das Zertifikat aktualisiert wurde, und die Gültigkeit verlängert sich um die bei der Erstellung eingestellte Gültigkeit.

Alternativ können Sie ein oder mehrere Zertifikate über den Button **Verlängern** oberhalb der Tabelle verlängern.

Mithilfe eines Abfrage mit Aktion-Objekts kann das Verlängern automatisch eingerichtet werden. (siehe **21.5 Beispiel: Abfrage mit Aktion zum automatischen Verlängern von Zertifikaten und CRLs**).

5.3.4.2 Zertifikate zurückziehen

Um ein Zertifikat zu zurückzuziehen, navigieren Sie zu **CA-Management → Zertifikate** und öffnen Sie mit einem Rechtsklick das Kontextmenü des Zertifikats. Wählen Sie die Option **Zurückziehen**. Geben Sie anschließend das Kennwort der CA, die das Zertifikat signiert hat, und das Kennwort für den privaten Schlüssel des Zertifikats ein, wenn Sie danach gefragt werden. War die Eingabe korrekt, erhalten Sie die Meldung, dass das Zertifikat aktualisiert wurde, und der Status ändert sich zu **Zurückgezogen** und die Angabe in der Spalte Gültig bis verschwindet.

Alternativ können Sie ein oder mehrere Zertifikate über den Button **Zurückziehen** oberhalb der Tabelle zurückziehen.

Beachten Sie, möchten Sie das Zertifikat einer Sub-CA zurückziehen, werden auch alle abhängigen Zertifikate ungültig.

5.3.4.3 Zertifikate vorübergehend ungültig setzen

Um ein Zertifikat vorübergehend ungültig zu setzen, navigieren Sie zu **CA-Management → Zertifikate** und öffnen Sie mit einem Rechtsklick das Kontextmenü des Zertifikats. Wählen Sie die Option **Vorübergehend ungültig setzen**. Geben Sie anschließend das Kennwort der CA, die das Zertifikat signiert hat, und das Kennwort für den privaten Schlüssel des Zertifikats ein, wenn Sie danach gefragt werden. War die Eingabe korrekt, erhalten Sie die Meldung, dass das Zertifikat aktualisiert wurde, und der Status ändert sich zu **On hold**.

Möchten Sie das Zertifikat wieder gültig setzen, wählen Sie die Option **Wieder gültig setzen** im Kontextmenü des Zertifikats aus. Geben Sie anschließend das Kennwort der CA, die das Zertifikat signiert hat, und das Kennwort für den privaten Schlüssel des Zertifikats ein, wenn Sie danach gefragt werden. War die Eingabe korrekt, erhalten Sie die Meldung, dass das Zertifikat aktualisiert wurde, und der Status ändert sich wieder zu **Gültig**. Die Laufzeit ändert sich nicht.

Alternativ können Sie ein oder mehrere Zertifikate über den Button **Halten beenden** oberhalb der Tabelle wieder gültig setzen.

Beachten Sie, möchten Sie das Zertifikat einer Sub-CA vorübergehend ungültig setzen, werden auch alle abhängigen Zertifikate ungültig.

5.4 Richtlinien

Richtlinien helfen bei der Erstellung von Zertifikaten, indem sie bestimmte Einstellungen als Standardwerte vorgeben, validieren oder Bedingungen festlegen, bei denen die Standardwerte angewendet werden. Sie können für einen Container oder eine CA festgelegt werden.

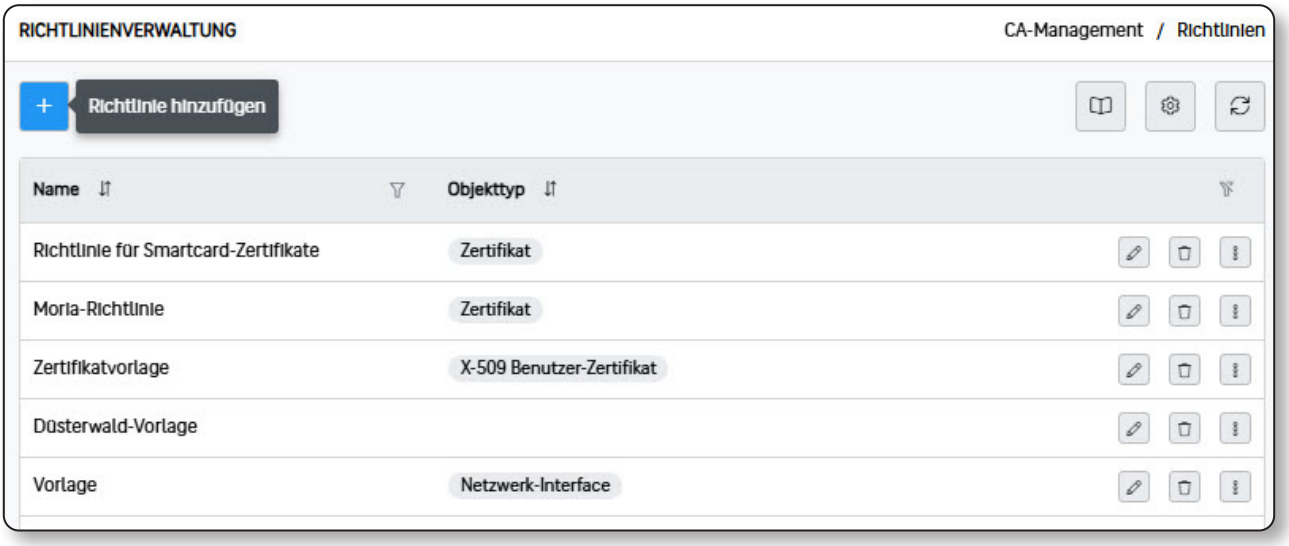


Abb. 5.36: *Übersicht der Richtlinien*

Wird ein neues Zertifikat in einem Container mit Richtlinie erstellt, werden die Vorgaben in der Richtlinie als Standardwerte eingetragen und Abweichungen können als Fehler deklariert werden.

Ähnlich verhält es sich bei Zertifikaten, die von einer CA mit einer Richtlinie signiert werden.

Es können auch Richtlinien von Containern und CAs zusammenspielen. Dabei gilt, je näher die Richtlinie dem eigentlichen Zertifikat ist, desto höher ist die Priorität der Richtlinien. Die Richtlinie einer CA hat die höchste Priorität und überschreibt die Werte aus den Richtlinien der Container, sofern diese abweichen. Eine Ausnahme bilden Werte, die als Standard erzwingen markiert wurden. Sie werden erzwungen. Haben verschiedene Richtlinien das gleiche Attribut mit unterschiedlichen Werten als erzwungen markiert, gilt auch hier die oben beschriebene Hierarchie der Richtlinien.

Beispiel: Ein Zertifikat soll in einem Untercontainer angelegt werden. Sowohl der Untercontainer als auch der übergeordnete Container haben jeweils eine Richtlinie, die einen Wert als Schlüssellänge vorschreibt. Zusätzlich hat die CA eine eigene Richtlinie, die ebenfalls eine Schlüssellänge vorgibt. Die Werte unterscheiden sich. Die Richtlinie für den Container gibt den Wert 4096 Bit vor. Die Richtlinie für den Untercontainer möchte einen Wert von 2048 Bit und die CA gibt einen Wert von 3072 Bit vor. In diesem Fall hat das Zertifikat eine Schlüssellänge von 3072 Bit, da die Richtlinie der CA die höchste Priorität besitzt. Ist der Wert der Container-Richtlinie als erzwungen markiert, hat das Zertifikat eine Schlüssellänge von 4096 Bit.

Es wird eine tabellarische Übersicht über die vorhandenen Richtlinien angezeigt .

5.4.1 Eine neue Richtlinie erstellen



Oberhalb der Tabelle können Sie eine neue Richtlinie hinzufügen.Es öffnet sich ein Konfigurationsobjekt.

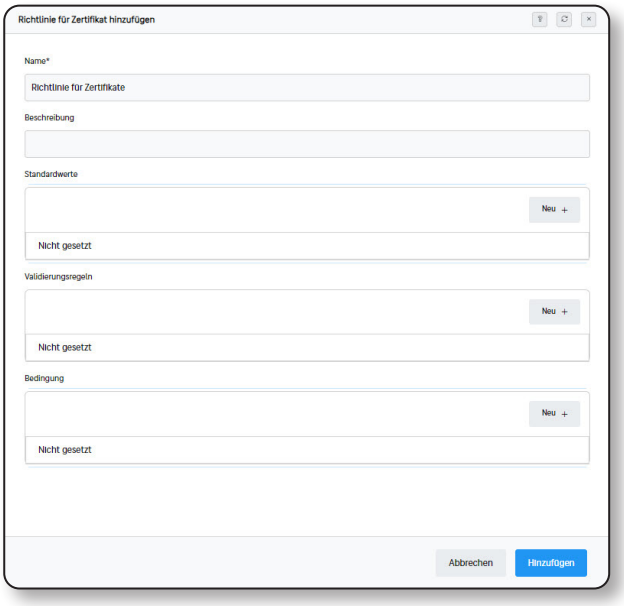


Abb. 5.37: *Neue Richtlinie erstellen*

Objekttyp: Wählen Sie, ob die Richtlinie für ein CA-Zertifikat oder ein Zertifikat gelten soll.

Name: Vergeben Sie einen aussagekräftigen Namen.

Beschreibung: Geben Sie optional eine Beschreibung der Richtlinie ein.

Standardwerte: Standardwerte geben Werte für Attribute vor, die beim Anlegen automatisch vorausgewählt sind. Fügen Sie einen neuen Wert über **Neu** hinzu. Es öffnet sich ein weiteres Fenster.

Attribut: Wählen Sie ein Attribut aus der Dropdown-Liste aus.

Default: Legen Sie den Standardwert, der sich nach dem ausgewählten Attribut richtet, z.B. eine bestimmte CA, die gewählt werden soll.

Standard erzwingen: Aktivieren Sie diese Option, wenn der Standardwert erzwungen werden soll. Ändern Sie das Attribut bei der Erstellung eines neuen (CA-)Zertifikats, wird die Änderung bei der Erstellung mit dem Standardwert überschrieben.

Umwandlung: Geben Sie hier eine DocExpression an, um Werte, z.B. die Kennwortlänge, zu prüfen oder mit berechneten Werten, z.B. dem aktuellen Datum zu belegen (siehe **25 DocExpressions**).

Aktiv: Aktivieren Sie diese Option, wenn die Regel in der Richtlinie aktiv sein soll.

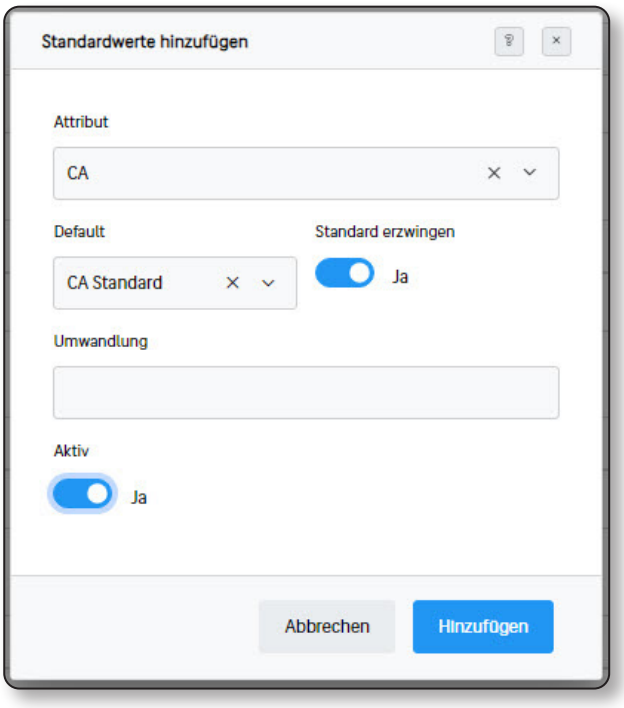


Abb. 5.38: *Neue Richtlinie: Standardwerte bestimmen*

Validierungsregeln: Validierungsregeln prüfen, ob die Werte beim Anlegen oder Ändern eines Objekts bestimmten Regeln entsprechen. Fügen Sie eine neue Regel über **Neu** hinzu. Es öffnet sich ein weiteres Fenster.

Attribut: Wählen Sie ein Attribut aus der Dropdown-Liste aus.

Aktiv: Aktivieren Sie diese Option, wenn die Regel in der Richtlinie aktiv sein soll.

Vergleich: Wählen Sie die Vergleichsoperation aus **(siehe 21.2.2 Erstellen von Vergleichen der Attribute)**.

Vergleichswert: Geben Sie den Wert an, mit dem der Wert des ausgewählten Attributs verglichen werden soll.

Verknüpfung: Wählen Sie die Verknüpfung zwischen den verschiedenen Validierungsregeln aus.

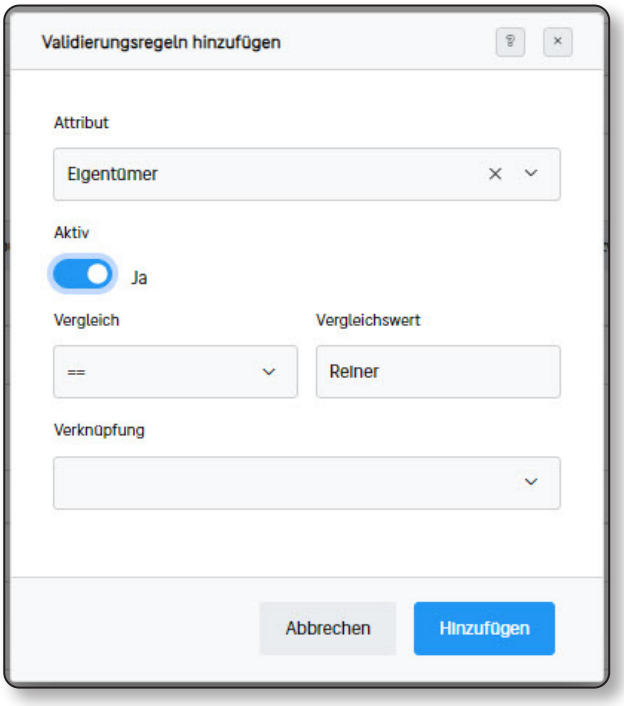


Abb. 5.39: *Neue Richtlinie: Validierungsregeln*

Bedingung: Bedingungen bestimmen, wann die Standardwerte und Validierungsregeln angewendet werden sollen. Dies ermöglicht, dass die Richtlinie nur auf bestimmte Objekte angewendet werden. Fügen Sie eine neue Bedingung über **Neu** hinzu. Es öffnet sich ein weiteres Fenster.

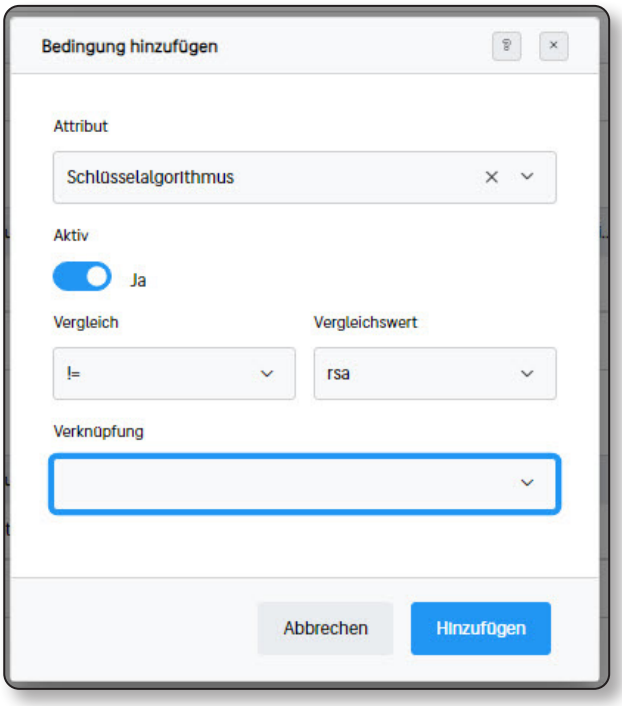


Abb. 5.40: *Neue Richtlinie: Bedingungen*

Attribut: Wählen Sie ein Attribut aus der Dropdown-Liste aus.

Aktiv: Aktivieren Sie diese Option, wenn die Bedingung in der Richtlinie aktiv sein soll.

Vergleich: Wählen Sie die Vergleichsoperation aus (siehe **21.2.2 Erstellen von Vergleichen der Attribute**).

Vergleichswert: Geben Sie den Wert an, mit dem der Wert des ausgewählten Attributs verglichen werden soll.

Verknüpfung: Wählen Sie die Verknüpfung zwischen den verschiedenen Bedingungen aus.

Bestätigen Sie die Eingaben mit **Hinzufügen**.

6 RA-Management

Eine Registrierungsstelle (Registration Authority, RA) nimmt Zertifikatanfragen (Certificate Signing Request, CSR) entgegen, prüft diese und leitet sie schließlich weiter an die entsprechende Zertifizierungsstelle (CA), damit diese den CSR signiert und somit zu einem validen Zertifikat macht.

Ein CSR kann über das Self-Service-Portal oder über die REST API eingereicht werden. Eingereichte CSRs werden im Bereich CSR-Inventar angezeigt und stehen zur Bearbeitung bereit (siehe **11 Self-Service-Portal**).

Info

Informationen zur REST API finden Sie auf der ECOS Webseite

6.1 CSR-Inventar

6.1.1 Aufbau

Rechts neben dem Seitenmenü wird das Container-Menü angezeigt. Neben den Menüs befindet sich eine tabellarische Übersicht über die vorhandenen Zertifikatanfragen, die u.a. über das Self-Service-Portal oder die REST API hereinkommen (siehe **11 Self-Service-Portal**).



Abb. 6.01: *RA-Management im Seitenmenü*

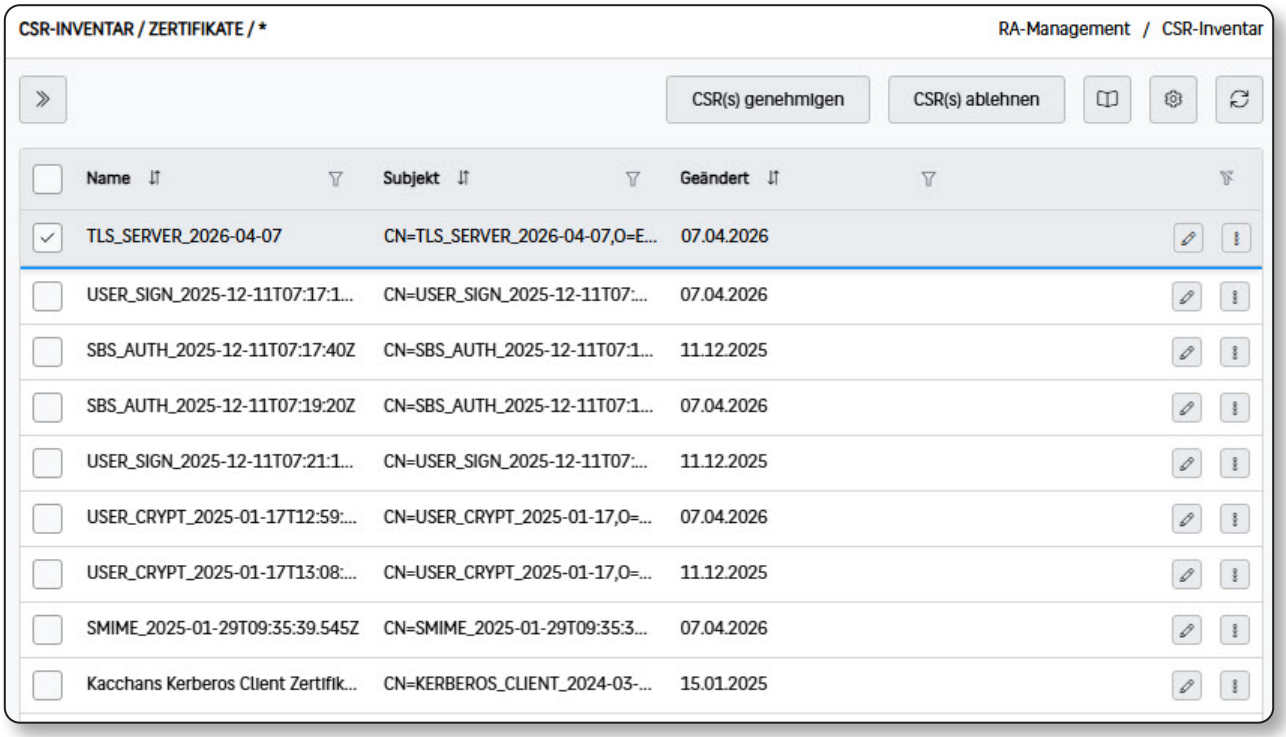


Abb. 6.02: *Übersicht RA-Management*

6.1.1.1 Tabelle

Oberhalb der Tabelle stehen neben den allgemeinen Tabellenfunktionen zusätzliche Buttons zur Verfügung.

CSR(s) genehmigen: Über diesen Button können die ausgewählten CSRs genehmigt werden.

CSR(s) ablehnen: Über diesen Button können die ausgewählten CSRs abgelehnt werden.

6.1.2 CSR genehmigen

Navigieren Sie zum Bereich **RA-Management → CSR-Inventar**. Es wird eine Übersicht über alle CSRs angezeigt, die zur Genehmigung warten.

Öffnen Sie den entsprechenden Zertifikatrequest über die Lupe. Es öffnet sich ein Wizard, der im oberen Teil Informationen zu dem Request bereitstellt und im unteren Teil Einstellungen des RA-Admins erfordert.

Zwischen der Zertifikatübersicht und den erforderlichen Einstellungen zur Genehmigung, werden Zertifikate und CSRs aufgelistet, die entweder ein ähnliches oder gleiches Subjekt oder SAN (DNS und IP) wie der zu genehmigende CSR haben.

1

Eigentümer: Standardmäßig wird hier der Benutzer als Besitzer eingetragen, der diesen Request gestellt hat. Über die Schaltfläche rechts können Sie die Bearbeitung aktivieren und einen anderen Besitzer auswählen.

Zielcontainer für Zertifikat: Wählen Sie den Container aus, in dem das Zertifikat gespeichert werden soll. Bitte beachten Sie, sind für den Container Richtlinien hinterlegt, können bestimmte Werte für das Zertifikat vorgegeben bzw. überschrieben werden. In diesem Assistenten werden Ihnen die Übereinstimmungen und Abweichungen mit den Richtlinien direkt angezeigt.

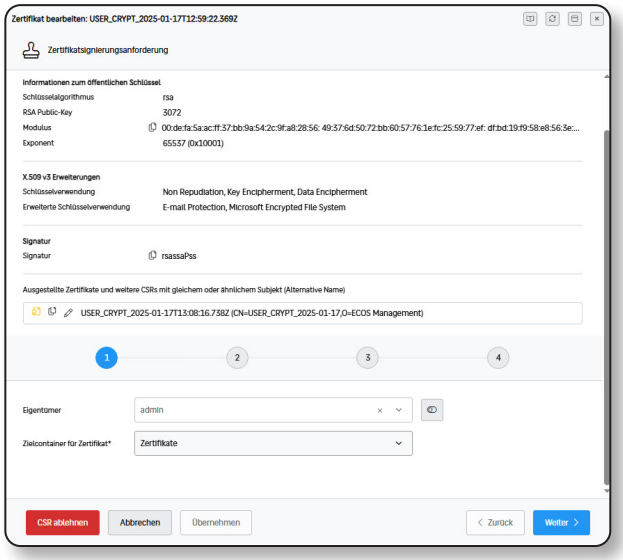


Abb. 6.03: *CSR genehmigen: Eigentümer & Container*

2

Übergeordnete Zertifizierungsstelle: Wählen Sie die CA aus, die das Zertifikat signieren soll.

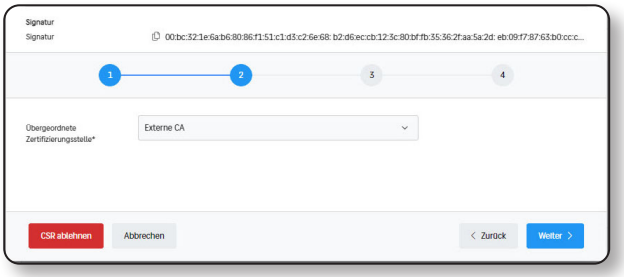


Abb. 6.04: *CSR genehmigen: CA auswählen*

3

Metadaten: Legen Sie hier zusätzliche Informationen für das Zertifikat fest. Es öffnet sich ein Konfigurationsfenster. Wählen Sie einen Bezeichner aus der Dropdown-Liste aus und vergeben Sie einen Wert. Neue Bezeichner können unter **Globale Einstellungen → Metadaten** erstellt werden (siehe 9.3.1 Neue Metadatenschlüssel anlegen).

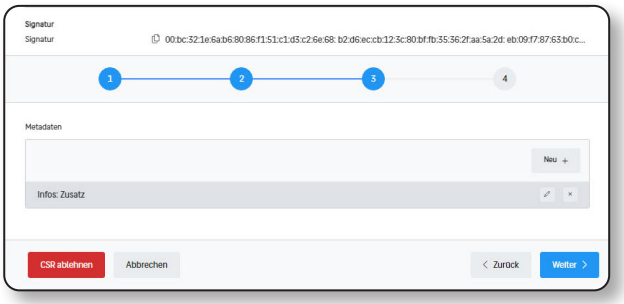


Abb. 6.05: *CSR genehmigen: Metadaten hinzufügen*

4

Ihnen wird eine Übersicht, über die von Ihnen gemachten Einstellungen gezeigt. Sie können zusätzlich Anmerkungen hinzufügen.

Stimmen alle Einstellungen, erstellen Sie das Zertifikat über den Button **Zertifikat ausstellen**.

Geben Sie das Kennwort der ausstellenden CA ein, wenn Sie danach gefragt werden. War die Erstellung erfolgreich, können Sie das Zertifikat herunterladen oder ansehen.

Schließen Sie den Assistenten.

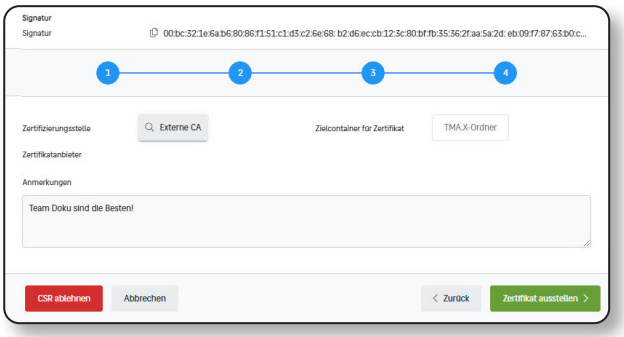


Abb. 6.06: *CSR genehmigen: Übersicht*

6.1.3 CSR ablehnen

Navigieren Sie zum Bereich **RA-Management → CSR-Inventar**. Es wird eine Übersicht über alle CSRs angezeigt, die zur Genehmigung warten.

Öffnen Sie den entsprechenden Zertifikatrequest über die Lupe. Es öffnet sich ein Wizard, der im oberen Teil Informationen zu dem Request bereitstellt und im unteren Teil Einstellungen des RA-Admins erfordert.

Zum Ablehnen klicken Sie links auf den roten Button **CSR ablehnen**. Es öffnet sich ein neues Fenster, in dem Sie eine Begründung für die Ablehnung eintragen können.

Ablehnungsgrund: Wählen Sie den Grund aus. Zur Verfügung stehen die Optionen **Kein Grund** und **Fehlerhafte Anfrage**.

Bemerkung: Geben Sie hier eine Bemerkung für die Ablehnung an, z.B. wenn falsche Parameter ausgewählt wurden.

Die Begründung für die Ablehnung sieht der Antragsteller im Self-Service-Portal.

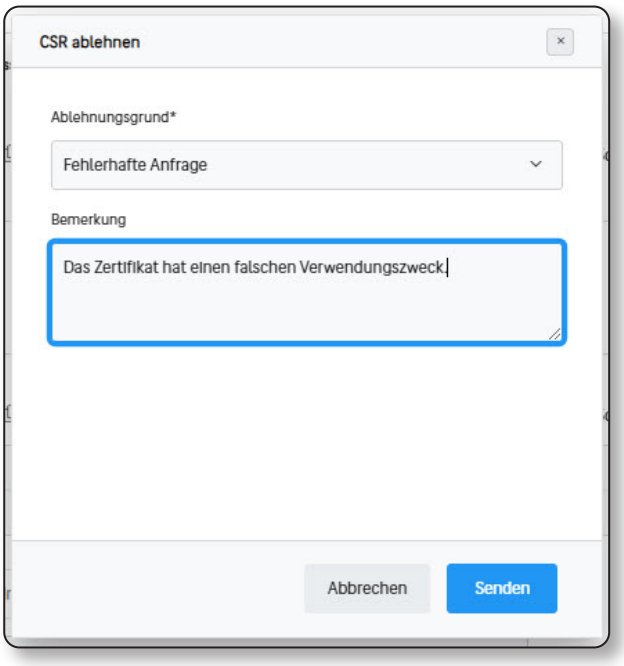


Abb. 6.07: *CSR ablehnen: Begründung*

7 Benutzerverwaltung

In der Benutzerverwaltung werden die Benutzerkonten und die verschiedenen Benutzerrollen, die die Berechtigungen der Benutzer festlegen, verwaltet.



Abb. 7.01: *Benutzerverwaltung im Seitenmenü*

7.1 Benutzer

Es wird eine tabellarische Übersicht über die vorhandenen Benutzerkonten angezeigt. Die Trust Management Appliance unterstützt manuell angelegte Benutzerkonto ebenso wie die Synchronisation aus einem Verzeichnisdienst, z.B. einem AD (siehe **19 Verzeichnissynchronisation**).

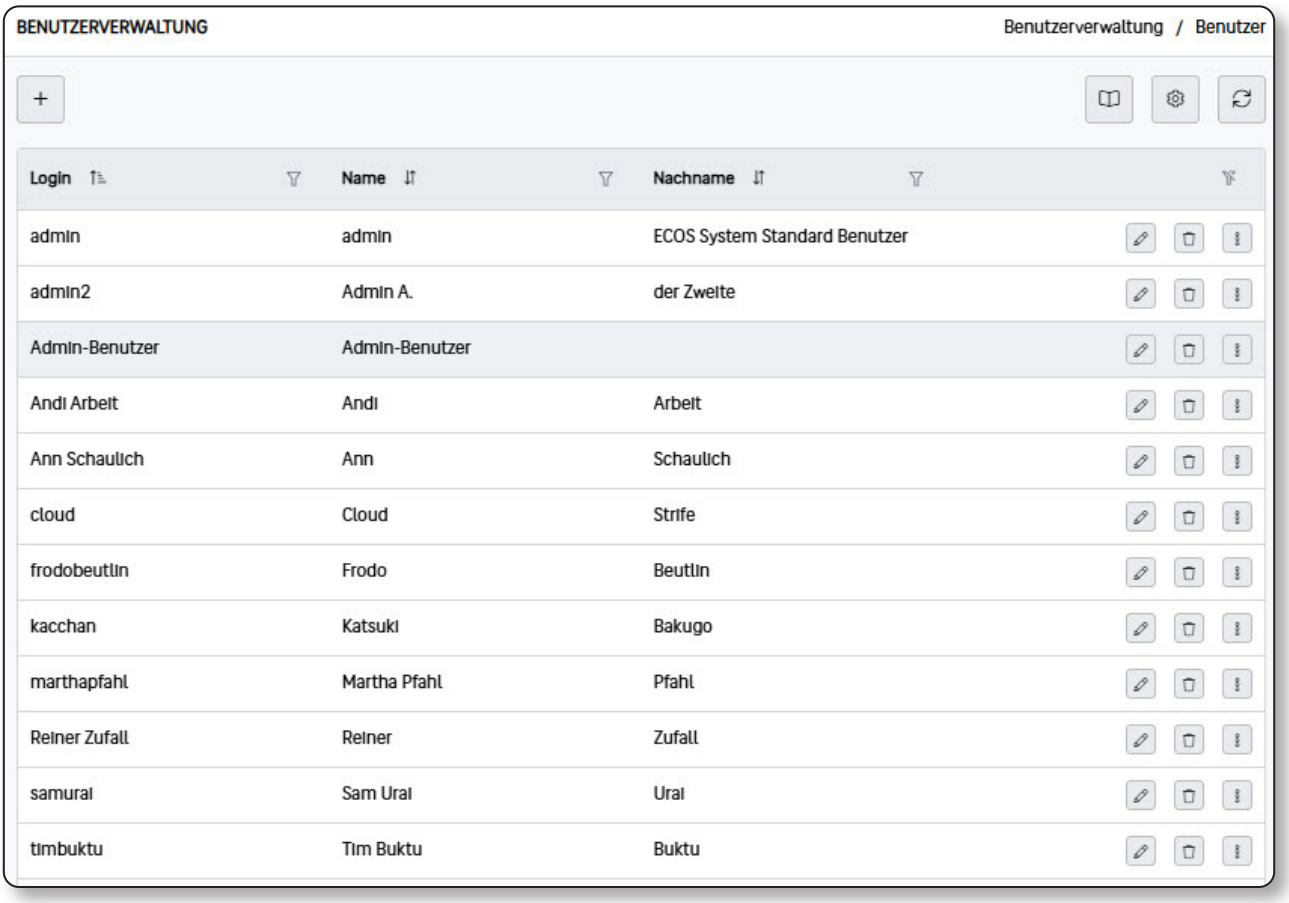


Abb. 7.02: *Übersicht Benutzerverwaltung*

7.1.1 Einen neuen Benutzer anlegen

+ Oberhalb der Tabelle fügen Sie einen neuen Benutzer hinzu. Es öffnet sich ein Konfigurationsobjekt mit mehreren Tabs.

Kontaktinformationen

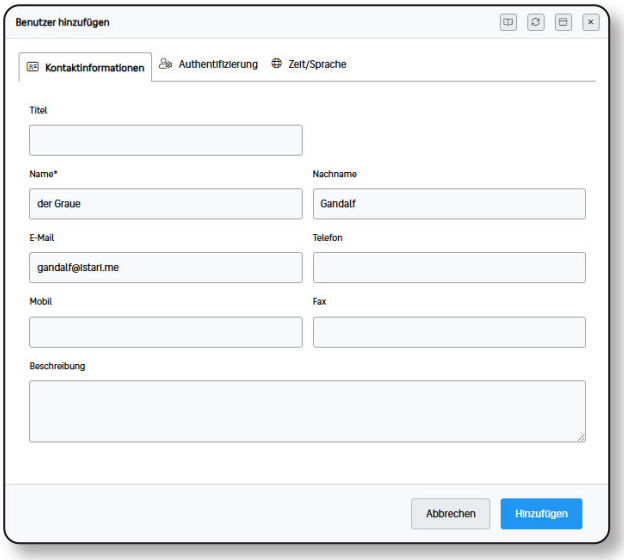


Abb. 7.03: *Benutzer anlegen: Kontaktinformationen*

Titel: Geben Sie den Titel des Mitarbeitenden an.

Name: Geben Sie den Vornamen des Mitarbeitenden an.

Nachname: Geben Sie den Nachnamen des Mitarbeitenden an.

E-Mail: Geben Sie die E-Mail-Adresse des Mitarbeitenden an.

Telefon: Geben Sie die Telefonnummer des Mitarbeitenden an.

Mobil: Geben Sie die Mobilfunknummer des Mitarbeitenden an.

Fax: Geben Sie die Faxnummer des Mitarbeitenden an.

Beschreibung: Geben Sie optional eine Beschreibung an.

Authentifizierung

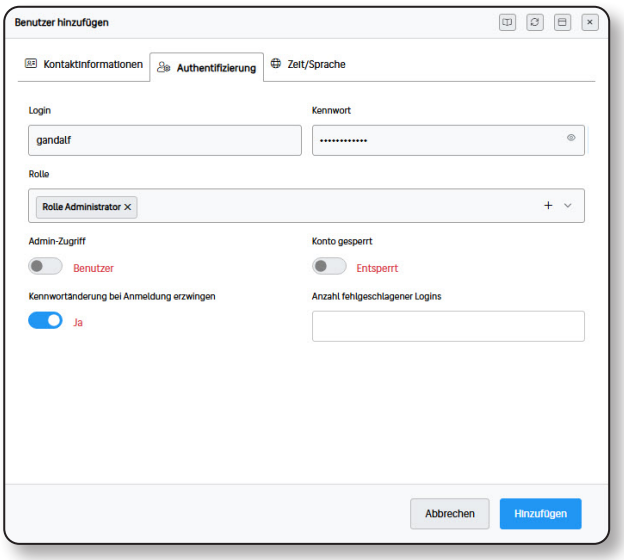


Abb. 7.04: *Benutzer anlegen: Authentifizierung*

Login: Geben Sie den Benutzernamen des Mitarbeitenden an.

Kennwort: Geben Sie das Kennwort des Mitarbeitenden an.

Rolle: Vergeben Sie eine Benutzerrolle für den Mitarbeitenden. Über das + öffnet sich ein Dialog zum Anlegen einer neuen Rolle.

Admin-Zugriff: Aktivieren Sie diese Option, wenn der Mitarbeitenden administrativen Zugriff auf die TMA bekommen soll.

Konto gesperrt: Aktivieren Sie dies Option, wenn das Benutzerkonto gesperrt werden soll.

Anzahl fehlgeschlagener Logins: Geben Sie hier die Anzahl der möglichen Fehlversuche für das Anmelden an. Nach Erreichen wird das Konto gesperrt und kann nur vom Systemadmin wieder entsperrt werden. Wird keine Anzahl angegeben, sind die Fehlversuche auf fünf beschränkt.

Kennwortänderung bei Anmeldung erzwingen: Aktivieren Sie diese Option muss der Benutzer bei der nächsten Anmeldung sein Kennwort ändern. Andere Aktionen sind bis zur Kennwortänderung für den Benutzer nicht möglich.

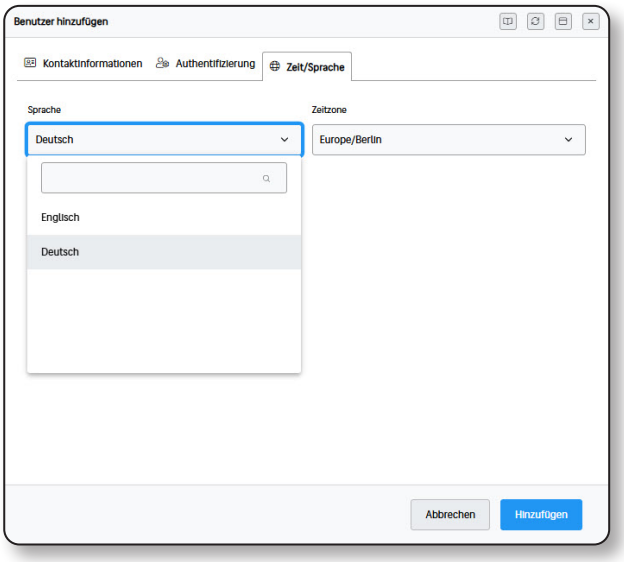


Abb. 7.05: *Benutzer anlegen: Zeit/Sprache*

Zeit/Sprache

Sprache: Legen Sie die Anzeigesprache für das Benutzerkonto fest. Aktuell stehen die Sprachen Deutsch und Englisch zur Auswahl.

Zeitzone: Wählen Sie die Zeitzone aus der Dropdown-Liste aus, in der sich der Mitarbeitende befindet.

Bestätigen Sie die Eingaben mit **Hinzufügen**.

7.1.2 Admin-Zugriff gewähren

Navigieren Sie zu **Benutzerverwaltung → Benutzer** und öffnen Sie das Benutzerobjekt, dem Sie Admin-Zugriff gewähren möchten.

Wählen Sie den Reiter Authentifizierung. Aktivieren Sie die Option Admin-Zugriff. Die Bezeichnung ändert sich von **Benutzer** zu **Administrator**.

Speichern Sie die Änderung.

Weitere Informationen finden Sie unter **15 Benutzerverwaltung (Experte)**.

Hinweis: Für den Betrieb in VS-NfD-Umgebungen muss jeder Benutzer mit Admin-Zugriff zusätzlich eine Zwei-Faktor-Authentifizierung über Smartcard verwenden. Die Aktivierung des Admin-Zugriffs ersetzt nicht die 2FA (siehe **1.5 Smartcard-Zugriff für Admin-Benutzer im VS-NfD-Umfeld**).

7.1.3 Kennwort ändern

Um das das Kennwort eines Benutzers zu ändern, navigieren Sie zu **Benutzerverwaltung → Benutzer** und öffnen Sie das entsprechende Benutzerobjekt.

Wählen Sie den Reiter Authentifizierung. Geben Sie ein neues Kennwort ein und **speichern** Sie die Änderung.

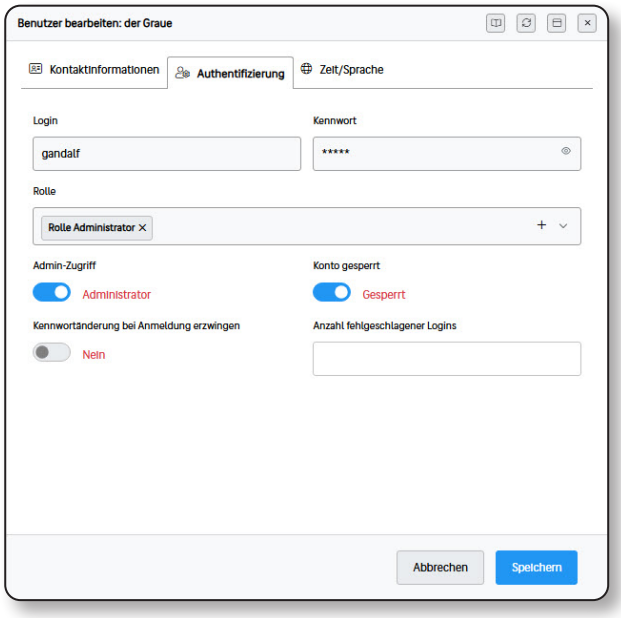


Abb. 7.06: *Benutzerkonto sperren*

7.1.4 Benutzerkonto deaktivieren

Um ein Benutzerkonto zu deaktivieren, navigieren Sie zu **Benutzerverwaltung → Benutzer** und öffnen Sie das entsprechende Benutzer-Objekt.

Wählen Sie den Reiter **Authentifizierung**. Aktivieren Sie die Option Konto gesperrt. Die Anzeige ändert sich von **Entsperrt** zu **Gesperrt**.

7.2 Benutzerrollen

Es wird eine tabellarische Übersicht über die vorhandenen Rollen angezeigt. Mithilfe der Benutzerrollen können verschiedene Zugriffsberechtigungen gewährt werden (siehe **15.1 Benutzer und Rollen 22 Berechtigungen**).

7.2.1 Eine neue Benutzerrolle anlegen

Oberhalb der Tabelle können Sie eine neue Rolle hinzufügen.Es öffnet sich ein Konfigurationsobjekt.

Name: Vergeben Sie einen aussagekräftigen Namen für die Benutzerrolle.

Bestätigen Sie die Eingaben mit **Hinzufügen**.

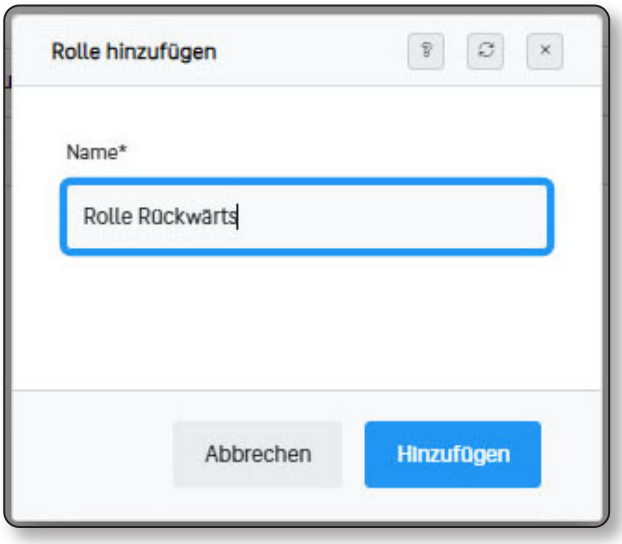


Abb. 7.07: *Benutzerrolle anlegen*

7.2.2 Eine Benutzerrolle zuweisen

Navigieren Sie zu **Benutzerverwaltung → Benutzer** und öffnen Sie das Benutzerobjekt, dem Sie eine Benutzerrolle zuweisen möchten.

Wählen Sie den Reiter Authentifizierung. Wählen Sie unter Rolle eine oder mehrere angelegte Rollen aus.

Speichern Sie die Änderungen.

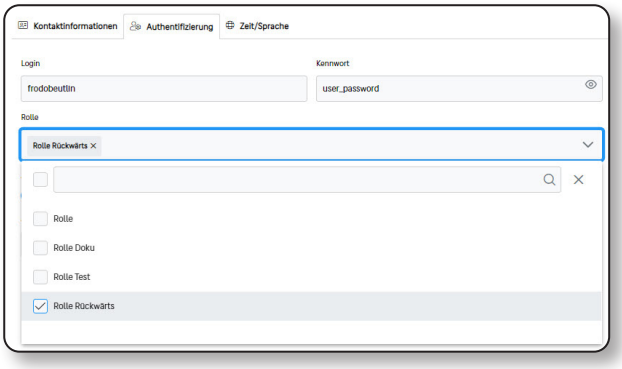


Abb. 7.08: *Benutzerrolle zuweisen*

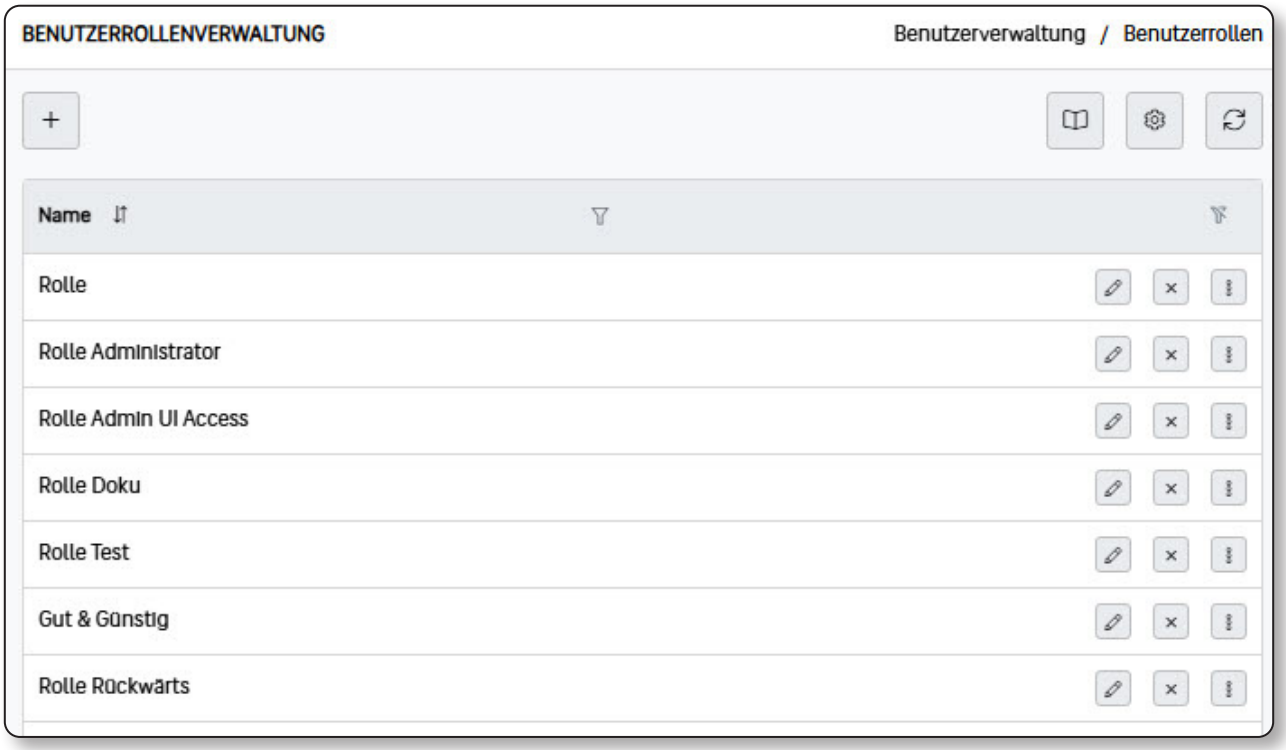


Abb. 7.09: *Übersicht Benutzerrollen*

Weitere Informationen zu Benutzern, Rollen und der Authentisierung finden Sie unter **15.1 Benutzer und Rollen.**

8 PKI-Dienste

In diesem Bereich werden verschiedene PKI-Dienste, u.a. zum Prüfen und Ausrollen von Zertifikaten, verwaltet.

8.1 Zugangspunkte

Es wird eine tabellarische Übersicht über die verschiedenen eingerichteten PKI- und Enrollment-Dienste mit ihren Serveradressen und Ports gezeigt.

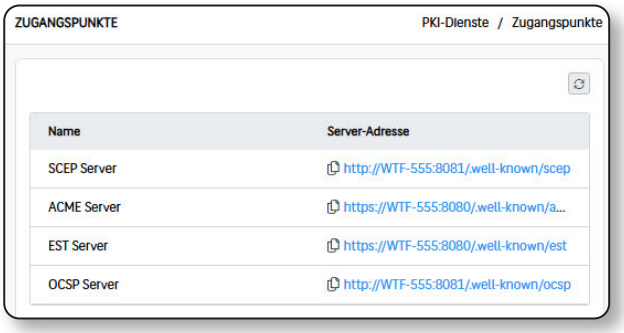


Abb. 8.01: *Übersicht Zugangspunkte*

9 Globale Einstellungen

In diesem Bereich werden globale Einstellungen der ECOS **TrustManagementAppliance®** (TMA) verwaltet.

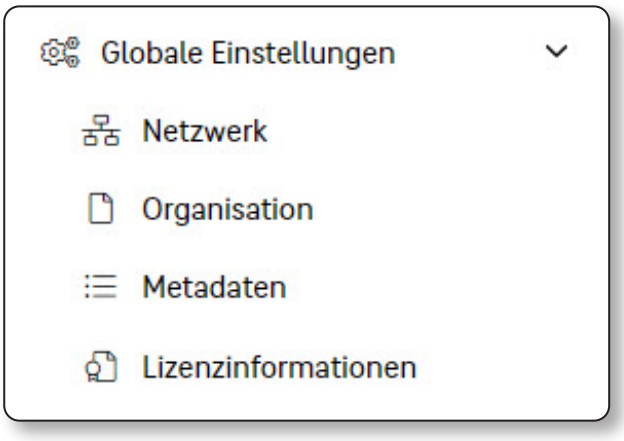


Abb. 9.01: *Globale Einstellungen im Seitenmenü*

9.1 Netzwerk

In den Netzwerkeinstellungen werden der DNS-Server, das Standard-Gateway und die NTP-Server definiert. Diese sind wichtig für den Betrieb der Trust Management Appliance.

9.1.1 DNS-Server

Der DNS-Server löst Hostnamen in IP-Adressen auf. Zusätzlich zum DNS-Server muss das Gateway bestimmt werden. Es leitet die Datenpakete an die Ziel-Hosts und Ziel-Netzwerke weiter.

Über das Dropdown-Menü wird eine Liste der verfügbaren Server angezeigt.

Über das + öffnet sich ein Dialog zum Anlegen eines neuen Servers.

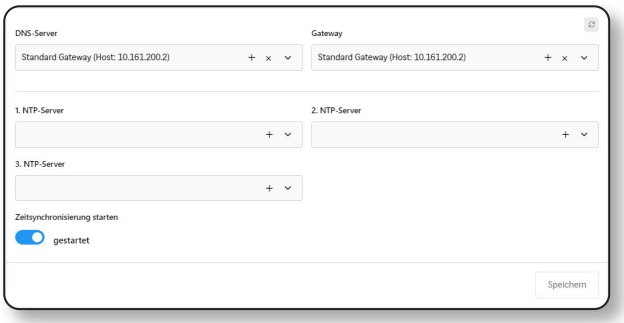


Abb. 9.02: *Netzwerkeinstellungen*

9.1.2 NTP-Server

Für die Zeitsynchronisation ist mindestens ein NTP-Server notwendig. Die Uhrzeit auf der TMA muss korrekt eingestellt sein, um Probleme mit der Synchronisation anderer Dienste oder mit Zertifikaten zu vermeiden. Die IP-Adressen der NTP-Server sollten statisch sein, andernfalls aktualisiert sich die IP-Adresse alle 60 Sekunden, was einen NTP-Neustart nach sich zieht.

Es können bis zu drei NTP-Server angegeben werden, bei denen es sich auch um öffentliche NTP-Server handeln kann. Um öffentliche NTP-Server nicht zu belasten, sollten sich nur maximal zwei Server eines internen Netzwerks mit den öffentlichen Servern synchronisieren. Alle weiteren Rechner und Server im LAN können die TMA als Zeitserver verwenden.

Über das Dropdown-Menü wird eine Liste der verfügbaren Server angezeigt.

Über das + öffnet sich ein Dialog zum Anlegen eines neuen Servers.

Der Schalter Zeitsynchronisation starten muss aktiviert werden, damit sich die TMA mit den angegebenen NTP-Servern synchronisiert.

9.2 Organisation

Name: Geben Sie hier den übergeordneten Namen der Organisation an. Beachten Sie, dass der Name der Organisation auch im Subjekt eines (CA-)Zertifikats einfließen kann, so dass der Name nicht ohne weiteres geändert werden kann.

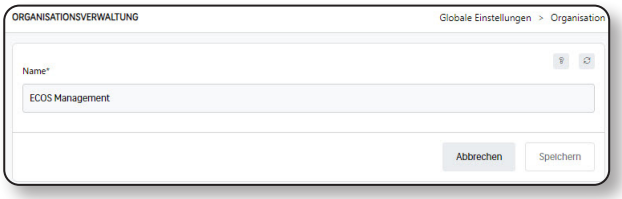


Abb. 9.03: *Organisation*

9.3 Metadaten

Metadaten erlauben, zusätzliche Informationen zu den Merkmalen eines Objekts zu speichern. Diese Informationen werden nicht weiterverarbeitet, können aber z.B. in Abfragen oder Richtlinie verwendet werden. Sie bestehen aus Schlüssel-/Wertepaaren. Die Schlüsselnamen werden hier festgelegt. Der Wert für einen Schlüssel wird im jeweiligen Zertifikat bestimmt.

Metadaten können auch zu einem bereits erstellten Zertifikat hinzugefügt werden.

Es wird eine tabellarische Übersicht über die vorhandenen Metadatenschlüssel angezeigt .

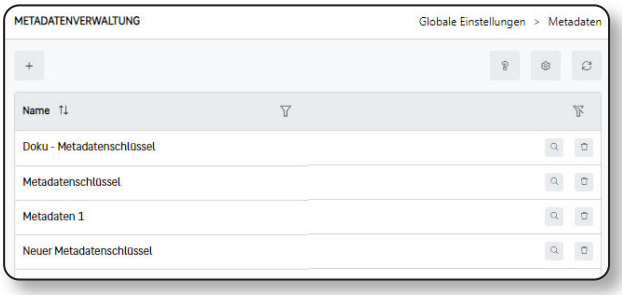


Abb. 9.04: *Übersicht Metadatenverwaltung*

9.3.1 Neue Metadatenschlüssel anlegen

\+ Oberhalb der Tabelle können Sie neue Metadatenschlüssel hinzufügen.Es öffnet sich ein Konfigurationsobjekt.

Name: Vergeben Sie einen aussagekräftigen Namen für die Metadatenschlüssel.

Tag: Wählen Sie einen Tag aus der Dropdown-Liste aus.

Optionen: Fügen Sie eine neue Option über Neu hinzu.

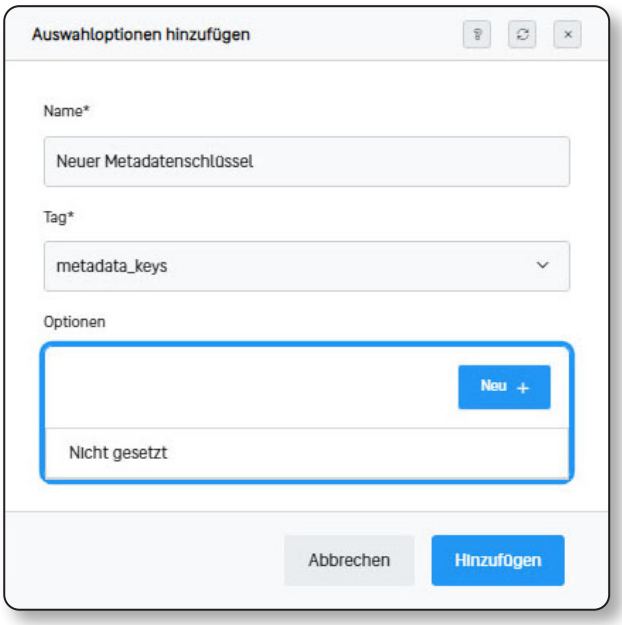


Abb. 9.05: *Metadatenschlüssel erstellen*

Tag: Legen Sie hier einen Tag fest. Das Tag ist ein internes Attribut und wird in der Datenbank gespeichert. Es sollte eindeutig sein. Wird ein Objekt mit diesen Metadaten angelegt, darf das Tag nicht mehr geändert werden. Andernfalls wird die Auswahl ungültig.

Text: Geben Sie hier den Text an, der als Schlüsselname zur Auswahl steht. Der Text kann problemlos geändert werden.

Bestätigen Sie die Eingaben mit **Hinzufügen**.

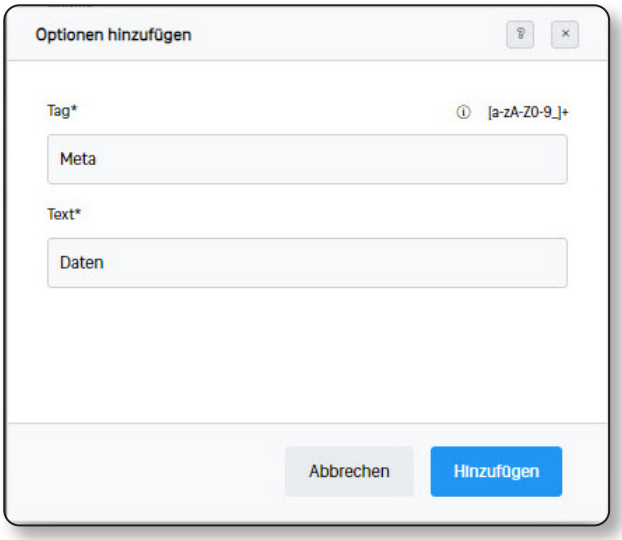


Abb. 9.06: *Optionen hinzufügen*

9.3.2 Metadaten zu einem bereits erstellten Zertifikat hinzufügen

Navigieren Sie zu den **CA-Management → CA-Zertifikate** oder **Zertifikate** und öffnen Sie das entsprechende Zertifikat über das Lupensymbol auf der rechten Seite der Tabelle.

Es öffnet sich ein Fenster mit den Informationen zum (CA-)Zertifikat. Bearbeiten Sie die Metadaten am Ende des Zertifikats.

Es öffnet sich ein weiteres Fenster, indem Sie einen Bezeichner aus der Dropdown-Liste wählen und den gewünschten Wert eingeben.

Speichern Sie die Änderungen.

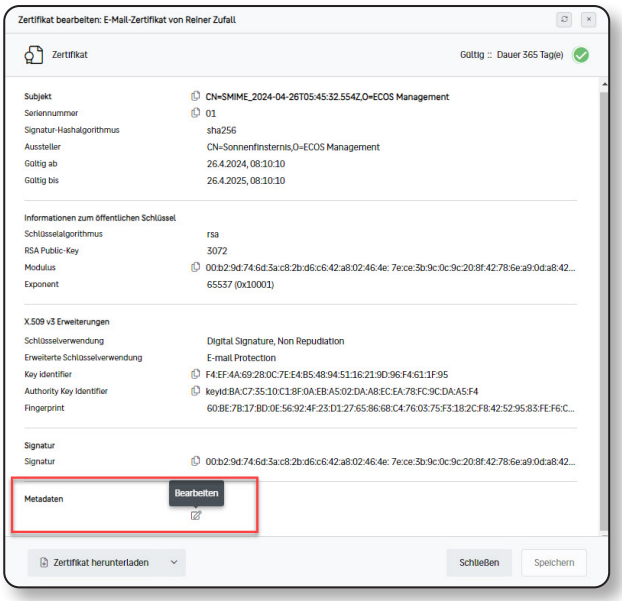


Abb. 9.07: *Metadaten hinzufügen*

9.4 Lizenzinformationen

Hier werden die Informationen zu der vorhandenen Lizenz zusammengefasst, darunter z.B. die Seriennummer sowie die Gültigkeit der Lizenz oder Informationen zu zusätzlichen Features, die in der Lizenz enthalten sind.

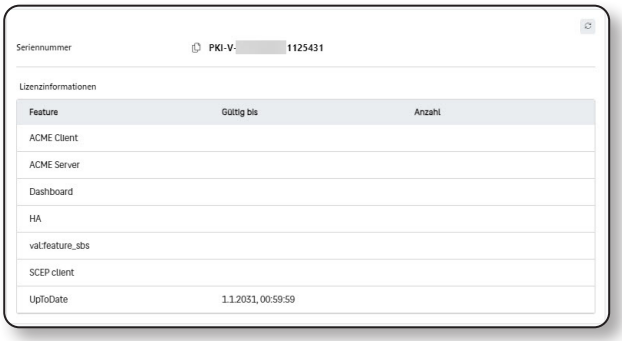


Abb. 9.08: *Lizenzinformationen*

10 Dokumentation

In diesem Bereich werden die Inhalte dieses Handbuchs kapitelweise angezeigt.

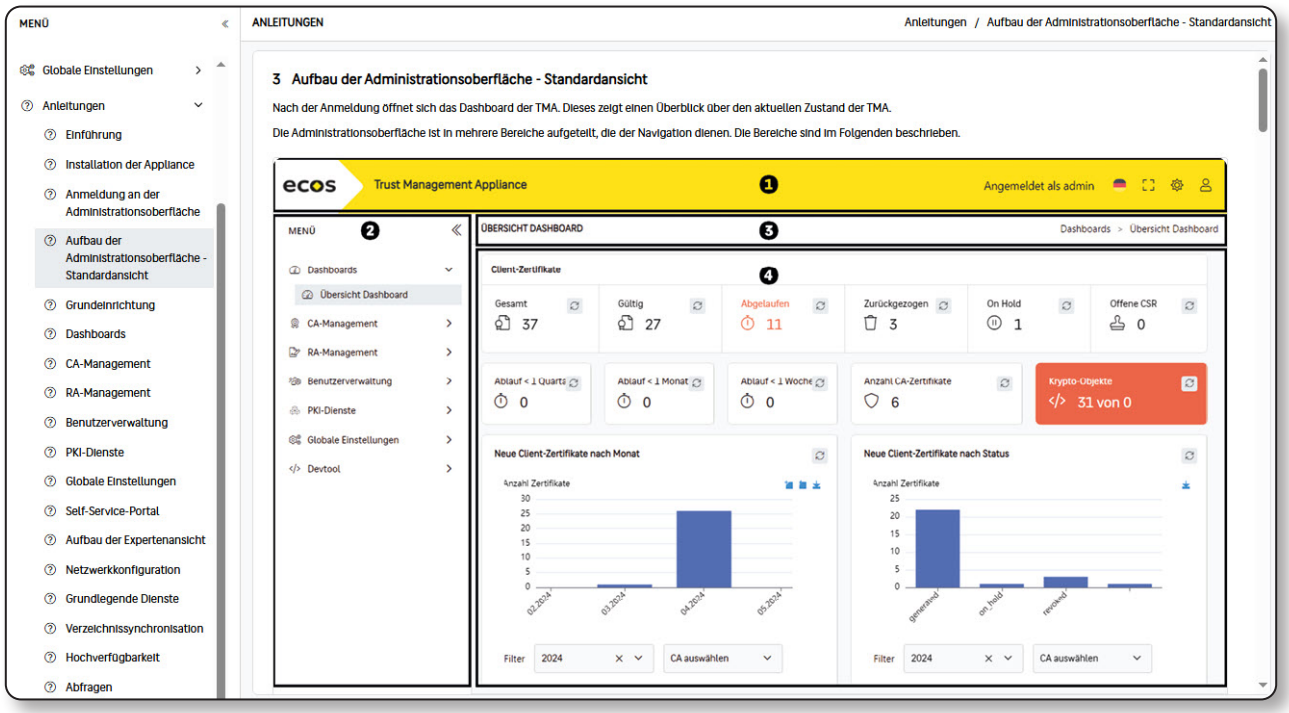


Abb. 10.01: *Dokumentation: Kapitelansicht*

11 Self-Service-Portal

Über das Self-Service-Portal können Mitarbeitende Zertifikate anfordern und die ihnen zugeordneten Zertifikate verwalten.

Zugriff auf das Self-Service-Portal erhalten Benutzer mit dem Privileg **Zugriff auf Self-Service-Portal**. Dies wird über eine Rolle einem Benutzer zugeordnet. Informationen zu den Rollen finden sich unter **15.1 Benutzer und Rollen.**

Das Self-Service-Portal wird über die Adresse der TMA mit dem Zusatz **/self-service/** aufgerufen.

Beispiel: Ist die Administrationsoberfläche über die URL **https://192.168.1.5:543** erreichbar, lautet die Adresse des Self-Service-Portals **https://192.168.1.5:543/self-service/**.

Damit sich die Mitarbeitenden am Self-Service-Portal anmelden können, müssen sie zuvor als Benutzerkonto angelegt werden.

Nach der Anmeldung gelangt der Benutzer in den Bereich **Self Service → Meine Zertifikate**.

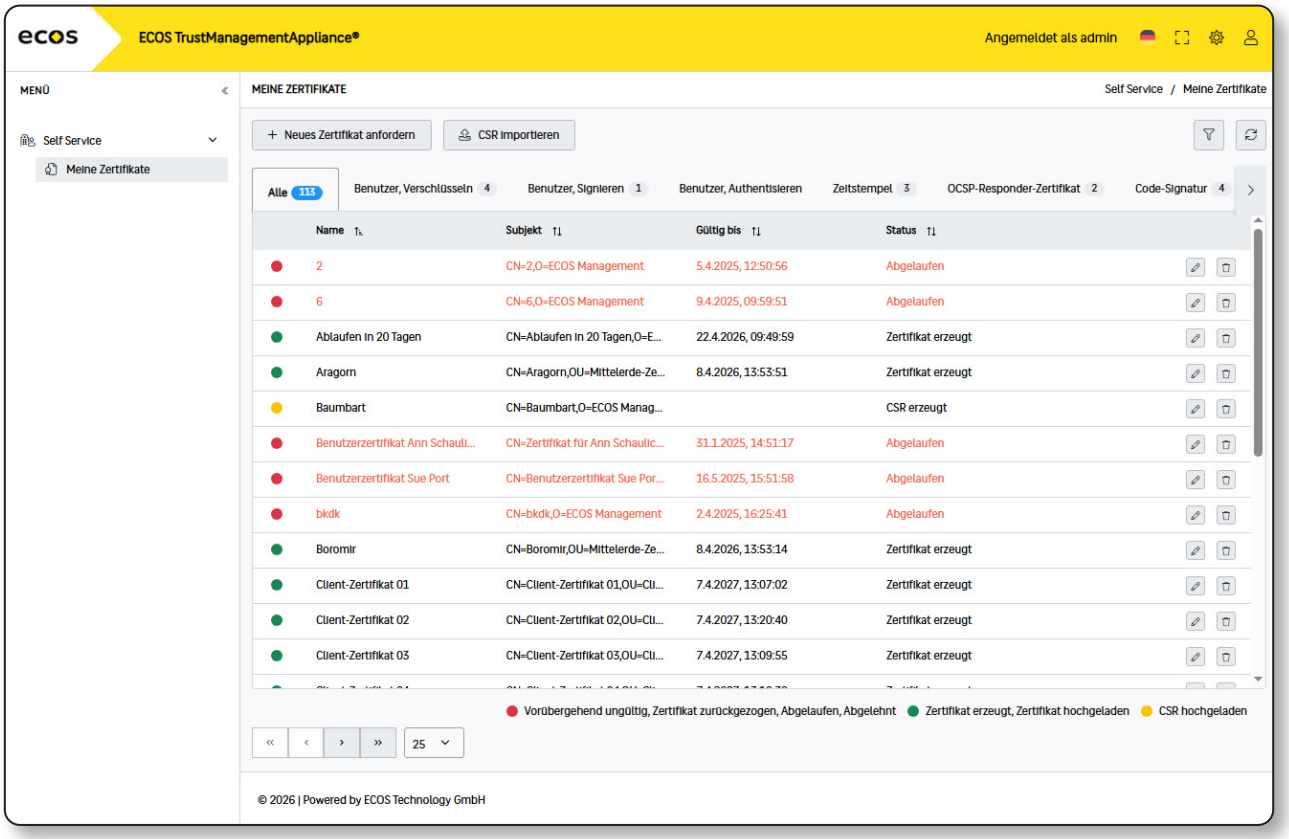


Abb. 11.01: *Übersicht des Self-Service-Portals*

11.1 Aufbau

Im Self-Service-Portal steht der Bereich **Meine Zertifikate** zur Verfügung, der die Zertifikate und CSRs des angemeldeten Benutzers auflistet.

11.1.1 Tabellen

Oberhalb der Tabelle stehen neben den allgemeinen Tabellenfunktionen zusätzliche Buttons zur Verfügung.

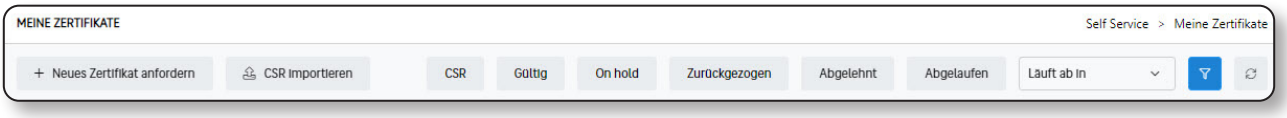


Abb. 11.02: *Schnellfilter oberhalb der Tabelle*

Neues Zertifikat anfordern: Über dieses Symbol wird ein neues Zertifikat angefragt. Es öffnet sich ein Fenster bzw. ein Assistent zur Konfiguration des neuen Objekts.

CSR importieren: Über dieses Symbol wird ein externen CSR importiert.

Schnellfilter ein-/ausblenden: Über dieses Symbol werden Schnellfilter über der Tabelle angezeigt, um z.B. die Zertifikate nach Status zu filtern. Der Filter wird durch ein erneutes Klicken auf den jeweiligen Button gelöscht. Ist die Funktion aktiv, ist das Symbol je nach eingestelltem Farbschema farbig hinterlegt.

11.1.2 Aufbau der Tabellen

Die Tabelle hat verschiedene Tabs, um die Zertifikate nach der Schlüsselverwendung zu sortieren. Sie hat voreingestellte Spalten.

Jede Spalte kann über den Tabellenkopf alphabetisch auf- bzw. absteigend sortiert werden.

In der ersten Spalte wird der visuelle Status des Zertifikats bzw. des CSRs angezeigt.

Grüner Punkt: Das Zertifikat ist ausgestellt und gültig.

Gelber Punkt: Der CSR ist in Bearbeitung und wartet auf Genehmigung durch einen RA-Admin.

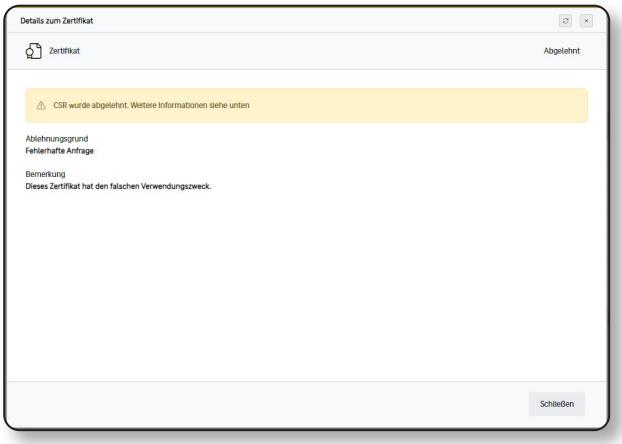


Abb. 11.03: *Zertifikatrequest wurde abgelehnt*

Roter Punkt: Das Zertifikat ist abgelaufen, auf Halten, zurückgezogen oder der CSR wurde abgelehnt. Wurde der CSR abgelehnt, kann über die Lupe weitere Informationen eingeholt werden. Es wird ein Grund für die Ablehnung angezeigt und zusätzliche Informationen, wenn diese vom Registrar zur Verfügung gestellt wurden.

11.2 Neues Zertifikat anfordern

Über den Button **Neues Zertifikat anfordern** erstellen Sie einen neuen CSR. Es öffnet sich ein Assistent zur Konfiguration des Requests.

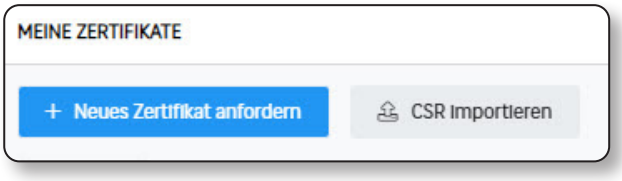


Abb. 11.04: *Neues Zertifikat anfordern*

1

Typ des Zertifikats: Wählen Sie das Einsatzgebiet für das Zertifikat aus der Liste aus. Möchten Sie den Verwendungszweck selbst bestimmen, wählen Sie die Option Auswahl (siehe **24.1 Voreingestellte Schlüsselverwendungszwecke**).

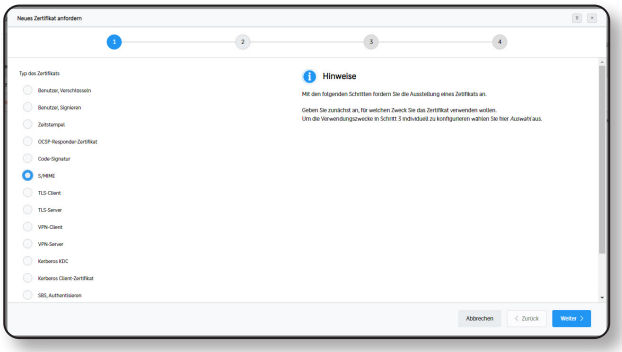


Abb. 11.05: *CSR-Assistent: Typ des Zertifikats*

2

Name: Vergeben Sie einen aussagekräftigen Namen. Standardmäßig wird der Name aus dem Verwendungszweck, das Datum und die Uhrzeit erstellt. Sie können ihn ändern.

Kennwort für privaten Schlüssel: Geben Sie hier das Kennwort für den privaten Schlüssel ein. Aktivieren Sie die Checkbox, dass Sie kein Kennwort für den Schlüssel vergeben möchten, ist das Feld ausgegraut.

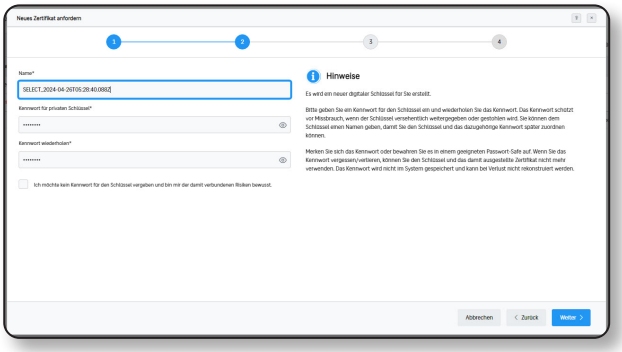


Abb. 11.06: *CSR-Assistent: Name & Kennwort*

Kennwort wiederholen: Wiederholen Sie das Kennwort. Stimmen die Kennwörter nicht überein, wird Ihnen das direkt angezeigt. Aktivieren Sie die Checkbox, dass Sie kein Kennwort für den Schlüssel vergeben möchten, ist das Feld ausgegraut.

3

Subjekt: Geben Sie das Subjekt als Distinguished Name (DN) an. Standardmäßig wird das Subjekt aus dem Namen als Common Name (CN), des Pfads als Organisational Unit (OU) und der Organisation (O) zusammengesetzt. Sie können das Subjekt ändern.

Die nachfolgenden Optionen stehen nur zur Verfügung, wenn bei Schritt 1 als Typ des Zertifikats die Option **Auswahl** gewählt wurde. Andernfalls sind diese Optionen ausgeblendet.

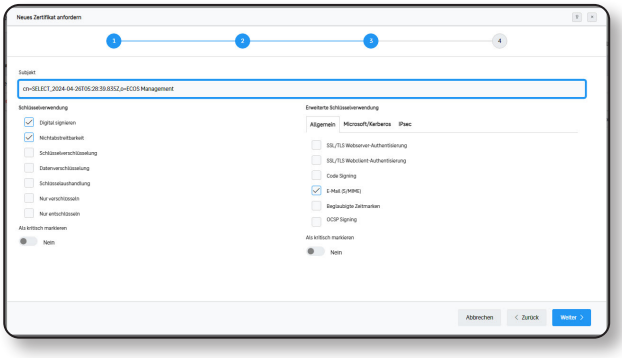


Abb. 11.07: *CSR-Assistent: Subjekt & Verwendungszweck*

Schlüsselverwendung: Haben Sie in Schritt 2 die Option **Auswahl** gewählt, können Sie hier den Schlüsselverwendungszweck bestimmen. Andernfalls werden Ihnen die automatisch ausgewählten Verwendungszwecke angezeigt (siehe **24.2 Schlüsselverwendungen**).

Erweiterte Schlüsselverwendung: Sie können weitere Schlüsselverwendungszwecke bestimmen. Sie sind in Kategorien zusammengefasst (siehe **24.3 Erweiterte Schlüsselverwendungen**).

Als kritisch markieren: Sie können den Verwendungszweck als kritisch markieren. Ist der Verwendungszweck als kritisch markiert, darf das Zertifikat nur für den oder die angegebenen Zwecke verwendet werden. Ist der Verwendungszweck nicht als kritisch markiert, wird er als Hinweisfeld behandelt, das die Verwendung des Zertifikats nicht auf die angegebenen Zwecke beschränkt. Enthält ein Zertifikat sowohl einen als kritisch markierten Schlüsselverwendungszweck als auch einen als kritisch markierten erweiterten Schlüsselverwendungszweck, werden beide unabhängig voneinander verarbeitet. Das Zertifikat darf nur für einen Zweck verwendet werden, der mit beiden Werten übereinstimmt.

4

Sie erhalten eine Übersicht über Ihre Einstellungen für die Zertifikatsanforderung. Möchten Sie Änderungen vornehmen, können Sie zurückblättern oder die Seitenzahl im Fortschrittsbalken zurückgehen.

Erstellen Sie den Request über den Button **CSR ausstellen**.

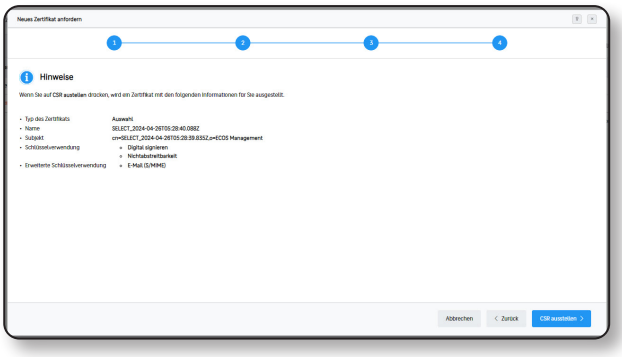


Abb. 11.08: *CSR-Assistent: Übersicht*

5

Der CSR wird erstellt. Anschließend erhalten Sie Informationen, ob die Erstellung erfolgreich war.

Schließen Sie den Assistenten.

Die Zertifikatsanforderung liegt jetzt auf der TMA im Bereich **RA-Management → CSR-Inventar** zur Genehmigung bereit.

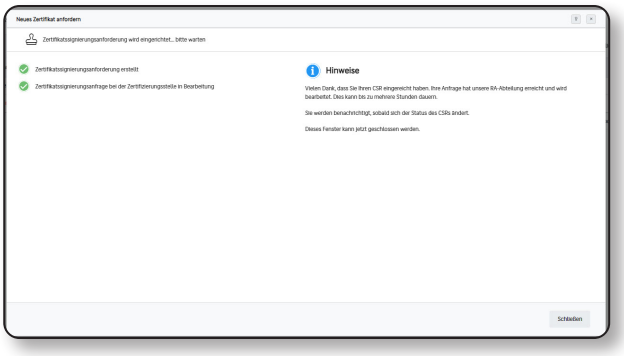


Abb. 11.09: *CSR-Assistent: Antrag wurde gestellt*

11.3 CSR importieren

Über den Button **CSR importieren** können Sie einen externen CSR hochladen. Es öffnet sich ein Fenster.

CSR-Datei auswählen: Über diesen Button öffnet sich ein Auswahldialog. Wählen Sie die Datei des CSRs, den Sie hochladen wollen, und bestätigen Sie mit **Öffnen**. Beide Fenster schließen sich und Sie erhalten die Information, ob der CSR importiert werden konnte.

Alternativ können Sie das base64-kodierte Zertifikat über das Eingabefeld einfügen und **Importieren**.

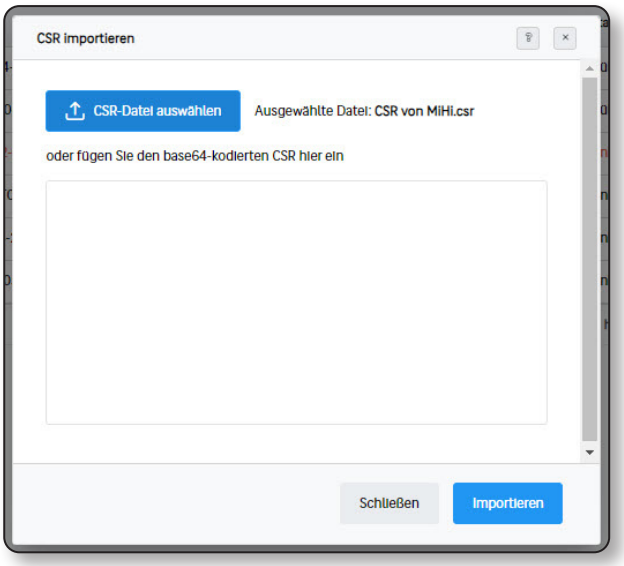


Abb. 11.10: *CSR importieren*



Teil III - Expertenansicht

12 Das ECOS Appliance-Objekt

Das ECOS Appliance-Objekt ist das zentrale Verwaltungsobjekt der TMA. Es dient sowohl zur Konfiguration als auch als Container für dazugehörige Konfigurationsobjekte und ist über die Expertenoberfläche konfigurierbar. Im Auslieferungszustand trägt es den Namen **bb5000**. Während des Basis-Setups wird ein neuer Name vergeben.

Bei einer kompakten Installation übernimmt das ECOS Appliance-Objekt die Rolle des Management-Servers, des Enrollment-Servers und des Software-Update-Servers.

Mit zwei oder mehr ECOS Appliance-Objekten als vollsynchronisierte Slave-Systeme kann ein hochverfügbarer HA-Cluster betrieben werden, entweder als passives Standby-System oder im Multi-Master-Betrieb: **20 Hochverfügbarkeit**.

12.1 Das Konfigurationsobjekt

12.1.1 Reiter Allgemein

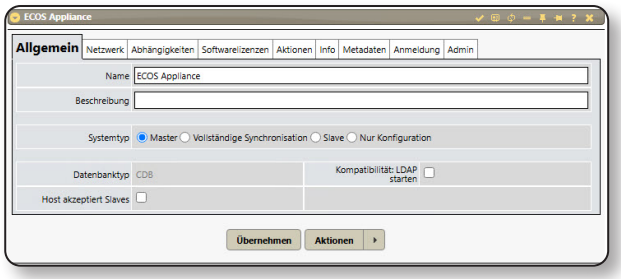


Abb. 12.01: *ECOS Appliance-Objekt - Reiter Allgemein*

Auf diesem Reiter werden neben dem Namen auch der Systemtyp konfiguriert. Ist das ECOS Appliance-Objekt als **Master** konfiguriert, besitzt es die vollständigen Informationen der Konfiguration. Wird als Systemtyp die Option **Vollständige Synchronisation** gewählt, besitzt das ECOS System die gleichen Berechtigungen wie als Master-System. Es dient vor allem als Backup für das Master-System. Im HA-Betrieb wird diese Option für vollsynchronisierte Slave-Appliances ausgewählt. Als **Slave**-System besitzt das ECOS System nur einen Teil der Konfiguration und wird vom Master-System gesteuert, von dem es alle erforderlichen Informationen erhält. Mit der Option **Nur Konfiguration** dient das ECOS Appliance-Objekt zur Konfigurationsvererbung im HA-Cluster.

Wird als Systemtyp **Vollständige Synchronisation** oder **Slave** gewählt, muss die Master-Adresse ausgewählt werden, mit der sich das Slave-System verbinden kann, um die Konfiguration zu erhalten.

Zusätzlich wird ein Lokaler Admin-Benutzer benötigt, der sich auf dem Slave-System mit lokalen Administrationsrechten auf der Administrationsoberfläche anmelden kann. Er kann unabhängig von der Appliance lokal Konfigurationsänderungen vornehmen. Der lokale Admin-Benutzer muss vorher als Benutzer-Objekt angelegt und mit einer Rolle mit den Privilegien **Administrator** oder **Zugriff auf Admin-Oberfläche** ausgestattet sein. Es muss ein Kennwort zur Authentisierung an der Administrationsoberfläche angegeben werden.

⚠ **Hinweis:** Der lokale Admin-Benutzer des Slave-Systems sollte aus Sicherheitsgründen vom Admin-Benutzer des Master-Systems unterscheiden und nur Zugriff auf das Slave-System haben.

12.1.2 Reiter Netzwerk

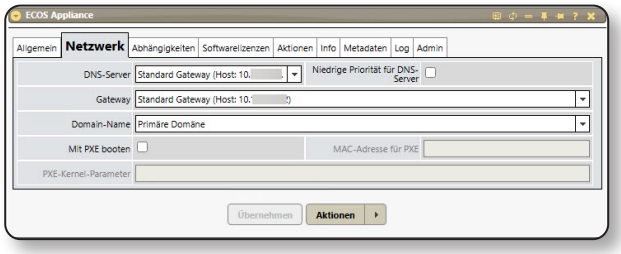


Abb. 12.02: *ECOS Appliance-Objekt - Reiter Netzwerk*

Dieser Reiter dient zur Konfiguration der grundlegenden Netzwerkeinstellungen für die TMA.

Zum einen wird ein DNS-Server benötigt. Dieser muss als Def.: Host-Name-Objekt angelegt sein. Mit einem Rechtsklick auf das Auswahlfeld kann über **Neu: Def.: Host-Name** ein neues Objekt angelegt werden. Es öffnet sich ein Fenster, in dem die IP-Adresse oder Host-Name und der Typ der IP-Adresse konfiguriert werden können. Es können auch Container ausgewählt werden, in denen mehrere Def.: Host-Name-Objekte zusammengefasst sind. Alle im Container enthaltenen Def.: Host-Name-Objekte werden als DNS-Server herangezogen. Für die Hierarchie sollte in den einzelnen Objekten die Priorität konfiguriert werden.

Zum anderen muss ein Gateway angegeben werden. Auch hier handelt es sich um ein Def.: Host-Name-Objekt, das entweder über die Dropdown-Liste gewählt oder über einen Rechtsklick neu angelegt werden kann.

12.1.3 Reiter Abhängigkeiten

Auf dem Reiter **Abhängigkeiten** können Konfigurationen von ECOS Systemen desselben Objekttyps, z.B. ECOS Appliance-Objekte, zwischen diesen Objekten vererbt werden. Dies ist vor allem für die Hochverfügbarkeit notwendig.

12.1.4 Reiter Softwarelizenzen

Der Reiter **Softwarelizenzen** gibt eine Übersicht über die installierten Lizenzen der TMA. Über das Feld Lizenzen können neue Lizenzen, z.B. nach einer Verlängerung, importiert werden. Die Lizenzen können als zip-Datei hochgeladen werden und nach dem erfolgreichen Import ändert sich der Lizenzstatus auf **ok**.

12.1.5 Reiter Aktionen

Der Reiter **Aktionen** steht nur in ausgewählten Objekten zur Verfügung und bietet verschiedene Funktionen für das jeweilige Objekt. Beim ECOS Appliance-Objekt stehen Aktionen zu Netzwerk, Update, Konfiguration, Neustart und Uhrzeit zur Verfügung.

Die einzelnen Funktionen stehen erst zur Verfügung, wenn eine der Aktionen ausgewählt wurde.

12.1.5.1 Netzwerktools

Es werden Tools zur Netzwerkdiagnose angezeigt, die bei Verbindungs- und Kommunikationsproblemen eine schnelle Fehleranalyse unterstützen. Die Aktion wird jeweils über den Button **Start** ausgeführt.

Tool: ping

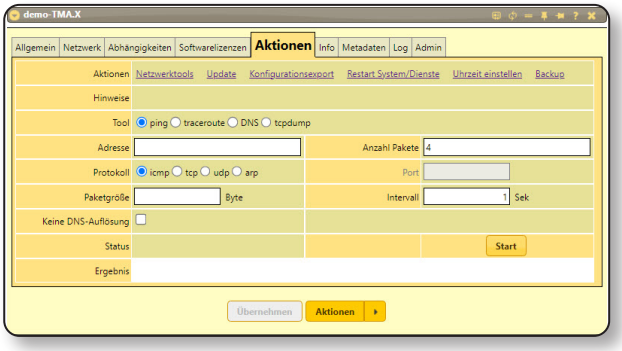


Abb. 12.03: *Reiter "Aktionen" - Netzwerktool ping*

Das Netzwerktool ping testet die Erreichbarkeit eines Netzwerkgeräts.

Adresse: Es wird die (IP-)Adresse des Netzwerkgeräts oder einer Webseite ein, die geprüft werden soll.

Anzahl Pakete: Es wird die Anzahl der Pakete bestimmt, die zum Test gesendet werden sollen. Standardmäßig sind **4** Pakete angegeben.

Protokoll: Das Protokoll für die ping-Abfrage wird ausgewählt. Standardmäßig ist **ICMP** ausgewählt. Für die Protokolle **TCP**, **UDP** und **ARP** wird die Erreichbarkeit mit nping getestet.

Port: Es wird der Port angegeben, wenn ein bestimmter Port geprüft werden soll. Diese Angabe steht nur für die Protokolle **TCP** und **UDP** zur Verfügung.

Paketgröße: Die Größe der Pakete wird in Byte bestimmt. Wird keine Angabe gemacht, werden standardmäßig Pakete mit einer Größe von 64 Byte gesendet.

Intervall: Das Intervall für das Senden der einzelnen Pakete wird in Sekunden angegeben. Standardmäßig ist ein Intervall von **1** Sekunde eingestellt.

Keine DNS-Auflösung: Wird diese Checkbox aktiviert, wird die zu prüfende Adresse nicht per DNS aufgelöst.

Status: Wurde die ping-Abfrage gestartet, wird hier der Status der Abfrage angezeigt.

Ergebnis: Hier wird das Ergebnis der ping-Abfrage angezeigt.

Tool: traceroute

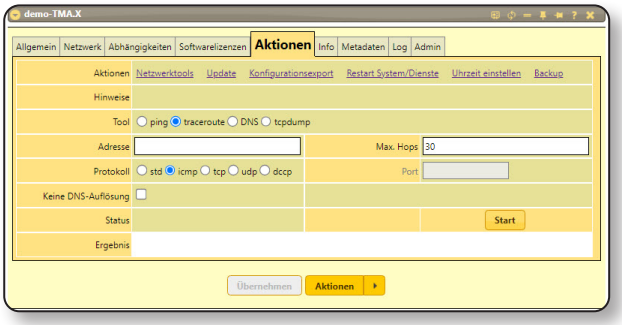


Abb. 12.04: *Reiter "Aktionen" - Netzwerktool traceroute*

Das Netzwerktool traceroute prüft die Route, die ein Paket zum Ziel zurücklegt.

Adresse: Es wird die (IP-)Adresse des Netzwerkgeräts oder einer Webseite eingegeben, die geprüft werden soll.

Max. Hops: Es wird die maximale Anzahl der Hops angegeben, die während der traceroute-Abfrage angezeigt werden sollen. Standardmäßig werden maximal **30** Hops angezeigt.

Protokoll: Das Protokoll für die traceroute-Abfrage wird ausgewählt. Standardmäßig ist **ICMP** ausgewählt.

Port: Es wird der Port angegeben, wenn ein bestimmter Port geprüft werden soll. Diese Angabe steht nur für die Protokolle **TCP** und **UDP** zur Verfügung.

Keine DNS-Auflösung: Wird diese Checkbox aktiviert, wird die zu prüfende Adresse nicht per DNS aufgelöst.

Status: Wurde die traceroute-Abfrage gestartet, wird hier der Status der Abfrage angezeigt.

Ergebnis: Hier wird das Ergebnis der traceroute-Abfrage angezeigt.

Tool: DNS

Das Netzwerktool dns prüft die Umsetzung zwischen Domain-Namen und IP-Adressen.

Adresse: Es wird die (IP-)Adresse des Netzwerkgeräts oder einer Webseite eingegeben, die geprüft werden soll.

DNS-Server: Es wird die (IP-)Adresse des DNS-Servers angegeben, der für die Auflösung zuständig ist.

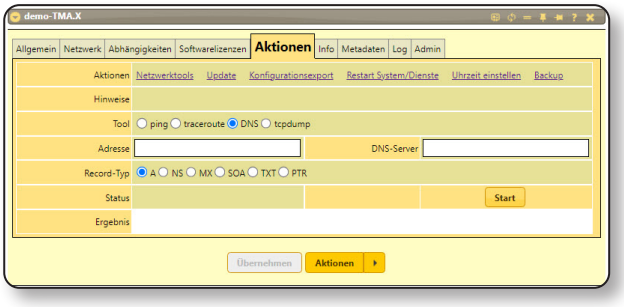


Abb. 12.05: *Reiter "Aktionen" - Netzwerktool dns*

Record-Typ: Es wird der Record-Typ, der geprüft werden soll, ausgewählt. Standardmäßig sind **A Records** ausgewählt.

- A (Address Record): Mit diesem Record-Typ wird einem DNS-Namen eine IPv4-Adresse zugeordnet.
- NS (Name Server Record): Dieser Record-Typ definiert, welcher Nameserver für diese Zone offiziell zuständig ist.
- MX (Mail Exchange Record): Dieser Record-Typ definiert, unter welchem FQDN der Mail-Server zu einer Domain oder Sub-Domain erreichbar ist.
- SOA (Start of Authority): Dieser Record-Typ enthält wichtige Angaben zur Verwaltung der Zone, insbesondere zum Zonentransfer.
- TXT (Text Record): Mit diesem Record-Typ kann ein frei definierbarer Text in einer DNS-Zone abgelegt werden.
- PTR (Pointer Record): Dieser Record-Typ ordnet im DNS einer IP-Adresse einen oder mehrere Hostnamen zu (Rückwerteauflösung).

Status: Wurde die dns-Abfrage gestartet, wird hier der Status der Abfrage angezeigt.

Ergebnis: Hier wird das Ergebnis der dns-Abfrage angezeigt.

Tool: tcpdump

Das Netzwerktool tcpdump analysiert den Netzwerkverkehr, der über eine bestimmte Netzwerkschnittstelle läuft.

Keine DNS-Auflösung: Wird diese Checkbox aktiviert, wird die zu prüfende Adresse nicht per DNS aufgelöst.

Inhalte anzeigen: Wird diese Checkbox aktiviert, werden die mitgeschnittenen Daten nach dem Speichern im PCAP-Format heruntergeladen.

Netzwerk-Interface: Es wird das Netzwerk-Interface für die Netzwerkverkehr-Analyse ausgewählt.

Max. Aufnahmezeit: Es wird die maximale Aufnahmezeit der tcpdump-Anfrage in Sekunden angegeben. Standardmäßig sind **300** Sekunden (entspricht 5 Minuten) eingestellt.

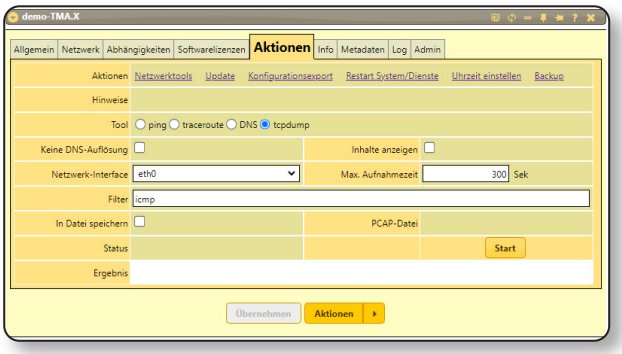


Abb. 12.06: *Reiter "Aktionen" - Netzwerktool tcpdump*

Filter: Es können Kriterien angegeben werden, um den Netzwerkverkehr zu filtern. Standardmäßig ist **ICMP** als Filter gesetzt Es können z.B. auch Portnummern eingeben. Mit **and** oder **or** können auch Verknüpfungen erstellt werden.

In Datei speichern: Wird diese Checkbox aktiviert, wird das Ergebnis der tcpdump-Anfrage in einer Datei gespeichert.

PCAP-Datei: Hier können die mitgeschnittenen Daten der tcpdump-Anfrage heruntergeladen werden. Dies ist nur möglich, wenn die Checkbox In Datei speichern aktiviert ist.

Status: Wurde die tcpdump-Abfrage gestartet, wird hier der Status der Abfrage angezeigt.

Ergebnis: Hier wird das Ergebnis der tcpdump-Abfrage angezeigt.

12.1.5.2 Update

Mit der Aktion **Update** wird das System aktualisiert. Dazu muss das Objekt Dienst: Software-Update unterhalb des ECOS Appliance-Objekts angelegt und konfiguriert sein. Das Update wird über den Button **Start** angestoßen.

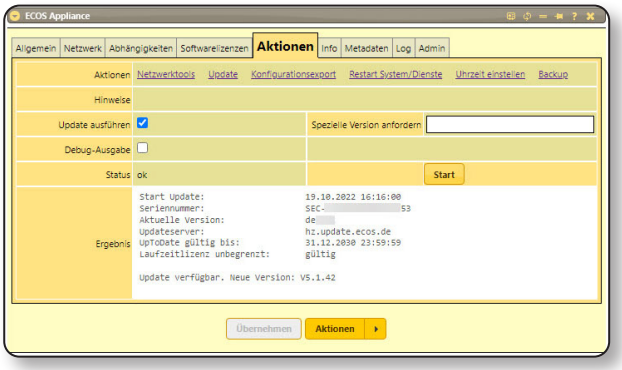


Abb. 12.07: *Reiter "Aktionen" - Manuelles Update*

Update ausführen: Wird diese Checkbox aktiviert, wird die neuste Version heruntergeladen und installiert.

Spezielle Version anfordern: Hier wird die Versionsnummer im Format **Vn.nn.n** angegeben, wenn nicht die neuste Version installiert werden soll.

Debug-Ausgabe: Wird diese Checkbox aktiviert, wird die Debug-Ausgabe während des Software-Updates angezeigt.

Status: Wurde das Update gestartet, wird hier der Status angezeigt.

Ergebnis: Hier wird das Ergebnis des Updates als neuen Versionsstand angezeigt.

12.1.5.3 Konfigurationsexport

Mit der Aktion **Konfigurationsexport** kann die Konfiguration der TMA auf ein anderes System übertragen werden. Vor der Übertragung muss die Master-Slave-Verbindung korrekt konfiguriert worden sein. Die Übertragung wird über den Button **Start** gestartet.

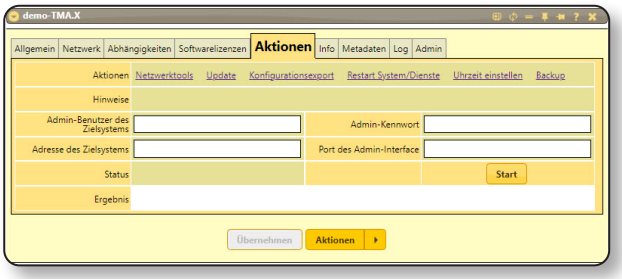


Abb. 12.08: *Reiter Aktionen - Konfigurationsexport*

Admin-Benutzer des Zielsystems: Hier wird der Benutzernamen eines Kontos mit Admin-Zugriff auf das Zielsystem eingegeben.

Admin-Kennwort: Hier wird das Kennwort des Kontos mit Admin-Zugriff auf das Zielsystem eingegeben.

Adresse des Zielsystems: Hier wird die (IP-)Adresse des Zielsystems eingegeben.

Port des Admin-Interface: Hier wird der Port des Zielsystems eingegeben. Der Standard-Port für eine ECOS Appliance ist 543.

Status: Wurde der Export gestartet, wird hier der Status angezeigt.

Ergebnis: Hier wird das Ergebnis der Übertragung angezeigt.

12.1.5.4 Restart System/Dienste

Mit der Aktion **Restart System/Dienste** können einzelne Dienste oder das ECOS System selbst über den Button **Start** neu gestartet werden.

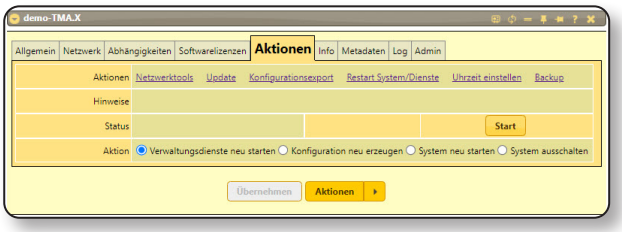


Abb. 12.09: *Reiter "Aktionen" - Restart System/Dienste*

Status: Wurde die Aktion gestartet, wird hier der Status angezeigt.

Aktion: Folgende Aktionen stehen zur Auswahl:

Verwaltungsdienste neu starten: Es werden nur die Verwaltungsdienste neu gestartet. Der laufende Betrieb des Systems wird nicht unterbrochen.

Konfiguration neu erzeugen: Es wird geprüft, ob die vom System erzeugte Konfiguration den aktuellen Einstellungen entspricht. Bei Abweichungen wird die Konfiguration des Systems aktualisiert. Einstellungen werden nicht geändert.

System neu starten: Das System wird neu gestartet. Dies dauert einige Minuten. Anschließend muss sich der Benutzer neu anmelden.

System ausschalten: Das System wird heruntergefahren.

12.1.5.5 Uhrzeit einstellen

Mit der Aktion **Uhrzeit einstellen** wird das Datum und die Uhrzeit des Systems konfiguriert. Die aktuelle Zeit des Systems wird über den Button **Start** in die leeren Felder zu Datum und Zeit eingetragen. Diese können geändert und mit einem erneuten Klick auf **Start** aktualisiert werden.

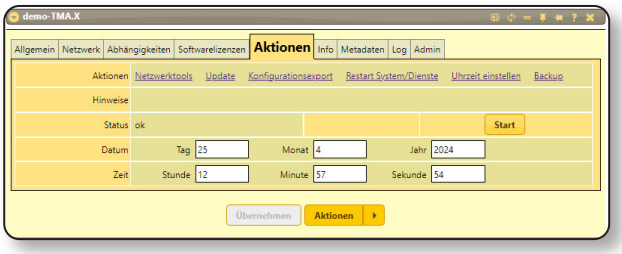


Abb. 12.10: *Reiter "Aktionen" - Uhrzeit*

12.1.5.6 Backup

Mit der Aktion **Backup** kann ein manuelles Backup der Konfiguration des Systems erstellt werden. Standardmäßig führt das System täglich ein automatisches Backup durch und speichert die Backup-Datei auf der lokalen Festplatte. Die Aktion wird über den Button **Start** ausgeführt.

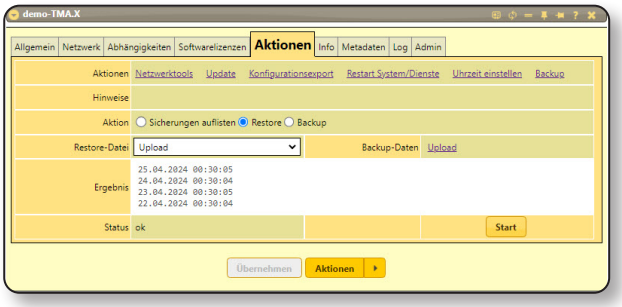


Abb. 12.11: *Reiter "Aktionen" - Backup*

Backups werden verschlüsselt und integritätsgesichert abgelegt. Die zur Sicherung verwendeten Schlüssel werden durch die TMA automatisch erzeugt und auf der Appliance gespeichert. Der Zugriff auf diese Schlüssel ist ausschließlich Benutzern mit administrativen Rechten möglich.

Aktion: Folgende Aktionen stehen zur Auswahl:

Sicherungen auflisten: Es wird eine Liste aller auf der lokalen Platte gespeicherten Backup-Dateien angezeigt.

Restore: Es wird ein Backup wiederhergestellt.

Restore-Datei: Hier wird die Datei zum Restore aus der Dropdown-Liste ausgewählt. Die lokalen Backups werden nur angezeigt, sofern sie zuvor aufgelistet wurden. Zusätzlich wird die Möglichkeit zum Upload einer externen Datei angezeigt.

Backup-Daten: Hier wird die externe Backup-Datei zum Upload ausgewählt.

Nach Abschluss des Restore-Vorgangs werden die Verwaltungsdienste neu gestartet, um die zurückgespielte Konfiguration zu aktivieren. Die Administrationsoberfläche ist während dieser Zeit nicht erreichbar. Beachten Sie, dass durch das Zurückspielen der Konfiguration ggf. auch eine geänderte Netzwerkkonfiguration aktiviert wird.

Backup: Es wird ein neues Backup erstellt. Die Datei wird im Anschluss unter Backup-Daten zum Download angeboten. Das Backup wird immer auf der lokalen Festplatte gespeichert. Steht nicht genug Speicherplatz zur Verfügung werden die ältesten Backup-Dateien gelöscht.

Status: Wurde die Aktion gestartet, wird hier der Status angezeigt.

Weitere Informationen und Konfigurationsmöglichkeiten sind unter **14.2 Dienst: Backup** verfügbar.

12.1.6 Reiter Info

Der Reiter Info steht nur in ausgewählten Objekten zur Verfügung und bietet Informationen über das System auf der die TMA läuft.

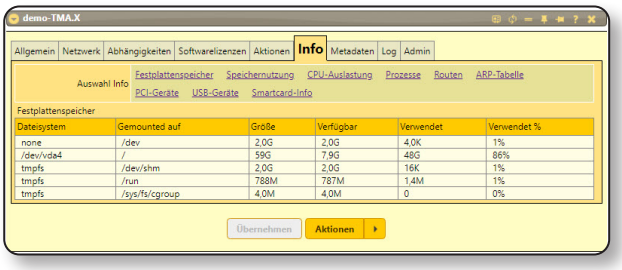


Abb. 12.12: *Reiter "Info"*

Festplattenspeicher: Es werden Informationen zur Festplatte und ihrer Partitionen angezeigt. Darunter fallen u.a. die Gesamtgröße sowie der belegte und freie Speicherplatz.

Speichernutzung: Es werden Informationen zum Arbeitsspeicher und die Speicherauslastung des Systems angezeigt.

CPU-Auslastung: Es werden Informationen zur Auslastung des Prozessors angezeigt.

Prozesse: Es werden alle laufenden Prozesse des Systems aufgelistet.

Routen: Es werden alle aktiven Routen aufgelistet.

ARP-Tabelle: Es werden die dem System bekannten IP-Adresse mit den dazugehörigen MAC-Adressen aufgelistet.

PCI-Geräte: Es werden alle angeschlossenen PCI-Geräte des Rechners angezeigt.

USB-Geräte: Es werden alle an das System angeschlossenen USB-Geräte angezeigt.

Smartcard-Info: Es werden Informationen zu einer vorhandenen Smartcard angezeigt, z.B. die darauf gespeicherten Zertifikate.

12.2 Das ECOS Appliance-Objekt als Container

Das ECOS Appliance-Objekt dient nicht nur als Konfigurationsobjekt, sondern auch als Container für verschiedene Dienste und Netzwerkobjekte.

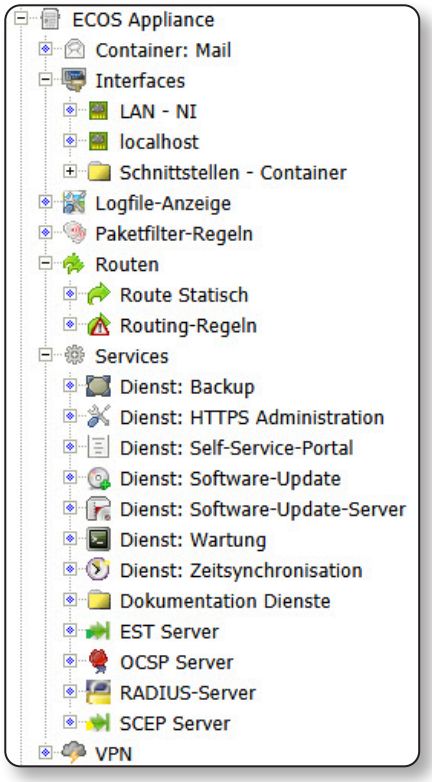


Abb. 12.13: *ECOS Appliance als Container*

12.2.1 Dienst-Objekte

Dienst-Objekte stellen verschiedene Dienste zur Verfügung. Dadurch dient die TMA als Server für diesen Dienst. Für jeden Dienst wird eine Server-Adresse und ein Port gebraucht.

Einige Dienste sind für einen reibungslosen Einsatz der TMA notwendig . Welche Dienste angelegt werden können, hängt von den genutzten Lizenzen ab.

Dienste können über das Kontextmenü im Navigationsbaum **Neu → Dienste** angelegt werden. Es öffnet sich ein Konfigurationsobjekt. Nach dem Speichern werden sie unterhalb des Container: Dienste angezeigt.

12.2.2 Netzwerk-Objekte

Das ECOS Appliance-Objekt dient außerdem als Container für verschiedene Netzwerk-Objekte. Dazu zählen Netzwerk-Interface-Objekte und Objekte fürs Routing des Netzwerkverkehrs.

12.2.2.1 Netzwerk-Interface

Im Auslieferungszustand befindet sich unterhalb der ECOS Appliance im Container: Interfaces ein Netzwerk-Interface mit den Namen **LAN**. Dort müssen die IPv4-Adresse und die Netzmaske für IPv4 angegeben werden, wenn sie nicht per DHCP bezogen werden, sondern sich um eine **Feste IP** handelt. Unterstützt das Zielsystem IPv6-Adressen, können sie alternativ konfiguriert werden. Andernfalls werden die Felder für IPv6 nicht angezeigt. Weitere Informationen finden sich unter **13 Netzwerkkonfiguration.**

12.2.2.2 Routing

Im Container: Routen unterhalb des ECOS Appliance-Objekts können die Objekte Route (statisch) und Routing-Regel angelegt werden.

Die Route (statisch) definiert feste Wege für Datenpakete. Sie benötigen ein Ziel-Host/Netzwerk und das nächste zur Verfügung stehende Gateway, über das das Ziel erreichbar ist. Eine statische Route sollte eingerichtet werden, wenn Server oder Netzwerke nur über ein bestimmtes Gateway erreichbar sind. Die Route wird als Eintrag zu einer Routing-Tabelle hinzugefügt.

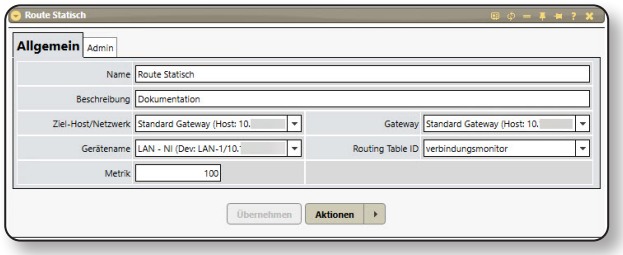


Abb. 12.14: *Route (statisch)*

Mit einer Routing-Regel können erweitere Regeln für Policy-Routing definiert werden. Sie bestimmen, wie mit eingehenden IP-Datenpaketen umgegangen wird. Eine Routing-Regel benötigt einen Selektor, auf den die IP-Datenpakete geprüft werden. Zusätzlich wird im Feld Interface / Adresse / Wert angegeben, was der Selektor prüfen soll. Unter Routing Table-ID wird die Routing-Tabelle gewählt, zu der die selektierten Pakete bei einer Übereinstimmung des Selektors hinzugefügt werden sollen.

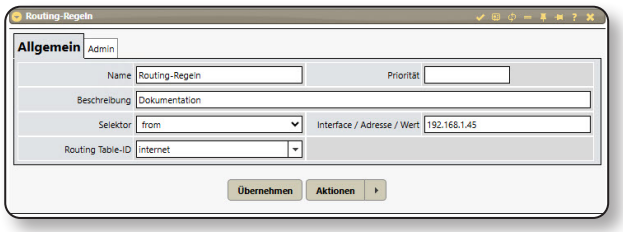


Abb. 12.15: *Routing-Regel*

13 Netzwerkkonfiguration

Für viele Dienste, die von der TMA übernommen werden sollen bzw. auf die die TMA zugreifen soll, werden Netzwerkschnittstellen, Server und Ports benötigt. Diese können im Expertenmodus angelegt werden.

13.1 Netzwerk-Interfaces definieren

Im Auslieferungszustand ist bereits ein Netzwerk-Interface-Objekt mit dem Namen **LAN** unter dem ECOS Appliance-Objekt im Container: Interfaces angelegt.

Sie können den Namen ändern. Das empfiehlt sich, wenn mehrere Netzwerk-Interfaces benötigt werden.

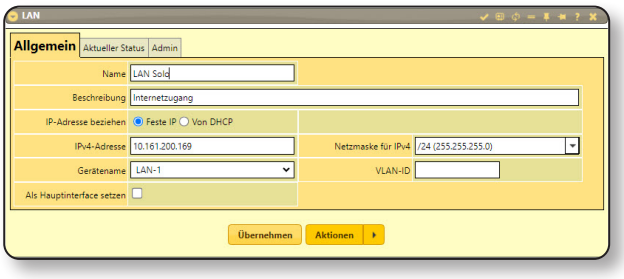


Abb. 13.01: *Netzwerk-Interface konfigurieren*

Geben Sie die IPv4-Adresse oder IPv6-Adresse an, die Sie bei der Installation der TMA festgelegt haben. Wählen Sie ebenso die Subnetzmaske für das Netzwerk-Interface aus.

13.2 Host-Namen definieren

Für viele Dienste und Objekte werden sogenannte Def.: Host-Name-Objekte benötigt. Es dient der zentralen Definition von Host-Namen und IP-Adressen. Dadurch erleichtert es die Administration, da die IP-Adresse nur an einer Stelle konfiguriert und gepflegt werden muss. Änderungen am Host-Objekt wirken sich überall aus, wo es referenziert wird.

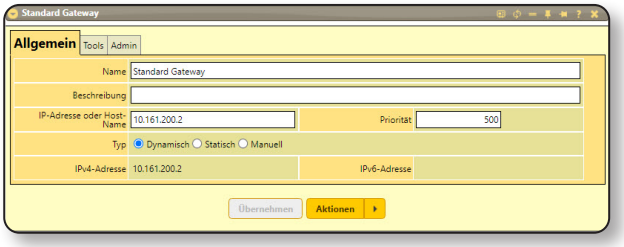


Abb. 13.02: *Host-Name konfigurieren*

Die Host-Objekte werden im Container: Hosts angelegt und verwaltet. Legen Sie ein Host-Objekt für das Standard-Gateway an.

Öffnen Sie das Kontextmenü des Container: Hosts mit einem Rechtsklick und wählen Sie **Neu → Netzwerk → Def.: Host-Name**. Es öffnet sich ein neues Konfigurationsobjekt.

Name: Vergeben Sie einen aussagekräftigen Namen.

IP-Adresse oder Host-Name: Geben Sie die IP-Adresse oder den Host-Namen des Standard-Gateways in Ihrem Netzwerk an. Stellen Sie bei der Angabe von Host-Namen sicher, dass die TMA diesen Host-Namen auch in eine IP-Adresse auflösen kann.

Priorität: Geben Sie eine Priorität in Zahlenform an. Sie bestimmt die Reihenfolge der Auflistung der Adressen. Je niedriger der Zahlenwert, desto höher ist die Priorität.

Typ: Bestimmen Sie, wie die IP-Adresse aus einem eingetragenen Host-Namen ermittelt wird.

Dynamisch: Die IP-Adresse des angegebenen Host-Namens wird per DNS ermittelt. Ein Hintergrunddienst aktualisiert kontinuierlich die ermittelte Adresse entsprechend der zugehörigen Time-to-Live (TTL) aus dem DNS. Kurz vor Ablauf der TTL wird die IP-Adresse erneut ermittelt.

Statisch: Die IP-Adressen des angegebenen Host-Namen wird per DNS ermittelt. Der DNS-Name wird nur bei der Eingabe in eine IP-Adresse aufgelöst. Er wird nicht nachgezogen, wenn sich der Name im DNS ändert. Ändert sich die IP-Adresse zu einem angegeben DNS-Namen, ist ein erneutes Übernehmen notwendig.

Manuell: Die IP-Adresse des angegebenen Host-Namens wird nicht per DNS ermittelt. Geben Sie die IP-Adresse manuell im Feld IPv4-Adresse oder IPv6-Adresse an. Im ECOS System wird ein Host-Eintrag (/etc/hosts) erzeugt, der den Namen fest mit der IP verknüpft. Dieser Typ eignet sich für Umgebungen, in denen kein DNS zur Verfügung steht oder in denen DNS nicht zur Namensauflösung verwendet werden soll.

Speichern Sie die Einstellungen mit **Übernehmen**.

13.3 Ports definieren

Ähnlich den Host-Namen werden Ports und Portbereiche zentral über die Objekte Def.: Service-Port und Def.: Service-Port-Bereich definiert und verwaltet. Dadurch erleichtert es die Administration, da die Ports nur an einer Stelle konfiguriert und gepflegt werden müssen. Änderungen am Port-Objekt wirken sich überall aus, wo es referenziert wird.

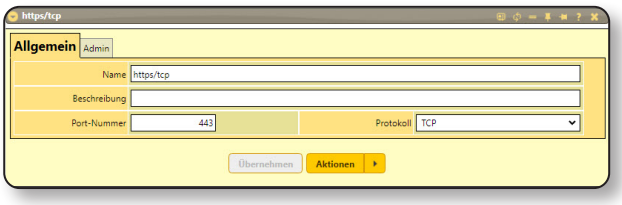


Abb. 13.03: *Port konfigurieren*

Die Port-Objekte werden im Container: Ports angelegt und verwaltet.

Öffnen Sie das Kontextmenü des Container: Ports mit einem Rechtsklick und wählen Sie **Neu → Netzwerk → Def.: Service-Port**. Es öffnet sich ein neues Konfigurationsobjekt.

Name: Vergeben Sie einen aussagekräftigen Namen.

Port-Nummer: Geben Sie die Port-Nummer des Server-Dienstes an. Beachten Sie, dass einige Server-Dienste international festgelegte Standard-Ports haben.

Protokoll: Wählen Sie das Protokoll aus, auf das sich der Port bezieht.

TCP: Das Transmission Control Protocol (TCP) ist ein verbindungsorientiertes Netzwerkprotokoll und definiert, wie Daten zwischen Netzwerkkomponenten ausgetauscht werden sollen.

UDP: Das User Datagram Protocol (UDP) ist ein verbindungsloses Netzwerkprotokoll, dessen Aufgabe der Transport von Daten und das Multiplexen von Verbindungen ist.

Speichern Sie die Einstellungen mit **Übernehmen**.

Für ein Def.: Service-Port-Bereich-Objekt geben Sie die Erste und Letzte Port-Nummer im Konfigurationsobjekt an.

13.4 Netzwerke definieren

Netzwerke werden ebenfalls zentral über ein Def.: Netzwerk-Objekt konfiguriert und verwaltet. Dadurch erleichtert es die Administration, da die Netzwerke nur an einer Stelle konfiguriert und gepflegt werden müssen. Änderungen am Netzwerk-Objekt wirken sich überall aus, wo es referenziert wird.

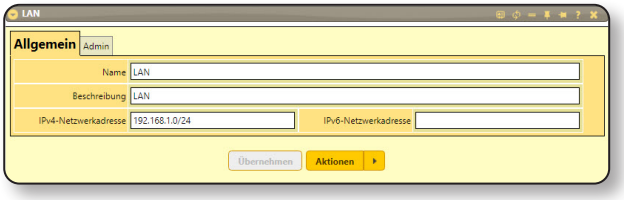


Abb. 13.04: *Netzwerke konfigurieren*

Die Netzwerk-Objekte werden im Container: Netzwerke angelegt und verwaltet.

Öffnen Sie das Kontextmenü des Container: Netzwerke mit einem Rechtsklick und wählen Sie **Neu → Netzwerk → Def.: Netzwerk**. Es öffnet sich ein neues Konfigurationsobjekt.

Name: Vergeben Sie einen aussagekräftigen Namen.

IPv4-Netzwerkadresse: Geben Sie die IPv4-Adresse mit der Subnetzmaske in der Suffix-Schreibweise an: **nnn.nnn.nnn.nnn/mm**

IPv6-Netzwerkadresse: Geben Sie die IPv6-Adresse mit der Subnetzmaske in der Suffix-Schreibweise an: **nnnn:nnnn:...:nnnn/mm**

Speichern Sie die Einstellungen mit **Übernehmen**.

14 Grundlegende Dienste

Für die korrekte Funktionsweise der Trust Management Appliance werden einige grundlegende Dienste benötigt. Diese werden in der Expertenansicht konfiguriert.

14.1 Dienst: HTTPS-Administration

Der Dienst: HTTPS-Administration regelt den HTTPS-Zugriff auf die Administrationsoberfläche per Webbrowser. Der Dienst ist zwingend notwendig, um auf die Administrationsoberfläche zugreifen zu können.

Der Dienst befindet sich unterhalb der **ECOS Appliance → Container: Dienste** im Navigationsbaum.

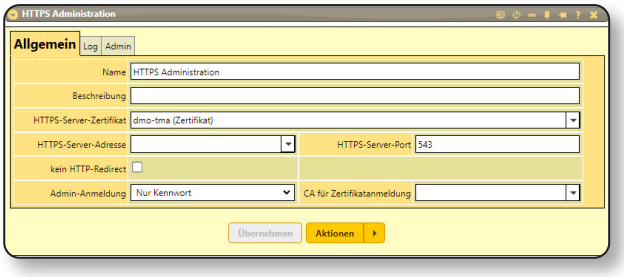


Abb. 14.01: *HTTPS-Administration einrichten*

Name: Vergeben Sie einen aussagekräftigen Namen.

HTTPS-Server-Zertifikat: Hier wird das Server-Zertifikat ausgewählt, über das sich das System beim Aufruf der Administrationsoberfläche gegenüber dem Browser authentifiziert. Während der Installation der Appliance wird automatisch ein Standard-Zertifikat mit dem Namen **Initiales Zertifikat** erzeugt und verwendet. Für den Zugriff auf die Administrationsoberfläche muss der Browser diesem Zertifikat permanent oder für die aktuelle Sitzung vertrauen.

Ersetzen Sie das automatisch erstellte Zertifikat durch ein eigenes Zertifikat, indem Sie mit Rechtsklick auf das Auswahlfeld ein Zertifikat anlegen. Sie können ein externes Zertifikat hochladen oder manuell eins erstellen. Wenn Sie ein manuelles Zertifikat erstellen, achten Sie darauf, dass Sie unter Alternative Namen einen Subject Alternative Name (SAN) für Host, Fully Qualified Domain Namen (FQDN) und/oder IP-Adresse angeben und als Verwendungszweck die Option **TLS-Server** auswählen.

Das System, aus dem die Administrationsoberfläche aufgerufen wird, muss der ausstellenden CA vertrauen. Dies kann einerseits durch den Import des CA-Zertifikats in den Zertifikatspeicher des Client-Systems oder andererseits durch die Nutzung einer öffentlichen CA, dem der Client von Haus aus vertraut, gewährleistet werden. Vertraut der Browser der ausstellenden CA und somit dem Zertifikat, wird in der Adresszeile ein Schloss angezeigt. Bei Chromium-basierten Browsern ist dies Voraussetzung, damit der Browser den Webcontent cachen kann. Dies beschleunigt den Seitenaufbau.

HTTPS-Server-Adresse: Wählen Sie hier die IP-Adresse oder den Host-Namen aus, unter dem die Administrationsoberfläche erreichbar ist. Standardmäßig ist keine Adresse ausgewählt. Bleibt die Server-Adresse leer und die Appliance besitzt mehrere Adressen, lauscht der Dienst auf allen IP-Adresse des Systems und die TMA kann über jede dieser Adressen erreicht werden.

HTTPS-Server-Port: Wählen Sie hier den Port aus, unter dem der Dienst erreichbar ist. Wird kein Port angegeben, wird der Standard-Port 443 genutzt. Die TMA ist standardmäßig unter dem Port 543 erreichbar, um ggf. Konflikte mit Diensten zu vermeiden, die den Port 443 nutzen.

Kein HTTP-Redirect: Aktivieren Sie diese Checkbox, wenn die Standardumleitung von Port 80 auf den konfigurierten HTTPS-Server-Port deaktiviert werden soll. Der HTTP-Redirect kann unterbunden werden, falls es nicht erwünscht ist oder falls Port 80 für einen anderen Dienst genutzt werden soll. Sollen jedoch die CA-Zertifikate (AIA) und CRLs (CRL Distribution Point) über Port 80 zur Verfügung gestellt werden, so darf diese Checkbox nicht aktiviert sein.

Admin-Anmeldung: Wählen Sie hier die Art der Authentisierung für alle Benutzer aus, die eine Rolle mit einem Privileg zum Zugriff auf die Administrationsoberfläche besitzen. Einstellungen, die in diesem Dienst vorgenommen werden, wirken sich auf alle Benutzer aus. Sollen für jeden Benutzer individuelle Authentisierungsmethoden definiert werden, erfolgt das über die Authentisierungsmethoden im jeweiligen Benutzer-Objekt. Standardmäßig ist die Option **Nur Kennwort** gewählt.

Nur Kennwort: Die Anmeldung erfolgt mit dem im Benutzer-Objekt hinterlegten Kennwort. Das Kennwort kann entweder gegen das im Benutzer-Objekt bestimmte Kennwort oder gegen einen RADIUS-Server geprüft werden. Es können sich nur Benutzer anmelden, die eine Rolle mit den Privilegien Administrator oder Zugriff auf Admin-Oberfläche zugewiesen haben.

Kennwort & Zertifikat: Die Anmeldung erfolgt mit dem im Benutzerobjekt hinterlegten Kennwort und einem Anmeldezertifikat. Das Zertifikat muss von der CA, die im Feld CA für Zertifikatanmeldung angegeben ist, signiert sein. In diesem CA-Zertifikat muss eine gültige CRL hinterlegt sein.

Eine CRL wird als gültig eingestuft, wenn sie eine valide Signatur der ausstellenden CA aufweist und der Zeitpunkt der Validierung zwischen dem Ausstellungsdatum und dem nächsten geplanten Update liegt (siehe **16.2 Zertifikatsperrliste (CRL)**).

Der Login wird abgelehnt, wenn:
1. Die CRL nicht gültig ist.
2. Das Zertifikat in der CRL als zurückgezogen gelistet ist

Zusätzlich muss das Anmeldezertifikat im Browser, im Zertifikatspeicher des Client-Systems oder auf einer Smartcard installiert sein. Weist der Browser bei der Anmeldung kein passendes Zertifikat vor, schlägt die Anmeldung fehl. Das Kennwort kann entweder gegen das im Benutzer-Objekt bestimmte Kennwort oder gegen einen RADIUS-Server geprüft werden. Es können sich nur Benutzer anmelden, die eine Rolle mit den Privilegien Administrator oder Zugriff auf Admin-Oberfläche zugewiesen haben.

Kennwort & Zertifikat mit CN: Die Anmeldung erfolgt mit dem im Benutzer-Objekt hinterlegten Kennwort und einem Anmeldezertifikat. Der CN des Anmeldezertifikats muss dabei dem Benutzernamen, der im Benutzer-Objekt im Feld Login angegeben ist, entsprechen.

Ansonsten verhält sich diese Einstellung identisch zu Kennwort & Zertifikat.

Nur Zertifikat: Die Anmeldung erfolgt ausschließlich mit einem Anmeldezertifikat. Der CN des Anmeldezertifikats muss dabei dem Benutzernamen, der im Benutzer-Objekt im Feld Login angegeben ist, entsprechen.

Ansonsten verhält sich diese Einstellung identisch zu Kennwort & Zertifikat.

CA für Zertifikatanmeldung: Wählen Sie die CA, die die Anmeldezertifikate signiert hat. Es kann z.B. mithilfe des CA-Zertifikat-Objekt eine unternehmensinterne CA konfiguriert werden, die im jeweiligen Browser oder Zertifikatspeicher des Client-Systems manuell installiert wird.

⚠ **Hinweis:** Für eine BSI-konforme Konfiguration der TMA müssen sich Admin-Benutzer und Benutzer mit Zugriff auf die Admin-Oberfläche mit ihrer Smartcard an der Administrationsoberfläche anmelden.
Wählen Sie dazu die Option Kennwort & Zertifikat mit CN oder Nur Zertifikat für die Admin-Anmeldung aus.

14.2 Dienst: Backup

Dieser Dienst dient der Sicherung der Konfigurationsdatenbank. Die erzeugten Backups werden auf dem lokalen Datenspeicher der Appliance abgelegt und stehen für die externe Archivierung oder eine Systemwiederherstellung zur Verfügung.

Für den Einsatz in VS-NfD-Umgebungen müssen Backups verschlüsselt werden. Zur Verschlüsselung wird ein symmetrischer Schlüssel verwendet. Dieser Schlüssel muss auf der TMA erzeugt und verwaltet werden.

⚠ **Hinweis:** Bei Neuinstallationen einer TMA wird automatisch ein **Backup-Key** vom Typ Symmetrischer Schlüssel und einer Schlüssellänge von **256 Bit** erzeugt. Er wird automatisch im Dienst: Backup im Feld Schlüssel ausgewählt. Der Schlüssel muss unabhängig vom Backup gesichert und aufbewahrt werden, um das Backup wieder einspielen zu können.
Bei bestehenden Systemen wird nach einem Update auf V8.3.0 der Backup-Key automatisch erzeugt, aber nicht im Dienst: Backup eingetragen. Dies muss manuell erfolgen.

14.2.1 Erzeugen und Sichern des Backup-Schlüssels

Zum Erzeugen des Backup-Schlüssels wird im Container: Zertifikate ein Objekt vom Typ Symmetrischer Schlüssel angelegt.

Schlüsselerzeugung: Wählen Sie die Option **Automatisch erzeugen**.

Schlüssellänge: Hier wird die Schlüssellänge in Bits angegeben. Im VS-NfD-Betrieb muss die Schlüssellänge mindestens 256 Bit betragen.

Nach **Übernehmen** der Einstellungen wird der symmetrische Schlüssel erzeugt.

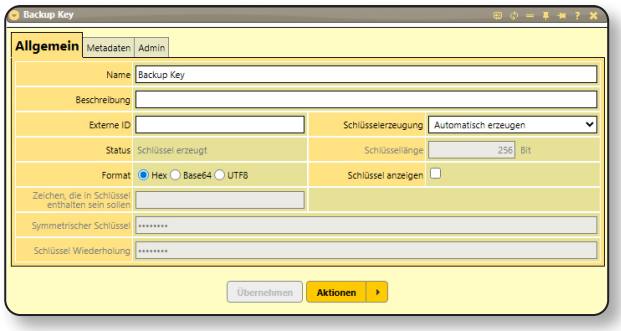


Abb. 14.02: *Konfiguration des Backup Keys*

Der Schlüssel muss anschließend im Dienst: Backup im Feld Schlüssel ausgewählt und die Checkbox Starten aktiviert werden.

Im Falle eines Ausfalls oder einer Neuinstallation der TMA ist eine Wiederherstellung bestehender Backups ohne den zuvor gesicherten Backup-Schlüssel nicht möglich. Der Backup-Schlüssel muss daher durch den Administrator exportiert und separat gesichert werden.

Der Schlüssel kann auf zwei Wegen exportiert werden:

- Im Reiter **Allgemein** durch Aktivieren der Checkbox Schlüssel anzeigen und manuellem Kopieren.
- Im Reiter **Admin** durch Download im Feld Im-/Export.

⚠ **Hinweis:** Der Zugriff auf Schlüssel ist durch die Rechteverwaltung der TMA geschützt. Ein Export des Backup-Schlüssels ist daher nur möglich, wenn der Admin-Benutzer über das Secret-Recht verfügt (siehe **15.1 Benutzer und Rollen**).

14.2.2 Ausführen von Backups

Die Erstellung der Backups erfolgt automatisch. Standardmäßig wird täglich ein Backup durchgeführt.

Optional kann die zeitliche Ausführung im Dienst: Backup angepasst werden. Die Konfiguration erfolgt im Reiter **Allgemein** und orientiert sich an der Crontab-Syntax.

Starten: Durch Aktivieren der Checkbox wird der Dienst mit der vorgenommenen Konfiguration eingeschaltet.

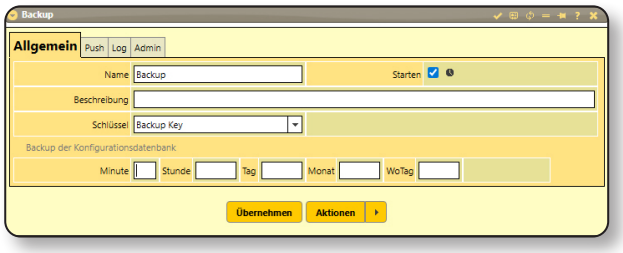


Abb. 14.03: *Dienst: Backup*

Schlüssel: Hier wird für die Backup-Verschlüsselung der auf der TMA erzeugte Backup Key ausgewählt.

Backup der Konfigurationsdatenbank: Hier werden die Zeiteinstellungen vorgenommen.

14.2.3 Bereitstellen von Backups

Backups können manuell abgerufen (Pull) oder automatisiert an ein externes System übertragen werden (Push).

Pull (manueller Abruf)
Um eine Backup-Datei herunterzuladen, kann im Dienst: Wartung (Reiter **Fernwartung**) der Zugriff für das SSH-Konto **remotebackup** aktiviert werden (siehe **14.3 Dienst: Wartung**).

Dieses Konto hat ausschließlich Zugriff auf das interne Backup-Verzeichnis der TMA. Die Authentifizierung erfolgt über einen hinterlegten SSH Public Key.

Push (automatische Übertragung)

Zur optionalen Auslagerung der Backups kann im Dienst: Backup im Reiter **Push** ein externer Zielserver konfiguriert werden. Die Übertragung erfolgt verschlüsselt über das SFTP-Protokoll. Das Ziel wird als URI (z.B. sftp://user@host/pfad) definiert.

Der Zugriff auf das Zielsystem erfolgt über auf der Appliance generierte Zugriffsschlüssel. Optional kann ein vorhandener privater Schlüssel importiert werden. Zur Verifikation der Gegenstelle wird der Hostkey des Zielsystems hinterlegt.

Nach Abschluss des Backups kann ein Protokoll über Umfang und Erfolg des Backups an definierte E-Mail-Empfänger versendet werden. Die Absenderadresse und die Domain müssen vom Mailsystem als vertrauenswürdig eingestuft sein.

Die korrekte Konfiguration der SFTP-Verbindung und des Mailversands kann über eine integrierte Testfunktion geprüft werden. Das Ergebnis wird direkt im Admin-Interface protokolliert.

14.2.4 Log

Sämtliche Backup-Vorgänge werden systemseitig protokolliert. Das **Log** enthält Informationen zu Datum, Quelle, Quellhost zur administrativen Kontrolle.

14.3 Dienst: Wartung

Im Dienst: Wartung werden Wartungszugänge konfiguriert.

Die Checkbox Starten im Reiter Fernwartung aktiviert die SSH-Fernwartung. Im Feld Port kann der Port angegeben werden, auf den der SSH-Dienst reagieren soll. Wird das Feld leer gelassen, wird der Standard-SSH-Port 22 verwendet.

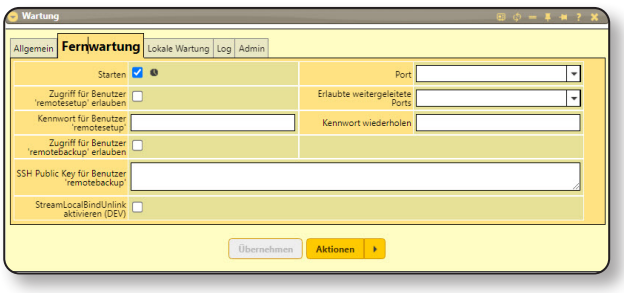


Abb. 14.04: *Wartungsdienst einrichten*

Durch Aktivieren der Checkbox Zugriff für Benutzer ‚remotesetup' erlauben wird für den Benutzer **remotesetup** die Anmeldung mit einem benutzerdefinierten Kennwort via SSH zugelassen, mit der er zum selben Menü wie bei der direkten Konsolenanmeldung gelangt. Im Feld Kennwort für Benutzer ‚remotesetup' muss hierzu ein entsprechendes Kennwort vergeben werden. Zusätzlich können für eine SSH-Portweiterleitung Erlaubte weitergeleitete Ports für diesen Benutzer ausgewählt werden.

Durch Aktivieren der Checkbox Zugriff für Benutzer ‚remotebackup' erlauben wird für den Benutzer **remotebackup** der SFTP-Zugriff auf die internen Konfigurationsbackups erlaubt. Dieser Benutzer hat nur Zugriff auf das Backupverzeichnis (/backup) der Appliance. So können Backupdateien per SFTP abgeholt werden, wenn sie z.B. zu groß sind, um über das Appliance-Objekt der Administrationsoberfläche heruntergeladen zu werden. Die Anmeldung über das SFTP-Protokoll ist nur durch Authentifizierung mit einem SSH-Schlüssel möglich. Der öffentliche Schlüssel wird im Feld SSH Public Key

für Benutzer ‚remotebackup' hinterlegt. Der Zugriff auf die Backupdateien kann mit einem beliebigen Tool per SFTP erfolgen (z.B. WinSCP).

Im Reiter **Lokale** Wartung werden die Einstellungen für den lokalen Wartungszugang konfiguriert. Bei der Ersteinrichtung muss die Checkbox Kennwort für Konsole aktiviert und ein neues Kennwort vergeben werden.

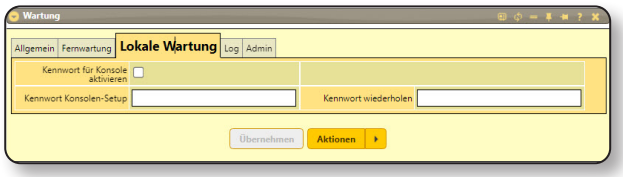


Abb. 14.05: *Lokale Wartung konfigurieren*

Die Anmeldung erfolgt mit dem Benutzernamen **setup**. Mit dem Standardkennwort **bb5000** besteht Zugang zu einem Menü, das grundlegende Wartungsaufgaben wie das Setzen der IP-Adresse oder das Senden eines Ping erlaubt.

14.4 Dienst: Smartcard-Enrollment

Der Dienst: Smartcard-Enrollment wird benötigt, um Zertifikate auf Smartcards zu speichern. Dazu wird zusätzlich eine Smartcard-Software benötigt, die auf der TMA hochgeladen werden muss.

Info

Informationen zum Hochladen von Smartcard-Software-Dateien finden Sie im Tutorial zum Smartcard-Enrollment auf der ECOS-Webseite.

Der Dienst: Smartcard-Enrollment muss unterhalb des ECOS Appliance-Objekts im Baum angelegt und mit folgenden Einstellungen konfiguriert sein:

Name: Vergeben Sie einen aussagekräftigen Namen.

Starten: Aktivieren Sie diese Checkbox.

Lokale Adresse für externe Anfragen: Wählen Sie eine Schnittstelle, um externe Anfragen zu ver-arbeiten. Standardmäßig können Sie die IP-Adresse der TMA auswählen.

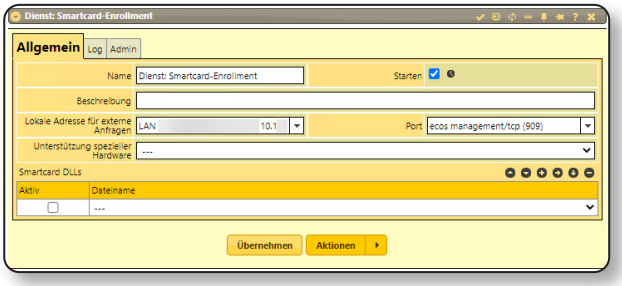


Abb. 14.06: *Dienst: Smartcard-Enrollment*

Port: Wählen Sie den Port für die oben angegebene Adresse. Standardmäßig können Sie den Management-Port der TMA (Port **909**) auswählen.

Smartcard DLLs: Wählen Sie unter Dateiname die Smartcard-Software-Dateien aus (einzeln oder einen Container) und aktivieren Sie die Checkbox Aktiv.

Speichern Sie die Änderungen mit **Übernehmen**.

14.5 Software-Updates

Die TMA kann auf zwei verschiedenen Arten aktualisiert werden. Zum einen besteht die Möglichkeit die Software-Update-Server von ECOS zu nutzen. Das ermöglicht ein automatisches Update der TMA. Zum anderen kann die TMA selbst als Update-Server fungieren.

14.5.1 Software-Update über die Software-Update-Server von ECOS

Mithilfe des Dienst: Software-Update-Objekts kann regelmäßig und automatisch nach Updates gesucht und diese installiert werden. Ebenso besteht die Möglichkeit, die TMA manuelle über das ECOS Appliance-Objekt zu aktualisieren.

14.5.1.1 Automatische Updates

Für das Update der Appliance wird ein Dienst: Software-Update benötigt. Ein neues Dienst: Software-Update-Objekt wird über das Kontextmenü **Neu → Dienste → Dienst: Software-Update** angelegt.

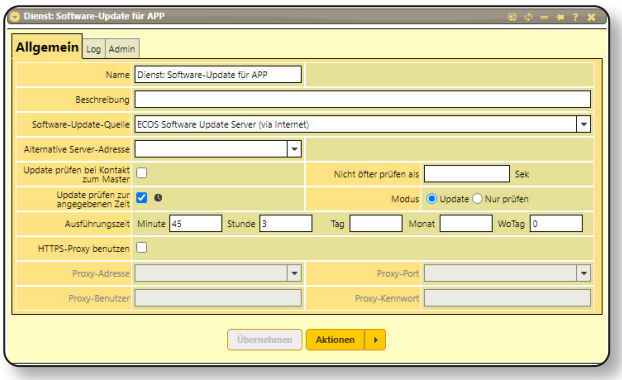


Abb. 14.07: *Dienst: Software-Update*

Name: Vergeben Sie einen aussagekräftigen Namen.

Software-Update-Quelle: Wählen Sie die Option **ECOS Software Update Server (via Internet)**. Die Updates werden über die von ECOS verwalteten Software-Update-Server im Rechenzentrum eingestellt.

Update prüfen zur angegebenen Zeit: Aktivieren Sie diese Checkbox, um regelmäßig und zu einer definierten Zeit (z.B. nachts) nach Updates zu suchen.

Modus: Wählen Sie die Option **Update**, um das neue Update automatisch zu installieren.

Ausführungszeit: Geben Sie hier die Zeit an, zu der die Prüfung auf Updates erfolgen soll. Nutzen Sie die cron-Syntax.

Beispiel: Soll wöchentlich sonntags um 3:45 nachts auf Updates geprüft werden, tragen Sie folgende Werte ein:

Minute: 45

Stunde: 3

WoTag: 0

Kann die ECOS Appliance keinen direkten Zugang zu den Software-Update-Servern von ECOS aufbauen, aktivieren und konfigurieren Sie die HTTPS-Proxy-Einstellungen.

Speichern Sie die Änderungen mit **Übernehmen**.

14.5.1.2 Manuelles Update

Öffnen Sie das ECOS Appliance-Objekt und navigieren Sie zum Reiter Aktionen.

Aktionen: Wählen Sie die Aktion **Update**.

Es erscheinen weitere Optionen.

Update ausführen: Aktivieren Sie diese Checkbox, wenn Sie die ECOS Appliance aktualisieren wollen. Andernfalls werden nur die Lizenzen aktualisiert und nach neuen Updates gesucht, diese aber nicht installiert.

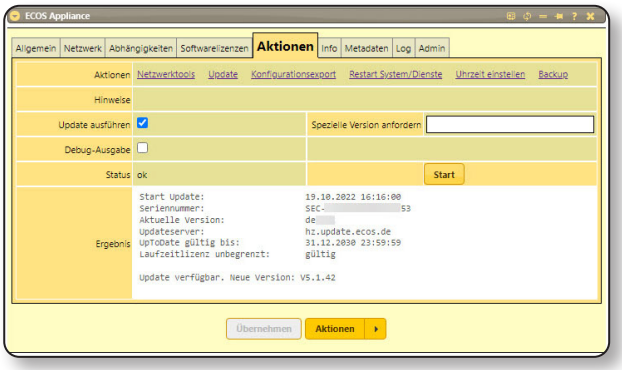


Abb. 14.08: *Reiter "Aktionen" - Manuelles Update*

Spezielle Version anfordern: Geben Sie hier die Versionsnummer an, auf die Sie die ECOS Appliance updaten wollen, wenn es sich dabei nicht um die aktuelle Version handelt.

Starten Sie den Updatevorgang mit dem Button **Start**.

Starten Sie die ECOS Appliance nach dem Update über den Reiter Aktionen und die Option Restart System/Dienste neu.

14.5.2 Software-Update über die ECOS Appliance

Soll die TMA selbst als Update-Server fungieren, wird zum einen der Dienst: Software-Update-Server konfiguriert. Zum anderen werden ein Software-Update-Image und eine Software-Update-Quelle benötigt.

14.5.2.1 Software-Image bereitstellen

Software-Images können auf zwei Arten zur Verfügung gestellt werden. Zum einen können die Software-Dateien manuell vom ECOS Software-Update-Server heruntergeladen werden. Zum anderen kann die ECOS Appliance die Dateien herunterladen, wenn sie Zugang (direkt oder per Proxy) zu den ECOS Software-Update-Servern hat.

Die Update-Dateien können unter https://files.update.ecos.de heruntergeladen werden. Dazu wird eine gültige Benutzerkennung benötigt. Die Zugangsdaten können über den ECOS Support angefordert werden.

Für jedes Software-Image wird eine eigenes Objekt Software-Update-Image benötigt. Zusammen mit den Software-Update-Quellen könne sie in einem Container: Software-Updates zusammengefasst werden.

Ein neues Software-Update-Image-Objekt wird über das Kontextmenü **Neu → Software-Updates → Software-Update-Image** angelegt.

Name: Vergeben Sie einen aussagekräftigen Namen.

Speichern Sie das Objekt ab, anschließend kann das Image über den **Upload**-Link hochgeladen werden.

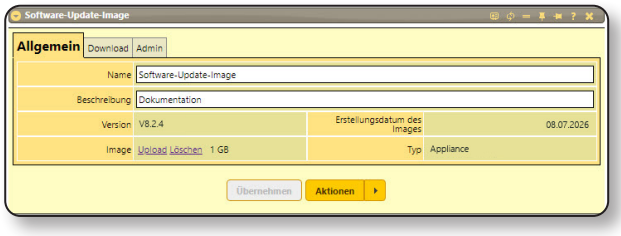


Abb. 14.09: *Software-Update-Image - Reiter Allgemein*

Nach dem Upload erscheinen Informationen zur Version, dem Erstellungsdatum des Images und dem Typ.

Sollen die Software-Images heruntergeladen werden, navigieren Sie zum Reiter **Download**.

Image-Typ: Wählen Sie für das Update der TMA den Typ Appliance aus.

Version: Geben Sie die Versionsnummer an, auf die Sie die TMA aktualisieren wollen, z.B. V8.3.0.

Starten Sie anschließend den Download. Den Fortschritt und Status werden in den Feldern Hinweise und Status angezeigt.

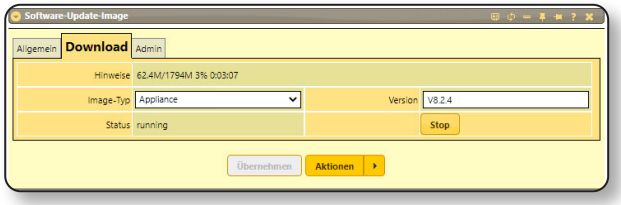


Abb. 14.10: *Software-Update-Image - Reiter Download*

14.5.2.2 Update-Quelle definieren

Neben dem Software-Update-Image wird auch eine Software-Update-Quelle benötigt. Ein neues Software-Update-Quelle-Objekt wird über das Kontextmenü **Neu → Software-Updates → Software-Update-Quelle** angelegt.

Name: Vergeben Sie einen aussagekräftigen Namen.

Image für Appliance: Wählen Sie hier das zuvor angelegt Software-Update-Image aus.

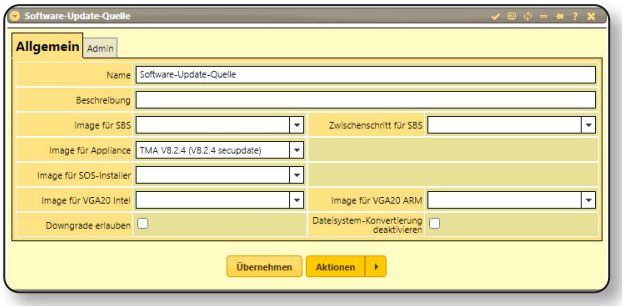


Abb. 14.11: *Software-Update-Quelle*

Bei einem neuen Update durch ein neues Image muss keine neue Software-Update-Quelle angelegt werden. Es reicht das Image für Appliance zu ändern und das Konfigurationsobjekt neu abzuspeichern.

14.5.2.3 Dienst: Software-Update-Server einrichten

Ein neues Dienst: Software-Update-Server-Objekt wird über das Kontextmenü **Neu → Dienste → Dienst: Software-Update-Server** angelegt.

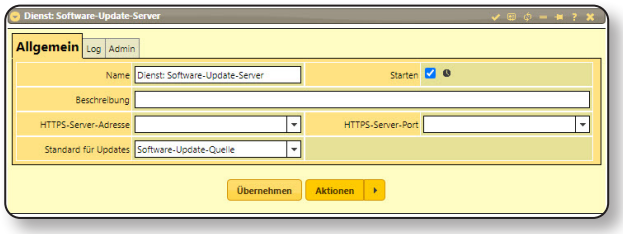


Abb. 14.12: *Dienst: Software-Update-Server*

Name: Vergeben Sie einen aussagekräftigen Namen.

Starten: Aktivieren Sie die Checkbox.

Standard für Updates: Wählen Sie hier die Software-Update-Quelle aus, in der sich das aktuelle Software-Update-Image für das Update befindet.

Eine HTTPS-Server-Adresse und ein HTTPS-Server-Port müssen nur angegeben werden, wenn der Software-Update-Server nicht über die Managementverbindung der ECOS Appliance genutzt werden soll.

14.5.2.4 Dienst: Software-Update einrichten

Ein neues Dienst: Software-Update-Objekt wird über das Kontextmenü **Neu → Dienste → Dienst: Software-Update** angelegt.

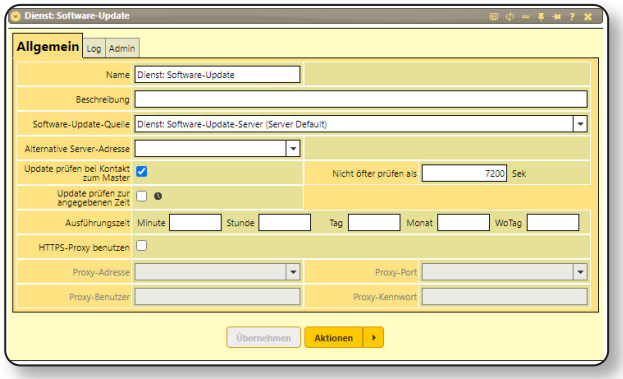


Abb. 14.13: *Dienst: Software-Update*

Name: Vergeben Sie einen aussagekräftigen Namen.

Software-Update-Quelle: Wählen Sie hier den angelegt Dienst: Software-Update-Server aus.

Informationen zu den weiteren Einstellungen des Diensts finden sich unter **14.5.1.1 Automatische Updates**.

15 Benutzerverwaltung (Experte)

15.1 Benutzer und Rollen

Damit Benutzer sich an der TMA anmelden können, benötigen sie Berechtigungen. Diese werden dem Benutzer erteilt, indem ihm eine oder mehrere Rollen zugewiesen werden.

Ein Benutzer kann mehrere Rollen mit unterschiedlichen Privilegien haben. Es kann aber auch Rollen ohne Privilegien geben, die dazu dienen Berechtigungen für Objekte zu vergeben. Sie werden im Benutzer-Objekt auf dem Reiter **Allgemein** im Feld Rolle zugewiesen.

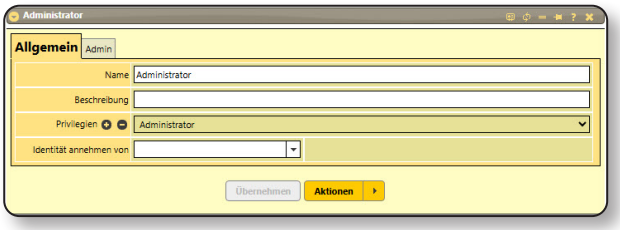


Abb. 15.01: *Privileg in Benutzerrolle*

Ein Benutzer kann sich nur anmelden, wenn er mindestens eine Rolle hat.

Auf was der Benutzer Zugriff erhält, hängt einerseits von den Berechtigungen, die ihm in den einzelnen Objekten zugewiesen wurden und andererseits von den Privilegien in den Rollen ab. Jede Rolle kann eine oder mehrere Privilegien haben. Sie werden im Rollen-Objekt im Feld Privilegien konfiguriert. Es stehen verschiedene vordefinierte Privilegien zur Verfügung:

Administrator: Mit diesem Privileg erhält der Benutzer uneingeschränkten Zugriff auf die Administrationsoberfläche.

Zugriff allgemein: Mit diesem Privileg erhält der Benutzer Zugriff auf die API. Die Berechtigungen richten sich nach dem im Reiter **Admin** eines Objekts zugeordneten Berechtigungen.

Identität eines Benutzers annehmen: Mit diesem Privileg kann der Benutzer die Identität eines anderen Benutzers annehmen. Die Identität wird im Feld Identität annehmen für festgelegt. Dadurch können Stellvertreter, z.B. für technische Benutzer, die die API benutzen, bestimmt werden, ohne dass die Anmeldung gewechselt werden muss.

Identität eines Abonnenten annehmen: Mit diesem Privileg kann der Benutzer die Identität eines Abonnenten annehmen. Es muss kein spezieller Abonnent ausgewählt werden. Benutzer können sich über die API als Abonnent ausgeben, um Zertifikate in deren Namen anzufordern.

Zugriff auf Admin-Oberfläche: Mit diesem Privileg erhält der Benutzer Zugriff auf die Administrationsoberfläche. Die Berechtigungen richten sich nach dem im Reiter **Admin** eines Objekts zugeordneten Berechtigungen. Außerdem erhält der Benutzer Zugriff auf die API (siehe **22 Berechtigungen**).

Zugriff auf Self-Service-Portal: Mit diesem Privileg erhält der Benutzer Zugriff auf das Self-Service-Portal. Über das Self-Service-Portal können Benutzer ihre Zertifikate anfordern und verwalten. Besitzt der Benutzer nur dieses Privileg, wird er bei der Anmeldung automatisch auf das Self-Service-Portal umgeleitet (siehe **11 Self-Service-Portal**).

Log: Mit diesem Privileg erhält der Benutzer Zugriff auf Loginfomationen.

Zertifikathistorie: Mit diesem Privileg kann der Benutzer die Historie aller Zertifikate anzeigen, auch wenn die Zertifikate selbst gelöscht sind. Ohne dieses Privileg kann der Benutzer nur die Historie der Zertifikate anzeigen, für die er die Anzeigerechte hat.

Zertifikatverifizier: Mit diesem Privileg erhält der Benutzer lesenden Zugriff auf alle Daten, die er zum Prüfen der Zertifikatgültigkeit benötigt, z.B. um daraus eine CRL zu erstellen.

Identität annehmen von: Hier wird die Identität ausgewählt, die der Benutzer mit dem Privileg Identität eines Benutzers annehmen annehmen darf.

Berechtigungen für einzelne Objekte können granular und losgelöst von den vordefinierten Privilegien vergeben werden. Genauso können zusätzliche Berechtigungen über die Privilegien hinaus vergeben werden. Beides wird über den Reiter **Admin** eines jeden Objekts konfiguriert (siehe **22 Berechtigungen**).

15.2 Authentisierung

Im Benutzer-Objekt wird die Authentisierung für die Anmeldung an der TMA definiert.

Im Reiter **Allgemein** können in der Tabelle Authentisierungsmethoden verschiedene Methoden zur Authentisierung konfiguriert werden.

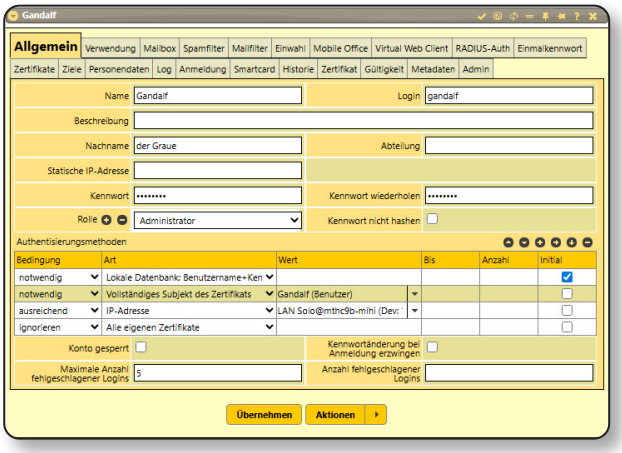


Abb. 15.02: *Authentisierungsmethoden im Benutzer-Objekt*

In der Spalte Bedingung wird festgelegt, ob die jeweilige Authentisierungsmethode für die Anmeldung **notwendig** bzw. **ausreichend** ist oder **ignoriert** wird. Für eine erfolgreiche Anmeldung müssen *alle* notwendigen Bedingungen erfüllt sein. Wurden ausreichende Bedingungen definiert, muss *eine* dieser Bedingungen für die Anmeldung erfüllt sein. Wurden sowohl notwendige als auch ausreichende Authentisierungsmethoden konfiguriert, müssen *alle notwendigen*, die vor der ersten ausreichenden Bedingung stehen, und *mindestens eine ausreichende* Bedingung erfüllt sein, damit sich der Benutzer erfolgreich anmelden kann. Authentisierungsmethoden, die als ignorieren eingestuft sind, werden bei der Anmeldung nicht berücksichtigt.

Die Authentisierungsmethoden selbst werden in der Spalte Art definiert. Die Option **Lokale Datenbank: Benutzername+Kennwort** nutzt die Anmeldedaten, die in den Feldern Login und Kennwort konfiguriert sind.

Bei der Option **Via RADIUS: Benutzername+Kennwort** werden die Zugangsdaten gegen einen RADIUS-Server geprüft, der es dann z.B. an ein Microsoft AD weiterleitet.

Wird **Zertifikat der CA** gewählt, erfordert jede Anmeldung ein gültiges Zertifikat, das von der CA signiert wurde, die im Dienst: HTTPS-Administration im Feld CA für Zertifikatanmeldung konfiguriert ist.

Die Option **Zertifikat mit CN als Login** benötigt ein Zertifikat, dessen CN dem Benutzernamen im Feld Login des Benutzer-Objekts entspricht. Das Zertifikat muss von der CA signiert sein, die im Dienst: HTTPS-Administration im Feld CA für Zertifikatanmeldung hinterlegt ist.

Bei der Option **Vollständiges Subjekt des Zertifikats** wird bei jeder Anmeldung ein Zertifikat gefordert, dessen Subjekt und Aussteller vollständig mit dem Zertifikat übereinstimmt, das in der Spalte Wert ausgewählt wird. Ebenso muss das Zertifikat von derselben CA signiert worden sein. Das Zertifikat kann ausgewählt werden, sobald das Konfigurationsobjekt gespeichert wurde.

Die Option **Exaktes Zertifikat** erfordert bei jeder Anmeldung ein Zertifikat, dessen Subjekt vollständig mit dem Zertifikat übereinstimmen, das in der Spalte Wert ausgewählt ist. Ebenso muss das Anmeldezertifikat von derselben CA ausgestellt worden sein und die Seriennummer muss identisch sein. Das stellt sicher, dass es sich genau um exakt dasselbe Zertifikat handelt.

Wird die Option **Alle eigenen Zertifikate** gewählt, erfordert jede Anmeldung ein Zertifikat, das als Eigentümer diese Identität eingetragen hat.

Bei der Option **Authentisierungszertifikat** wird für jede Anmeldung ein Zertifikat gefordert, das als Eigentümer diese Identität eingetragen hat und als Authentisierungszertifikat ausgestellt wurde. Authentisierungszertifikate, müssen als Othername **1.3.6.1.4.1.9705.21;UTF8:** eingetragen haben. Die wird z.B. zur Authentisierung des Dienst: Certificate Enrollment Agent benutzt.

Wird die Option **IP-Adresse** gewählt, erfordert die Anmeldung die IP-Adresse, die in der Spalte Wert angegeben wird.

In der Spalte Bis kann ein Datum eingetragen werden, bis wann die Authentisierungsmethode gültig ist und genutzt werden kann. Es kann ein Datum mit Uhrzeit im Format TT.MM.JJJJ hh:mm angegeben werden. Nach Ablauf ist die Anmeldung mit dieser Methode nicht mehr möglich.

Die Zahl der Anmeldeversuche kann in der Spalte Anzahl festgelegt werden. Sie bestimmt, wie oft diese Authentisierungsmethode zur Anmeldung genutzt werden kann. Dabei zählen sowohl erfolgreiche als auch fehlgeschlagene Anmeldeversuche. Sobald die Anzahl erreicht ist, ist die Anmeldung mit dieser Methode nicht mehr möglich.

⚠ **Hinweis:** IP-Adressen eignen sich gundsätzlich nicht als alleinige Identifizierungsmerkmale, sondern dienen ausschießlich als ergänzende Restriktionen.

16 Zertifikate

Zertifikate können nicht nur über die Standardoberfläche und die Assistenten eingerichtet werden, sondern auch im Expertenmodus konfiguriert werden. Dort stehen weitere Einstellungsmöglichkeiten zur Verfügung.

Die Zertifikate können dabei sowohl auf der TMA erzeugt als auch von extern importiert oder nur signiert werden

Für beide Zertifikatvarianten erfolgt die Erzeugung in zwei Schritten. Zuerst wird das jeweilige Objekt über das Kontextmenü im Navigationsbaum erstellt. Es werden die verschiedenen Parameter konfiguriert. Im zweiten Schritt wird im Feld Erstellen des Zertifikats die Option **Automatisch erzeugen** gesetzt und das ganze Objekt gespeichert. Alle Parameter, die Teil eines Zertifikats sind, können nach der Erzeugung nicht mehr geändert werden. Sie werden ausgegraut. Für den Import von Zertifikaten siehe **16.3 Im- und Export**.

16.1 Wichtige Zertifikatparameter

Viele der allgemeinen Zertifikatparameter sind für beide Zertifikat-Objekttypen identisch und befinden sich auf dem Reiter **Allgemein** im jeweiligen Objekt. Darüber hinaus gibt es Parameter, die jeweils spezifisch für eines der beiden Objekttypen sind.

16.1.1 Gemeinsame Zertifikatparameter

Reiter Allgemein:

CA/Parent-CA: Die CA signiert (CA-)Zertifikate mit ihrem privaten Schlüssel. Dadurch können andere Teilnehmer mit dem öffentlichen Schlüssel der signierenden CA das Zertifikat auf Gültigkeit oder die Signatur prüfen.

Bei Zertifikat-Objekten heißt der Parameter CA und bei CA-Zertifikaten Parent-CA. Damit die signierende CA ausgewählt werden kann, muss diese vorher als CA-Zertifikat-Objekt erzeugt bzw. hochgeladen worden sein.

Bei CA-Zertifikaten kann über diesen Parameter eine Zertifikathierarchie aufgebaut werden. Wird bei CA-Zertifikat-Objekten keine Parent-CA ausgewählt, handelt es sich bei dem CA-Zertifikat um eine Root-CA. Wird eine Parent-CA ausgewählt, spricht man von Sub-CA.

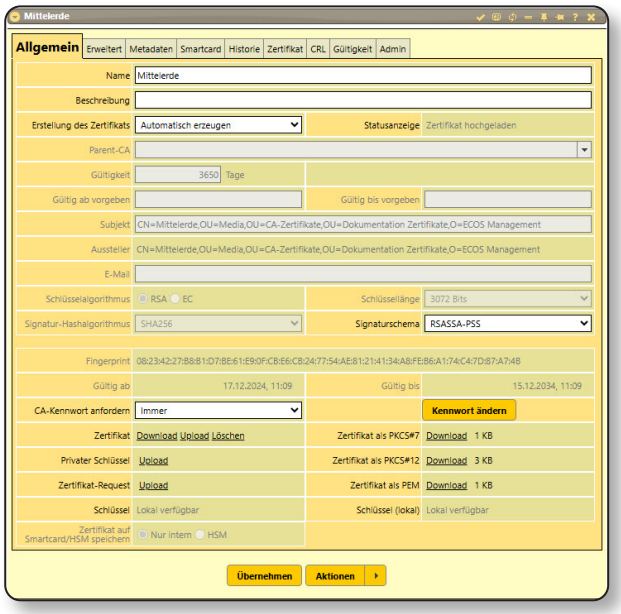


Abb. 16.01: *CA-Zertifikat-Objekt - Reiter Allgemein*

Gültigkeit: Zertifikate sind nur eine begrenzte Zeit gültig. Die Gültigkeit wird in Tagen angegeben. Die Standardeinstellung für CAs liegt bei **3650 Tagen** (10 Jahre) und bei Zertifikaten bei **365 Tage** (1 Jahr). Diese kann beliebig angepasst werden.

Nach Ablauf dieser Zeit ist das Zertifikat ungültig und die Prüfung schlägt fehl, so dass z.B. eine Anmeldung nicht mehr möglich ist. Ein (CA-)Zertifikat kann nicht länger gültig sein als seine signierende CA.

Die Laufzeiten von Zertifikaten können verlängert werden. Ebenso ist es möglich, Zertifikate vorzeitig für ungültig zu erklären (siehe **5.3.4 Zertifikat-Lifecycle-Management**).

Subjekt: Das Subjekt bezeichnet die Instanz, für wen oder was das Zertifikat ausgestellt werden soll. Dabei kann es sich z.B. um eine Person, einen Server oder ein anderes System handeln. Es verhält sich wie der Name des Zertifikats. Das Subjekt wird als Distinguished Name (DN) angegeben und setzt sich aus verschiedenen Relative Distinguished Names (RDN) zusammen, die durch Komma getrennt sind.

Mögliche RDNs sind:

CN: Common Name	C: Country	DC: Domain Component
O: Organization	S: State/Province	
OU: Organizational Unit	L: Locality	

Wird der Parameter nicht manuell eingetragen, wird das Subjekt beim Erzeugen des Zertifikats automatisch erstellt. Das Subjekt setzt sich dann aus dem Namen des Zertifikat-Objekts als CN, dem Pfad des Zertifikat-Objekts als OU und dem Namen des Organisation-Objekts als O zusammen. Ist im Container: Zertifikate ein Basispfad für Zertifikate angegeben, fließt dieser Pfad als DC anstelle des O in das Subjekt ein.

Schlüsselalgorithmus: Der Schlüsselalgorithmus bestimmt, wie das Schlüsselpaar erzeugt wird. Zur Auswahl stehen **RSA** (Rivest-Shamir-Adleman-Verfahren) und **Elliptische Kurven** (EC). Das RSA-Verfahren ist die Standardeinstellung.

Schlüssellänge: Hier wird die Schlüssellänge für das RSA-Verfahren ausgewählt. Standardmäßig sind **3072 Bit** voreingestellt. Diese Einstellung entspricht den aktuellen Anforderungen und Empfehlungen des BSI für die Mindestlänge von RSA-Schlüsseln in VS-NfD-Umgebungen.

Außerhalb von VS-NfD-Umgebungen können abweichende Schlüssellängen je nach Einsatzszenario und Kompatibilität der eingesetzten Systeme oder Hardwarekomponenten erforderlich sein.

Elliptische Kurve: Hier wird die elliptische Kurve für das ECC-Verfahren ausgewählt. Standardmäßig ist **prime256v1** eingestellt. Diese Einstellung entspricht den aktuellen Anforderungen und Empfehlungen des BSI für die Mindestlänge von ECC-Schlüsseln in VS-NfD-Umgebungen.

Außerhalb von VS-NfD-Umgebungen können abweichende Schlüssellängen je nach Einsatzszenario und Kompatibilität der eingesetzten Systeme oder Hardwarekomponenten erforderlich sein.

Signatur-Hashalgorithmus: Mit dem Signatur-Hashalgorithmus wird die Prüfsumme bei der Erstellung der digitalen Signatur berechnet. Die Prüfsumme wird anschließend mit dem privaten Schlüssel der ausstellenden CA verschlüsselt. Mit dem öffentlichen Schlüssel der CA kann die Prüfsumme entschlüsselt werden und so die Authentizität des Zertifikats bestätigt werden. Standardmäßig ist der Signatur-Hashalgorithmus **SHA256** ausgewählt.

16.1.2 CA-Zertifikat-spezifische Parameter

Aufgrund ihrer Funktion als Zertifizierungsstelle haben CA-Zertifikate spezielle Parameter, die sonstige Zertifikate nicht haben.

Reiter Allgemein:

CA-Kennwort abfragen: Beim Erstellen eines CA-Zertifikats muss ein Kennwort festgelegt werden. Bei diesem Parameter wird festgelegt, wann dieses Kennwort abgefragt wird. Standardmäßig ist die Option **Immer** gewählt. Das Kennwort wird bei jeder Operation, die den privaten Schlüssel der CA erfordert, abgefragt.

Die Option **Beim Erstellen** fragt das Kennwort der CA nur beim Erstellen neuer Zertifikate ab. Für Verlängerungen wird das Kennwort nicht benötigt, daher sollte diese Option gewählt werden, wenn Zertifikate automatisch verlängert werden sollen.

Sollen weitere Vorgänge der CA automatisiert durchgeführt werden, dann sollte die Option **Nie** gewählt werden.

Bei der Option **Nicht für CRL** wird das CA-Kennwort beim Erzeugen der CRL nicht angefordert, jedoch beim Erstellen und Verlängern von Zertifikaten. Dadurch kann die CRL automatisch verlängert werden.

Wird die Einstellung nachträglich geändert, ist bei der ersten Operation nach der Änderung einmalig die Eingabe des CA-Kennworts erforderlich. Die TMA speichert das Kennwort nicht ab. Geht das Kennwort verloren, gibt es keine Möglichkeit, das Kennwort zurückzusetzen.

E-Mail: Bei einem CA-Zertifikat wird die E-Mail-Adresse des Ausstellers angegeben. Sie wird Bestandteil des Subjekts. Mehrere E-Mail-Adressen werden mit einem Leerzeichen getrennt angegeben.

Reiter Erweitert:

Initiale Seriennummer: Zertifikate erhalten beim Signieren durch eine CA eine Seriennummer, die nicht mehr geändert werden kann. Die Seriennummer für das erste Zertifikat, das von der CA signiert wird, wird initial festgelegt. Dabei handelt es sich um einen hexadezimal Wert, der automatisch hochgezählt wird.

Typ der Seriennummer: Die Seriennummer für die Zertifikate kann zum einen **sequenziell** oder **zufällig** erzeugt werden. Wird die Seriennummer fortlaufend erzeugt, dann wird sie anhand der vergebenen initialen Seriennummer berechnet.

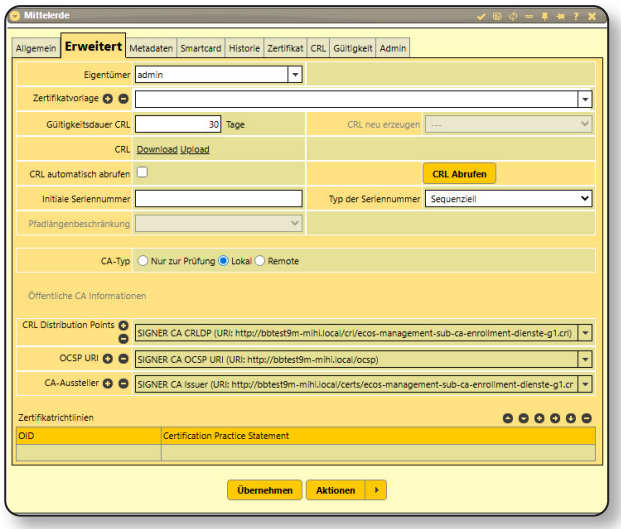


Abb. 16.02: *CA-Zertifikat-Objekt - Reiter Erweitert*

Öffentliche CA-Informationen: Bei den öffentlichen CA-Informationen handelt es sich um verschiedene Informationen, die in die Zertifikate als Authority Info Access (AIA) eingebettet werden. Dazu gehören Informationen, wo Dritte die Zertifikate prüfen und die CA herunterladen können.

Die CRL Distribution Points geben an, wo die CRL der signierenden CA heruntergeladen werden können.

Bei OCSP URI wird ein **OCSP URI**-Objekt ausgewählt. In diesem Objekt wird die Serveradresse für den Onlinevalidierungsdienst OCSP konfiguriert. Der OCSP dient, ähnlich wie die CRL, zur Prüfung von Zertifikaten auf ihre Gültigkeit. Die Abfrage über OCSP ist i.d.R. schneller und aktueller als der Abgleich mit der CRL.

Im Feld CA-Aussteller wird ein **CA-Aussteller**-Objekt ausgewählt. Mit diesem Objekt wird der Downloadpfad für das CA-Zertifikat gespeichert. Dies wird im Abschnitt *Authority Information Access/CA Issuers* in allen von dieser CA signierten Zertifikaten übernommen.

Zertifikatrichtlinien: Zusätzliche Informationen, die für die Benutzer eines CA-Zertifikats relevant sind, können über die Zertifikatrichtlinien veröffentlicht werden. Dazu zählen z.B. Regeln und Prozeduren für die Ausstellung, Nutzung, Verlängerung und den Widerruf von Zertifikaten.

Sie werden in Form einer **OID** (Object Identifier) in Kombination mit einem **Certification Practice Statement (CPS)** angegeben. Eine OID ist eine internationale Kennung von Informationsobjekten, z.B. Organisationen, Klassifikationen, Certificate Policys oder Certificate Practice Statements. Sie muss beantragt werden.

Ein CPS ist ein Policy-Dokument, das von einer Zertifizierungsstelle oder einem Mitglied eines Web of Trust veröffentlicht wird und ihre Praxis bei der Ausstellung und Verwaltung von Public-Key-Zertifikaten beschreibt. Sie werden als URL angegeben und im signierten Zertifikat eingebettet.

16.1.3 Zertifikat-spezifische Parameter

Zertifikate haben – ähnlich wie CA-Zertifikate – spezielle Parameter, die CA-Zertifikate nicht haben.

Reiter Allgemein:

Schlüssel verschlüsselt ablegen: Dieser Parameter legt fest, wie der private Schlüssel des Zertifikats abgelegt werden soll. Unabhängig von der Einstellung, wird der Schlüssel durch die allgemeinen Sicherheitsmechanismen der TMA geschützt und der Zugriff unterliegt den eingestellten Zugriffsrechten.

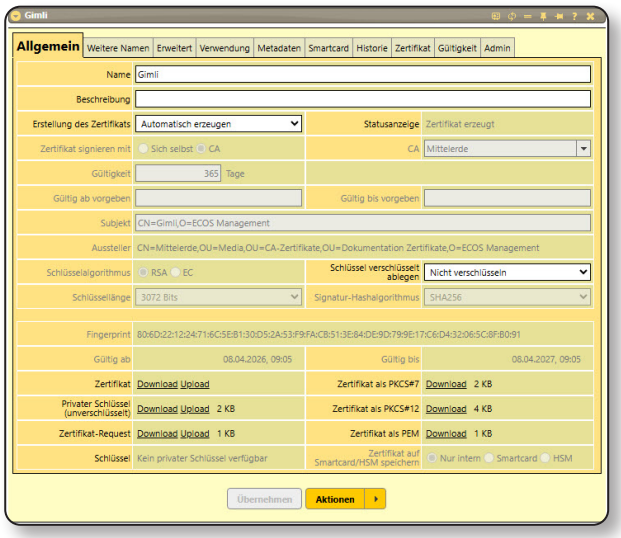


Abb. 16.03: *Zertifikat-Objekt - Reiter Allgemein*

Bei der Option **Verschlüsselt und unverschlüsselt** wird der Schlüssel sowohl verschlüsselt als auch unverschlüsselt abgelegt. Es öffnet sich ein Fenster beim Erzeugen des Zertifikats, um ein Kennwort für den privaten Schlüssel festzulegen. Nach dem Download ist der Schlüssel nur mit dem individuellen Kennwort zu benutzen. Operationen, wie z.B. der VPN-Aufbau, funktionieren ohne Abfrage des Kennworts.

Wird der private Schlüssel **Nur verschlüsselt** abgelegt, wird das individuelle Kennwort bei jeder Nutzung des privaten Schlüssels abgefragt.

Sollen Zertifikate automatisch angelegt werden, kann ein Kennwort nicht automatisch angegeben werden. In dem Fall ist die Option **Nicht verschlüsseln** zu wählen. Der Schlüssel wird ohne Kennwort in der Datenbank hinterlegt. Alle Operationen mit dem privaten Schlüssel werden ohne Kennwortabfrage durchgeführt.

Reiter Weitere Namen:

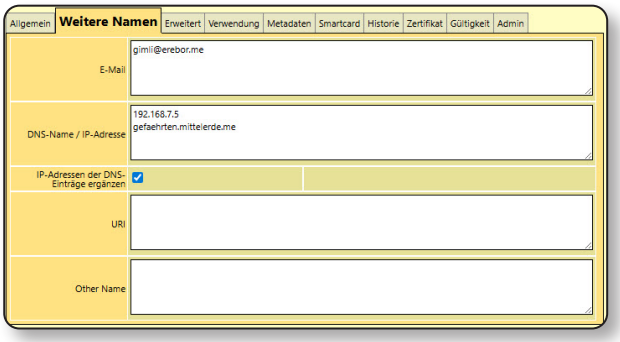


Abb. 16.04: *Zertifikat-Objekt - Reiter Weitere Namen*

Weitere Namen: Hier können zusätzliche Informationen zum Zertifikat angegeben werden. Diese alternativen Namen, auch Subject Alternative Name (SAN) genannt, können zusätzlich oder anstelle der Identität im Subjektfeld des Zertifikats angegeben werden, z.B. wenn ein Server mehrere Namen hat.

Es kann z.B. eine E-Mail-Adresse angegeben werden. Des Weiteren kann ein DNS-Name/IP-Adresse angegeben werden. Das ist z.B. bei modernen Browsern Pflicht, damit überprüft dieser während einer HTTPS-Verbindung, ob die Angaben im Zertifikat mit den tatsächlichen DNS-Namen und/oder IP-Adressen übereinstimmen. Sollen die DNS-Namen in IP-Adressen aufgelöst werden, ist die Checkbox IP-Adressen der DNS-Einträge ergänzen zu aktivieren. Das ist sinnvoll, wenn z.B. Systeme mit statischen IP-Adressen arbeiten. Auch eine URI kann angegeben werden. Damit kann z.B. die Herkunft eines Zertifikats auf entfernten Systemen überprüft werden. Weitere alternative Namen können unter Other Name angegeben werden, z.B. in Zertifikaten, die auf einer Smartcard gespeichert werden, um sich im Windows-System oder an einem Rechner anzumelden.

Reiter Verwendung:

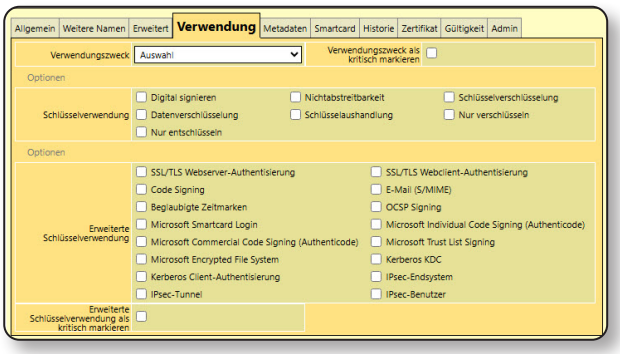


Abb. 16.05: *Zertifikat-Objekt - Reiter Verwendung*

Verwendungszweck: Auf dem Reiter **Verwendung** wird der Verwendungszweck für das Zertifikat eingestellt. Die Verwendung des öffentlichen Schlüssels kann dadurch auf bestimmte Zwecke eingeschränkt werden. Ob der Verwendungszweck geprüft wird, hängt von der Software ab, die das Zertifikat nutzt. Es gibt voreingestellte Verwendungszwecke, bei denen die Schlüsselverwendung und die Erweiterte Schlüsselverwendung vordefiniert sind. Bei der Option **Auswahl** können

die Schlüsselverwendungen manuell eingestellt werden. Weitere Informationen zu den voreingestellten Verwendungszwecken und den einzelnen Schlüsselverwendungen finden sich in **24 Schlüsselverwendungszwecke**.

16.2 Zertifikatsperrliste (CRL)

Die Zertifikatsperrliste, auch Certificate Revocation List (CRL) genannt, dient zur Überprüfung von Authentizität und Gültigkeit von Zertifikaten. Die CRL wird von der jeweiligen CA signiert und enthält die Seriennummern der Zertifikate, die widerrufen bzw. abgelaufen sind.

Die CRL wird von der Appliance generiert und zum Download bereitgestellt, so können andere Applikationen die Zertifikatsperrliste nutzen. Damit Applikationen wissen, wo sie die CRL herbekommen, wird ein sogenannter CRL Distribution Point benötigt. In diesem Objekt wird die URL zum Herunterladen der CRL festgelegt. Im CA-Zertifikat-Objekt wird der CRL Distribution Point im Reiter **Erweitert** im entsprechenden Feld ausgewählt. Dadurch wird die Information zum CRL Distribution Point in jedes Zertifikat, das von der CA signiert wird, eingebettet. Ein CRL Distribution Point kann für verschiedene CAs genutzt werden. Genauso kann eine CA mehrere CRL Distribution Points haben.

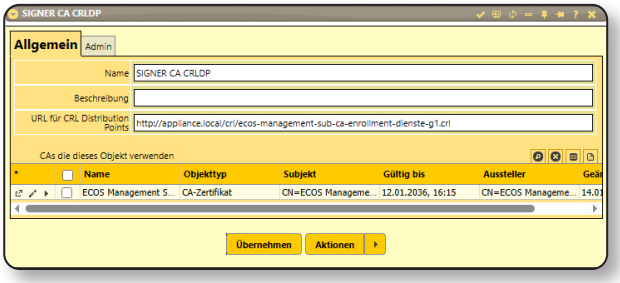


Abb. 16.06: *CRL Distribution Point*

Die Appliance stellt die CRL unter folgender URL zur Verfügung:

http://<Servername>/crl/<Name der CA>.crl

16.2.1 Gültigkeit der CRL

Im CA-Zertifikat-Objekt können auf dem Reiter **Erweitert** weitere Einstellungen zur CRL vorgenommen werden.

Die Gültigkeit der CRL wird im Feld Gültigkeit CRL in Tagen angegeben. Standardmäßig ist eine CRL **30 Tage** gültig. Die CRL wird nicht automatisch verlängert.

Die automatische Verlängerung der CRL erfolgt mithilfe eines Abfrage mit Aktion-Objekts. Dazu ist es notwendig, dass im Feld CA-Kennwort anfordern, nicht die Option **Immer** gewählt wird. Ansonsten wird die Eingabe des CA-Kennworts für die Generierung der CA gefordert, was nicht automatisch erfolgen kann.

Wird ein Zertifikat zurückgezogen, wird die CRL grundsätzlich neu erzeugt.

Die CRL kann über das Feld CRL neu erzeugen manuell erzeugt werden. Es kann gewählt werden, ob die vorhandene **CRL neu signiert** oder komplett **neu aufgebaut** werden soll.

16.3 Im- und Export

16.3.1 Import von Zertifikaten und Dateien

Es gibt grundsätzlich zwei Möglichkeiten, um Dateien und Zertifikate hochzuladen. Zum einen können Dateien über die Zertifikat-Objekte einzeln und direkt hochgeladen werden. Zum anderen besteht die Möglichkeit mehrere Zertifikate gleichzeitig über den Zertifikatimport im Container: Zertifikate hochzuladen.

Zertifikat: Über den **Upload**-Link kann ein Zertifikat direkt in das Zertifikat-Objekt hochgeladen werden. Es werden die Formate DER, PEM, PKCS#7 und PKCS#12 akzeptiert. Ist der private Schlüssel in den Dateien enthalten, wird dieser ebenfalls mit hochgeladen. Die Werte im Zertifikat-Objekt werden mit den Werten des Zertifikats gefüllt. Die Statusanzeige ändert sich nach dem Hochladen auf **Zertifikat hochgeladen**. Ein zuvor hochgeladenes Zertifikat kann über den **Löschen**-Link entfernt werden.

Privater Schlüssel: Über den **Upload**-Link kann der private Schlüssel eines Zertifikats separat hochgeladen werden, wenn z.B. Zertifikat und privater Schlüssel in zwei verschiedenen Dateien zur Verfügung stehen. Es werden die Formate DER und PEM akzeptiert.

Zertifikat-Request: Über den **Upload**-Link kann ein Certificate Signing Request (CSR) hochgeladen werden. Ist der CSR mit einem Kennwort geschützt, wird dieses beim Upload abgefragt. Damit aus dem CSR ein Zertifikat erzeugt werden kann, muss zum einen im Feld CA ein CA-Zertifikat zum Signieren ausgewählt werden. Zum anderen muss bei Erstellung des Zertifikats die Option **CSR signieren** ausgewählt werden. Das Zertifikat wird über den Button **Übernehmen** erzeugt, ggf. wird beim Erzeugen das Kennwort der signierenden CA abgefragt. Nach dem erfolgreichen Signieren ändert sich die Statusanzeige zu **Zertifikat erzeugt** und das Zertifikat kann in verschiedenen Formaten heruntergeladen werden.

Beim Upload einer größeren Menge an Zertifikaten und CA-Zertifikaten, empfiehlt es sich, dies über den Zertifikatimport im Container: Zertifikate zu machen.

Sollen ganze Zertifikathierarchien importiert werden, ist zwingend zu beachten, dass die Stufen sukzessive von oben nach unten (root-to-end) importiert werden müssen. Andernfalls treten Fehler auf und der Import muss wiederholt werden, da eine nachträgliche Zuordnung von CA-Zertifikat zu Zertifikat nicht möglich ist.

Über den **Upload**-Link werden die Dateien für den Massenimport ausgewählt. Es werden die Formate DER, PEM, PKCS#7 und PKCS#12 unterstützt. Während des Importvorgangs wird automatisch ein Container **Upload** unterhalb des Container: Zertifikate angelegt, in dem die importierten Zertifikate gespeichert werden. Die Statusanzeige in den einzelnen Zertifikat-Objekten ändert sich zu **Zertifikat hochgeladen**.

Enthalten die zu importierenden Zertifikate kennwortgeschützte private Schlüssel, werden die Kennwörter während des Importvorgangs abgefragt. Der Massenimport kann mit einer zweispaltigen Liste im CSV-Format automatisiert werden, die folgende Voraussetzungen erfüllen muss:

- Die erste Spalte enthält die Namen der Zertifikatdateien ohne die Dateinamenserweiterung.
- Die zweite Spalte enthält die dazugehörigen Kennwörter.

Die CSV-Datei wird unter Kennwörter für Zertifikatimport hochgeladen.

16.3.2 Export von Zertifikaten und Dateien

Neben dem Import von Zertifikaten und Dateien steht auch ein Export dieser Dateien zur Verfügung,

Zertifikat: Über den **Download**-Link kann das signierte Zertifikat im DER-Format heruntergeladen werden.

Zertifikat als PKCS#7: Über den **Download**-Link kann das signierte Zertifikat im PKCS#7-Format heruntergeladen werden. Der PKCS#7-Standard wird genutzt, um verschlüsselte und signierte Daten mit den nötigen Zusatzinformationen in einer Datei zu speichern. Zusätzlich zum eigentlichen Zertifikat enthält das PKCS#7-Format noch das dazugehörige CA-Zertifikat. Bei einer Root-CA ist nur das CA-Zertifikat enthalten. Sollen die CA-Zertifikate nicht mit in der PKCS#7-Datei enthalten sein, muss auf dem Reiter **Erweitert** die Checkbox PKCS#7 ohne Stammzertifikate aktiviert werden.

Privater Schlüssel: Über den **Download**-Link kann der private Schlüssel heruntergeladen werden. Dies ist nur möglich, wenn das Zertifikat auf der TMA erstellt wurde. Wurde im Feld Schlüssel verschlüsselt abgelegen die Option **Nicht verschlüsseln** gewählt, wird der private Schlüssel unverschlüsselt heruntergeladen. Der private Schlüssel einer CA kann nicht einzeln heruntergeladen werden.

Zertifikat als PKCS#12: Über den **Download**-Link kann das Zertifikat im PKCS#12-Format heruntergeladen werden. Der PKCS#12-Standard wird genutzt, um den privaten Schlüssel mit dem zugehörigen Zertifikat kennwortgeschützt zu speichern. Zusätzlich zum privaten Schlüssel und dem Zertifikat sind alle Ausstellerzertifikate (CAs) des Zertifikats in der Datei enthalten. Das Kennwort der heruntergeladenen Datei entspricht dem Kennwort, das bei der Erstellung des Zertifikats festgelegt wurde.

Zertifikat-Request: Über den **Download**-Link kann ein Certificate Signing Request (CSR) heruntergeladen werden. Um einen CSR auf der TMA zu erzeugen, wird beim Anlegen des Zertifikat- oder CA-Zertifikat-Objekts im Feld Erstellung des Zertifikats die Option **CSR erzeugen** gewählt. Die anderen Parameter werden nach Bedarf und Einsatz entsprechend ausgefüllt. Mit dem Speichern des Konfigurationsobjekts wird ein Schlüsselpaar und ein CSR erzeugt. Die Statusanzeige ändert sich auf **CSR erzeugt**. Der CSR kann heruntergeladen und z.B. an eine externe CA zum Signieren gegeben werden. Das anschließend signierte Zertifikat kann über den **Upload**-Link im Feld Zertifikat in das Objekt hochgeladen werden.

Zertifikat als PEM: Über den **Download**-Link kann das Zertifikat base64-kodiert im PEM-Format heruntergeladen werden.

16.4 Externe Speicherung für Zertifikate und Schlüssel

Zertifikate und Schlüssel können extern auf Smartcards oder in Hardware Security Modulen (HSM) gespeichert werden.

16.4.1 Speicherung auf der Smartcard

Um ein Zertifikat auf einer Smartcard zu speichern, sind einige Vorbereitungen zu treffen.

Für das Ausrollen von Zertifikaten und Smartcards wird eine Middleware benötigt. Die Dateien der Middleware werden in einem Container: Software-Updates-Objekt hochgeladen. Anschließend

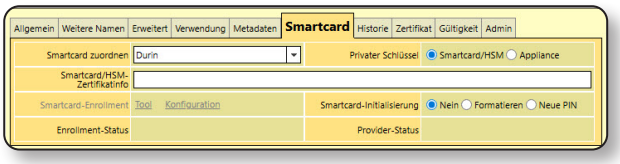


Abb. 16.07: *Zertifikat-Objekt - Reiter Smartcard*

können sie im Dienst: Smartcard-Enrollment unterhalb des ECOS Appliance-Objekts im Feld Smartcard DLLs ausgewählt werden. Der Dienst muss gestartet werden.

Im Zertifikat-Objekt muss auf dem Reiter **Allgemein** im Feld Zertifikat auf Smartcard/HSM speichern die Option **Smartcard** ausgewählt werden. Auf dem Reiter **Smartcard** wird unter Smartcard zuordnen die gewünschte Smartcard ausgewählt. Diese wird als Smartcard/Token-Objekt angelegt.

Unter Privater Schlüssel wird der Speicherort des privaten Schlüssels bestimmt. Wird der private Schlüssel auf der **Appliance** gespeichert, werden das Zertifikat und der private Schlüssel beim Enrollment nur auf die Smartcard kopiert. Bei Verlust oder Defekt der Smartcard ist ein Backup auf der Appliance vorhanden. Bei der Option **Smartcard/HSM** wird der private Schlüssel auf der Smartcard bzw. dem HSM erzeugt und auch nur dort gespeichert. Bei Verlust oder Defekt der Smartcard ist kein Backup des Schlüssels vorhanden.

Das Enrollment-Tool kann unter Smartcard-Enrollment heruntergeladen werden. Wurde das **Tool** bereits bei einem früheren Enrollment heruntergeladen und auf dem ausführenden PC gespeichert, kann auch nur die **Konfiguration** heruntergeladen und mit dem Enrollment-Tool geöffnet werden. Dazu muss das Enrollment-Tool im Programmordner des PCs gespeichert werden.

Wird eine Smartcard das erste Mal ausgerollt (Zero-PIN-Status) oder sollen die auf der Smartcard vorhandenen Zertifikate verlängert werden, muss unter Smartcard-Initialisierung **Nein** ausgewählt werden. Bei der Erstinitialisierung wird sowohl die PIN als auch die PUK für die Smartcard festgelegt. Sollen die Daten auf der Smartcard überschrieben werden, wird die Option **Formatieren** verwendet. Es wird eine neue PIN festgelegt. Die PUK, die bei der Erstinitialisierung festgelegt wurde, wird abgefragt. Die Option **Neue PIN** wird gewählt, um die PIN der Smartcard zu ändern. Alle anderen Daten bleiben unverändert. Zum Ändern der PIN über das Enrollment-Tool wird die alte PIN benötigt.

⚠ **Hinweis:** Die PIN lässt sich nachträglich ändern, die PUK nicht. Bewahren Sie die PUK daher sicher auf.

Zusätzlich muss der Smartcard-Reader, mit dem die Smartcards beschrieben werden, an dem PC angeschlossen sein, auf dem die Administrationsoberfläche der TMA geöffnet ist.

Soll das Zertifikat auf eine andere Smartcard geschrieben werden, muss unter Erstellung des Zertifikats die Option **Erneut kopieren** gewählt werden. Anschließend kann der Enrollment-Prozess erneut gestartet werden, vorausgesetzt der private Schlüssel wurde auf der TMA erzeugt.

Treten beim Enrollment-Vorgang Fehler auf oder wird der Vorgang nicht korrekt abgeschlossen, kann der Status des Zertifikats mit der Option **Status löschen** im Feld Erstellung des Zertifikats wieder gelöscht werden und das Enrollment erneut gestartet werden. Diese Option dient nicht zum Löschen oder Zurückziehen eines Zertifikats.

16.4.2 Speicherung auf einem HSM

Ein Hardware Security Modul (HSM) dient zum sicheren Ausführen von kryptografischen Operationen und Speichern von privaten Schlüsseln.

Im Zertifikat-Objekt wird unter Zertifikat auf Smartcard/HSM speichern die Option **HSM** gewählt. Auf dem Reiter **Smartcard** muss ein HSM-Token-Objekt im Feld HSM Slot zuordnen ausgewählt werden.

16.4.2.1 Anbinden eines HSM

In VS-NfD-Umgebungen wird für den Schutz von CA-Schlüsseln der Einsatz eines zugelassenen HSM empfohlen. Dabei sind die jeweils geltenden sicherheitstechnischen Anforderungen an kryptographische Module zu berücksichtigen. Die Generierung und Speicherung von Schlüsseln kann alternativ auch auf der Appliance erfolgen, sofern die geltenden Sicherheitsanforderungen nichts anderes bestimmen.

Zur Anbindung des HSM wird im Container: Smartcards & Token ein Konfigurationsobjekt vom Typ HSM angelegt. Folgende Parameter müssen konfiguriert werden:

HSM: Hier wird der Hersteller ausgewählt.

Crypto-Serveradresse: Hier wird die Adresse des HSM angegeben (z.B. **3002@10.161.200.92**)

HSM-Authentisierungsschlüssel: Hier wird der Authentisierungsschlüssels für den Zugriff auf das HSM angegeben.

Nach Abschluss der Konfiguration kann das HSM im CA-Zertifikat im Reiter **Smartcard** unter HSM-Slot zuordnen ausgewählt werden.

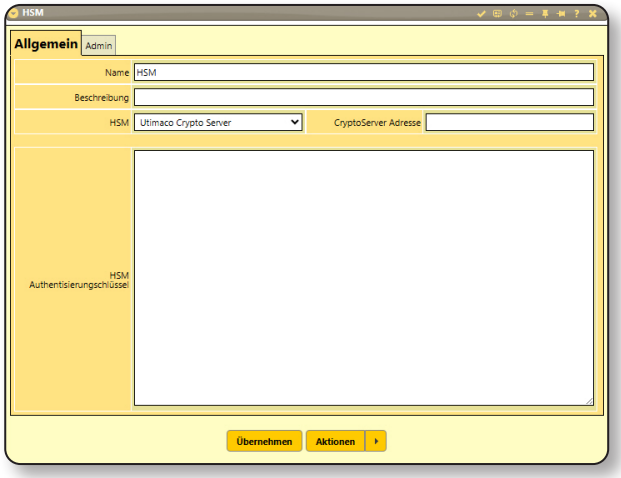


Abb. 16.08: *Konfiguration eines HSM*

17 Zertifikat-Enrollment mit Standardprotokollen

Für das Zertifikat-Enrollment gibt es unterschiedliche Standardprotokolle. Die TMA unterstützt aktuell vier Standardprotokolle für das Zertifikat-Enrollment: ACME, CMP, EST und SCEP. Das Prinzip dieser Protokolle in Bezug auf das Zertifikat-Enrollment ist das gleiche.

Ein Gerät erzeugt ein Schlüsselpaar und nutzt eines der Enrollment-Protokolle, um eine Zertifikatanfrage (CSR) an die TMA und ihren entsprechenden Protokoll-Server zu senden. Der Server nimmt den CSR entgegen und gleicht die Attribute ggf. mit definierten Richtlinien ab. Stimmen die Attribute überein, wird die Anfrage an die Zertifizierungsstelle (CA) weitergeleitet und signiert. Anschließend wird das Zertifikat an das Gerät zurückgesendet.

Stimmen die Attribute nicht überein, wird die Anfrage abgelehnt.

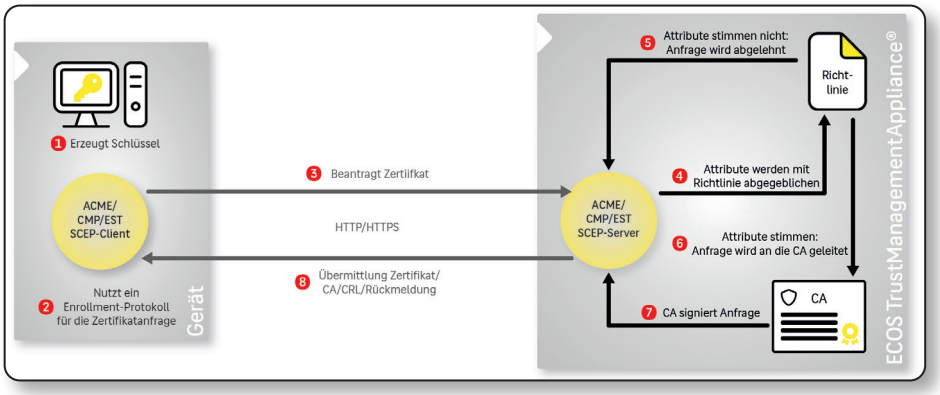


Abb. 17.01: *Ablauf des Zertifikat-Enrollments*

Die TMA kann auf zwei Arten genutzt werden. Zum einen kann die TMA als Zertifizierungsstelle fungieren, bei der Clients, Geräte und Dienste Zertifikate anfragen. Zum anderen fragt die TMA als Client Zertifikate bei einer anderen Zertifizierungsstelle an und verteilt diese weiter an die eigentlichen Endgeräte.

Für jedes Enrollment-Protokoll gibt es folgende Objekte:

- ein Server-Objekt
- ein Providerkonto
- ein Abonnentenkonto

Je nach Einsatz werden für das automatische Enrollment unterschiedliche Objekte benötigt:

TMA als Zertifizierungsstelle	TMA als Client
Server-Objekt	Providergruppe
Abonnentengruppe	Providerkonto
Abonntenkonto	Externes CA-Zertifikat
CA-Abonnentenverknüpfung	
CA-Zertifikat	

17.1 Die TMA als Zertifizierungsstelle

Die TMA fungiert als Zertifizierungsstelle mit eigenen CA-Zertifikaten. Für das Zertifikat-Enrollment werden bestimmte Objekte benötigt. Abhängig vom Protokoll muss ein entsprechender Server-Dienst und ein Container: Abonnentengruppe angelegt werden. In dem Container werden die Abonnen-

tenkonten angelegt. Dies kann entweder automatisch während des Enrollment-Vorgangs erfolgen oder durch Import vor dem Enrollment.

17.1.1 Vorbereitungen

Unabhängig vom Protokoll müssen einige Vorbereitungen getroffen werden. Dazu zählen die Erzeugung und Konfiguration eines CA-Zertifikats zur Signierung der Client-Zertifikate, eines TLS-Server-Zertifikats für den Dienst und eines Zielcontainers für die Zertifikate.

17.1.1.1 CA-Zertifikat zum Signieren der Client-Zertifikate

Bei der Ersteinrichtung werden ein Root- und ein Sub-CA-Zertifikat über den Assistenten angelegt (siehe **1.4.4.1 Root-CA erstellen**). Es empfiehlt sich, das Signer-CA Zertifikat für das Signieren der Client-Zertifikate zu nutzen.

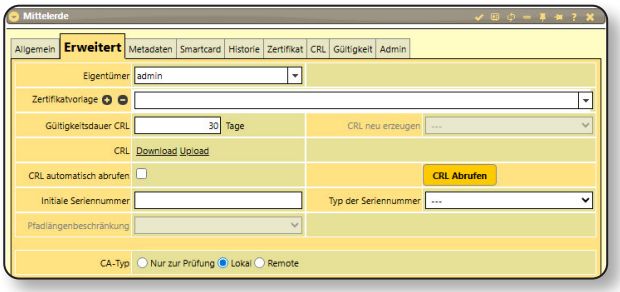


Abb. 17.02: *CA-Zertifikat - CA-Typ bestimmen*

Soll ein anderes CA-Zertifikat zum Signieren genutzt werden, kann dies über die Standardoberfläche erzeugt werden (siehe **5.1.2 Eigenes CA-Zertifikat erstellen**). Dabei ist zu beachten, dass im Feld CA-Kennwort abfragen die Option **Nie** ausgewählt wird, da ansonsten die automatische Zertifikaterstellung nicht möglich ist.

In der Expertenansicht werden neue CA-Zertifikate über das Kontextmenü im Navigationsbaum **Neu → Zertifikate & Smartcards → CA-Zertifikat** angelegt.

Auf dem Reiter **Erweitert** muss der CA-Typ auf **Lokal** stehen.

17.1.1.2 TLS-Server-Zertifikat für den Server-Dienst

Das TLS-Server-Zertifikat wird für die Authentisierung des Enrollment-Servers gegenüber dem Client benötigt. Für die Enrollment-Protokolle CMP und SCEP ist ein TLS-Server-Zertifikat optional.

Bei der Ersteinrichtung wird für jeden konfigurierten PKI-Dienst ein entsprechendes TLS-Server-Zertifikat über den Assistenten erzeugt (siehe **1.4.4 PKI-Dienste einrichten**).

Wird ein neues Zertifikat benötigt, kann dies über die Standardoberfläche erzeugt werden (siehe **5.3.2 Eigenes Zertifikat erstellen**). Dabei ist zu beachten, dass als Verwendungszweck die Option **TLS-Server** ausgewählt wird.



Abb. 17.03: *TLS-Serverzertifikat - Verwendungszweck*

In der Expertenansicht werden neue Zertifikate über das Kontextmenü im Navigationsbaum **Neu → Zertifikate & Smartcards → Zertifikat** angelegt.

Damit der Server sich beim Client mit diesem Zertifikat authentisieren kann, muss der Client dem CA-Zertifikat, das das TLS-Server-Zertifikat signiert hat, vertrauen.

17.1.1.3 Container: Abonnentengruppe anlegen

In einem Container: Abonnentengruppe werden die einzelnen Abonnentenkonten zusammengefasst. Abonnentenkonten dienen dazu Zugangsdaten und Authentisierungsmethoden für die Zielsysteme zu verwalten. Für jedes Zielsystem wird ein eigenes Abonnentenkonto benötigt. In den Abonnentenkonten werden die Zertifikate für das jeweilige Zielsystem zusammengefasst.

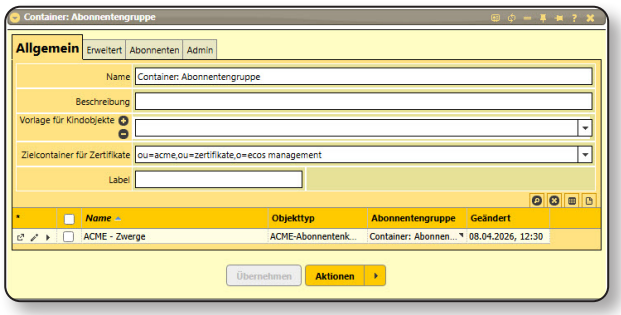


Abb. 17.04: *Container: Abonnentengruppe - Reiter Allgemein*

Werden mehrere Protokolle für das Enrollment genutzt, empfiehlt es sich, für jedes Protokoll einen eigenen Container anzulegen. Der Container: Abonnentengruppe wird unterhalb des Container: PKI-Management angelegt.

17.1.1.4 Zielcontainer für Zertifikate anlegen

Bei der Ersteinrichtung wird für jeden PKI-Dienst, der konfiguriert wird, automatisch ein Container für Zertifikate unterhalb des Container: Zertifikate angelegt.

Manuell kann ein neuer Container für Zertifikate über das Containermenü in der Standardoberfläche angelegt werden (siehe **2.4 Container-Menü**).

Über die Expertenansicht werden neue Container über das Kontextmenü im Navigationsbaum **Neu → Allgemein → Container** angelegt.

Der Zielcontainer für Zertifikate kann in verschiedenen Objekten zugeordnet werden. Die Zuordnungen werden in folgender Reihenfolge hierarchisch behandelt:

1. Abonnentenkonto
2. Abonnentengruppe
3. Server

Der Zielcontainer für Container muss in einem der genannten Objekte bestimmt werden. Wird er in mehreren Objekten konfiguriert, werden die Zertifikate entsprechend der Hierarchie gespeichert.

17.1.1.5 CA-Abonnentenverknüpfung

Damit die Zertifikate von der richtigen CA signiert werden, muss die CA den Abonnentenkonten des Enrollment-Diensts zugeordnet werden. Dazu wird das Objekt CA-Abonnentenverknüpfung benötigt. Dieses wird im Container: PKI-Management angelegt.

In der Tabelle CA-Abonnentenverknüpfung wird die CA der Abonnentengruppe zugeordnet und das entsprechende Protokoll aktiviert. Eine Abonnentengruppe kann mehrere Abonnentenkonten beinhalten. Für jedes dieser Konten signiert die zugeordnete CA die Zertifikate. Zusätzlich wird festgelegt, in welchem Zeitraum die CA die Zertifikate signiert. Dazu werden die Felder Gültig von und

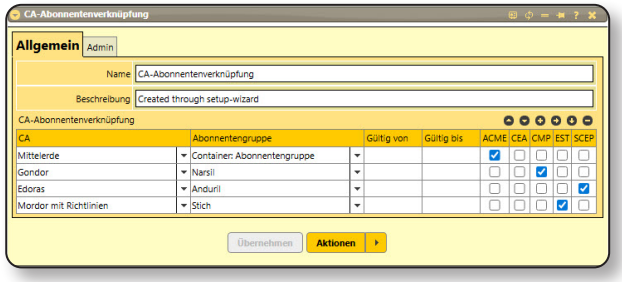


Abb. 17.05: *CA-Abonnentenverknüpfung*

Gültig bis konfiguriert. So kann der Übergang zu einer neuen CA, z.B. rechtzeitig vor Ablauf des CA-Zertifikats, automatisch erfolgen.

17.1.2 Zertifikat-Enrollment mit ACME

Das Automatic Certificate Management Environment (ACME) ist ein Protokoll zur Automatisierung des Enrollments von Webserverzertifikaten. Über den ACME-Dienst kann ein Client ein Zertifikat oder andere zertifikatbezogene Funktionen anfordern.

Für das interne ACME-Enrollment werden zusätzlich zu den oben angelegten Objekten, folgende Objekte benötigt:

- Dienst: ACME-Server
- ACME-Abonnentenkonto

17.1.2.1 Dienst: ACME-Server anlegen

Wurde der Dienst: ACME-Server nicht über den Einrichtungsassistenten angelegt und konfiguriert, kann er manuell im Expertenmodus unter **ECOS Appliance → Container: Dienste** über das Kontextmenü angelegt werden.

Reiter Allgemein:

Für die Nutzung des Dienst: ACME-Server muss eine Server-Adresse und Port definiert werden. Als Server-Adresse wird in der Regel die LAN-Adresse der TMA genutzt. Diese ist als Netzwerk-Interface im Container: Interfaces konfiguriert. Es können auch andere Server-Adressen gewählt werden. Sie müssen vorher entweder als Netzwerk-Interface oder Def.: Host-Name auf der TMA konfiguriert werden.

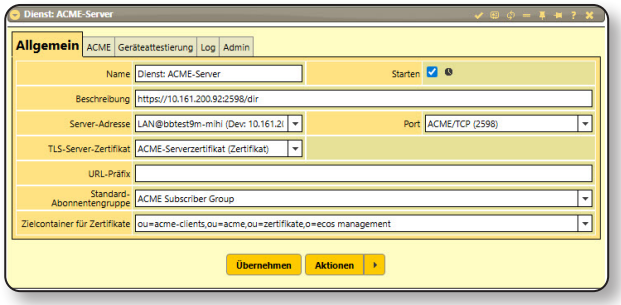


Abb. 17.06: *Dienst: ACME-Server - Reiter Allgemein*

Es muss ein Port verwendet werden, an dem keine andere Instanzen der ECOS Appliance lauschen, um Konflikte zu vermeiden.

Im Feld TLS-Server-Zertifikat wird das Zertifikat-Objekt ausgewählt, dass entweder manuell oder über den Ersteinrichtungsassistenten angelegt wurde, ausgewählt. Es sichert die HTTPS-Verbindung des Servers ab. Voraussetzung dafür ist, dass der Client dem Zertifikat bzw. dem CA-Zertifikat, das das TLS-Server-Zertifikat signiert hat, vertrauen muss.

Ist der Server von außen erreichbar, wird der Name als URL-Präfix angegeben. Bleibt das Feld leer, wird der Präfix aus Hostname/IP und Port abgeleitet. In der Serverkonfiguration muss /dir als Einstiegspunkte gewählt werden, es muss nicht als Teil des URL-Präfix angegeben werden.

Unter Standard-Abonnentengruppe wird der Container: Abonnentengruppe ausgewählt, in der die einzelnen ACME-Abonnentenkonto-Objekte automatisch angelegt werden sollen. Sie werden damit automatisch auch einer CA zugeordnet, die in der CA-Abonnentenverknüpfung der Abonnentengruppe zugeordnet wurde.

Sollen einzelne Konten anderen CAs zugeordnet werden, müssen sie vorher angelegt und mit dem verpflichtenden Account-Binding (External Account Binding, EAB) aktiviert oder nachträglich verschoben werden. Der Server kann Account-Binding verpflichtend verlangen. Ist das Account-Binding nicht verpflichtend, kann der Client trotzdem ein Account-Binding machen. Dadurch ist es möglich, dass das Abonnentenkonto für den Client nicht in der Standard-Abonnentengruppe landet. Er hat eventuell vordefinierte Autorisierungen und muss für vorauthentisierte Bezeichner keine Challenges erfüllen.

Im Dienst-Objekt kann der Zielcontainer für Zertifikate ausgewählt werden.

Der Dienst startet durch Aktivieren der Checkbox Starten. Im Reiter **Log** können Informationen zum Dienst eingesehen werden.

Der Dienst ist anschließend unter dem Pfad https://<ip-adresse>:<port>/.well-known/acme erreichbar.

Reiter ACME:

Auf diesem Reiter können zusätzliche Einstellungen für den ACME-Server vorgenommen werden. Dazu zählen neben dem Log-Level für die Fehlersuche, auch der Webserver-FQDN, ein DNS-Server für DNS-Challenges, die TOS-URL für die Nutzungsbedingungen (Terms of Service) oder die Webseite des Betreibers. Die Informationen werden im Serververzeichnis eingetragen.

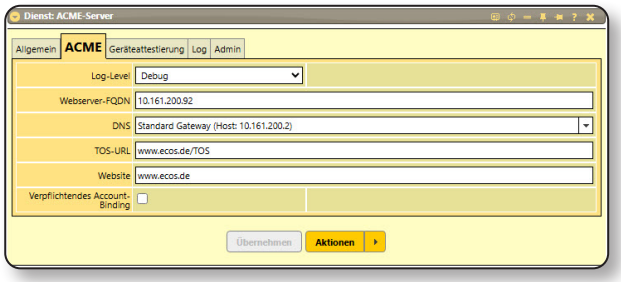


Abb. 17.07: *Dienst: ACME-Server - Reiter ACME*

Sollen sich nur Geräte anmelden, die dem System bekannt sind, dann muss auf diesem Reiter die Checkbox Verpflichtendes Account-Binding aktiviert werden.

Beim verpflichtenden Account-Binding akzeptiert der ACME-Server der TMA ausschließlich Anmeldungen von Konten, die zuvor ein Geheimnis in Form eines symmetrischen Schlüssels mit einem zugehörigen Identifier erhalten haben.

Für das verpflichtende Account-Binding müssen zusätzlich Einstellungen im ACME-Abonnentenkonto vorgenommen werden.

17.1.2.2 ACME-Abonnentenkonto anlegen

Mit dem ACME-Abonnentenkonto werden Zugangsdaten für das ACME-Enrollment-Protokoll konfiguriert. Für jedes Zielgerät wird ein Abonnentenkonto empfohlen.

Über den Ersteinrichtungsassistenten kann ein Beispielkonto angelegt werden.

Das ACME-Abonnentenkonto muss nicht manuell angelegt werden. Während des Enrollment-Vorgangs werden die Abonnentenkonten automatisch in der im Dienst-Objekt des Protokoll-Servers ausgewählten Container: Abonnentengruppe erzeugt.

Wird im Dienst: ACME-Server auf dem Reiter **ACME** die Option **Verpflichtendes Account-Binding** aktiviert, muss für jedes Gerät ein ACME-Abonnentenkonto vor dem Enrollment manuell unter **ECOS Appliance → Container: PKI-Management → Container: Abonnentengruppe → Neu** angelegt werden.

Reiter Allgemein:

Wird ein Zielcontainer für Zertifikate ausgewählt, wird dieser beim Speichern von Zertifikaten bevorzugt behandelt.

Im Feld Abonnentengruppe wird der Container: Abonnentengruppe ausgewählt, in dem das ACME-Abonnentenkonto gespeichert wird. Durch Ändern des Container: Abonnentengruppe wird das Abonnentenkonto verschoben. Alternativ kann das Objekt über den Navigationsbaum per Drag and Drop verschoben werden.

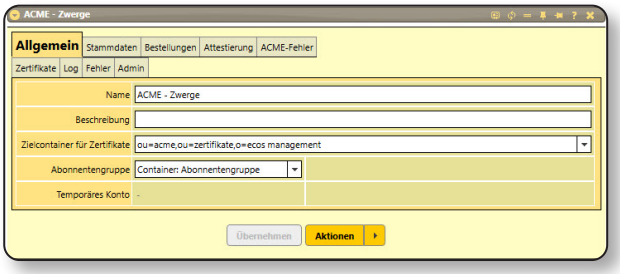


Abb. 17.08: *ACME-Abonnentenkonto - Reiter Allgemein*

Reiter Stammdaten:

Bei der Verwendung von Account-Binding, muss im ACME-Abonnentenkonto unter Externer Schlüssel der Symmetrische Schlüssel für die Kommunikation mit dem ACME-Server ausgewählt werden. Zusätzlich muss der Kontostatus auf **Bereit zur Anmeldung** stehen. Diese Einstellungen müssen konfiguriert werden, wenn der ACME-Server das Account Binding verlangt. Ist es nicht verpflichtend, sind die Angaben optional. Werden sie definiert, wird Account-Binding gemacht.

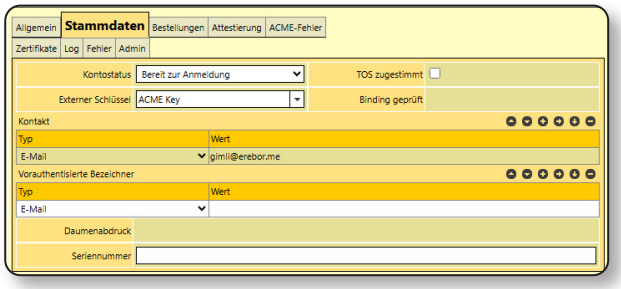


Abb. 17.09: *ACME-Abonnentenkonto - Reiter Stammdaten*

Wird Account-Binding gemacht, können Vorautorisierte Bezeichner bestimmt werden. Sie müssen nicht weiter autorisiert werden.

Reiter Bestellungen:

Dieser Reiter zeigt Informationen über die Bestellungen und Challenges des ACME-Abonnentenkonto angezeigt. Es können keine Änderungen der Informationen über diesen Reiter **vorgenommen** werden.

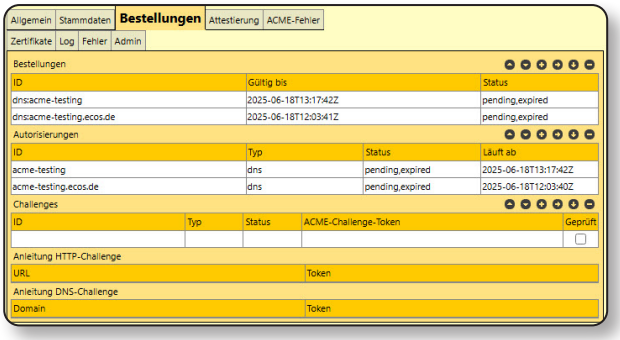


Abb. 17.10: *ACME-Abonnentenkonto - Reiter Bestellungen*

Reiter ACME-Fehler:

In der Fehleranzeige werden die vom Server übermittelten Fehlermeldungen angezeigt. Sie können über die Checkbox Zurücksetzen zurückgesetzt werden. Ebenso ist es möglich, die Bestellungen/ Autorisierungen zurückzusetzen.

Reiter Zertifikate:

Auf diesem Reiter werden alle Zertifikate aufgelistet, die für dieses Abonnentenkonto angefragt und ausgestellt wurden.

17.1.3 Zertifikat-Enrollment mit CMP

Das Certificate Management Protocol (CMP) wird für die Verwaltung von Zertifikaten genutzt. Es regelt die Kommunikation zwischen Clients und Komponenten der PKI. Das Protokoll selbst ist sehr umfangreich. In der TMA ist nur eine leichtgewichtige Variante des Protokolls implementiert.

Für das interne CMP-Enrollment werden zusätzlich zu den oben angelegten Objekten, folgende Objekte benötigt:

- Dienst: CMP-Server
- CMP-Abonnentenkonto

17.1.3.1 Dienst: CMP-Server anlegen

Wurde der Dienst: CMP-Server nicht über den Einrichtungsassistenten angelegt und konfiguriert, kann er manuell im Expertenmodus unter **ECOS Appliance → Container: Dienste** über das Kontextmenü angelegt werden.

Reiter Allgemein:

Für die Nutzung des Dienst: CMP-Server kann eine Server-Adresse und Port definiert werden. Als Server-Adresse wird in der Regel die LAN-Adresse der TMA genutzt. Diese ist als Netzwerk-Interface im Container: Interfaces konfiguriert. Es können auch andere Server-Adressen gewählt werden. Sie müssen vorher entweder als Netzwerk-Interface oder Def.: Host-Name auf der TMA konfiguriert werden. Der CMP-Server lauscht nur an der hier angegeben Adresse. Bleiben die Felder leer, hört der CMP-Server an allen Adressen.

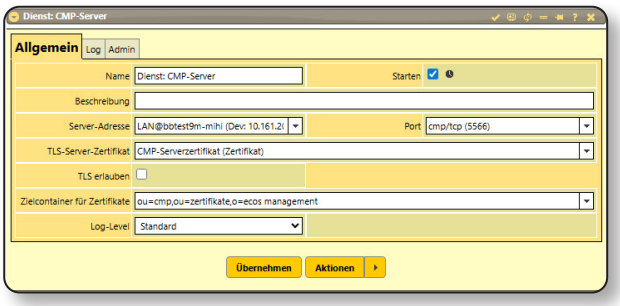


Abb. 17.11: *Dienst: CMP-Server - Reiter Allgemein*

Es muss ein Port verwendet werden, an dem keine andere Instanzen der ECOS Appliance lauschen, um Konflikte zu vermeiden.

Im Feld TLS-Server-Zertifikat wird das Zertifikat-Objekt ausgewählt, dass entweder manuell oder über den Ersteinrichtungsassistenten angelegt wurde, ausgewählt. Es sichert die HTTPS-Verbindung des Servers ab. Voraussetzung dafür ist, dass der Client dem Zertifikat bzw. dem CA-Zertifikat, das das TLS-Server-Zertifikat signiert hat, vertrauen muss.

Wird die Checkbox TLS erlauben aktiviert, wird zusätzlich die TLS-Verschlüsselung genutzt. Dafür muss ein TLS-Port ausgewählt bzw. angelegt werden. Es muss ein Port verwendet werden, an dem keine andere Instanzen der ECOS Appliance lauschen, um Konflikte zu vermeiden.

Im Dienst-Objekt kann der Zielcontainer für Zertifikate ausgewählt werden.

Der Dienst startet durch Aktivieren der Checkbox Starten. Im Reiter **Log** können Informationen zum Dienst eingesehen werden.

Der Dienst ist anschließend unter dem Pfad https://<ip-adresse>:<port>/.well-known/cmp erreichbar.

17.1.3.2 CMP-Abonnentenkonto anlegen

Für jedes Gerät, dass ein Zertifikat braucht, wird ein eigenes CMP-Abonnentenkonto benötigt. Diese können z.B. über die API oder eine Verzeichnissynchronisation, z.B. mit einer CSV-Datei, auf der TMA angelegt werden. Die meisten Einstellungen können über die Synchronisation vorgegeben werden.

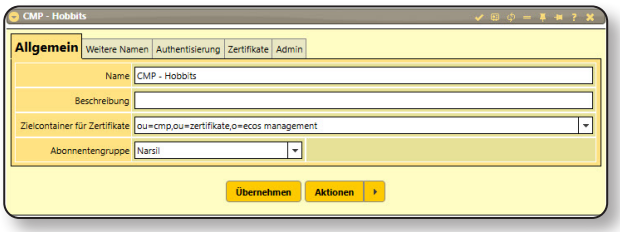


Abb. 17.12: *CMP-Abonnentenkonto - Reiter Allgemein*

Reiter Weitere Namen:

Hier können zusätzliche Informationen zum Zertifikat angegeben werden. Diese alternativen Namen, auch Subject Alternative Name (SAN) genannt, können zusätzlich oder anstelle der Identität im Subjektfeld des Zertifikats angegeben werden, z.B. wenn ein Server mehrere Namen hat. Diese Informationen werden in den Zertifikaten hinterlegt, die mit dem Abonnentenkonto bestellt werden. Werden SANs durch den CSR eingereicht, haben die hier angegebenen SANs Vorrang. Sie entsprechen denen im Zertifikat-Objekt auf dem Reiter **Weitere Namen**.

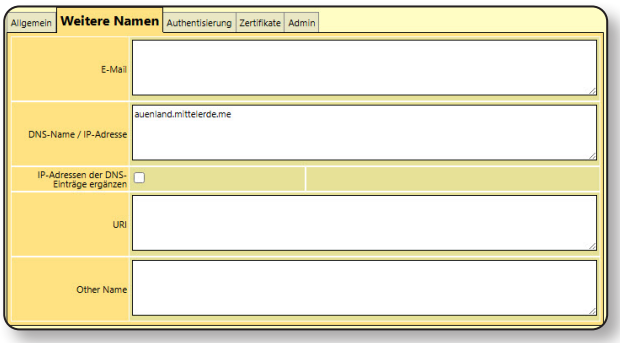


Abb. 17.13: *CMP-Abonnentenkonto - Reiter Weitere Namen*

Reiter Authentisierung:

Damit sich das Abonnentenkonto beim entsprechenden Server-Dienst anmelden kann, muss mindestens eine Authentisierungsmethode konfiguriert werden.

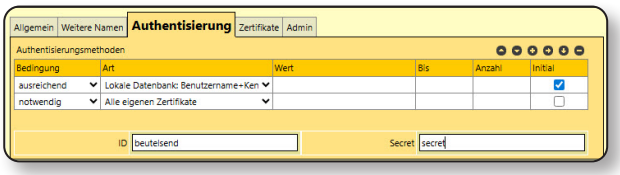


Abb. 17.14: *CMP-Abonnentenkonto - Reiter Authentisierung*

In der Spalte Bedingung wird festgelegt, ob die jeweilige Authentisierungsmethode für die Anmeldung **notwendig** bzw. **ausreichend** ist oder **ignoriert** wird. Für eine erfolgreiche Anmeldung müssen *alle* notwendigen Bedingungen erfüllt sein. Wurden ausreichende Bedingungen definiert, muss *eine* dieser Bedingungen für die Anmeldung erfüllt sein. Wurden sowohl notwendige als auch ausreichende Authentisierungsmethoden konfiguriert, müssen *alle notwendigen*, die vor der ersten ausreichenden Bedingung stehen, und *mindestens eine ausreichende* Bedingung erfüllt sein, damit die Anmeldung erfolgreich ist. Authentisierungsmethoden, die als ignorieren eingestuft sind, werden bei der Anmeldung nicht berücksichtigt.

Standardmäßig sind die Authentisierungsmethoden **Lokale Datenbank: Benutzername+Kennwort** als ausreichend und die Methode **Alle eigenen Zertifikate** als notwendig konfiguriert. Durch die aktivierte Checkbox Initial ist es möglich, dass diese Authentisierungsmethode nur bei der ersten Anmeldung mit ID und Secret erfolgt. Jede weitere Anmeldung erfordert ein Zertifikat dieses Abonnenten (siehe **15 Benutzerverwaltung (Experte)**).

In der Spalte Bis kann ein Datum eingetragen werden, bis wann die Authentisierungsmethode gültig ist und genutzt werden kann. Es kann ein Datum mit Uhrzeit im Format TT.MM.JJJJ hh:mm angegeben werden. Nach Ablauf ist die Anmeldung mit dieser Methode nicht mehr möglich.

Die Zahl der Anmeldeversuche kann in der Spalte Anzahl festgelegt werden. Sie bestimmt, wie oft diese Authentisierungsmethode zur Anmeldung genutzt werden kann. Dabei zählen sowohl erfolgreiche als auch fehlgeschlagene Anmeldeversuche. Ist die Anzahl erreicht, ist die Anmeldung mit dieser Methode nicht mehr möglich.

Der Benutzername (ID) muss eindeutig sein. Diese können entweder manuell bestimmt oder über die Verzeichnissynchronisation importiert werden.

Grundsätzlich können auch die anderen Methoden zur Authentisierung benutzt werden.

Wird die Checkbox Nur Lesezugriff aktiviert, erhält der Abonnent nur lesend Zugriff auf die Zertifikate. Er kann keine neuen Zertifikate anlegen oder bestehende ändern.

Reiter Zertifikat:

Auf diesem Reiter werden alle Zertifikate aufgelistet, die für dieses Abonnentenkonto angefragt und ausgestellt wurden.

17.1.4 Zertifikat-Enrollment mit EST

Das Enrollment over Secure Transport-Protokoll (EST) dient zum automatischen Ausstellen von Zertifikaten. Über den EST-Dienst kann ein Client Zertifikate und andere zertifikatbezogene Funktionen anfordern.

Für das interne EST-Enrollment werden zusätzlich zu den oben angelegten Objekten, folgende Objekte benötigt:

- Dienst: EST-Server
- EST-Abonnentenkonto

17.1.4.1 Dienst: EST-Server anlegen

Wurde der Dienst: EST-Server nicht über den Einrichtungsassistenten angelegt und konfiguriert, kann er manuell im Expertenmodus unter **ECOS Appliance → Container: Dienste** über das Kontextmenü angelegt werden.

Reiter Allgemein:

Für die Nutzung des Dienst: EST-Server muss eine Server-Adresse und Port definiert werden. Als Server-Adresse wird in der Regel die LAN-Adresse der TMA genutzt. Diese ist als Netzwerk-Interface im Container: Interfaces konfiguriert. Es können auch andere Server-Adressen gewählt werden. Sie müssen vorher entweder als Netzwerk-Interface oder Def.: Host-Name auf der TMA konfiguriert werden. Der EST-Server lauscht nur an der hier angegeben Adresse. Bleiben die Felder leer, hört der EST-Server an allen Adressen.

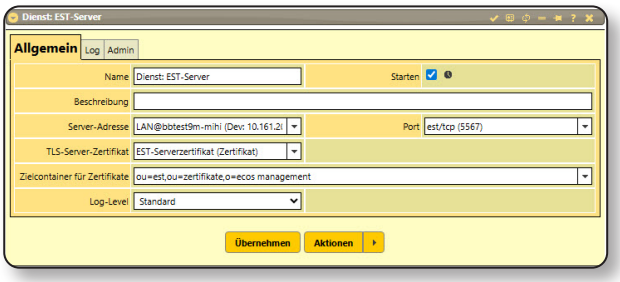


Abb. 17.15: *Dienst: EST-Server - Reiter Allgemein*

Es muss ein Port verwendet werden, an dem keine andere Instanzen der ECOS Appliance lauschen, um Konflikte zu vermeiden.

Im Feld TLS-Server-Zertifikat wird das Zertifikat-Objekt ausgewählt, dass entweder manuell oder über den Ersteinrichtungsassistenten angelegt wurde, ausgewählt. Es sichert die HTTPS-Verbindung des Servers ab. Voraussetzung dafür ist, dass der Client dem Zertifikat bzw. dem CA-Zertifikat, das das TLS-Server-Zertifikat signiert hat, vertrauen muss.

Im Dienst-Objekt kann der Zielcontainer für Zertifikate ausgewählt werden.

Der Dienst startet durch Aktivieren der Checkbox Starten. Im Reiter **Log** können Informationen zum Dienst eingesehen werden.

Der Dienst ist anschließend unter dem Pfad https://<ip-adresse>:<port>/.well-known/est erreichbar.

17.1.4.2 EST-Abonnentenkonto anlegen

Für jedes Gerät, dass ein Zertifikat braucht, wird ein eigenes EST-Abonnentenkonto benötigt. Diese können z.B. über die API oder eine Verzeichnissynchronisation, z.B. mit einer CSV-Datei, auf der TMA angelegt werden. Die meisten Einstellungen können über die Synchronisation vorgegeben werden.

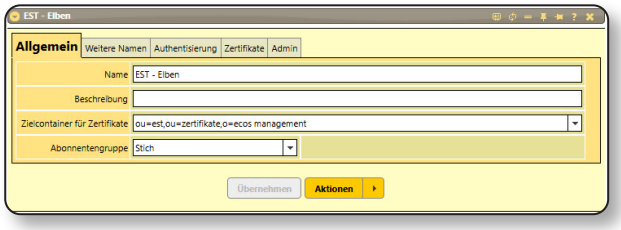


Abb. 17.16: *EST-Abonnentenkonto - Reiter Allgemein*

Reiter Weitere Namen:

Hier können zusätzliche Informationen zum Zertifikat angegeben werden. Diese alternativen Namen, auch Subject Alternative Name (SAN) genannt, können zusätzlich oder anstelle der Identität im Subjektfeld des Zertifikats angegeben werden, z.B. wenn ein Server mehrere Namen hat. Diese Informationen werden in den Zertifikaten hinterlegt, die mit dem Abonnentenkonto bestellt werden. Werden SANs durch den CSR eingereicht, haben die hier angegebenen SANs Vorrang. Sie entsprechen denen im Zertifikat-Objekt auf dem Reiter **Weitere Namen**.

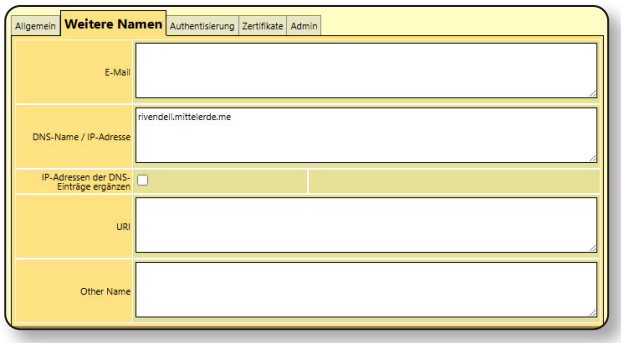


Abb. 17.17: *EST-Abonnentenkonto - Reiter Weitere Namen*

Reiter Authentisierung:

Damit sich das Abonnentenkonto beim entsprechenden Server-Dienst anmelden kann, muss mindestens eine Authentisierungsmethode konfiguriert werden.

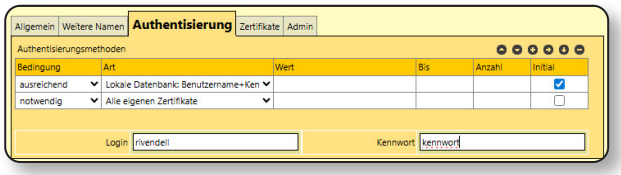


Abb. 17.18: *EST-Abonnentenkonto - Reiter Authentisierung*

In der Spalte Bedingung wird festgelegt, ob die jeweilige Authentisierungsmethode für die Anmeldung **notwendig** bzw. **ausreichend** ist oder **ignoriert** wird. Für eine erfolgreiche Anmeldung müssen *alle* notwendigen Bedingungen erfüllt sein. Wurden ausreichende Bedingungen definiert, muss *eine*

dieser Bedingungen für die Anmeldung erfüllt sein. Wurden sowohl notwendige als auch ausreichende Authentisierungsmethoden konfiguriert, müssen *alle notwendigen*, die vor der ersten ausreichenden Bedingung stehen, und *mindestens eine ausreichende* Bedingung erfüllt sein, damit die Anmeldung erfolgreich ist. Authentisierungsmethoden, die als ignorieren eingestuft sind, werden bei der Anmeldung nicht berücksichtigt.

Standardmäßig sind die Authentisierungsmethoden **Lokale Datenbank: Benutzername+Kennwort** als ausreichend und die Methode **Alle eigenen Zertifikate** als notwendig konfiguriert. Durch die aktivierte Checkbox Initial ist es möglich, dass diese Authentisierungsmethode nur bei der ersten Anmeldung mit Login und Kennwort erfolgt. Jede weitere Anmeldung erfordert ein Zertifikat dieses Abonnenten (siehe **15 Benutzerverwaltung (Experte)**).

In der Spalte Bis kann ein Datum eingetragen werden, bis wann die Authentisierungsmethode gültig ist und genutzt werden kann. Es kann ein Datum mit Uhrzeit im Format TT.MM.JJJJ hh:mm angegeben werden. Nach Ablauf ist die Anmeldung mit dieser Methode nicht mehr möglich.

Die Zahl der Anmeldeversuche kann in der Spalte Anzahl festgelegt werden. Sie bestimmt, wie oft diese Authentisierungsmethode zur Anmeldung genutzt werden kann. Dabei zählen sowohl erfolgreiche als auch fehlgeschlagene Anmeldeversuche. Ist die Anzahl erreicht, ist die Anmeldung mit dieser Methode nicht mehr möglich.

Der Benutzername (Login) muss eindeutig sein. Diese können entweder manuell bestimmt oder über die Verzeichnissynchronisation importiert werden.

Grundsätzlich können auch die anderen Methoden zur Authentisierung benutzt werden.

Wird die Checkbox Nur Lesezugriff aktiviert, erhält der Abonnent nur lesend Zugriff auf die Zertifikate. Er kann keine neuen Zertifikate anlegen oder bestehende ändern.

Reiter **Zertifikat**:

Auf diesem Reiter werden alle Zertifikate aufgelistet, die für dieses Abonnentenkonto angefragt und ausgestellt wurden.

17.1.5 Zertifikat-Enrollment mit SCEP

Das Simple Certificate Enrollment-Protokoll (SCEP) dient zum sicheren Ausrollen und Verlängern von Zertifikaten für eine große Anzahl von Netzwerkgeräten. Über den SCEP-Dienst kann ein Client Zertifikate oder andere zertifikatbezogene Funktionen anfordern.

Für das interne SCEP-Enrollment werden zusätzlich zu den oben angelegten Objekten, folgende Objekte benötigt:

- Dienst: SCEP-Server
- SCEP-Abonnentenkonto

17.1.5.1 Dienst: SCEP-Server anlegen

Wurde der Dienst: SCEP-Server nicht über den Einrichtungsassistenten angelegt und konfiguriert, kann er manuell im Expertenmodus unter **ECOS Appliance → Container: Dienste** über das Kontextmenü angelegt werden.

Reiter Allgemein:

Für die Nutzung des Dienst: SCEP-Server muss eine Server-Adresse und Port definiert werden. Als Server-Adresse wird in der Regel die LAN-Adresse der TMA genutzt. Diese ist als Netzwerk-Interface im Container: Interfaces konfiguriert. Es können auch andere Server-Adressen gewählt werden. Sie müssen vorher entweder als Netzwerk-Interface oder Def.: Host-Name auf der TMA konfiguriert werden. Der SCEP-Server lauscht nur an der hier angegeben Adresse. Bleiben die Felder leer, hört der SCEP-Server an allen Adressen.

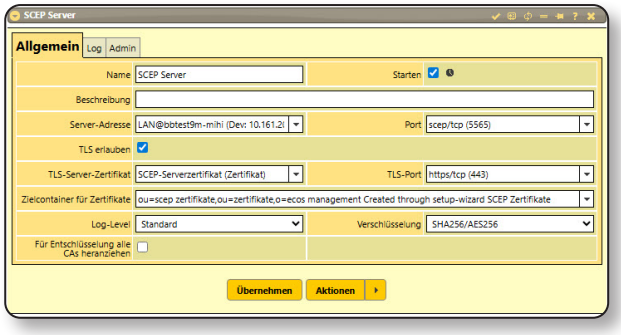


Abb. 17.19: *Dienst: SCEP-Server - Reiter Allgemein*

Es muss ein Port verwendet werden, an dem keine andere Instanzen der ECOS Appliance lauschen, um Konflikte zu vermeiden.

Wird die Checkbox TLS erlauben aktiviert, wird der SCEP-Dienst mit und ohne TLS-Verschlüsselung genutzt. Zusätzlich muss dann ein TLS-Port ausgewählt bzw. angelegt werden. Es muss ein Port verwendet werden, an dem keine andere Instanzen der ECOS Appliance lauschen, um Konflikte zu vermeiden.

Im Feld TLS-Server-Zertifikat wird das Zertifikat-Objekt ausgewählt, dass entweder manuell oder über den Ersteinrichtungsassistenten angelegt wurde, ausgewählt. Es sichert die HTTPS-Verbindung des Servers ab. Voraussetzung dafür ist, dass der Client dem Zertifikat bzw. dem CA-Zertifikat, das das TLS-Server-Zertifikat signiert hat, vertrauen muss.

Im Dienst-Objekt kann der Zielcontainer für Zertifikate ausgewählt werden.

Bei SCEP muss ein Verschlüsselungsverfahren für die Übertragung gewählt werden. Standardmäßig ist als Verschlüsselung **SHA256/AES256** eingestellt.

Kann ein SCEP-Client nicht ordnungsgemäß mit mehrstufigen CAs umgehen, wird die Checkbox Für Entschlüsselung alle CAs heranziehen aktiviert. Dadurch werden für die Entschlüsselung der SCEP-Pakete die CAs der gesamten CA-Kette herangezogen. Dieses Verhalten entspricht nicht dem Standard und sollte nur verwendet werden, wenn der Enrollment-Client dies zwingend erfordert.

Der Dienst startet durch Aktivieren der Checkbox Starten. Im Reiter **Log** können Informationen zum Dienst eingesehen werden.

Der Dienst ist anschließend unter dem Pfad https://<ip-adresse>:<port>/.well-known/scep erreichbar.

17.1.5.2 SCEP-Abonnentenkonto anlegen

Für jedes Gerät, dass ein Zertifikat braucht, wird ein eigenes SCEP-Abonnentenkonto benötigt. Diese können z.B. über die API oder eine Verzeichnissynchronisation, z.B. mit einer CSV-Datei, auf der TMA angelegt werden. Die meisten Einstellungen können über die Synchronisation vorgegeben werden.

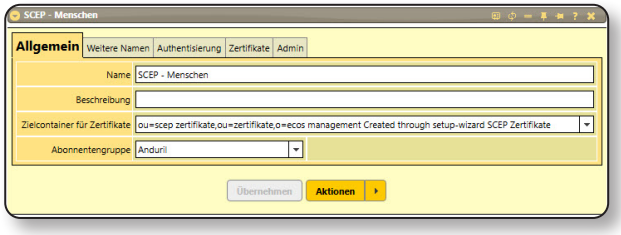


Abb. 17.20: *SCEP-Abonnentenkonto - Reiter Allgemein*

Reiter Weitere Namen:

Hier können zusätzliche Informationen zum Zertifikat angegeben werden. Diese alternativen Namen, auch Subject Alternative Name (SAN) genannt, können zusätzlich oder anstelle der Identität im Subjektfeld des Zertifikats angegeben werden, z.B. wenn ein Server mehrere Namen hat. Diese Informationen werden in den Zertifikaten hinterlegt, die mit dem Abonnentenkonto bestellt werden. Werden SANs durch den CSR eingereicht, haben die hier angegebenen SANs Vorrang. Sie entsprechen denen im Zertifikat-Objekt auf dem Reiter **Weitere Namen**.

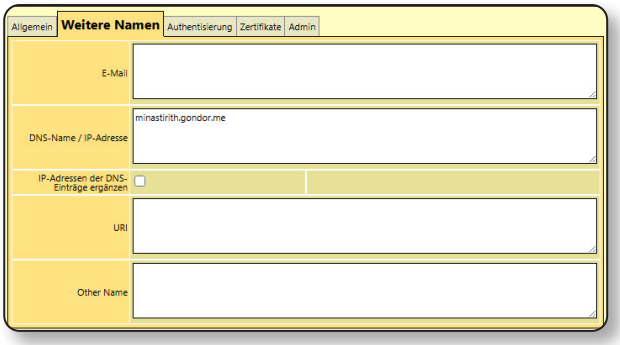


Abb. 17.21: *SCEP-Abonnentenkonto - Reiter Weitere Namen*

Reiter Authentisierung:

Damit sich das Abonnentenkonto beim entsprechenden Server-Dienst anmelden kann, muss mindestens eine Authentisierungsmethode konfiguriert werden.

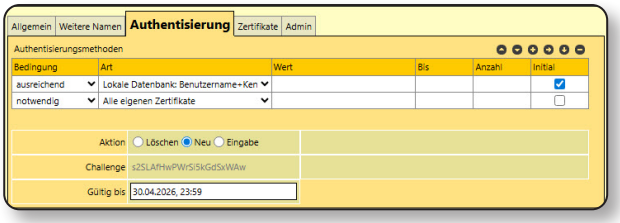


Abb. 17.22: *SCEP-Abonnentenkonto - Reiter Authentisierung*

In der Spalte Bedingung wird festgelegt, ob die jeweilige Authentisierungsmethode für die Anmeldung **notwendig** bzw. **ausreichend** ist oder **ignoriert** wird. Für eine erfolgreiche Anmeldung müssen *alle* notwendigen Bedingungen erfüllt sein. Wurden ausreichende Bedingungen definiert, muss *eine* dieser Bedingungen für die Anmeldung erfüllt sein. Wurden sowohl notwendige als auch ausreichende Authentisierungsmethoden konfiguriert, müssen *alle notwendigen*, die vor der ersten ausreichenden Bedingung stehen, und *mindestens eine ausreichende* Bedingung erfüllt sein, damit die Anmeldung erfolgreich ist. Authentisierungsmethoden, die als ignorieren eingestuft sind, werden bei der Anmeldung nicht berücksichtigt.

Standardmäßig sind die Authentisierungsmethoden **Lokale Datenbank: Benutzername+Kennwort** als ausreichend und die Methode **Alle eigenen Zertifikate** als notwendig konfiguriert. Bei SCEP bedeutet die Authentisierung Lokale Datenbank: Benutzername+Kennwort, dass eine Challenge genutzt wird. Sie wird i.d.R. zufällig generiert. Durch die aktivierte Checkbox Initial ist es möglich, dass diese Authentisierungsmethode nur bei der ersten Anmeldung mit einer Challenge erfolgt. Jede weitere Anmeldung erfordert ein Zertifikat dieses Abonnenten (siehe **15 Benutzerverwaltung (Experte)**).

In der Spalte Bis kann ein Datum eingetragen werden, bis wann die Authentisierungsmethode gültig ist und genutzt werden kann. Es kann ein Datum mit Uhrzeit im Format TT.MM.JJJJ hh:mm angegeben werden. Nach Ablauf ist die Anmeldung mit dieser Methode nicht mehr möglich.

Die Zahl der Anmeldeversuche kann in der Spalte Anzahl festgelegt werden. Sie bestimmt, wie oft diese Authentisierungsmethode zur Anmeldung genutzt werden kann. Dabei zählen sowohl erfolgreiche als auch fehlgeschlagene Anmeldeversuche. Ist die Anzahl erreicht, ist die Anmeldung mit dieser Methode nicht mehr möglich.

Grundsätzlich können auch die anderen Methoden zur Authentisierung benutzt werden.

Wird die Checkbox Nur Lesezugriff aktiviert, erhält der Abonnent nur lesend Zugriff auf die Zertifikate. Er kann keine neuen Zertifikate anlegen oder bestehende ändern.

Um Zugriff auf alle mit SCEP ausgerollte Zertifikate zu erhalten, muss die Checkbox Zugriff auf alle SCEP-Zertifikate aktiviert werden.

Unter Aktion kann ausgewählt werden, wie die Challenge generiert wird oder was mit ihr passiert. Die Aktion **Löschen** löscht die Challenge aus dem SCEP-Abonnentenkonto. Ohne Challenge kann der Client keine Zertifikate mehr anfordern. Mit der Option **Neu** wird eine neue Challenge generiert. Die Option **Eingabe** ermöglicht die manuelle Eingabe einer Challenge. Jede dieser Aktion greift erst, wenn das Objekt mit Übernehmen gespeichert wurde.

Im Feld Challenge wird die Challenge angezeigt bzw. kann eingegeben werden, wenn die entsprechende Aktion ausgewählt wurde.

Die Challenge hat eine Gültigkeit, die unter Gültig bis eingetragen werden kann. Wird eine neue Challenge generiert, ist sie standardmäßig für eine Stunde gültig. Dies kann manuell geändert werden.

Reiter Zertifikat:

Auf diesem Reiter werden alle Zertifikate aufgelistet, die für dieses Abonnentenkonto angefragt und ausgestellt wurden.

17.2 Die TMA als Client für andere Zertifizierungsstellen

Die TMA kann als Client fungieren und Zertifikate bei anderen bzw. externen Zertifizierungsstellen anfragen. Sie nimmt die Zertifikate entgegen und verteilt sie weiter an die Endgeräte.

17.2.1 Vorbereitungen

Unabhängig vom Protokoll müssen einige Vorbereitungen getroffen werden. Dazu zählen die Registrierung beim Provider und das Hochladen eines externen CA-Zertifikats.

17.2.1.1 Registrierung beim Provider

Für das Zertifikat-Enrollment wird ein aktives Konto bei einem externen Provider benötigt. Dies wird meist über die Webseite des Providers kostenpflichtig registriert. Anschließend stehen in der Regel CA-Zertifikate zum Herunterladen zur Verfügung.

17.2.1.2 Externes CA-Zertifikat zum Signieren der Client-Zertifikate

Die externen CA-Zertifikate müssen vom Provider bezogen werden. Anschließend werden sie manuell in ein CA-Zertifikat-Objekt im Container: Zertifikate hochgeladen (siehe **16.3 Im- und Export**).

Im CA-Zertifikat muss auf dem Reiter **Erweitert** als CA-Typ die Option **Remote** aktiviert werden. Anschließend muss der Container: Providergruppe unter Providergruppe ausgewählt werden. Alle Zertifikate, die von ein Providerkonto innerhalb dieses Container: Providergruppe bezogen werden, werden mit dem CA-Zertifikat signiert.

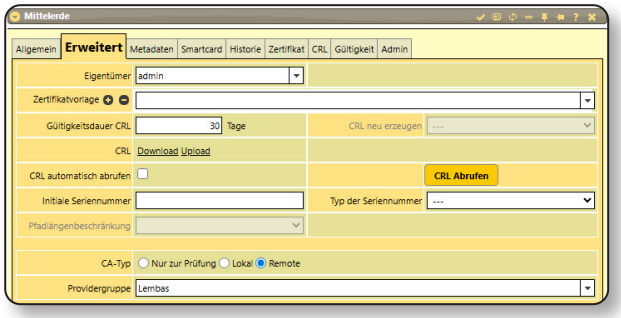


Abb. 17.23: *CA-Zertifikat - CA-Typ bestimmen*

17.2.2 Zertifikat-Enrollment mit ACME

Für das Zertifikat-Enrollment mit ACME steht vor allem der Provider Let's Encrypt zur Verfügung. Es können aber auch andere Provider konfiguriert werden, wenn die notwendigen Daten bekannt sind.

Externe Provider bieten oft Staging-Umgebungen an, in denen die Einrichtung von Providerkonten und der Bezug von Zertifikaten sicher getestet werden können, ehe eine Live- oder Produktionsumgebung umgesetzt wird.

Informationen zur ACME Staging Environment von Let's Encrypt finden sich unter https://letsencrypt.org/de/docs/staging-environment

Es wird ein ACME-Providerkonto für jeden Provider gebraucht.

Reiter Allgemein:

Dem Providerkonto wird eine Providergruppe zugeordnet. Durch Ändern der Providergruppe, wird das Konto in eine andere Gruppe verschoben.

Die URL für den externen ACME-Server wird unter Server-URL angegeben. Für die Staging-Umgebung von Let's Encrypt wäre das z.B. https://acme-staging-v02.api.letsencrypt.org/directory.

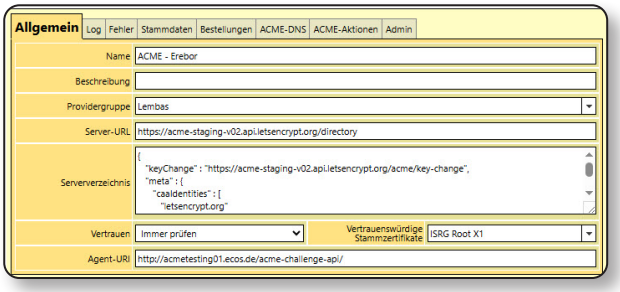


Abb. 17.24: *ACME-Providerkonto - Reiter Allgemein*

Im Serververzeichnis im JSON-Format angezeigt. Das Serververzeichnis informiert die Clients über die erforderlichen URLs für ACME-Operationen. Es enthält auch die URL zu den Terms of Service (TOS). Das Serververzeichnis wird auf dem Reiter **ACME-Aktionen** über den Link **Verzeichnis** unter den Aktionen abgerufen.

Zur Absicherung der HTTPS-Verbindung mit dem Server muss das Vertrauen konfiguriert werden. Das Serverzertifikat wird beim ersten Kontakt mit dem externen ACME-Server überprüft und der Herausgeber ermittelt. Steht das Vertrauen auf **Nie prüfen**, wird dem ACME-Server immer vertraut und das Server-Zertifikat nicht geprüft. Die Option **TOFU** (Trust on first use) sucht und prüft die zugehörige CA beim ersten Kontakt mit dem externen ACME-Server. Sie wird im Feld Vertrauenswürdige Stammzertifikate hinterlegt und zukünftig vertraut. Bei der Option **Immer prüfen** wird das Serverzertifikat bei jedem Kontakt mit dem ACME-Server geprüft. Das zugehörige Stammzertifikat wird unter Vertrauenswürdige Stammzertifikate angegeben. Steht das Vertrauen auf **CA fehlt**, ist kein Stammzertifikat zur Überprüfung der TLS-Verbindung vorhanden. Ist im Feld Vertrauenswürdige Stammzertifikate ein CA-Zertifikat ausgewählt, sollte zunächst überprüft werden, ob das Stammzertifikat korrekt in das CA-Zertifikat-Objekt hochgeladen wurde.

Die Optionen können nur geändert werden, wenn das Providerkonto auf dem Reiter **Stammdaten** im Kontostatus **Bereit zur Anmeldung** ist.

Sind Vertrauenswürdige Stammzertifikate des Herausgebers hinterlegt, wird er als vertrauenswürdig eingetragen. Andernfalls wird ein leeres CA-Zertifikat-Objekt erzeugt, in welches das Stammzertifikat vom externen Provider hochgeladen werden muss.

Unter der Agent-URI wird die Adresse angegeben, unter der der ACME-Client die Informationen zur Challenge im JSON-Format postet.

Reiter Stammdaten:

Der Kontostatus gibt an, in welchem Zustand sich das Providerkonto befindet. Die Option **Bereit zur Anmeldung** bedeutet, dass das ACME-Providerkonto bereit zur Registrierung ist, sich aber noch nicht am Server registriert hat. In diesem Zustand kann das Vertrauen auf dem Reiter **Allgemein** konfiguriert werden. Steht der Status auf **Gültig**, ist das Konto aktiv und gültig. Der Client kann alle Aktionen durchführen. Die Option **Deaktiviert** bedeutet, dass das Konto clientseitig deaktiviert wurde. Bei der Option **Zurückgezogen** wurde das Konto serverseitig zurückgezogen.

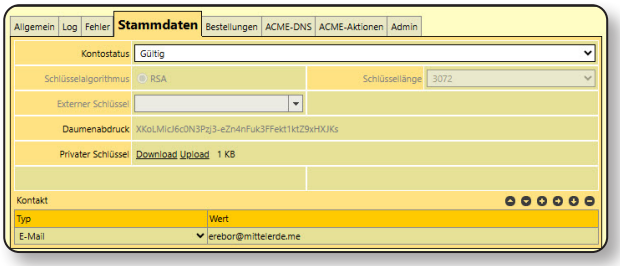


Abb. 17.25: *ACME-Providerkonto - Reiter Stammdaten*

Für das Providerkonto wird ein Schlüsselpaar für die Kontoanmeldung benötigt. Dazu werden der Schlüsselalgorithmus und die Schlüssellänge festgelegt. Wird die Option **RSA** gewählt, ist standardmäßig eine Schlüssellänge von **3072 Bit**s angegeben. Das ist die vom BSI empfohlene Mindestlänge für RSA-Schlüssel.

Ist das External Account Binding aktiviert, wird ein Symmetrischer Schlüssel benötigt, der im Feld Externer Schlüssel ausgewählt wird. Mit dem External Account Binding wird einem ACME-Konto erlaubt, Autorisierungen zu verwenden, die einem externen, nicht-ACME-Konto erteilt wurden. So können Ausstellungszenarien realisiert werden, die noch nicht vollständig automatisiert werden können, z.B. die Ausstellung von Extended-Validation-Zertifikaten.

Reiter Bestellungen:

Dieser Reiter **zeigt** Informationen über die Bestellungen und Challenges des ACME-Providerkonto angezeigt. Es können keine Änderungen der Informationen über diesen Reiter vorgenommen werden.

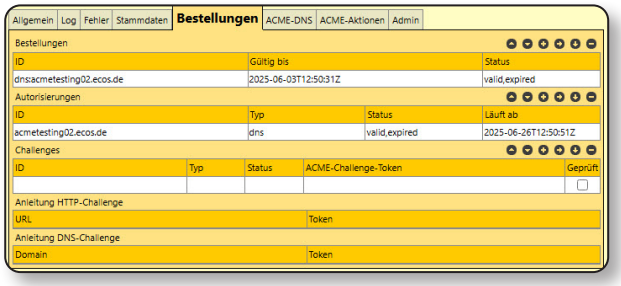


Abb. 17.26: *ACME-Providerkonto - Reiter Bestellungen*

Reiter ACME-Aktionen:

Dieser Reiter ermöglicht es, Aktionen für das ACME-Providerkonto manuell auszuführen. Zum einen kann über **Verzeichnis** das Serververzeichnis des externen ACME-Servers heruntergeladen werden. Es wird anschließend im Reiter **Allgemein** unter

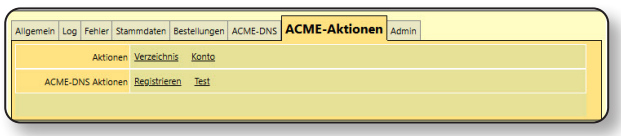


Abb. 17.27: *ACME-Providerkonto - Reiter ACME-Aktionen*

Serververzeichnis im JSON-Format angezeigt. Zum anderen kann mit **Konto** die Registrierung des Kontos beim externen ACME-Server ausgelöst werden.

17.2.3 Zertifikat-Enrollment mit CMP

Für das Zertifikat-Enrollment mit CMP stehen vor allem die Provider D-Trust und EJBCA zur Verfügung. Es können aber auch andere Provider konfiguriert werden, wenn die notwendigen Daten bekannt sind.

Externe Provider bieten oft Staging-Umgebungen an, in denen die Einrichtung von Providerkonten und der Bezug von Zertifikaten sicher getestet werden können, ehe eine Live- oder Produktionsumgebung umgesetzt wird.

Es wird ein CMP-Providerkonto für jeden Provider gebraucht.

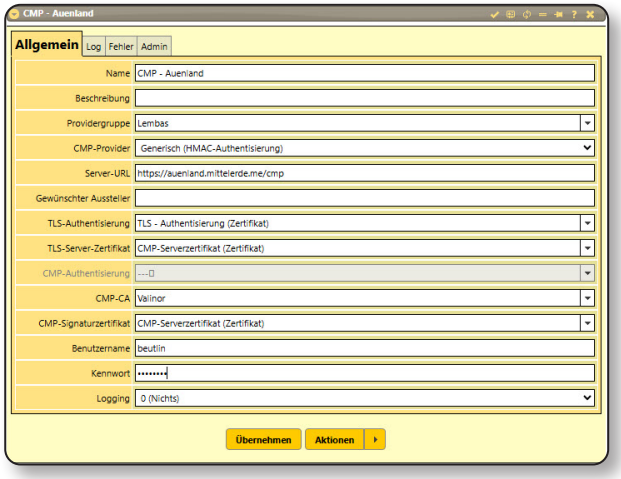


Abb. 17.28: *CMP-Providerkonto-Anmeldung mit Zugangsdaten*

Reiter Allgemein:

Dem Providerkonto wird eine Providergruppe zugeordnet. Durch Ändern der Providergruppe, wird das Konto in eine andere Gruppe verschoben.

Unter CMP-Provider wird der externe CMP-Provider ausgewählt, von dem die Zertifikate bezogen werden. Es stehen neben den selbst zu konfigurierenden auch einige vorkonfigurierte Provider zur Auswahl. Die CMP-Provider können nach Art der Authentisierung konfiguriert werden. Die Authentisierung mit Zertifikat erfordert die Angabe eines Zertifikats zur CMP-Authentisierung. Die HMAC-Authentisierung benötigt Benutzername und Kennwort für die Authentisierung am CMP-Server.

Die Option **Generisch** muss selbst konfiguriert werden. Es muss die Server-URL konfiguriert werden, unter der der externe CMP-Server erreichbar ist. Wenn die Zertifikate von einer bestimmten CA ausgestellt werden sollen, kann diese unter Gewünschter Aussteller angegeben werden.

Wird **D-Trust** als CMP-Provider gewählt, wird die Server-URL vorgegeben. Ein Gewünschter Aussteller kann vorgegeben werden.

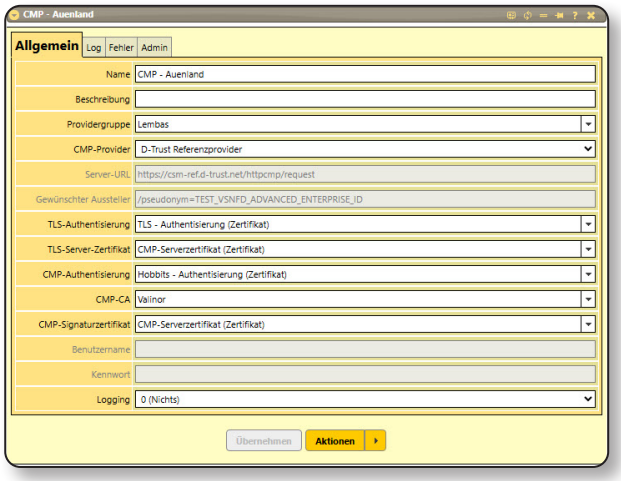


Abb. 17.29: *CMP-Providerkonto - Anmeldung mit Zertifikat*

Bei der Option **D-Trust Referenzprovider** werden Server-URL und Gewünschter Aussteller vorgeben. Der Referenzprovider dient vor allem zu Testzwecken.

Wird **EJBCA** gewählt muss die Server-URL einer EJBCA-Instanz angegeben werden. Ein Gewünschter Aussteller kann vorgegeben werden.

Unabhängig von dem gewählten CMP-Provider sind weitere Einstellungen nötig. Für die TLS-Verschlüsselung des Clients mit dem CMP-Server wird ein Zertifikat zur TLS-Authentisierung gebraucht. Abhängig vom Provider kann das Zertifikat zur TLS-Authentisierung dem Zertifikat zur CMP-Authentisierung entsprechen. Der CMP-Provider D-Trust stellt das TLS-Zertifikat zur Verfügung.

Des Weiteren muss eine CMP-CA gewählt werden. Dabei handelt es sich um ein CA-Zertifikat, gegen die der Client die CMP-Messages prüft. Alternativ kann ein CMP-Signaturzertifikat angegeben werden, mit dem die Antwort des CMP-Servers signiert sein muss.

18 Zertifikat-Enrollment mit dem Certificate Enrollment Agent

Nicht alle Geräte und Systeme können über die Standard-Enrollment-Protokolle Zertifikate erhalten. Hier kommt der Certificate Enrollment Agent ins Spiel. Das Programm bietet die Möglichkeit, dass auf diese Geräte und Systeme ebenfalls Zertifikaten automatisch ausgerollt werden können.

Der Certificate Enrollment Agent kann auf zwei Arten benutzt werden: Im **Push**-Modus läuft der Agent auf der TMA selbst. Er meldet sich per SSH auf den Zielsystemen an und führt dort konfigurierte Befehle für das Zertifikat-Enrollment aus. Beim **Pull**-Modus wird der Agent auf dem Zielsystem installiert. Die Zertifikate holt sich der Agent über die REST-API der TMA. Er kann als Systemdienst im Dauerbetrieb laufen und in konfigurierbaren Intervallen Abfragen ausführen.

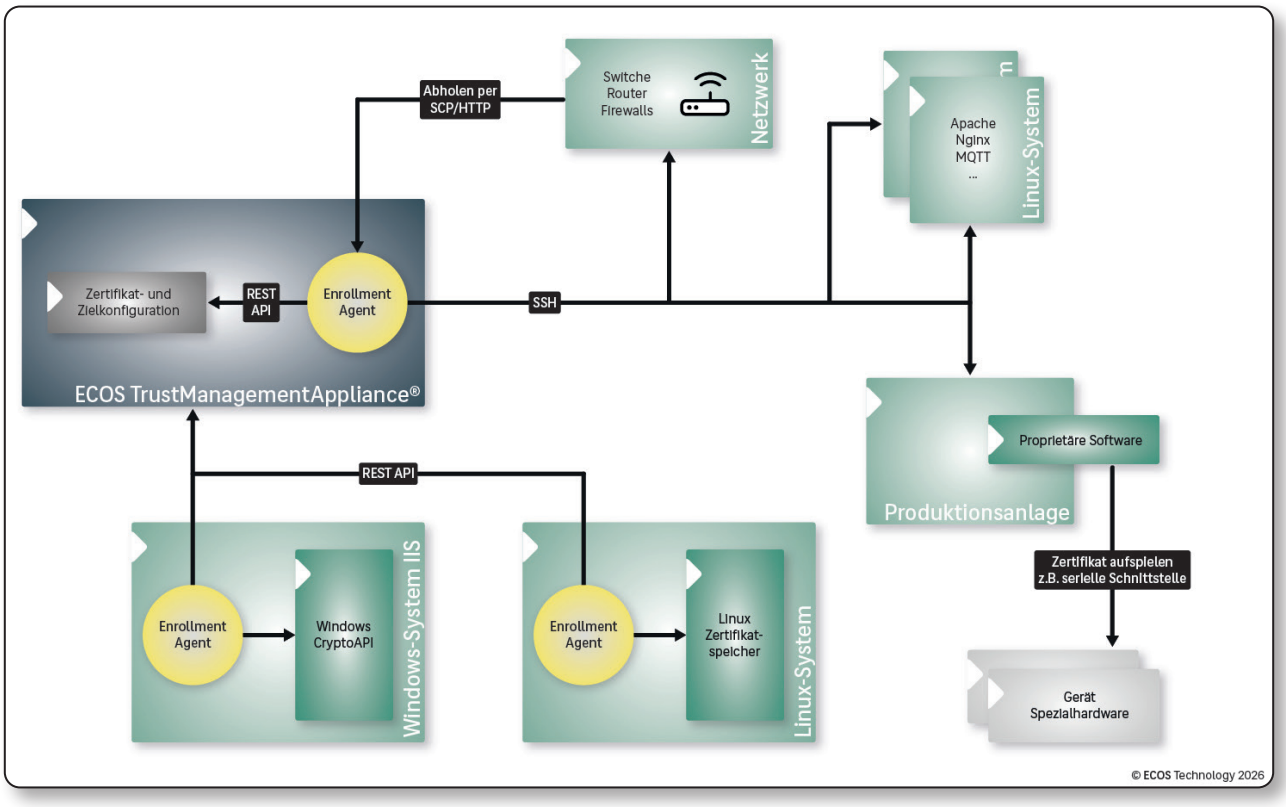


Abb. 18.01: *Zertifikat-Enrollment mit dem Certificate Enrollment Agent*

Die Zertifikate können direkt in den Zertifikatspeicher des jeweiligen Betriebssystems auf dem Zielgerät abgespeichert werden.

⚠ **Hinweis:** Informationen zu den möglichen Kommandozeilenbefehlen und -optionen, sowie den Variablen und der Fehlersuche finden sich unter **26 Certificate Enrollment Agent - Anhänge.**

Plattform	Betrieb im Push-Modus	Betrieb im Pull-Modus	Architektur
Linux	Ja (Zugriff per SSH)	Ja (systemd-Dienst oder über Kommandozeile	x86 (32bit), x86 (64bit), ARMv7*
Windows	Ja (Zugriff per SSH)	Ja (Windows-Dienst oder über Kommandozeile)	x86 (64bit)
Sonstige Systeme	Ja (Zugriff per SSH oder HTTPS)	Nein	-

* Weitere Architekturen für den Pull-Modus auf Anfrage.

18.1 Vorbereitungen

Für die Nutzung des Certificate Enrollment Agent spielen verschiedene Objekte auf der TMA zusammen.

Folgende Objekte werden benötigt:

Objekt	Funktion
Dienst: Certificate Enrollment Agent	Konfigurationsobjekt für den Agent
Abonnentenkonto für Agent	Anmeldung an der TMA
Zertifikatplan für Agent	Konfiguration für Zertifikate
Deploymentinfo für Agent	Enrollment für Zertifikate
CA-Zertifikat	Signieren der Zertifikate
Zielcontainer für Zertifikate	Speicherort für die Zertifikate auf der TMA

Informationen zum Anlegen eines CA-Zertifikats, eines Zielcontainers für Zertifikate und der Zuordnung der CAs zu den Abonnentengruppen finden sich unter **17.1.1 Vorbereitungen.**

18.1.1 Dienst: Certifcate Enrollment Agent anlegen

Der Dienst: Certificate Enrollment Agent wird manuell im Expertenmodus unter **ECOS Appliance → Container: Dienste** über das Kontextmenü angelegt.

Reiter Allgemein:

Im Dienst-Objekt kann der Zielcontainer für Zertifikate ausgewählt werden. Dieser dient als Standard, falls kein Zielcontainer im Abonnentenkonto für Agent selbst oder in der Abonnentengruppe definiert ist.

Für den Pull-Modus (Agent auf dem Zielsystem installiert) müssen keine weiteren Einstellungen vorgenommen werden (die Checkbox Starten muss nicht aktiviert werden).

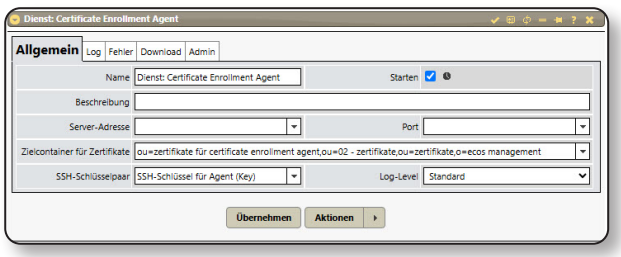


Abb. 18.02: *Dienst: Certificate Enrollment Agent - Reiter Allgemein*

Im Push-Modus muss der Dienst durch Aktivieren der Checkbox Starten gestartet werden.

Soll das Zielsystem Zertifikate per SCP von der TMA abholen, müssen eine Server-Adresse und Port definiert werden. Als Server-Adresse wird in der Regel die LAN-Adresse der TMA genutzt. Diese ist als Netzwerk-Interface im Container: Interfaces konfiguriert. Es können auch andere Server-Adressen gewählt werden. Sie müssen vorher entweder als Netzwerk-Interface oder Def.: Host-Name auf der TMA konfiguriert werden. Es muss ein Port verwendet werden, an dem keine anderen Instanzen der ECOS Appliance lauschen, um Konflikte zu vermeiden. Adresse und Port müssen vom Zielsystem aus erreichbar sein. Zusätzlich muss ein SSH-Schlüsselpaar angegeben werden. Dies dient als Hostkey für den SSH-Server. Schlüssel können im Container: Zertifikate mit dem Privater/Öffentlicher Schlüssel-Objekt angelegt werden (siehe **18.4.2.1 Deploymentinfo für Agent anlegen**).

Auf den Reitern **Log** und **Fehler** können Informationen und Fehlermeldungen zum Dienst eingesehen werden.

Reiter Download:

Auf diesem Reiter **kann** der Certificate Enrollment Agent heruntergeladen werden. Es stehen Installationsdateien für verschiedene Prozessorarchitekturen für die Betriebssysteme Linux und Windows zur Verfügung (**18.2 Installation auf dem Zielsystem (Pull-Modus)**).

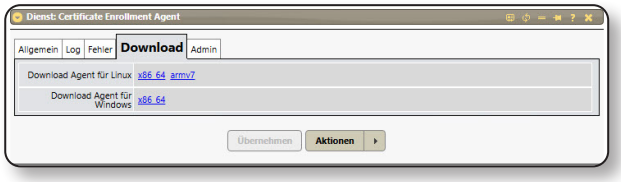


Abb. 18.03: *Dienst: Certificate Enrollment Agent - Reiter Download*

18.1.2 Abonnentenkonto für Agent anlegen

Für jedes Gerät und Zielsystem, das ein Zertifikat braucht, wird ein eigenes Abonnentenkonto für Agent benötigt. Diese können z.B. über die API oder eine Verzeichnissynchronisation, z.B. mit einer CSV-Datei, auf der TMA angelegt werden. Die meisten Einstellungen können über die Synchronisation vorgegeben werden. Manuell wird es über **Container: PKI-Management → Container: Zertifikatabonnenten → Container: Abonnentengruppe → Neu** angelegt.

Wird der Certificate Enrollment Agent im Pull-Modus genutzt, muss ein Abonnentenkonto für Agent vor der Installation des Agent auf dem Zielsystem angelegt sein.

Reiter Allgemein:

Damit das Abonnentenkonto vom Certificate Enrollment Agent bearbeitet wird, muss es Aktiv geschaltet sein.

Unter Zertifikatpläne können ein oder mehrere zentral angelegte Zertifikatplan für Agent-Objekte ausgewählt werden. Sie sind für die Erstellung und Verteilung von Zertifikaten notwendig. Alternativ können Zertifikatpläne aber auch unterhalb des Abonnenten angelegt werden.

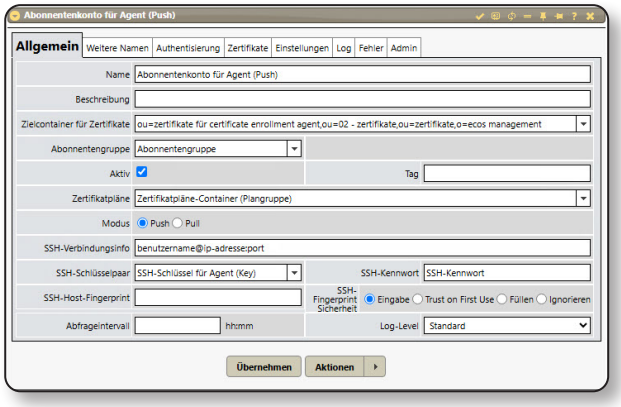


Abb. 18.04: *Abonnentenkonto für Agent - Reiter Allgemein*

Der Modus bestimmt, ob sich die TMA mit dem Zielsystem, dem dieses Abonnentenkonto zugeordnet wird, verbindet (**Push**) oder ob sich das Zielsystem mit der TMA verbindet (**Pull**).

Im **Push**-Modus benötigt das Abonnentenkonto Informationen, um sich per SSH mit dem Zielsystem zu verbinden. Die SSH-Verbindungsinfo wird im Format `benutzername@ip-adresse:port` angegeben. Zusätzlich muss entweder ein SSH-Schlüsselpaar oder ein SSH-Kennwort angegeben werden. Wird beides konfiguriert, erfolgt die Anmeldung per SSH-Schlüsselpaar. Bei dem SSH-Schlüsselpaar handelt es sich um ein Privater/Öffentlicher Schlüssel-Objekt, das im Container: Zertifikate erzeugt wird.

Um die Sicherheit der SSH-Verbindung zu erhöhen, kann ein SSH-Host-Fingerprint hinterlegt werden. Dadurch wird beim Verbindungsaufbau geprüft, ob der SSH-Fingerprint des Zielsystems mit dem hinterlegten Fingerprint übereinstimmt. Ist das nicht der Fall, wird die Verbindung abgelehnt. Zusätzlich kann im Feld SSH-Fingerprint-Sicherheit festgelegt werden, wie der Fingerprint hinterlegt und wie streng er geprüft wird. Bei der Option **Eingabe** muss der Fingerprint manuell eingetragen werden. Stimmen die Fingerprints nicht überein oder ist das Feld SSH-Host-Fingerprint leer, wird die Verbindung abgelehnt. Mit **Trust on First Use** wird der Fingerprint automatisch bei der ersten Verbindung hinterlegt. Bei jeder weiteren Verbindung wird er überprüft und die Verbindung abgelehnt, wenn sie nicht übereinstimmen. Wird die Option **Füllen** gewählt, wird der Fingerprint ebenfalls automatisch bei der ersten Verbindung eingetragen. Anschließend muss er verifiziert werden und die Auswahl auf **Eingabe** umgestellt werden. Soll jeder Fingerprint akzeptiert werden, muss die Option **Ignorieren** gewählt werden. Das Feld SSH-Host-Fingerprint kann in diesem Fall leer bleiben.

Das Abfrageintervall bestimmt, in welchem Zeitraum der Certificate Enrollment Agent bei der TMA anstehende Aufgaben abfragt. Bleibt das Feld leer, wird der Wert, der bei der Installation des Agents festgelegt wurde, übernommen. Standardmäßig sind das **25000s** (7 Stunden).

Reiter Weitere Namen:

Hier können Subject Alternative Name (SAN) zusätzlich oder anstelle der Identität im Subjektfeld des Zertifikats angegeben werden, z.B. wenn ein Server mehrere Namen hat. Diese Informationen werden in den Zertifikaten hinterlegt, die mit dem Abonnentenkonto bestellt werden. Werden SANs durch den CSR eingereicht, haben die hier angegebenen SANs Vorrang.

Sind hier keine SANs angeben, werden die SANs aus dem eingereichten CSR übernommen. Alternativ können SANs auch über eine Richtlinie festgelegt werden. Die Eingabefelder entsprechen denen im Zertifikat-Objekt auf dem Reiter **Weitere Namen**: **16.1.3 Zertifikat-spezifische Parameter**.

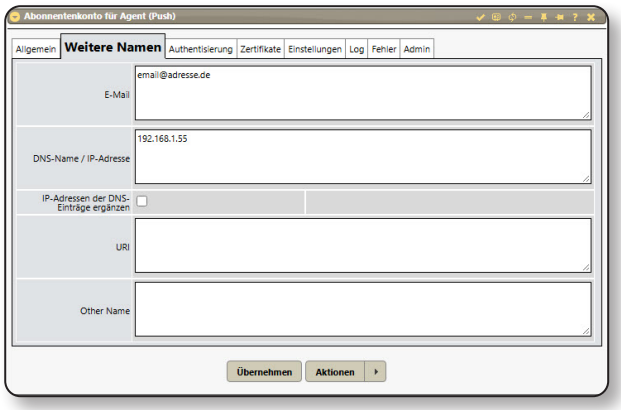


Abb. 18.05: *Abonnentenkonto für Agent - Reiter Weitere Namen*

Reiter Authentisierung:

Auf diesen Reiter wird festgelegt, wie sich der Certificate Enrollment Agent im **Pull**-Modus gegenüber der TMA authentifiziert. Im **Push**-Modus sind die Werte auf dem Reiter **Authentisierung** nicht relevant. Es kann eine oder mehrere Authentisierungsmethoden festgelegt werden. Bevor der Agent aktiv werden kann, muss er sich zunächst registrieren (siehe **18.3 Registrierung und Authentisierung**). Für diese Registrierung können andere Authentisierungsmethoden festgelegt werden.

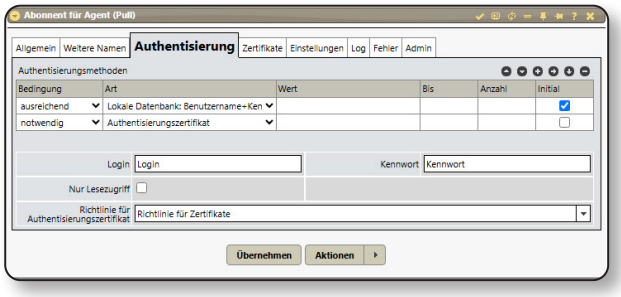


Abb. 18.06: *Abonnentenkonto für Agent - Reiter Authentisierung*

In der Spalte Bedingung wird festgelegt, ob die jeweilige Authentisierungsmethode für die Anmeldung **notwendig** bzw. **ausreichend** ist oder **ignoriert** wird. Für eine erfolgreiche Anmeldung müssen *alle* notwendigen Bedingungen erfüllt sein. Wurden ausreichende Bedingungen definiert, muss *eine* dieser Bedingungen für die Anmeldung erfüllt sein. Wurden sowohl notwendige als auch ausreichende Authentisierungsmethoden konfiguriert, müssen *alle notwendigen*, die vor der ersten ausreichenden Bedingung stehen, und *mindestens eine ausreichende* Bedingung erfüllt sein, damit die Anmeldung erfolgreich ist. Authentisierungsmethoden, die als ignorieren eingestuft sind, werden bei der Anmeldung nicht berücksichtigt.

Standardmäßig sind für den Certificate Enrollment Agent die Authentisierungsmethoden **Lokale Datenbank: Benutzername+Kennwort** als ausreichend und die Methode **Authentisierungszertifikat** als notwendig konfiguriert. Die aktivierte Checkbox Initial bei ersterer Authentisierungsmethode bewirkt, dass die erste Anmeldung mit Login und Kennwort erfolgt. Jede weitere Anmeldung erfordert das Authentisierungszertifikat dieses Abonnenten (siehe **15.2 Authentisierung**).

Der Benutzername (Login) muss eindeutig sein. Diese können entweder manuell bestimmt oder über die Verzeichnissynchronisation importiert werden.

Im Feld Richtlinie für Authentisierungszertifikat kann eine Richtlinie hinterlegt werden. Sie gibt Werte für die Ausstellung des Authentisierungszertifikat vor, z.B. Schlüssellänge oder Gültigkeit. Wird keine Richtlinie ausgewählt, wird das Zertifikat mit den Standardwerten und dem Schlüsseltyp der entsprechenden Richtlinien der signierenden CA und des Container in dem die Zertifikate abgelegt werden, erzeugt. Dabei hat die hier eingestellt Richtlinie höchste Priorität, gefolgt von der CA und dann den ggf. gegebenen Richtlinien in den Containern.

Neben den standardmäßig vorausgewählten Authentisierungsmethode stehen noch weitere Methoden zur Authentisierung zur Verfügung (siehe **15.2 Authentisierung**).

Reiter Zertifikate:

Dieser Reiter listet alle Zertifikate auf, die für dieses Abonnentenkonto angefragt und ausgestellt wurden.

Reiter Einstellungen:

Auf diesem Reiter werden zusätzliche Attribute definiert, die innerhalb der Deploy-Skripte eingesetzt werden können (siehe **18.4.2.1 Deploymentinfo für Agent anlegen**).

18.2 Installation auf dem Zielsystem (Pull-Modus)

Soll der Certificate Enrollment Agent im **Pull**-Modus laufen, muss er auf dem Zielsystem installiert werden. Die Installationsdatei kann im Dienst: Certificate Enrollment Agent auf dem Reiter **Download** für die Betriebssysteme Linux und Windows in verschiedenen Prozessorarchitekturen heruntergeladen werden.

18.2.1 Voraussetzungen

Um den Certificate Enrollment Agent auf dem Zielsystem zu installieren, braucht das Zielsystem Zugriff auf die REST-API der TMA über das Netzwerk.

Es muss ein Abonnentenkonto für Agent angelegt sein, mit dem sich der Agent bei der TMA anmelden kann: **18.1.2 Abonnentenkonto für Agent anlegen**

Außerdem werden Root- bzw. Administrationsrechte auf dem Zielsystem benötigt.

18.2.2 Automatische Installation unter Linux

Auf Zielgeräten mit Betriebssystemen, die auf einem Linux-Kernel basieren, kann der Certificate Enrollment Agent automatisch installiert werden.

Dabei wird in einem Schritt alles Notwendige auf dem Zielsystem eingerichtet. Es wird ein dedizierter Systembenutzer **ecos-tma** angelegt. Das Programm wird nach `/usr/bin/tma-cert-enrollment-agent` kopiert. Der Certificate Enrollment Agent wird bei der TMA registriert und es wird ein Authentisierungszertifikat erzeugt. Der Agent wird als systemd-Dienst eingerichtet, um dauerhaft im Pull-Modus zu laufen. Zusätzlich wird eine Beispieldatei mit `sudo`-Berechtigungen angelegt, um z.B. einen Dienst nach der Zertifikatinstallation neu zu starten.

Für die Installation muss die Installationsdatei im Dienst: Certificate Enrollment Agent auf dem Reiter **Download** heruntergeladen und ggf. auf das Zielsystem übertragen werden. Anschließend wird folgender Befehl über die Kommandozeile ausgeführt:

```
sudo ./tma-cert-enrollment-agent --install --address tma.example.com --user meinsystem -I
```

Option	Erklärung
`--install`	Die Installation wird automatisch gestartet.
`--address tma.example.com`	`tma.example.com` muss durch die tatsächliche Adresse der TMA ersetzt werden.
`--user meinsystem`	`meinsystem` muss durch den Login vom Reiter **Authentisierung** des Abonnentenkonto für Agent ersetzt werden, das zuvor angelegt wurde.

Option	Erklärung
`-I` (entspricht `–accept-invalid-cert`)	Die Prüfung des TLS-Server-Zertifikats der TMA wird vorübergehend deaktiviert. Dies sollte nur genutzt werden, wenn sichergestellt ist, dass der Agent während der Installation mit der richtigen TMA spricht. Ansonsten müssen die benutzten CA-Zertifikate vorher auf dem Zielsystem manuell installiert werden, damit der Agent die Identität der TMA prüfen kann.

Während der Installation ruft der Certificate Enrollment Agent die CA-Zertifikate von der TMA ab. Dadurch wird die Identität der TMA bei allen weiteren Vorgängen automatisch geprüft.

Nach der Installation kann der Agent zum Testen als Benutzer **ecos-tma** gestartet werden:

```
sudo -u ecos-tma tma-cert-enrollment-agent
```

Es müssen keine Argumente angegeben werden. Ist der Agent korrekt registriert, verbindet er sich automatisch mit der TMA und führt die dort hinterlegten Operationen aus.

Der Agent kann als Dienst im Hintergrund gestartet werden:

```
systemctl start tma-cert-enrollment-agent
```

Weiterhin können folgende Befehle ausgeführt werden:

```
# den Status des Daemon anzeigen
systemctl status tma-cert-enrollment-agent
```

```
# die Logs des Daemon anzeigen
journalctl -u tma-cert-enrollment-agent -f
```

Bei der Installation wird ein systemd-Dienst erzeugt, der den Certificate Enrollment Agent als Benutzer **ecos-tma** startet:

```
[Unit]
Description=TMA Certificate Enrollment Agent
```

```
[Service]
User=ecos-tma
Group=ecos-tma
ExecStart=/usr/bin/tma-cert-enrollment-agent --loop 25000
RestartSec=300s
Restart=always
```

```
[Install]
WantedBy=multi-user.target
```

Das Abfrageintervall für Anfragen an die TMA beträgt nach der Installation standardmäßig **25000** Sekunden (7 Stunden). Es kann auf der TMA im Abonnentenkonto für Agent im Feld Abfrageintervall konfiguriert und überschrieben werden.

18.2.2.1 Reinstallation

Um den Certificate Enrollment Agent erneut mit anderen Parametern (z.B. mit einer neuen TMA-Adresse) auf dem Zielsystem zu installieren, kann der Befehl `--reinstall` benutzt werden. Dabei wird das Home-Verzeichnis des Benutzers **ecos-tma** gelöscht. Dazu gehört auch das alte Authentisierungszertifikat. Die Installation wird vollständig wiederholt:

```
sudo tma-cert-enrollment-agent --reinstall --address tma.example.com --user mein-system -I
```

18.2.3 Manuelle Installation unter Linux

Wenn die automatische Installation nicht gewünscht ist, weil z.B. kein separater Systembenutzer angelegt werden soll oder eine bestehende systemd-Konfiguration wiederverwendet wird, dann kann der Certificate Enrollment Agent unter Linux manuell installiert werden.

Dazu wird die Installationsdatei im Dienst: Certificate Enrollment Agent auf dem Reiter **Download** heruntergeladen und ggf. auf das Zielsystem übertragen.

Mit folgendem Befehl wird sie gebaut bzw. bereitgestellt:

```
sudo cp tma-cert-enrollment-agent /usr/bin/
```

Anschließend wird die Registrierung manuell durchgeführt: **18.3 Registrierung und Authentisierung**

Ein eigener systemd-Dienst kann optional zum oben gezeigten Beispiel angelegt werden.

18.2.4 Installation unter Windows

Läuft auf dem Zielsystem ein Windowsbetriebssystem, kann die entsprechende Installationsdatei im Dienst: Certificate Enrollment Agent auf dem Reiter **Download** heruntergeladen und ggf. auf das Zielsystem übertragen werden.

Die Installation kann mit einem Doppelklick auf die MSI-Datei gestartet werden. Im sich öffnenden Installationsassistenten werden die notwendigen Parameter, wie die Adresse der TMA und der Login des Abonnentenkonto für Agent, abgefragt. Der Certificate Enrollment Agent wird als Windows-Dienst installiert, sofern die Option im Assistenten nicht abgewählt wurde, und automatisch an der TMA registriert.

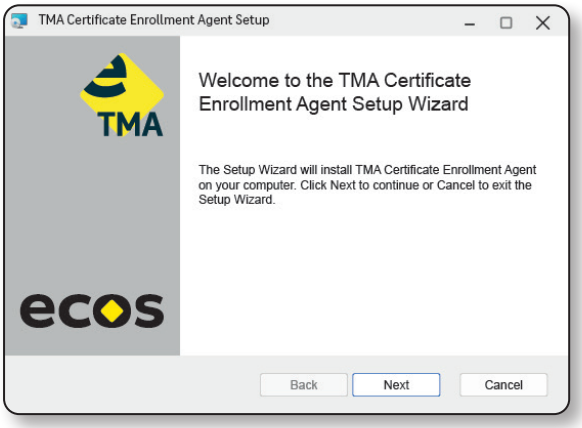


Abb. 18.07: *Starten des Windows-Installers*

Während der Installation werden administrative Rechte (erhöhte Eingabeaufforderung) angefordert.

Die Installation führt folgende Schritte durch:

- Anlegen des Windows-Dienst „TMA Certificate Enrollment Agent“ (sofern die Option nicht abgewählt wurde)
- Registrierung des Certificate Enrollment Agents an der TMA
- Starten des Diensts
- Anlegen eines Eintrags in der Ereignisanzeige

Das Authentifizierungszertifikat wird standardmäßig im Zertifikatspeicher des lokalen Computers gespeichert, wenn der Certificate Enrollment Agent als Windows-Dienst läuft. Andernfalls wird das Authentisierungszertifikat im Zertifikatspeicher des aktuellen Benutzers hinterlegt. Über die Kommandozeile kann das mit der Option `--use-local-machine` beeinflusst werden.

Es stehen weitere Windows-spezifische Befehle zur Verfügung:

Befehl	Erklärung
`tma-cert-enrollment-agent.exe --uninstall`	Der Dienst wird gestoppt und entfernt, die TMA-Registrierung bleibt erhalten.
`tma-cert-enrollment-agent.exe --start-service`	Der Dienst wird gestartet.
`tma-cert-enrollment-agent.exe --stop-service`	Der Dienst wird angehalten.

18.2.5 Unattended Installation unter Windows

Der Certificate Enrollment Agent kann unter Windows auch ohne den Installationsassistenten installiert werden.

Dazu wird folgender Befehl über die Kommandozeile ausgeführt:

```
tma-cert-enrollment-agent.msi /qr TMA_USERNAME=ihrUsername TMA_PASSWORD=ihrKennwort TMA_ADDRESS=ihreIP TMA_PORT=543 TMA_INSTALL_AS_SERVICE=1
```

Option	Erklärung
`TMA_USERNAME=ihrUsername`	`ihrUsername` muss durch den Login vom Reiter **Authentisierung** des Abonnentenkonto für Agent ersetzt werden, das zuvor angelegt wurde.
`TMA_PASSWORD=ihrKennwort`	`ihrKennwort` muss durch das Kennwort vom Reiter **Authentisierung** des Abonnentenkonto für Agent ersetzt werden.
`TMA_ADDRESS=ihreIP`	`ihreIP` muss durch die tatsächliche Adresse der TMA ersetzt werden.
`TMA_INSTALL_AS_SERVICE=1`	Der Certificate Enrollment Agent wird als Windows-Dienst installiert. Soll der Agent nicht als Windows-Dienst installiert werden, muss der Befehl von `1` auf `0` geändert werden.

18.3 Registrierung und Authentisierung

18.3.1 Registrierung im Pull-Modus

Bei der Installation des Certificate Enrollment Agent wird auch die Registrierung durchgeführt. Dazu wird ein Abonnentenkonto für Agent benötigt. Im Standardfall müssen für die Registrierung im **Pull**-Modus auf dem Reiter **Authentisierung** die Authentisierungsmethoden **Lokale Datenbank: Benutzername+Kennwort** als **ausreichend** und **Initial** und **Authentisierungszertifikat** als **notwendig** konfiguriert sein.

Für die Registrierung wird standardmäßig die Authentisierung mit Login und Kennwort genutzt. Es können aber auch davon abweichende Authentisierungsmethoden eingestellt werden, wenn der Agent bei der Registrierung passend parametrisiert wird. Dazu können folgende Optionen genutzt werden:

Authentisierungsmethode	Optionen
Lokale Datenbank: Benutzername+Kennwort	`--user` `--password`
Authentisierungszertifikat (PKCS#12)	`--auth-cert` `--auth-password`

Nach erfolgreicher Registrierung erfolgt die Authentisierung über das Authentisierungszertifikat. Die Registrierungsanmeldedaten sind dann nicht mehr nötig.

18.3.1.1 Ablauf der Registrierung

Die Registrierung läuft i.d.R. während der Installation als Teil von `--install` automatisch ab. Sie kann aber auch manuell durchgeführt werden:

```
tma-cert-enrollment-agent --new-agent-auth meinsystem --address tma.example.com
--password "geheim" -I
```

Option	Erklärung
`--new-agent-auth meinsystem`	`meinsystem` muss durch den Login vom Reiter **Authentisierung** des Abonnentenkonto für Agent ersetzt werden, das zuvor angelegt wurde.
`--address tma.example.com`	`tma.example.com` muss durch die tatsächliche Adresse der TMA ersetzt werden.
`--password "geheim"`	`"geheim"` muss durch das Kennwort vom Reiter **Authentisierung** des Abonnentenkonto für Agent ersetzt werden, das zuvor angelegt wurde.

Option	Erklärung
`-I` (entspricht `–accept-invalid-cert`)	Die Prüfung des TLS-Server-Zertifikats der TMA wird vorübergehend deaktiviert. Dies sollte nur genutzt werden, wenn sichergestellt ist, dass der Agent während der Installation mit der richtigen TMA spricht. Ansonsten müssen die benutzten CA-Zertifikate vorher auf dem Zielsystem manuell installiert werden, damit der Agent die Identität der TMA prüfen kann.

Bei der Registrierung wird ein neues Authentisierungszertifikat für den Agent erzeugt und bei der TMA angemeldet.

Im ersten Schritt der Registrierung meldet sich der Certificate Enrollment Agent mit den Anmeldedaten aus dem Abonnentenkonto für Agent an der TMA an.

Anschließend wird die Konfiguration des Abonnentenkonto ermittelt und geprüft, ob eine Richtlinie für Authentisierungszertifikat hinterlegt ist. Die Richtlinie gibt Werte für das Zertifikat vor, so kann z.B. der Schlüsselalgorithmus und die Schlüsselgröße bestimmt werden. Ist keine Richtlinie hinterlegt, wird ein Zertifikat mit Standardwerten und demselben Schlüsseltyp wie die ausstellende Zertifizierungsstelle erzeugt.

Es wird ein neues Schlüsselpaar sowie ein CSR erzeugt und ein Zertifikat bei der TMA beantragt. Das erzeugte und signierte Zertifikat wird als PKCS#12-Datei auf dem Zielsystem im Verzeichnis unter `~/.ecos-tma/auth/` abgelegt. Unter Windows wird die Datei im Windows-Zertifikatspeicher des aktuellen Benutzers hinterlegt.

Bei jeder weiteren Verbindung zur TMA verwendet der Certificate Enrollment Agent dieses Zertifikat anstelle der Anmeldedaten mit Login und Kennwort.

Unter Windows kann mit der zusätzlichen Option `--use-local-machine` das Zertifikat im Zertifikatspeicher des lokalen Rechners statt des aktuellen Benutzers abgelegt werden.

Soll sich der Agent gegen eine andere TMA registrieren oder ein neues Authentisierungszertifikat erzeugt werden, kann mit `--reinstall` (Linux) die komplette Installation wiederholt werden (siehe **18.2.2.1 Reinstallation**).

18.3.1.2 Automatische Erneuerung des Authentisierungszertifikats

Bei jedem Aufruf prüft der Agent im **Pull**-Modus, ob ein neues Zertfikat auf der TMA zur Verfügung steht.. Bei Bedarf wird es automatisch erneuert, ohne dass ein manueller Aufruf mit `--new-agent-auth` notwendig ist. Für die automatische Erneuerung auf der TMA siehe **21.5 Beispiel: Abfrage mit Aktion zum automatischen Verlängern von Zertifikaten und CRLs**.

18.3.2 Authentisierung im Push-Modus

Im Push-Modus läuft der Certificate Enrollment Agent auf der TMA und verbindet sich per SSH oder HTTP/HTTPS mit dem Zielsystem. Für den SSH-Zugriff müssen im Abonnentenkonto für Agent die SSH-Informationen hinterlegt werden.

18.4 Zertifikat-Enrollment

Für das Zertifikat-Enrollment werden sowohl im **Pull**- als auch im **Push**-Modus mindestens ein Zertifikatplan für Agent und eine Deploymentinfo für Agent benötigt.

18.4.1 Zertifikate erstellen

18.4.1.1 Zertifikatplan für Agent anlegen

Ein Zertifikatplan für Agent dient dazu, die Zertifikate zu konfigurieren, die über den Certificate Enrollment Agent bezogen werden. Für jedes Zertifikat, das ein Zielsystem braucht, wird ein Zertifikatplan benötigt.

Er wird unterhalb des Abonnentenkonto für Agent angelegt werden: **Container: PKI-Management → Container: Zertifikatabonnenten → Container: Abonnentengruppe → Abonnentenkonto für Agent → Neu**.

Reiter Allgemein:

Damit der Zertifikatplan für das Erstellen eines Zertifikats genutzt wird, muss er Aktiv geschaltet sein.

Der Zertifikatname-Typ legt fest, wie der Name für das Zertifikat generiert wird. So kann er z.B. aus dem Namen des Abonnentenkonto und dem Namen des Zertifikatplans zusammengesetzt werden. Außerdem kann ein Label hinterlegt werden, dass für die Namensgenerierung des Zertifikats herangezogen werden kann.

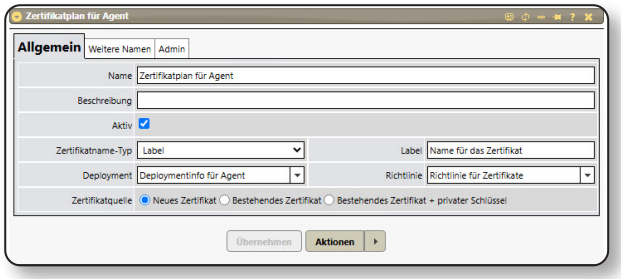


Abb. 18.08: *Zertifikatplan für Agent - Reiter Allgemein*

Zusätzlich muss ein Deployment für Agent im Feld Deployment ausgewählt werden. Es bestimmt, wie das Zertifikat auf das Zielsystem übertragen und wo es gespeichert wird.

Um die genauen Werte für das Zertifikat vorzugeben, kann eine Richtlinie hinterlegt werden. Eine Richtlinie gibt Standardwerte und Bedingungen vor und kann in einer Zertifikatanfrage (CSR) bestehende Werte mit denen der Richtlinie abgleichen. Sie kann über **Container: Management → Neu** angelegt werden.

Im Feld Zertifikatquelle wird festgelegt, woher das Zertifikat des Zertifikatplans stammt. Die Option **Neues Zertifikat** prüft bei jedem Durchlauf, ob auf dem Zielsystem ein gültiges Zertifikat vorhanden ist, das zu diesem Zertifikatplan passt. Fehlt es oder ist nicht mehr gültig, erzeugt der Agent ein neues Schlüsselpaar samt CSR und lässt es von der TMA signieren. Mit der Option Bestehendes Zertifikat wird ein auf der TMA hinterlegtes Zertifikat verteilt. Das Zertifikat muss bereits signiert worden sein und wird im Feld Zu übertragende Zertifikate ausgewählt. Der private Schlüssel bleibt auf der TMA und wird nicht auf der Zielsystem übertragen. Bei der Option **Bestehendes Zertifikat + privater Schlüssel** wird zusätzlich zum bestehenden Zertifikat auch der private Schlüssel übertragen.

Reiter Weitere Namen:

Hier können zusätzliche Informationen zum Zertifikat angegeben werden. Diese alternativen Namen, auch Subject Alternative Name (SAN) genannt, können zusätzlich oder anstelle der Identität im Subjektfeld des Zertifikats angegeben werden, z.B. wenn ein Server mehrere Namen hat. Diese Informationen werden in den Zertifikaten hinterlegt, die mit dem Abonnentenkonto bestellt werden. Werden SANs durch den CSR eingereicht, haben die hier angegebenen SANs Vorrang. Sie entsprechen denen im Zertifikat-Objekt auf dem Reiter **Weitere Namen: 16.1.3 Zertifikat-spezifische Parameter**.

18.4.1.2 Mehrere Zertifikatpläne nutzen

Ein Abonnent kann beliebig viele Zertifikatpläne enthalten, die auch unterschiedliche Deploymentinfo für Agents verwenden.

Wird ein Zertifikatplan für Agent unterhalb eines Abonnentenkonto für Agent angelegt, ist er nur für dieses Abonnentenkonto verfügbar. Zertifikatpläne können auch zentral unterhalb des Container: Zertifikatpläne angelegt werden: **Container: PKI-Management → Container: Zertifikatpläne → Neu**. Dadurch stehen sie allen Abonnentenkonto für Agent-Objekten zur Verfügung. Sie können dort im Feld Zertifikatpläne ausgewählt werden. Dies kann z.B. genutzt werden, um CA-Zertifikate für die Validierung auf mehrere Zielsysteme zu verteilen. Dazu wird als Zertifikatquelle die Option **Bestehendes Zertifikat** verwendet.

Um bei Zertifikatplänen, die von mehreren Abonnenten genutzt werden, spezifische SANs angeben zu können, können SAN-Platzhalter eingefügt werden, die dann mit den konkreten Werten des Abonnenten ersetzt werden (siehe **26.2 Template-Variablen**).

18.4.2 Zertifikate ausrollen

18.4.2.1 Deploymentinfo für Agent anlegen

Das Deploymentinfo für Agent-Objekt legt fest, wie ein Zertifikat auf das Zielsystem übertragen wird. Es wird im Zertifikatplan für Agent-Objekt zugeordnet. Verschiedene Zertifikatpläne können dieselbe Deploymentinfo nutzen.

Reiter Allgemein:

Wichtig für die Deploymentinfo ist, das Betriebssystem des Zielsystem. Unter Ziel-OS stehen die Betriebssysteme **Linux**, **Windows** oder **Anderes** zur Auswahl. Sie bestimmen auch, welche Deployment-Methoden zur Verfügung stehen, und welche Skript-Sprache verwendet wird.

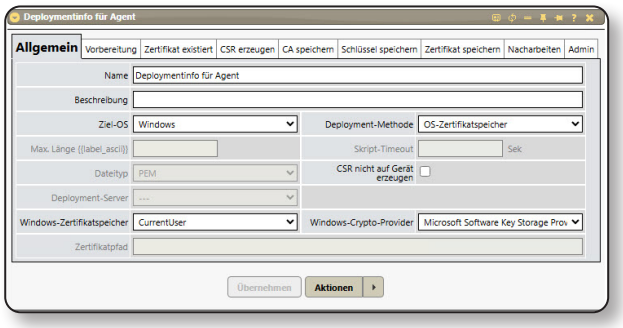


Abb. 18.09: *Deploymentinfo für Agent - Reiter Allgemein*

Die Deployment-Methode bestimmt die eigentliche Übertragungsart der Zertifikate auf das Zielsystem. Zur Auswahl stehen **OS-Zertifikatspeicher**, **Pfad/Verzeichnis**, **Shell-Skript** oder **HTTP-Skript**. Je nach Deployment-Methode werden unterschiedliche Konfigurationsmöglichkeiten freigeschaltet.

Die weiteren Reiter werden je nach Deployment-Methode und Notwendigkeit konfiguriert und enthalten Skripte für das Zertifikat-Enrollment auf die Zielsysteme.

Ist die Checkbox CSR nicht auf Gerät erzeugen aktiviert, wird der CSR nicht auf dem Zielsystem, sondern auf der TMA erzeugt. Dies kann z.B. notwendig sein, wenn das Zielsystem keinen brauchbaren Zufallsgenerator für die Schlüsselerzeugung besitzt.

Reiter Vorbereitung

Auf diesem Reiter können Skripte hinterlegt werden, die der Vorbereitung der eigentlichen Zertifikatverteilung dienen.

Reiter Zertifikat existiert

Hier können Skripte konfiguriert werden, die prüfen, ob auf dem Zielsystem bereits ein (gültiges) Zertifikat vorhanden ist.

Reiter CSR erzeugen

Auf diesem Reiter können Skripte hinterlegt werden, die ein Schlüsselpaar mit CSR als PEM auf dem Zielsystem erzeugen, sofern die Checkbox CSR nicht auf Gerät erzeugen nicht aktiviert ist.

Reiter CA speichern

Hier können Skripte zum Speichern von CA-Zertifikaten konfiguriert werden.

Reiter Schlüssel speichern

Auf diesem Reiter können Skripte zum Speichern von Schlüsseln hinterlegt werden.

Reiter Zertifikat speichern

Hier können Skripte zum Speichern von Zertifikaten konfiguriert werden.

Reiter Nacharbeiten

Auf diesem Reiter können Skripte hinterlegt werden, die nach der Zertifikatverteilung ausgeführt werden, z.B. um Dienste neu zu laden.

Auf jedem dieser Skripte-Reiter kann ein Regex hinterlegt werden, der den Erfolg des Skripts prüft.

⚠ **Hinweis:** Alle Skripte können Variablen verwenden, eine Übersicht mit ausführlichen Beispielen finden sich in **26 Certificate Enrollment Agent - Anhänge**.

18.4.2.2 Deployment-Methoden

Die Deployment-Methode legt die Übertragungsart der Zertifikate auf das Zielsystem fest. Sie ist abhängig vom Modus im Abonnentenkonto für Agent und dem Ziel-OS in der Deploymentinfo für Agent.

Nicht jede Kombination führt zu einer erfolgreichen Übertragung der Zertifikate auf das Zielsystem. Wird eine nicht unterstützte Kombination konfiguriert, bricht der Agent die Bearbeitung des betroffenen Zertifikatplans mit einer entsprechenden Fehlermeldung ab (siehe **26.3 Fehlersuche und Logging**).

Modus	Ziel-OS	OS-Zertifikatspeicher	Pfad/Verzeichnis	Shell-Skript	HTTP-Skript
Pull	Linux	✓	✓	✓	✓
Pull	Windows	✓	✓	✓	✓
Pull	Anderes	✗	✗	✗	✗
Push	Linux	✓	✓	✓	✓
Push	Windows	✓	✓	✓	✓
Push	Anderes	✗	✗	✓	✓

Im Weiteren werden die verschiedenen Deployment-Methoden mit Beispiel-Skripten auf den jeweiligen Reitern erklärt.

OS-Zertifikatspeicher

Mit der OS-Zertifikatspeicher-Methode werden Zertifikate direkt im Zertifikatspeicher des Betriebssystems gespeichert. Ein eigenes Speicher-Skript muss nicht konfiguriert werden. Lediglich ein Skript zum **Nacharbeiten** kann hinterlegt werden. Diese Methode steht für die Betriebssysteme Linux und Windos sowohl im **Pull**-, als auch im **Push**-Modus zur Verfügung.

Wird der **OS-Zertifikatspeicher** als Deployment-Methode ausgewählt, werden zusätzliche Einstellungen benötigt.

Bei Zielsystemen, die mit Windows laufen, muss zum einen der Windows-Zertifikatspeicher ausgewählt werden. Es bestimmt, ob die Zertifikate im Zertifikatspeicher des aktuellen Benutzers (**CurrentUser**) oder im Zertifikatsspeicher für Computer-Zertifikate (**LocalMachine**) hinterlegt werden. Standardmäßig ist **CurrentUser** ausgewählt.

Zum anderen muss der Windows-Crypto-Provider bestimmt werden. Standardmäßig ist der **Microsoft Software Key Storage Provider** ausgewählt.

Beispiel: Skript zum Neustart einer Anwendung

Reiter Nacharbeiten:

```
# Skript: Nacharbeiten
Restart-Service -Name "MeineAnwendung"
```

Unter Linux entspricht diese Methode einem Datei-Keystore unterhalb von `~/.ecos-tma/certs`. Auch hier kann ein Skript zum **Nacharbeiten** konfiguriert werden.

Pfad/Verzeichnis

Mit der **Pfad/Verzeichnis**-Methode werden Zertifikate und Schlüssel in einem festen, konfigurierbaren Verzeichnis abgelegt. Der Verzeichnisname bleibt über mehrere Zertifikaterneuerungen stabil, so dass eine Anwendung ihn festreferenzieren kann. Diese Methode steht für die Betriebssysteme Linux und Windos sowohl im **Pull**-, als auch im **Push**-Modus zur Verfügung.

Wird **Pfad/Verzeichnis** als Deployment-Methode ausgewählt, werden zusätzliche Einstellungen benötigt.

Der Verzeichnispfad, über den das Zielsystem die Zertifikate und Schlüssel herunterladen kann, wird im Feld Zertifikatpfad festgelegt, unter Linux z.B. `/etc/myapp/tls`.

Es kann ein Skript zum **Nacharbeiten** hinterlegt werden.

Beispiel: Skript zum Neustart einer Anwendung

Reiter Nacharbeiten

```
# Skript: Nacharbeiten
sudo systemctl reload myapp
```

Shell-Skript

Beim **Shell-Skript** werden Zertifikate und CSRs über frei konfigurierbare Skripte geprüft, erzeugt und gespeichert. Es bietet eine hohe Flexibilität. Es kann im **Pull**-Modus mit den Betriebssystemen Linux und Windows genutzt werden. Im **Push**-Modus kann es für jedes Betriebssystem konfiguriert werden.

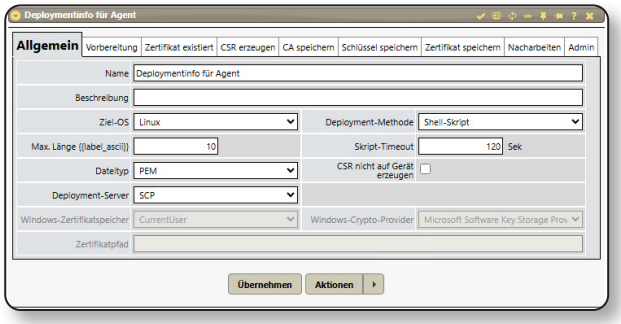


Abb. 18.10: *Deploymentinfo für Agent - Shell-Skript*

Wird das **Shell-Skript** als Deployment-Methode ausgewählt, werden zusätzliche Einstellungen benötigt.

Es sollte eine Max. Länge {{label_ascii}} festgelegt werden. Dies ist notwendig, wenn das Zielsystem keine langen Dateinamen verarbeiten kann.

Das Skript-Timeout bestimmt die maximale Laufzeit der einzelnen Skripte in Sekunden.

Unter Dateityp wird das Dateiformat der Zertifikate festgelegt, die auf das Zielsystem übertragen werden. Zur Auswahl stehen **PEM**, **PEM (Zertifikat & Schlüssel)**, **PEM (incl. CAs)**, **DER**, **PKCS#7** und **PKCS#12**.

Im Feld Deployment-Server kann ein Protokoll für die Übertragung gewählt werden, wenn das Zielsystem Dateien von der TMA herunterladen soll. Es stehen die Protokolle **SCP** oder **SFTP** zur Verfügung. Der Deployment-Server läuft nur, wenn ein Skript ausgeführt wird. Wird kein Protokoll ausgewählt, startet der Server nicht, selbst wenn ein Skript ausgeführt wird.

⚠ **Hinweis:** Alle Skripte können Variablen verwenden, eine Übersicht mit ausführlichen Beispielen finden sich in **26.2 Template-Variablen**.

Beispiel: Deployment mit Linux-OS, OpenSSL-Skripte für Apache-Webserver

Reiter Zertifikat existiert:

```
# Skript: Zertifikat existiert
diff -q <(openssl x509 -in {{cert_dir}}/cert.pem -pubkey -noout -outform pem) \
        <(openssl pkey -in {{cert_dir}}/key.pem -pubout -outform pem) \
  && openssl x509 -noout -fingerprint -sha256 -in {{cert_dir}}/cert.pem
true
```

Regex: Zertifikat ist gültig: `(?i)sha256 Fingerprint={{fingerprint}}`

Reiter CSR erzeugen

```
# Skript: CSR erzeugen als PEM
mkdir -p {{cert_dir}} || exit $?
openssl req -new -utf8 -nodes \
    -subj '{{subject_compat}}' \
    -keyout {{cert_dir}}/key.pem -out {{cert_dir}}/req.pem \
    {{#if keytype.RSA}}
      -newkey rsa:{{keytype.RSA.key_size}} \
    {{else}}
      -newkey ec -pkeyopt 'ec_paramgen_curve:{{keytype.EC.curve_name}}' \
    {{/if}}
    || exit $?
cat {{cert_dir}}/req.pem || exit $?
```

Reiter CA speichern:

```
# Skript: CA speichern
mkdir -p {{cert_dir}} || exit $?
cat - <<EOF > {{cert_dir}}/ca.pem
{{ca_pem_fullchain}}
EOF
```

Reiter Schlüssel speichern:

```
# Skript: Schlüssel speichern
mkdir -p {{cert_dir}} || exit $?
cat - <<EOF > {{cert_dir}}/key.pem
{{key_pem}}
EOF
chmod 600 {{cert_dir}}/key.pem
```

Reiter Zertifikat speichern:

```
# Skript: Zertifikat speichern
mkdir -p {{cert_dir}} || exit $?
cat - <<EOF > {{cert_dir}}/cert.pem
{{cert_pem}}
EOF
```

Reiter Nacharbeiten:

```
# Skript: Nacharbeiten
install -m 644 {{cert_dir}}/cert.pem /etc/ssl/certs/{{label_ascii}}.crt
install -m 600 {{cert_dir}}/key.pem  /etc/ssl/private/{{label_ascii}}.key
install -m 644 {{cert_dir}}/ca.pem   /etc/ssl/certs/{{label_ascii}}-ca.crt
sudo systemctl reload apache2
```

Beispiel: Deployment mit Windows, PowerShell mit .NET-Boardmitteln

Für Windows-Systeme werden im Regelfall PowerShell-Skripte hinterlegt.

Reiter Zertifikat speichern:

```
# Skript: Zertifikat speichern
[System.IO.File]::WriteAllText("{{cert_dir}}\cert.pem", "{{ps_escape cert_pem}}",
[System.Text.Encoding]::ASCII)
```

Reiter Nacharbeiten:

```
# Skript: Nacharbeiten
Import-Certificate -FilePath "{{cert_dir}}\cert.pem" -CertStoreLocation Cert:\Local-
Machine\My
Restart-Service -Name "MeineAnwendung"
```

HTTP-Skript

Beim **HTTP-Skript** erfolgt die Übertragung per HTTP(S)-Anfragen (Hurl-Skript), z.B. um Zertifikate über die REST-API einer Anwendung zu verteilen. Es kann im **Pull**-Modus mit den Betriebssystemen Linux und Windows genutzt werden. Im **Push**-Modus kann es für jedes Betriebssystem konfiguriert werden.

Wird das **HTTP-Skript** als Deployment-Methode ausgewählt, werden zusätzliche Einstellungen benötigt.

Es sollte eine Max. Länge {{label_ascii}} festgelegt werden. Dies ist notwendig, wenn das Zielsystem keine langen Dateinamen verarbeiten kann.

Das Skript-Timeout bestimmt die maximale Laufzeit der einzelnen Skripte in Sekunden.

Unter Dateityp wird das Dateiformat der Zertifikate festgelegt, die auf das Zielsystem übertragen werden. Zur Auswahl stehen **PEM**, **PEM (Zertifikat & Schlüssel)**, **PEM (incl. CAs)**, **DER**, **PKCS#7** und **PKCS#12**.

Beispiel: Zertifikat per PUT-Anfrage in DER-Format an eine Anwendung übertragen

Reiter Schlüssel speichern:

```
# Skript: Schlüssel speichern
PUT https://10.1.2.3/api/v2/certificates/{{label_ascii}}/key
Content-Type: application/octet-stream
base64,{{key_der_base64}}
HTTP 200
```

Reiter Zertifikat speichern:

```
# Skript: Zertifikat speichern
PUT https://10.1.2.3/api/v2/certificates/{{label_ascii}}
Content-Type: application/octet-stream
base64,{{cert_der_base64}}
HTTP 200
```

⚠ **Hinweis:** Der Agent verwendet für das Ausführen von HTTP(S)-Anfragen das Tool Hurl und kann entsprechende Skripte ausführen. Informationen zum Tool und den Skripten finden sich unter: https://hurl.dev/docs/entry.html.

18.4.3 Ablauf der Zertifikatverteilung

Für jeden Zertifikatplan für Agent ist der Ablauf gleich:

1. Es wird geprüft, ob auf dem Zielsystem bereits ein gültiges Zertifikat vorhanden ist (Deployment für Agent → **Zertifikat existiert**). Ist als Zertifikatquelle die Option **Bestehendes Zertifikat** gewählt, entfällt dieser Schritt. Das Zertifikat wird direkt übertragen, wenn es sich geändert hat.
2. Falls notwendig wird ein CSR erzeugt, entweder auf dem Zielsystem oder auf der TMA, wenn die Checkbox CSR nicht auf Gerät erzeugen aktiviert ist, und das Zertifikat bei der TMA beantragt.
3. Entsprechend der gewählten Deployment-Methode werden Zertifikat, Schlüssel, CA-Kette und ggf. die CRL auf dem Zielsystem abgelegt.
4. Nachdem alle Zertifikatpläne eines Abonnenten abgearbeitet wurden, wird das Nacharbeiten-Skript jedes geänderten Deployments ausgeführt.

18.4.4 Zertifikate verlängern

Um bestehende Zertifikate automatisch zu verlängern, wird eine Abfrage mit Aktion angelegt. Damit können Zertifikate automatisch vor Ablauf verlängert werden. Informationen zum Konfigurieren einer Abfrage mit Aktion zum Verlängern von Zertifikaten finden sich unter **21.5 Beispiel: Abfrage mit Aktion zum automatischen Verlängern von Zertifikaten und CRLs**.

Um die verlängerten Zertifikate auf das Zielsystem zu übertragen, wird im Zertifikatplan für Agent, der zum verlängerten Zertifikat gehört, die Zertifikatquelle auf **Bestehendes Zertifikat** geändert. Soll auch der private Schlüssel mit übertragen werden, wird die Option **Bestehendes Zertifikat + privater Schlüssel** gewählt.

Zusätzlich wird das Zertifikat im Feld Zu übertragende Zertifikate ausgewählt.

Beim nächsten Durchgang wird das frisch verlängerte Zertifikat auf das Zielsystem übertragen.

19 Verzeichnissynchronisation

Mittels der Verzeichnissynchronisation ist es möglich, Objekte aus einem Verzeichnisdienst zu im- oder exportieren, z. B. können Benutzerobjekte automatisch angelegt werden, die im Active Directory (AD) in einer bestimmten Gruppe Mitglied sind. Dazu werden die drei Konfigurationsobjekte Verzeichnisdienst, Verzeichnis-Map und Verzeichnissynchronisation benötigt.

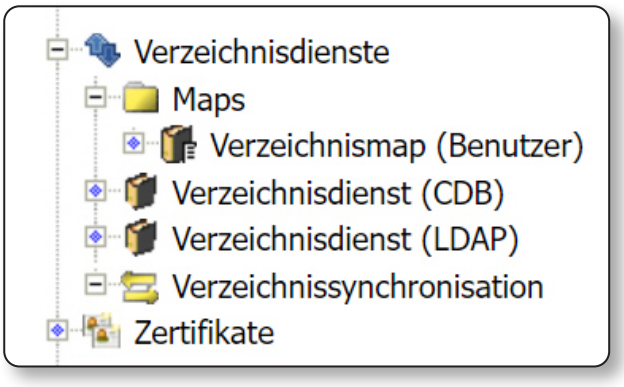


Abb. 19.01: *Verzeichnissynchronisation im Navigationsbaum*

19.1 Verzeichnisdienst konfigurieren

Es werden zwei Konfigurationsobjekte Verzeichnisdienst benötigt. In einem wird die Quelle und im anderen das Ziel der Verzeichnissynchronisation konfiguriert.

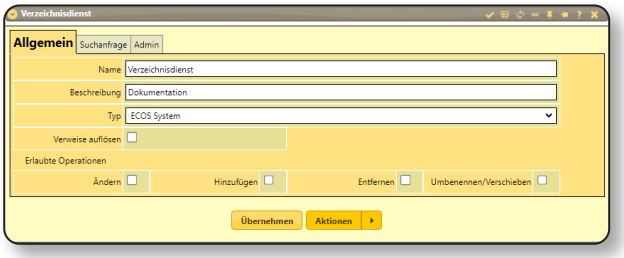


Abb. 19.02: *Verzeichnisdienst - Typ ECOS System*

Im Feld Typ wird der Typ des Verzeichnisses ausgewählt. Einer der folgenden Werte ist möglich:

ECOS System: die ECOS **TrustManagement-Appliance®** selbst

LDAP: ein beliebiger LDAP-Server

Microsoft ADS: Microsoft Active Directory

Datei: Eine externe Datei im CSV- oder XML-Format.

Je nach Auswahl öffnet sich ein Untermenü, in welchem die notwendigen Einstellungen für den jeweiligen Typ getroffen werden.

Unter Erlaubte Operationen werden folgende Lese- und Schreibberechtigungen für das Verzeichnis vergeben:

Ändern: Objekte dürfen geändert werden.

Hinzufügen: Die Verzeichnissynchronisation darf neue Objekte hinzufügen.

Entfernen: Die Verzeichnissynchronisation darf bestehende Objekte löschen, soweit sie im Quellverzeichnis nicht mehr vorhanden sind.

Umbenennen/Verschieben: Die Verzeichnissynchronisation darf bestehende Objekte verschieben und umbenennen.

Im Reiter Suchanfrage können weitere Einstellungen zur Suche der zu synchronisierenden Objekte getroffen werden.

Im Feld Such-Basis DN wird die Basis angegeben, unter der die zu synchronisierenden Objekte für den Report gesucht werden. Hier ist die Angabe eines vollständigen DNs notwendig. Wird das Feld leer gelassen, wird das gesamte Verzeichnis durchsucht. Bei dem Ziel Verzeichnisdienstobjekt legt das Feld Such-Basis-DN den Container fest, in dem die neuen Objekte angelegt werden.

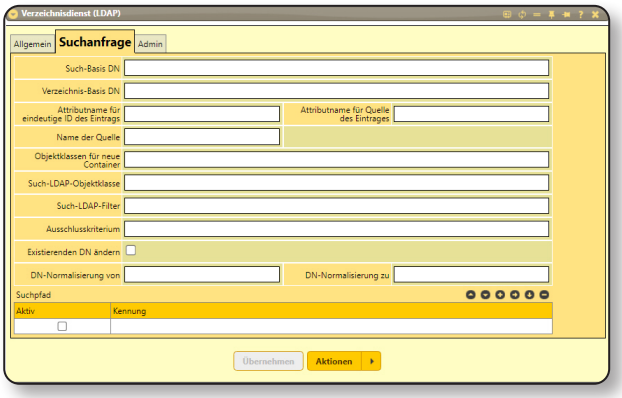


Abb. 19.03: *LDAP - Reiter "Suchanfrage"*

Beim Typ **LDAP** kann ein LDAP-Suchfilter angegeben werden und so die Quellobjekte z. B. auf eine Gruppe eingeschränkt werden.

19.2 Verzeichnis-Map konfigurieren

Im Objekt Verzeichnis-Map wird eine Attributliste angelegt, in der die Quellattribute entsprechenden Zielattributen zugeordnet werden. Im Feld Quell-Objektklasse wird die Objektklasse definiert, für die das Mapping angewendet werden soll. Das Feld Ziel-Objektklasse gibt an, welche Objektklasse beim Anlegen neuer Objekte verwendet wird.

Das ECOS System hat bereits verschiedene Default-Mappings vorkonfiguriert. Mithilfe des Feldes Default Map erzeugen und Klicken auf **Übernehmen**, können diese aufgerufen werden. Dabei werden alle anderen Felder überschrieben. Die vorkonfigurierten Felder können anschließend bei Bedarf noch angepasst werden.

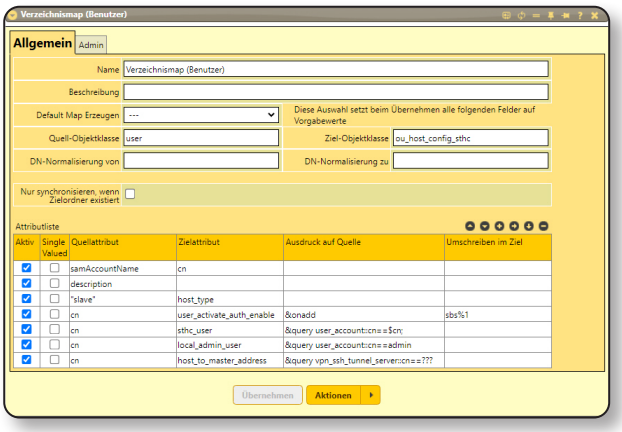


Abb. 19.04: *Verzeichnismap einrichten*

Es können mehrere Verzeichnis-Map-Objekte in einem Container angelegt werden, in denen das Mapping einzelner Objektklassen definiert wird. Der Container kann anschließend im Objekt Verzeichnissynchronisation als Map übergeben werden. Dadurch ist es möglich, aus einem Quellobjekt (z. B. aus einem Benutzer), mehrere Zielobjekte (z. B. einen Benutzer und ein Zertifikat) anzulegen.

19.3 Verzeichnissynchronisation konfigurieren

Im Konfigurationsobjekt Verzeichnissynchronisation müssen Quelle und Ziel, sowie eine Map zwischen den beiden Verzeichnissen angegeben werden.

Durch Setzen eines Häkchens bei Starten wird die automatische Verzeichnissynchronisation aktiviert. Wann diese jeweils ausgeführt wird, wird im übergeordneten Container: Verzeichnisdienste festgelegt. Eine manuelle Verzeichnissynchronisation kann unabhängig davon, ob das Objekt aktiviert ist oder nicht, ausgeführt werden.

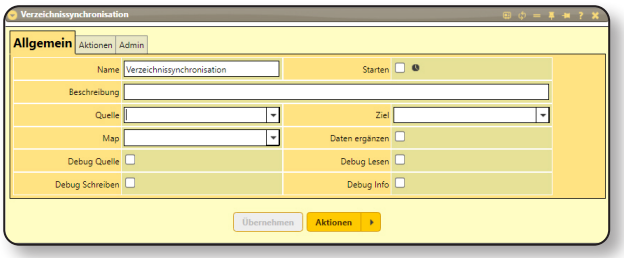


Abb. 19.05: *Verzeichnissynchronisation einrichten*

Die Felder Quelle und Ziele bestimmen den Provider, welcher die Quelldaten zur Verfügung stellt, bzw. den Provider, über den die Daten in das Zielverzeichnis geschrieben werden.

Im Feld Map wird das Verzeichnis-Map-Objekt referenziert, in dem festgelegt ist, welche Attribute synchronisiert werden und wie diese gegebenenfalls einander zugeordnet werden. Es kann auch ein Container mit mehreren Mapping-Objekten ausgewählt werden. In diesem Fall wird das passende Mapping anhand der Quellklasse im Mapping-Objekt bestimmt bzw. mehrere Zielobjekte angelegt, wenn mehrere Quell-Objektklassen übereinstimmen.

Ist das Häkchen bei Daten ergänzen gesetzt, werden in bestehenden Objekten Daten hinzugefügt, nicht aber neue Objekte angelegt oder bestehende Objekte gelöscht. Dies ist nur dann sinnvoll, wenn mehrere Verzeichnissynchronisationen in das gleiche Zielobjekt schreiben sollen. Normalerweise sollte diese Option nicht ausgewählt sein.

Über den Reiter Aktionen kann die Synchronisation manuell über den Button **Start** angestoßen werden und die Verzeichnissynchronisation wird direkt gestartet. Dies geschieht unabhängig davon, ob das Häkchen bei Starten im Objekt gesetzt ist.

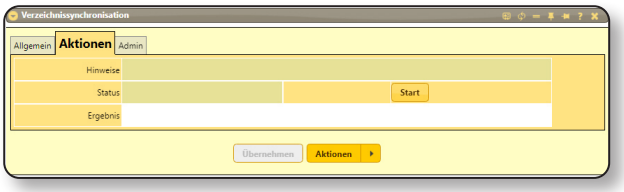


Abb. 19.06: *Manuelle Synchronisation anstoßen*

20 Hochverfügbarkeit

Die Hochverfügbarkeitskonfiguration (auch HA für High Availabilty genannt) dient dazu, beim Ausfall eines Systems den Betrieb sicherzustellen. Dazu werden zwei oder mehr Appliances so konfiguriert, dass die notwendigen Funktionen von mehr als einer Appliance zur Verfügung gestellt werden können. Im Normalbetrieb ist es dabei sowohl möglich, dass nur eine Appliance aktiv ist, wie auch, dass mehrere Appliances aktiv sind. In diesem Fall besteht die Möglichkeit eine Lastverteilung für bestimmte Dienste einzurichten. Alle Appliances zusammen bilden ein Cluster.

Das Vertrauen zwischen verschiedenen Appliance-Instanzen der TMA wird hergestellt, indem die öffentlichen Schlüssel der betreffenden Instanzen untereinander ausgetauscht werden. Danach können sich die Instanzen gemäß Public-Key-Authentisierung des SSH-Protokolls sicher gegenseitig identifizieren.

Technisch erfolgt dies durch die Übertragung der Konfiguration von einer Master-Appliance zu einer Slave-Appliance **20.4 Synchronisation aufbauen.**

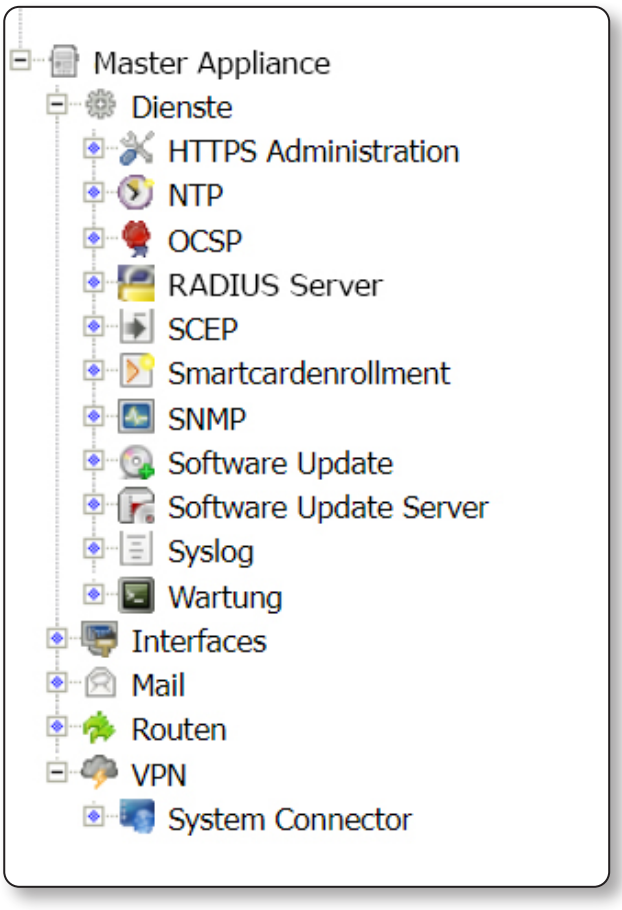


Abb. 20.01: *Container der Master-Appliance*

20.1 Voraussetzungen für High Availability (HA)

Um ein Cluster aufzubauen und hochverfügbar zu machen, müssen mindestens zwei ECOS Appliance-Objekte konfiguriert werden:

- Genau eine Appliance vom Systemtyp **Master**
- Eine oder mehrere Appliances vom Systemtyp **Vollständige Synchronisation**

Das Master-System ist das erste System, welches konfiguriert wird. Auf diesem wird die vollständige Konfiguration erstellt. Dieses Objekt wird als Master-Appliance bezeichnet.

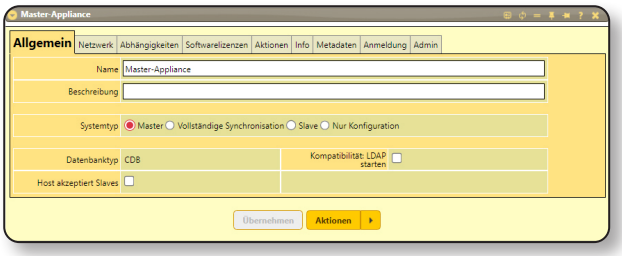


Abb. 20.02: *Einrichten der Master-Appliance*

Nach dem Erstellen der Konfiguration auf dem Master wird eine bidirektionale Synchronisation mit diesem System eingerichtet. Im Folgenden wird es als Master-Slave-Verbindung genannt. Danach sind beide Systeme gleichberechtigt. Dieses Objekt wird als vollsynchronisierte Slave-Appliance bzw. Slave-Appliance bezeichnet.

Optional können noch weitere System-Objekte angelegt werden, die der Vereinfachung der Konfiguration bzw. dem Umschwenken der Konfiguration zwischen den Systemen beim Ausfall eines Systems dienen. Diese Appliance-Objekte sind vom Systemtyp **Nur Konfiguration**.

Das Vertrauen zwischen verschiedenen Appliance-Instanzen der TMA wird hergestellt, indem die öffentlichen Schlüssel der betreffenden Instanzen untereinander ausgetauscht werden. Danach können sich die Instanzen gemäß Public-Key-Authentisierung des SSH-Protokolls sicher gegenseitig identifizieren.

Technisch erfolgt dies durch die Übertragung der Konfiguration von einer Master-Appliance zu einer Slave-Appliance (siehe **20.4 Synchronisation aufbauen**).

20.1.1 Master-Appliance einrichten

Die Master-Appliance benötigt ein ECOS System Connector-Objekt, damit sich die Slave-Appliance verbinden kann. Der ECOS System Connector wird unter der ECOS Appliance im Container: VPN angelegt. Damit er aktiv ist, muss das Häkchen bei Starten gesetzt sein. Zusätzlich muss die Netzwerkadresse, über die er erreichbar sein soll, im Feld Lokale Adresse für externe Anfragen angegeben werden. Optional kann zusätzlich eine Lokale Adresse für Anfragen aus dem LAN angegeben werden. Es ist nur eine der beiden Adressen notwendig, diese muss aber von der Slave-Appliance aus erreichbar sein. Im Feld Port kann der gewünschte Port für die Master-Slave-Verbindung konfiguriert werden. Wird kein Port angegeben, wird der Standard-Port 909 verwendet.

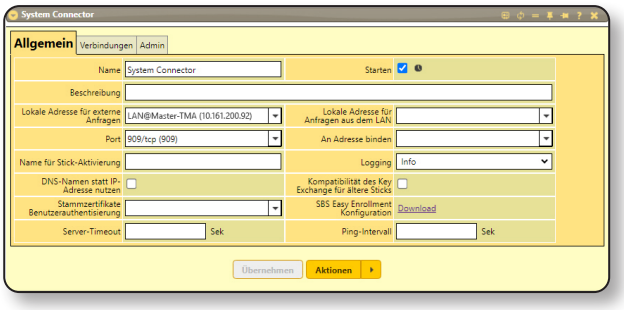


Abb. 20.03: *ECOS System Connectors für eine Master-Appliance*

Um die Konfigurationen verteilen zu können, wird das Dienst: Software Update Server-Objekt benötigt. Dieses wird unterhalb der Master-Appliance im Container: Dienste angelegt. Damit es aktiv ist, muss das Häkchen bei Starten gesetzt sein.

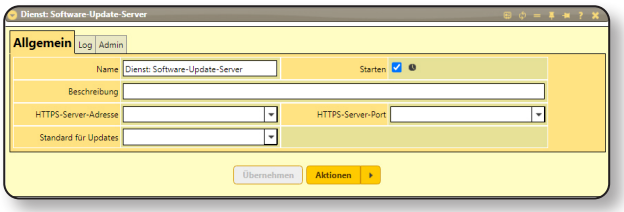


Abb. 20.04: *Aktivieren des Software-Update-Servers*

20.1.2 Vollsynchronisierte Slave-Appliance einrichten

Um die Slave-Appliance anzulegen, dupliziert man am einfachsten die Konfiguration der Master-Appliance und passt diese an. Hierzu wählt man bei der Master-Appliance durch Klicken auf die Schaltfläche **Aktionen** die Option Duplizieren. Es wird eine zweite Appliance erstellt.

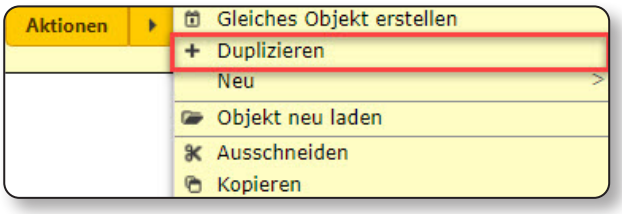


Abb. 20.05: *Duplizieren des Appliance-Objekts*

Im Formular der zweiten Appliance muss zunächst der Name geändert werden und der Systemtyp auf **Vollständige Synchronisation** eingestellt werden.

Im Feld Masteradresse wird der zuvor angelegte ECOS System Connector ausgewählt. Bei Lokaler Admin-Benutzer muss ein Benutzer, der dadurch Admin-Rechte auf der Slave-Appliance bekommt, ausgewählt werden. Gegebenenfalls muss im Reiter Netzwerk, das Gateway sowie der DNS-Server angepasst werden.

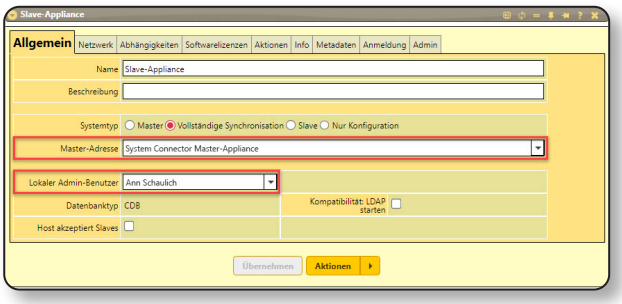


Abb. 20.06: *Slave-Appliance einrichten*

Weiterhin ist es notwendig, die IP-Adresse im Netzwerk-Interface-Objekt abzuändern. Ggf. sind weitere Abweichungen zwischen den Appliances entsprechend anzupassen. Das ECOS System Connector-Objekt kann auf der Slave-Appliance gelöscht werden.

20.2 Vereinfachung der Konfiguration durch Vererbung

Es besteht die Möglichkeit, Konfigurationsobjekte, die für beide Appliances gleich sind, in eine gemeinsame Basis-Konfiguration auszulagern. Dies hat den Vorteil, dass die Konfiguration nur einmal vorhanden sein muss und dass bei Änderungen diese automatisch auf beide Appliances angewendet wird.

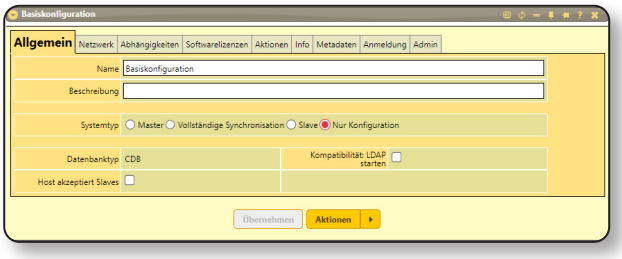


Abb. 20.07: *Appliance-Objekt für Basiskonfiguration*

20.2.1 Basis-Konfiguration erstellen

Eine Basis-Konfiguration wird wie eine normale Appliance angelegt, nur, dass im Appliance-Objekt beim Systemtyp **Nur Konfiguration** ausgewählt wird. Ansonsten können unterhalb des Appliance-Objektes alle Konfigurationsobjekte ganz normal angelegt werden und bilden damit die Basis-Konfiguration.

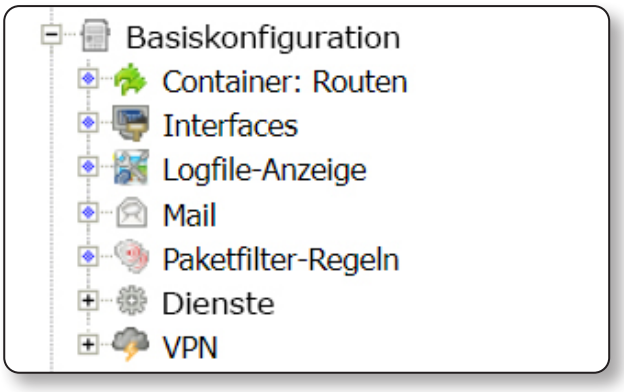


Abb. 20.08: *Container der Basiskonfiguration*

20.2.2 Vererbung konfigurieren

Bei allen Appliances, die von einer Basis-Konfiguration erben sollen, muss auf dem Reiter **Abhängigkeiten** im Feld Basiert auf das Basis-Objekt ausgewählt werden.

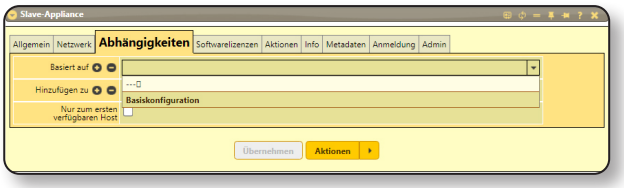


Abb. 20.09: *Vererbung der Basiskonfiguration einrichten*

Die so konfigurierten Systeme erben nun die Konfiguration der Basis-Konfiguration, d.h. alle Dienste, die in der Basis-Konfiguration angelegt sind, werden damit auch Teil der Konfiguration des Systems, das erbt. Sind in der Konfiguration des Systems, das erbt, bereits Konfigurationen vorhanden, so haben diese Vorrang vor der Konfiguration in der Basis-Konfiguration. Für Objekte, von denen es mehr als eines geben kann (wie z.B. Netzwerk-Interfaces), werden sowohl die Konfigurationsobjekte aus der Basis-Konfiguration, als auch die Konfigurationsobjekte aus dem System, das erbt, Teil der Konfiguration.

Eine Appliance kann dabei von mehr als einer Basis-Konfiguration erben, ebenso wie Basis-Konfigurationen wieder von anderen Basis-Konfigurationen erben können.

Soweit vorhanden, können Konfigurationen, die auf allen Appliances vorhanden sind, damit in die Basis-Konfiguration verschoben werden.

20.3 Konfiguration bei Ausfall umschwenken

Es besteht die Möglichkeit, Konfigurationseinstellungen nur auf einem System zu aktivieren und diese bei Ausfall dieses Systems, auf ein anderes System umzuschwenken. Dies ermöglicht z.B. das „Wandern“ einer HA-IP-Adresse von einem System zum anderen, sobald das System, auf dem die HA-IP-Adresse konfiguriert wurde, nicht mehr verfügbar ist. Dadurch sind nun unter der gleichen IP-Adresse die Dienste der zweiten Appliance erreichbar. Dies ist nicht nur für IP-Adressen, sondern für jegliche Konfiguration möglich.

20.3.1 HA-Konfiguration einrichten

Konfigurationseinstellungen, die von einem System zum anderen „wandern“ sollen, werden als HA-Konfiguration, ähnlich wie eine Basis-Konfiguration angelegt Auch hier ist der Systemtyp **Nur Konfiguration** zu wählen.

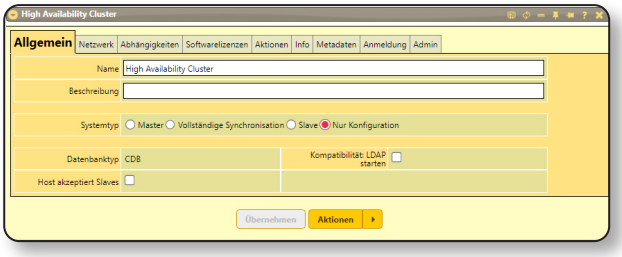


Abb. 20.10: *Einrichten der Appliance als HA-Basiskonfiguration*

20.3.1.1 HA-Konfiguration zu Appliance-Objekten hinzufügen

Um den gewünschten Effekt zu erzielen, muss im Appliance-Objekt der HA-Konfiguration ausgewählt werden, zu welchen Systemen sie hinzugefügt werden soll. Dazu auf dem Reiter **Abhängigkeiten**, über das Feld Hinzufügen zu die Master-Appliance und dann die Slave-Appliance auswählen. Wird ein Haken bei Nur zum ersten verfügbaren Host gesetzt, wird die HA-Konfiguration nur zu der Konfiguration hinzugefügt, die als erstes in der Liste angegeben ist. Ist dieses System nicht verfügbar, so wird sie zum zweiten Objekt hinzugefügt. Dadurch „wandert“ die Einstellung der HA-Konfiguration quasi zwischen den Systemen, sobald das erste System nicht mehr verfügbar ist oder wieder verfügbar wird.

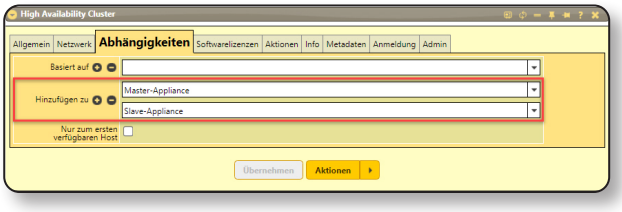


Abb. 20.11: *Einrichten der HA-Konfiguration*

20.4 Synchronisation aufbauen

20.4.1 Übertragung der Konfiguration vom Master zum Slave

Um die Konfiguration zu übertragen, wird im Konfigurationsobjekt der Master-Appliance auf dem Reiter **Aktionen** die Option **Konfigurationsexport** ausgewählt. Es öffnet sich ein Untermenü, in dem die Felder Admin-Benutzer des Zielsystems, Admin-Kennwort, Adresse des Zielsystems und Port des Admin-Interface gefüllt werden müssen.

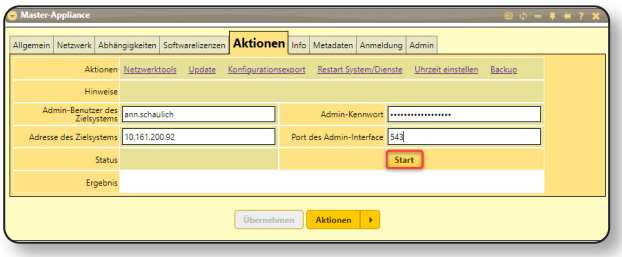


Abb. 20.12: *Konfiguration von Master zu Slave übertragen*

Durch Klicken auf die Schaltfläche **Start** wird der Konfigurationsexport gestartet, die öffentlichen Schlüssel der Appliance-Instanzen ausgetauscht, um die gegenseitige Vertrauensstellung herzustellen und die Synchronisation eingerichtet.

20.4.2 Privater Schlüssel der CA übertragen

Aus Sicherheitsgründen wird der private Schlüssel der CAs während der Konfigurationsübertragung nicht weitergegeben. Private Schlüssel der Root-CAs werden nicht synchronisiert. Damit der private Schlüssel vom Master auf die Slave-Appliance übertragen wird, muss auf der Master-Appliance im CA-Objekt über das Feld Zertifikat als PKCS#12 der private Schlüssel heruntergeladen werden und dann im Admin-Interface der Slave-Appliance im selben Objekt wieder hochgeladen werden.

20.4.3 Systeme prüfen

Im System Connector-Objekt im Reiter Verbindungen wird angezeigt, welche die Slave-Appliances sind, mit denen der Master sich verbunden hat.

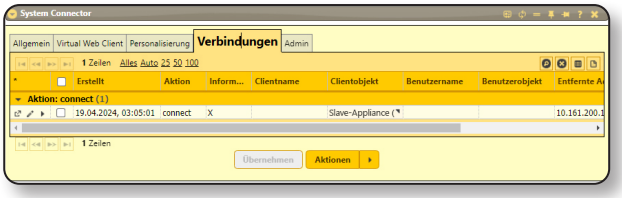


Abb. 20.13: *Verbindungen zum Master*

Um die Synchronisation zu testen, können Konfigurationsänderungen auf einer Appliance vorgenommen werden (z.B. Name oder Beschreibung). Bei erfolgreicher Synchronisation kann man die Änderung im Admin-Interface der anderen Appliances sehen. Änderungen werden in beide Richtungen übertragen.

21 Abfragen

Mithilfe des Abfrage-Objektes lassen sich Übersichtstabellen von beliebigen anderen Konfigurationsobjekten erstellen und verwalten. Die Tabelle besitzt dabei alle Eigenschaften und Funktionen, die im Kapitel zu den Tabellen erläutert sind.

Das Formular des Abfrage-Objektes besteht aus den Reitern **Allgemein, Abfrage, Felder** und **Hervorhebungen**.

21.1 Reiter Allgemein

Im Reiter **Allgemein** kann der Name des Konfigurationsobjektes und, falls gewünscht, eine Beschreibung eingegeben werden. Außerdem wird die Übersichtstabelle angezeigt.

Die Konfiguration der Tabelle erfolgt in den weiteren Reitern.

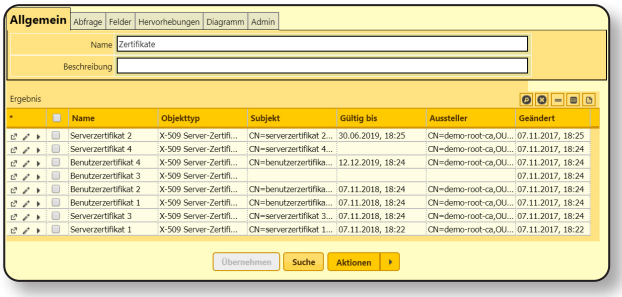


Abb. 21.01: *Abfrage - Reiter "Allgemein"*

21.2 Reiter Abfrage

21.2.1 Auswahl des Objekttyps

Im Reiter **Abfrage** wird zunächst der Objekttyp bestimmt, für den eine Abfrage erstellt werden soll. Nach Auswahl eines Objekttyps, wie im Beispiel Zertifikat, werden alle Konfigurationsobjekte dieses Typs in der Tabelle aufgelistet.

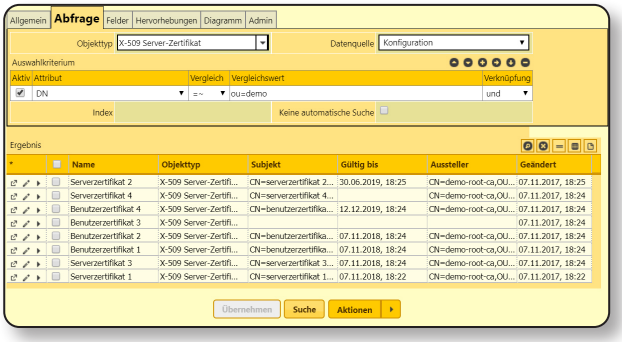


Abb. 21.02: *Abfrage - Reiter "Abfrage"*

21.2.2 Erstellen von Vergleichen der Attribute

Sollen nur Konfigurationsobjekte mit einem bestimmten Attributwert angezeigt werden, kann das im Reiter **Abfrage** eingestellt werden. Dafür das gewünschte Attribut aus der Dropdownliste, das erscheint, wenn man auf den Pfeil im Feld Attribut klickt, auswählen, wie im Beispiel **Gültig bis** und den Vergleich, mit dem der Attributwert verglichen werden soll.

Mögliche Vergleichsoperatoren:

Vergleichsoperator	Vergleich	Erklärung
==	gleich	
!=	ungleich	

Vergleichsoperator	Vergleich	Erklärung
>	größer	
<	kleiner	
>=	größer gleich	
<=	kleiner gleich	
=*	Wildcard	Suche nach Begriffen, die Platzhalter enthalten: ? für genau ein Zeichen * für beliebig viele (auch keine) Zeichen
!*	nicht Wildcard	gibt alle Werte zurück, die nicht den Vergleichswert enthalten (Gegenteil von Wildcard)
=~	Regulärer Ausdruck	http://perldoc.perl.org/perlre.html#Regular-Expressions
!~	nicht regulärer Ausdruck	gibt alle Werte zurück, die den regulären Ausdruck nicht enthalten

Das Feld Vergleichswert passt sich dabei immer dem ausgewählten Attribut an. Handelt es sich um ein Datum wie bei **Gültig bis**, wird ein Kalender angezeigt, in dem man den Vergleichswert auswählen kann (alternativ lässt sich das Datum auch eintippen).

Wählt man dagegen zum Beispiel **CA**, erscheint durch Anklicken des Pfeils im Feld Vergleichswert eine Dropdownliste mit den möglichen Eingaben.

Bei einem Datumsfeld besteht des Weiteren die Möglichkeit, einen Ausdruck wie z. B. **d+30** einzugeben. Dabei steht **d** für day (Tag) und **+30** für die Anzahl der Tage, also 30 Tage nach dem heutigen Tag. Wahlweise besteht die Möglichkeit **m** für month (Monat) und **y** für year (Jahr) zu verwenden. Soll ein Datum in der Vergangenheit ausgewählt werden, wird anstatt dem **+** ein **-** verwendet. Auf diese Weise lassen sich Abfragen in Abhängigkeit vom aktuellen Datum erstellen. Zum Beispiel: Welches Zertifikat läuft in den nächsten 30 Tagen aus?

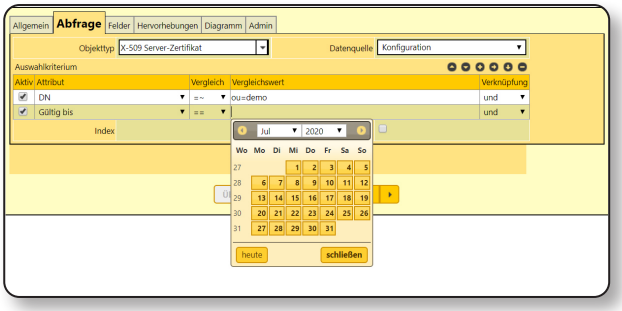


Abb. 21.03: *Datum auswählen*

Im folgenden Beispiel werden nur Zertifikate aufgelistet, deren Gültigkeit vor dem 31.12.2020 ausläuft und bei deren CA es sich um die **ECOS Demo CA** handelt.

Mittels der Symbole **+** und **-** aus der Symbolleiste der Auswahlfunktion lassen sich weitere Vergleiche hinzufügen bzw. bereits vorhandene Vergleiche löschen.

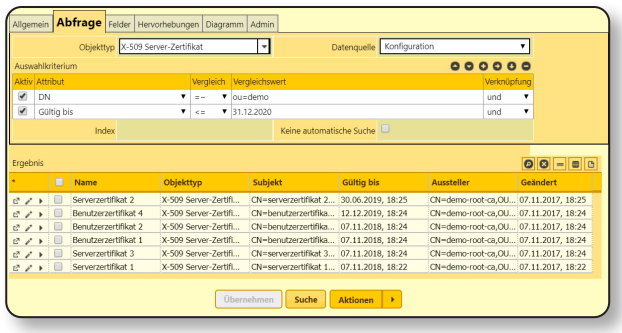


Abb. 21.04: *Abfrage für ablaufende Zertifikate*

Um einen Vergleich zu löschen, muss er zuvor durch Anklicken markiert werden.

Änderungen werden erst angezeigt, wenn der Vergleich durch einen Haken bei Aktiv aktiviert wurde und die Änderungen durch **Übernehmen** abgespeichert wurden.

21.2.3 Keine automatische Suche

Normalerweise lädt sich die Tabelle der Abfrage automatisch, wenn die Abfrage geöffnet wird und jedes Mal, wenn Parameter der Abfrage geändert und durch **Übernehmen** bestätigt werden. Wird ein Haken bei Keine automatische Suche gesetzt, wird dies unterbunden.

Mithilfe der Schaltfläche **Suchen** am Ende des Formulars, wird die Tabelle manuell neu geladen.

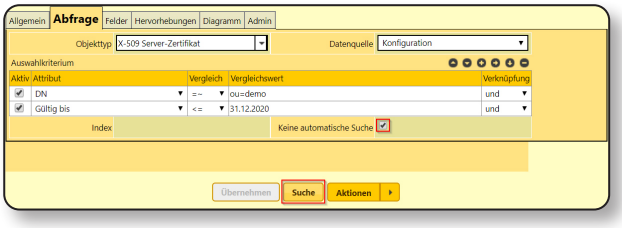


Abb. 21.05: *Keine automatische Suche*

21.3 Reiter Felder

Im Reiter **Felder** wird bestimmt, welche Eigenschaften der aufgelisteten Konfigurationsobjekte in der Tabelle auftauchen sollen. Dabei kann unter Quelle für Feldliste zwischen **Standard**, **Definieren** und **Aus anderer Abfrage** ausgewählt werden. Wird **Standard** ausgewählt, werden in der Tabelle die vordefinierten Attribute angezeigt, die für das entsprechende Konfigurationsobjekt sinnvoll sind.

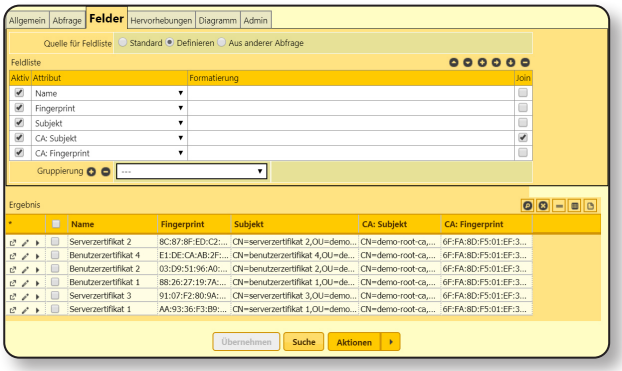


Abb. 21.06: *Abfrage - Reiter "Felder"*

21.3.1 Felder selbst definieren

Über die Funktion **Definieren** lassen sich die gewünschten Felder frei unter den Attributen des entsprechenden Konfigurationsobjektes auswählen.

In der Feldliste wird das gewünschte Attribut in der Dropdownliste ausgewählt, das erscheint, wenn auf den Pfeil im Feld Attribut geklickt wird.

Um die Änderung wirksam zu machen, muss ein Haken im Feld Aktiv gesetzt und auf **Übernehmen** geklickt worden sein.

Um weitere Felder hinzuzufügen oder vorhandene Felder zu löschen, werden die Symbole **+** und **-** in der Symbolleiste der Feldliste verwendet.

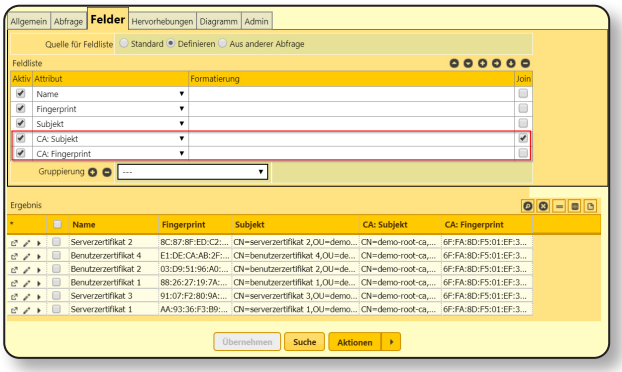


Abb. 21.07: *Felder aus einer CA übernehmen*

Mithilfe der Pfeil-Symbole kann man die Reihenfolge der Felder anpassen.

Neben den Attributen des Objekttyps selbst lassen sich auch einige Zusatzfelder auf verbundenen Objekten als Spalten für die Tabelle wählen. So können z. B. beim Objekttyp Zertifikat die Attribute Fingerprint und Subjekt des Konfigurationsobjektes CA-Zertifikat als Felder wählen.

Fügt man Felder ein, die sich auf andere Konfigurationsobjekte beziehen, so besteht die Möglichkeit auch deren Attribute in der Tabelle anzuzeigen. Dafür muss ein Haken bei Join gesetzt sein. Ist der Haken gesetzt, tauchen die Attribute des Konfigurationsobjektes nun auch in der Dropddownliste der Attribute auf. Im Beispiel wurde das Feld **CA** eingefügt und Join aktiviert. Attribute von CA sind in der Dropdownliste der Attribute durch ein vorangestelltes **CA ->** gekennzeichnet.

Diese zusätzlichen Attribute werden dann ebenfalls in der Auswahlfunktion des Reiters **Abfrage** aufgelistet.

Mithilfe des Feldes Formatierung in der Feldliste lässt sich die Ansicht der Tabellenfelder anpassen. Der Ausdruck **text = xy** bei Formatierung führt dazu, dass der Name des entsprechenden Spaltenkopfes in **xy** umbenannt wird.

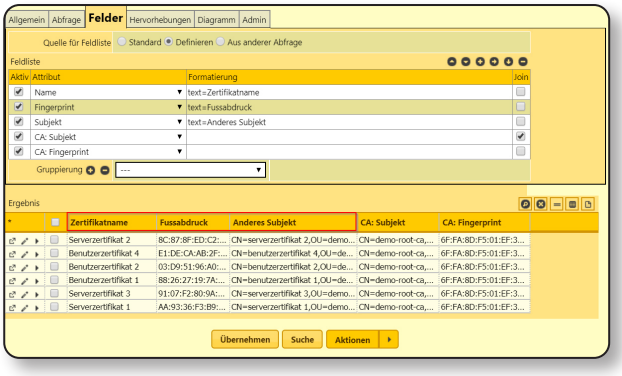


Abb. 21.08: *Felder formatieren*

21.4 Reiter Hervorhebungen

Konfigurationsobjekte können in der Tabelle farblich hervorgehoben werden. Dies funktioniert nach demselben Prinzip wie die Auswahlfunktion im Reiter **Abfrage**. Man wählt im Reiter **Hervorhebungen** unter der gewünschten Farbe (rot, gelb, grün und blau) das Kriterium aus, nach dem das Objekt markiert werden sollen, und aktiviert die Hervorhebung über die Box Aktiv sowie die Funktion **Übernehmen**. Erfüllt ein Konfigurationsobjekt die Kriterien von Hervorhebungen mit unterschiedlichen Farben, wird es mit der Farbe mit der höchsten Priorität markiert. Die Prioritäten in absteigender Reihenfolge sind: rot, gelb, grün, blau.

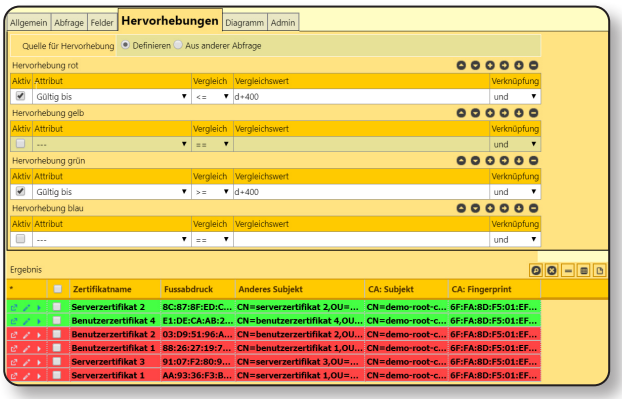


Abb. 21.09: *Abfrage - Reiter Hervorhebungen*

21.5 Beispiel: Abfrage mit Aktion zum automatischen Verlängern von Zertifikaten und CRLs

Zertifikate, genauso wie CRL, können mit einem Abfrage mit Aktion-Objekt automatisch verlängert werden, bevor sie ablaufen. Dieses wird durch Rechtsklick im Baum **Neu → Allgemein → Abfrage mit Aktion** angelegt.

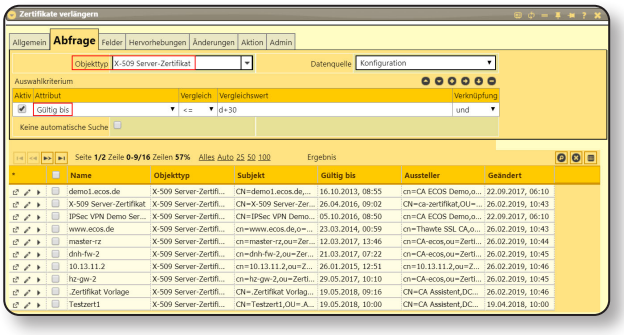


Abb. 21.10: *Abfrage mit Aktion - Reiter "Abfrage"*

Es wird zunächst eine Abfrage erstellt, die alle Zertifikate, die automatisch verlängert werden sollen, umfasst. Dazu auf dem Reiter **Abfrage** bei Objekttyp den passenden Zertifikat-Objekttyp (z.B. Zertifikat oder CA-Zertifikat) auswählen.

Danach wird in der Tabelle Auswahlkriterium, in der Spalte Attribut **Gültig bis** und bei Vergleich **<=** ausgewählt. Dann den Vergleichswert so setzen, dass Zertifikate aus dem gewünschten Zeitraum angezeigt werden, z.B. führt **d+60** dazu, dass alle Zertifikate, die in den nächsten 60 Tagen ablaufen, ausgewählt werden.

Im folgenden Beispiel werden nur Zertifikate aufgelistet, deren Gültigkeit weniger oder in genau 30 Tagen auslaufen.

Auf dem Reiter **Aktion** wird die Verlängerung ausgeführt, indem das Attribut **Erstellung des Zertifikats** und der Wert **Verlängern** ausgewählt werden. Bei dem Feld Aktion muss **Objekt ändern** ausgewählt werden. Um die Aktion manuell auszuführen, kann auf die Schaltfläche **Jetzt ausführen** geklickt werden.

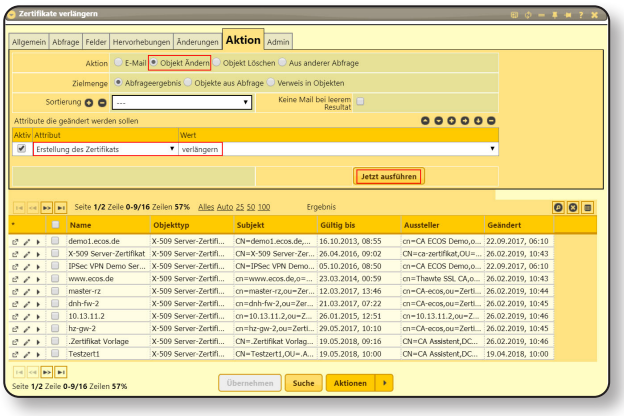


Abb. 21.11: *Abfrage mit Aktion - Reiter "Aktion"*

Um die Verlängerung automatisch zu einem bestimmten Zeitpunkt auszuführen, wird über den Reiter **Änderungen Zeitgesteuert** als Quelle für Änderungen ausgewählt. Bei Ausführungszeit wird die Zeit im Crontab-Format eingegeben.

Um die CRL zu verlängern, ist der Vorgang ähnlich wie beim Zertifikate verlängern. Beim Reiter **Abfrage** wird CA-Zertifikat als Objekttyp ausgewählt, da die CA die CRL signiert. Bei Auswahlkriterium kann eingeschränkt werden für welche CAs die CRL automatisch verlängert wird. Auf dem Reiter **Aktion** wird das Attribut **CRL neu erzeugen** und der Wert **CRL neu signieren** ausgewählt. Damit die CRL auch automatisch neu erzeugt werden kann, bevor dieser Zeitraum abgelaufen ist, ist es notwendig im CA-Zertifikat-Objekt bei CA-Kennwort anfordern nicht die Option **Immer** anzugeben, da ansonsten für die Generierung der CRL die Eingabe des CA-Kennwortes notwendig ist und diese dann nur manuell erzeugt werden kann.

22 Berechtigungen

Jedem Benutzer lassen sich Berechtigungen zuweisen, die festlegen, auf welche Konfigurationsobjekte er Zugriff hat. Einzelnen Benutzern kann im Formular des jeweiligen Benutzerobjekts unter dem Reiter Allgemein Admin-Zugriff erteilt werden. Als Administrator hat dieser Benutzer sämtliche Berechtigungen und kann auf alle Konfigurationsobjekte und Funktionen zugreifen und diese auch beliebig bearbeiten und löschen.

Soll ein Benutzer nur eingeschränkte Berechtigungen erhalten, wird ihm eine Rolle zugewiesen. Rollen können individuell angelegt und mit ausgewählten Berechtigungen verknüpft werden.

Dazu ist es notwendig, im jeweiligen Benutzerobjekt die Option Zugriff auf Admin-Oberfläche zu aktivieren. Nur dann kann sich dieser überhaupt an der Admin-Oberfläche anmelden. Welche Objekte er dann sieht bzw. ändern darf, wird über die Zuordnung der Rollen bestimmt.

Wie eine Rolle einem Benutzer zugewiesen wird, wird im Kapitel **7.2.2 Eine Benutzerrolle zuweisen** erklärt.

22.1 Rollen zu Gruppen zusammenfassen

Angelegte Rollen können zu Sicherheitsgruppen zusammengefasst werden, denen wiederum Berechtigungen zugewiesen werden können. Zum Anlegen einer neuen Sicherheitsgruppe, mit der rechten Maustaste auf den Container: Benutzer klicken und unter **Neu → Benutzer → Sicherheitsgruppe** auswählen. Daraufhin öffnet sich das Formular für die Sicherheitsgruppe, in welchem die Sicherheitsgruppe benannt und ihr Rollen zugeordnet werden können.

Durch Klicken auf den Pfeil rechts neben der Auswahlbox Rollen öffnet sich ein Auswahl-Menü mit allen angelegten Rollen. Über die Schaltflächen **+** und **-** können weitere Rollen hinzugefügt bzw. gelöscht werden.

Mithilfe der Schaltfläche **Anlegen** wird die Gruppe gespeichert.

22.2 Gruppen Berechtigungen zuweisen

Im Reiter Admin des Konfigurationsobjektes, dessen Zugriff man regulieren möchte, können einer Sicherheitsgruppe oder einer einzelnen Rolle Berechtigungen zugewiesen werden. Berechtigungen können nur von Benutzern, die Admin-Zugriff haben oder das Recht **Rechte** für das entsprechende Objekt besitzen, vergeben werden.

In der Tabelle Berechtigungen kann die Sicherheitsgruppe oder Rolle ausgewählt und die gewünschten Berechtigungen durch Setzen der entsprechenden Haken in den Feldern Browsen, Lesen, Schreiben, Erstellen, Löschen, Secrets, Rechte, Admin, Eltern und Vererben vergeben werden.

Um die Berechtigungen zu aktivieren, muss der Haken bei Aktiv links in der Tabelle gesetzt und die

Änderungen mithilfe von **Übernehmen** gespeichert worden sein.

Welche Rollen welche Berechtigungen für das aktuell angezeigte Objekt besitzen, lässt sich in der Tabelle Effektive Berechtigungen nachvollziehen.

Weiterhin können die Berechtigungen auf einen bestimmten Objekttyp beschränkt werden. Dies ergibt Sinn im Zusammenhang mit dem Recht **Vererben**. Dabei wird die entsprechende Einstellung nur auf Objekte des ausgewählten Typs angewandt.

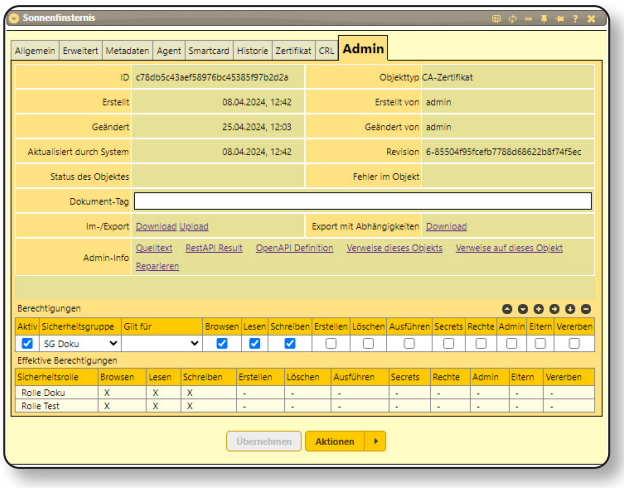


Abb. 22.01: *Berechtigungen verteilen*

22.3 Rechtearten

Browsen: Benutzer mit der Berechtigung **Browsen** sehen das entsprechende Konfigurationsobjekt im Baum. Außerdem wird das Konfigurationsobjekt in der Suche angezeigt. Die Benutzer können das Formular des Konfigurationsobjektes jedoch nicht öffnen.

Lesen: Benutzer mit der Berechtigung **Lesen** für ein Konfigurationsobjekt, können das entsprechende Formular öffnen, jedoch keine Änderungen darin vornehmen.

Schreiben: Benutzer mit der Berechtigung **Schreiben** können das entsprechende Konfigurationsobjekt öffnen und Änderungen in seinem Formular vornehmen.

Löschen: Benutzer mit der Berechtigung **Löschen** können bereits vorhandene Konfigurationsobjekte des entsprechenden Typs löschen.

Secrets: Benutzer mit der Berechtigung **Secrets** erhalten Zugriff auf Authentisierungsinformationen, wie z.B. Passwörter.

Rechte: Benutzer mit der Berechtigung **Rechte** dürfen an andere Benutzer Rechte vergeben.

Admin: Benutzer mit der Berechtigung **Admin** haben Zugriff auf die Administration eines Objekts. Sie können sich z. B. den Quelltext anzeigen lassen und Objekte reparieren.

Eltern: Ist ein Haken bei **Eltern** gesetzt, erhalten automatisch alle Konfigurationsobjekte, die im Baum über dem entsprechenden Konfigurationsobjekt stehen, das **Browsen**-Recht, so dass der Anwender im Baum zu dem berechtigten Objekt navigieren kann.

Vererben: Ist ein Haken bei **Vererben** gesetzt, gelten die zugewiesenen Berechtigungen automatisch auch für Konfigurationsobjekte, die im Baum unter dem entsprechenden Konfigurationsobjekt existieren. Im Reiter Admin der untergeordneten Objekte lassen sich die Berechtigungen anpassen.

22.4 Sonderfälle bei Berechtigungen

22.4.1 Eine Rolle wird mehreren Gruppen zugeordnet

Eine Rolle kann mehreren Sicherheitsgruppen gleichzeitig zugeordnet sein. Ist dies der Fall, so verhalten sich die Berechtigungen der beiden Gruppen additiv, das heißt, besitzen die beiden Sicherheitsgruppen unterschiedliche Rechte für dieselben Objekte, so erhält der Benutzer die Berechtigungen beider Gruppen.

Beispiel: Sicherheitsgruppe 1 hat für das Objekt Lese- und Schreib-Zugriff. Sicherheitsgruppe 2 hat für dasselbe Objekt Lese-, und Lösch-Zugriff. Ein Benutzer, dessen Rolle beiden Sicherheitsgruppen zugeordnet wird, erhält Lese-, Schreib- und Lösch-Zugriff für dieses Objekt.

22.4.2 Unterschiedliche Rechte für Eltern und untergeordnete Objekte

Wird die Berechtigung **Vererben** bei einem Konfigurationsobjekt für eine Sicherheitsgruppe oder Rolle gesetzt, erhält diese Sicherheitsgruppe oder Rolle automatisch die ausgewählten Berechtigungen für alle Konfigurationsobjekte, die im Baum unter dem Objekt stehen. Wird der Sicherheitsgruppe oder Rolle andere Berechtigungen für ein untergeordnetes Objekt zugewiesen, so überschreibt diese Berechtigungsauswahl die des Eltern-Objektes.

Beispiel: Im Container: Zertifikate wird der Sicherheitsgruppe **Gruppe Zertifikate** das **Browsen-**, **Lesen-**, **Erstellen-** und **Löschen-**Recht gegeben. Außerdem sind die Berechtigungen **Eltern** und **Vererben** gesetzt. Unter dem Feld Effektive Berechtigungen lässt sich ablesen, welche Rollen welche Berechtigungen besitzen. In diesem Fall haben alle Rollen, die in der Sicherheitsgruppe **Gruppe Zertifikate** sind, die oben aufgezählten Rechte.

Da **Vererben** aktiv ist, gelten diese auch für alle untergeordneten Objekte, also sämtliche Zertifikate in diesem Fall.

Soll der Sicherheitsgruppe oder Rolle für einzelne untergeordnete Objekte oder auch Container mehr oder weniger Rechte zugewiesen werden, kann dies im Reiter **Admin** des entsprechenden Objektes geregelt werden. Die Rechte des Eltern-Objektes werden dadurch überschrieben und sind nicht mehr gültig.

Im Beispiel hat die Sicherheitsgruppe **Gruppe Zertifikate** nur noch **Browsen-**, **Lesen-**, **Eltern-** und **Vererben-**Berechtigungen für sämtliche Objekte des Containers **CA-DEMO**. Die Berechtigungen **Erstellen** und **Löschen** sind nicht mehr gesetzt, obwohl sie im Eltern-Objekt Zertifikate zugewiesen sind.

Teil IV - Anhänge

23 Fehlerbeseitigung

Problem/Fehlerbeschreibung	Mögliche Ursache	Maßnahme/Fehlerbehebung
Allgemeine Verbindungsprobleme, z.B.: - AUTH-API nicht erreichbar - API nicht erreichbar - Administrationsoberfläche nicht erreichbar - Online-Status von Zertifikaten nicht abrufbar, OCSP-Dienst nicht erreichbar - Zertifikatsperrliste nicht abrufbar - RADIUS-Authentisierung nicht erreichbar und in der Folge Netzwerkanmeldung / WLAN-Nutzung nicht möglich - Enrollment-Dienste nicht erreichbar	- Sie verwenden eine falsche Adresse für den angefragten Dienst. - Defekt im Netzwerk oder Firewall-, Switch-, Routingprobleme - Sie befinden sich nicht in einem Netzwerksegment, das Zugriff auf Dienste der TMA ermöglicht. - Die angegebene Adresse kann wegen eines DNS-Defekts nicht aufgelöst werden. - Das Netzwerk ist überlastet. - Der Dienst der TMA ist ausgefallen. - Der Dienst der TMA ist überlastet.	- Überprüfen Sie die von Ihnen verwendete Adresse. Korrigieren Sie die Adresse ggf. - Wenden Sie sich an Ihre IT-Administration oder Anwenderbetreuung.
Ein Aufruf an einen Dienst bzw. die API wird mit dem HTTP-Status 401 „Unauthorized“ beantwortet	- Sie versuchen eine Funktion zu nutzen, die eine gültige Authentifizierung des Aufrufers erfordert. Sie liefern das dafür erforderliche Zugriffstoken (Access Token) im Aufruf nicht mit. - Ihr Zugriffstoken ist abgelaufen	- Beziehen Sie ein gültiges Zugriffstoken vom AUTH-API. - Erneuern Sie Ihr Zugriffstoken, falls dieses abgelaufen ist. - Stellen Sie sicher, dass Sie das Zugriffstoken in gültiger Form als „Bearer-Token“ im Authorization-Header Ihres Aufrufs mitliefern (Authorization: Bearer <TOKEN-WERT>).
Ein Aufruf an einen Dienst bzw. die API wird mit dem HTTP-Status 403 „Forbidden“ beantwortet	- Sie versuchen auf eine Funktion oder ein Objekt zuzugreifen, für das Sie nicht berechtigt sind.	- Überprüfen Sie die verwendete URL, insbesondere den darin verwendeten Ressourcennamen sowie die ID. - Wenden Sie sich ggf. an Ihre IT-Administration oder Anwenderbetreuung, um Ihre Berechtigungen zu überprüfen.
Ein Aufruf an einen Dienst bzw. die API wird mit dem HTTP-Status 404 „Not Found“ beantwortet	- Sie versuchen auf eine Funktion oder ein Objekt zuzugreifen, das nicht existiert.	- Überprüfen Sie die verwendete URL, insbesondere den darin verwendeten Ressourcennamen sowie die ID. - Korrigieren Sie Ihre Angaben ggf.

Problem/Fehlerbeschreibung	Mögliche Ursache	Maßnahme/Fehlerbehebung
Ein Aufruf an einen Dienst bzw. die API wird mit dem HTTP-Status 400 „Bad Request“ beantwortet	- Sie versuchen auf eine Funktion zuzugreifen, liefern aber nicht die dafür erforderlichen Parameter. - Die gelieferten Parameter werden nicht im richtigen Format geliefert oder liegen nicht im gültigen Wertebereich.	- Überprüfen Sie die angegebenen Parameter - Korrigieren Sie Ihre Angaben ggf.
Ein Aufruf an einen Dienst bzw. die API wird mit dem HTTP-Status 500 „Internal Server Error“ beantwortet	Die Bearbeitung Ihrer Anfrage hat serverseitig zu einem unerwarteten Zustand geführt. Die Bearbeitung musste deshalb abgebrochen werden.	Wenden Sie sich an Ihre IT-Administration oder Anwenderbetreuung. Beschreiben Sie möglichst genau den Aufruf, ggf. Parameter und vorgenommene Einstellungen, um die Fehleranalyse und -behebung zu unterstützen.
Ein Aufruf an einen Dienst bzw. die API wird mit dem HTTP-Status 502 „Bad Gateway“ beantwortet	Der angefragte Dienst ist ausgefallen und konnte bislang nicht wieder hergestellt werden.	Wenden Sie sich an Ihre IT-Administration oder Anwenderbetreuung.
Ein Aufruf an einen Dienst bzw. die API wird mit dem HTTP-Status 503 „Service Unavailable“ beantwortet	- Der angefragte Dienst steht vorübergehend nicht zur Verfügung (z.B. zu Wartungszwecken). - Der angefragte Dienst ist überlastet und kann Ihre Anfrage deswegen zurzeit nicht annehmen.	- Warten Sie einige Sekunden und wiederholen Sie die Anfrage. - Bei wiederkehrendem Auftreten wenden Sie sich an Ihre IT-Administration oder Anwenderbetreuung.
Die Enrollment-Dienste der TMA sind erreichbar, Sie können aber keine Verbindung aufbauen, um ein Zertifikat zu beziehen und erhalten eine SSL-Fehlermeldung (z.B.: ERR_BAD_SSL_CLIENT_AUTH_CERT, SSL_ERROR_HANDSHAKE_FAILURE_ALERT).	- Der Dienst erfordert eine gegenseitige zertifikatbasierte Authentisierung beim Aufbau der HTTPS-Verbindung (TLS - in Vorgängerversionen als SSL bezeichnet). Auf Ihrem Gerät steht das erforderliche, vorkonfigurierte Zertifikat nicht zur Verfügung.	- Wenden Sie sich an Ihre IT-Administration oder Anwenderbetreuung.

Problem/Fehlerbeschreibung	Mögliche Ursache	Maßnahme/Fehlerbehebung
Die API der TMA bzw. die Administrationsoberfläche sind erreichbar, Sie können sich aber nicht als Administrator einer CA anmelden.	- Sie besitzen keine Smartcard, die für Sie mit dem erforderlichen Zertifikat ausgestellt wurde, damit Sie sich in der für Administratoren einer CA geforderten Weise über zwei Faktoren authentisieren können. - Ihre Smartcard mit dem erforderlichen Zertifikat steckt nicht im Smartcard-Reader Ihrer Arbeitsstation. - Ihre Smartcard oder der Smartcard-Reader ist defekt. - Das erforderliche Zertifikat auf der Smartcard ist ungültig, zurückgezogen oder abgelaufen.	- Wenden Sie sich an Ihre IT-Administration oder Anwenderbetreuung.

24 Schlüsselverwendungszwecke

Je nach Einsatzgebiet eines Zertifikats ist es unter Umständen notwendig, bestimmte Schlüsselverwendungen für den öffentlichen Schlüssel im Zertifikat zu definieren.

Dies kann durch voreingestellte Verwendungszwecke, die feste Schlüsselverwendungen und erweiterte Schlüsselverwendungen definiert haben, oder manuell konfiguriert werden.

24.1 Voreingestellte Schlüsselverwendungszwecke

Verwendungszweck	Schlüsselverwendung	Erweiterte Schlüsselverwendung
Benutzer, Verschlüsseln	Nichtabstreitbarkeit Schlüsselverschlüsselung Datenverschlüsselung	E-Mail (S/MIME) Microsoft Encrypted File System
Benutzer, Signieren	Digital signieren Nichtabstreitbarkeit Schlüsselverschlüsselung	E-Mail (S/MIME)
Zeitstempel	Digital signieren Nichtabstreitbarkeit	Beglaubigte Zeitmarken
OCSP Responder-Zertifikat	Digital signieren	OCSP Signing
Code-Signatur	Digital signieren	Code Signing
S/MIME	Digital signieren Nichtabstreitbarkeit	E-Mail (S/MIME)
TLS-Client	Digital signieren Schlüsselaushandlung	SSL/TLS Webclient-Authentisierung
TLS-Server	Digital signieren Schlüsselverschlüsselung	SSL/TLS Webserver-Authentisierung
VPN-Client	Digital signieren Schlüsselaushandlung	SSL/TLS Webclient-Authentisierung
VPN-Server	Digital signieren Schlüsselverschlüsselung	SSL/TLS Webserver-Authentisierung
Kerberos KDC	Digital signieren Nichtabstreitbarkeit Schlüsselverschlüsselung Datenverschlüsselung	SSL/TLS Webserver-Authentisierung SSL/TLS Webclient-Authentisierung Microsoft Smartcard Login Kerberos KDC
Kerberos Client-Zertifikat	Digital signieren Schlüsselverschlüsselung Datenverschlüsselung	Kerberos Client-Authentisierung
SBS, Authentisieren*	Digital signieren Schlüsselverschlüsselung Datenverschlüsselung	SSL/TLS Webclient-Authentisierung

Verwendungszweck	Schlüsselverwendung	Erweiterte Schlüsselverwendung
SBS, Verschlüsseln*	Digital signieren Schlüsselverschlüsselung Datenverschlüsselung	-

* Die voreingestellten Schlüsselverwendungszwecke beziehen sich auf die Nutzung und Verwaltung des ECOS SecureBootStick (SBS). Die Verwendung im Rahmen der TMA ist unüblich.

24.2 Schlüsselverwendungen

Digital signieren: Der öffentliche Schlüssel wird für die Überprüfung von digitalen Signaturen verwendet, vor allem im Zusammenhang mit SSL/TLS, OCSP oder S/MIME.

Nichtabstreitbarkeit: Der öffentliche Schlüssel wird für die Überprüfung von digitalen Signaturen eines Verbindlichkeitsdienstes (Non-Repudiation Service) verwendet. Die Nichtabstreitbarkeit schützt vor dem fälschlichen Abstreiten einer Aktion durch die signierende Entität (mit Ausnahme der Signatur von Zertifikaten oder CRLs).

Schlüsselverschlüsselung: Der öffentliche Schlüssel wird zur Verschlüsselung von privaten oder geheimen Schlüsseln verwendet.

Datenverschlüsselung: Der öffentliche Schlüssel wird zur direkten Verschlüsselung von Benutzerdaten verwendet, bei denen es sich nicht um kryptografische Schlüssel handelt.

Schlüsselaushandlung: Der öffentliche Schlüssel wird für die Schlüsselvereinbarung verwendet, z.B. wenn ein Diffie-Hellman-Schlüssel für den Schlüsselaustausch verwendet werden soll. Dieser Wert wird in Kombination mit Nur verschlüsseln und Nur entschlüsseln gesetzt.

Nur verschlüsseln: Der öffentliche Schlüssel wird zur Verschlüsselung von Daten bei der Durchführung der Schlüsselvereinbarung verwendet. Dieser wird nur in Verbindung mit Schlüsselaushandlung gesetzt.

Nur entschlüsseln: Der öffentliche Schlüssel wird zur Entschlüsselung von Daten bei der Durchführung der Schlüsselvereinbarung verwendet. Dieser wird nur in Verbindung mit Schlüsselaushandlung gesetzt.

24.3 Erweiterte Schlüsselverwendungen

SSL/TLS Webserver-Authentisierung: Der öffentliche Schlüssel wird in Zusammenhang mit einer SSL/TLS-Webserver-Authentisierung verwendet. Passende Schlüsselverwendungen sind Digital signieren, Schlüsselverschlüsselung und Schlüsselaushandlung.

SSL/TLS Webclient-Authentisierung: Der öffentliche Schlüssel wird in Zusammenhang mit einer SSL/TLS-Webclient-Authentisierung verwendet. Passende Schlüsselverwendungen sind Digital signieren und/oder Schlüsselaushandlung.

Code Signing: Der öffentliche Schlüssel wird zum Signieren von herunterladbarem und ausführbarem Code verwendet. Passende Schlüsselverwendung ist Digital signieren.

E-Mail (S/MIME): Der öffentliche Schlüssel wird für die E-Mail-Verschlüsselung verwendet. Passende Schlüsselverwendungen sind Digital signieren, Nichtabstreitbarkeit, Schlüsselverschlüsselung und/oder Schlüsselaushandlung.

Beglaubigte Zeitmarken: Der öffentliche Schlüssel wird für vertrauenswürdige Zeitstempel verwendet. Passende Schlüsselverwendungen sind Digital signieren und/oder Nichtabtreitbarkeit.

OCSP Signing: Der öffentliche Schlüssel wird zum Signieren von OCSP-Antworten verwendet. Passende Schlüsselverwendungen sind Digital signieren und/oder Nichtabtreitbarkeit.

Microsoft Smartcard Login: Der öffentliche Schlüssel wird für Microsoft Smartcard Login verwendet.

Microsoft Individual Code Signing (Authenticode): Der öffentliche Schlüssel wird in Zusammenhang mit einem Individual-Code-Signing-Zertifikat und einer Microsoft-Authenticode-Signatur verwendet. Mit diesen Zertifikaten können Entwickler z.B. Software signieren, die für den Betrieb mit Microsoft-Produkten bestimmt ist.

Microsoft Commercial Code Signing (Authenticode): Der öffentliche Schlüssel wird in Zusammenhang mit einem Commercial-Code-Signing-Zertifikat und einer Microsoft-Authenticode-Signatur verwendet. Mit diesen Zertifikaten können Unternehmen z.B. Software signieren, die für den Betrieb mit Microsoft-Produkten bestimmt ist.

Microsoft Trust List Signing: Der öffentliche Schlüssel wird in Zusammenhang mit Microsoft Trust-List-Signing-Zertifikaten verwendet. Hierbei handelt es sich um vordefinierte Listen, z.B. Hashes von Zertifikaten, die von einer vertrauenswürdigen Instanz signiert sind.

Microsoft Encrypted File System: Der öffentliche Schlüssel wird in Zusammenhang mit EFS-Zertifikaten verwendet.

Kerberos KDC: Der öffentliche Schlüssel wird für ein Kerberos Key Distribution Center verwendet.

Kerberos Client-Authentisierung: Der öffentliche Schlüssel wird für die Kerberos Client-Authentisierung verwendet.

IPsec-Endsystem: Das Zertifikat wird für ein IPsec-Endsystem verwendet.

IPsec-Tunnel: Das Zertifikat wird für IPsec-Tunneling verwendet.

IPsec-Benutzer: Das Zertifikat wird für IPsec-Benutzer verwendet.

25 DocExpressions

DocExpressions dienen dazu Werte aus verschiedenen Quellen zusammen zu setzen bzw. zu berechnen. DocExpressions führen eine oder mehrere Operationen auf ihr Eingangswerte aus und liefern ein Ergebnis. Dieses kann dann für Validierungen oder als Standardwert in Richtlinien verwendet oder im Rahmen von Assistenten herangezogen werden. Weiterhin ist es bei Abfragen möglich komplexe Abfragen mittels DocExpressions zu formulieren.

Als Eingangswerte können in DocExpressions neben Konstanten auch Attribute von Konfigurationsobjekten verwendet werden. Ebenso ist es möglich Verweise innerhalb von Konfigurationsobjekten auf andere Konfigurationsobjekten zu verfolgen und dann deren Attribute als Eingangswerte zu verwenden.

DocExpressions greifen immer nur lesend auf Konfigurationsobjekte zu. Innerhalb der DocExpressions findet keine Veränderung an Konfigurationsobjekten statt.

25.1 DocExpressions Anwendungen

25.1.1 Validierung

Innerhalb von Richtlinien können DocExpressions dazu verwendet werden, um sicherzustellen, dass nur erlaubte Werte in ein Konfigurationsobjekt gespeichert werden. DocExpressions kommen dann zum Einsatz, wenn die Validierung mit den einfachen Operatoren nicht abgebildet werden kann.

25.1.2 Vorbelegung

DocExpressions liefern einen Wert, der in Richtlinien oder Assistenten zur Vorbelegung benutzt werden kann. Dieser Wert kann aus beliebigen anderen Attributen, anderen Objekten oder auch z.B. auch mittels Datum und Zeit berechnet werden. Neu anzulegende Objekte können so sinnvoll vorbelegt werden. Für Zertifikate kann z.B. eine Gültigkeit bis zu einem festen Termin in der Zukunft berechnet werden.

25.2 Konfigurationsobjekt DocExpression Debugger

DocExpressions sind unter Umständen komplex zu schreiben. Um diese korrekt zu entwickeln und zu testen, bevor sie angewendet werden, kann man ein DocExpression Debugger-Objekt verwenden. Dies kann durch Rechtsklick auf dem Organisation-Objekt **Neu → Management → DocExpression Debugger** angelegt werden.

25.2.1 Reiter Allgemein

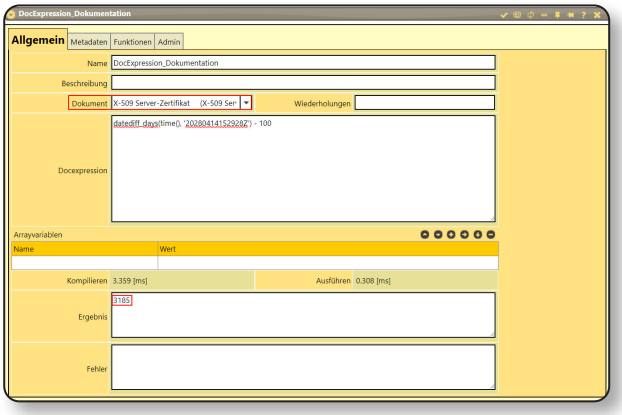


Abb. 25.01: *DocExpression Debugger*

Im Reiter **Allgemein** wird über das Feld Objekt ein beliebiges Objekt ausgewählt. Attribute innerhalb der DocExpressions beziehen sich dann auf dieses Objekt. Wird kein Objekt ausgewählt, bezieht sich die DocExpressions auf den DocExpression Debugger selbst.

Über das Feld DocExpression wird der Ausdruck eingegeben. Ist die Schreibweise korrekt eingegeben, erscheint der Rückgabewert im Feld Ergebnis. Ist die DocExpression falsch eingegeben, erscheint eine Meldung im Feld Fehler. Im DocExpression-Feld werden Zeichen, die nach einem **#**-Zeichen kommen ignoriert.

Das Feld Wiederholungen ermöglicht die Performance der DocExpressions zu messen.

Über die Tabelle Arrayvariablen können Arrays getestet werden. Das erste Element des Arrays hat den Index 0.

25.2.2 Reiter Metadaten

Das Attribut **metadata** entspricht den Metadaten im Reiter **Metadaten** und kann zum Testen von Hashes verwendet werden.

25.2.3 Reiter Funktionen

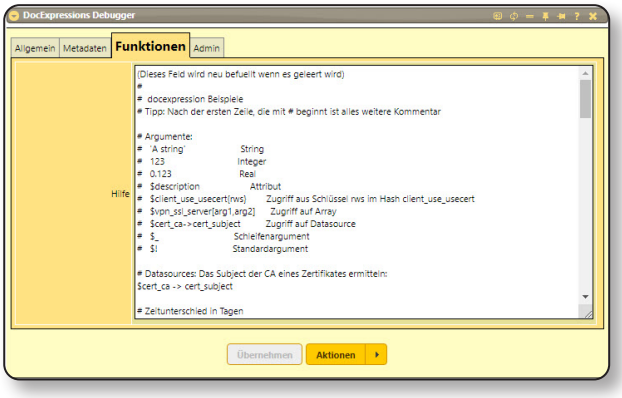


Abb. 25.02: *DocExpression Debugger - Reiter "Funktionen"*

Im Reiter **Funktionen** sind alle Funktionen, die in DocExpressions verwendet werden können, aufgelistet. Diese Übersicht dient als Hilfestellung.

25.3 Syntax

DocExpressions bestehen aus Konstanten, Attributen von Konfigurationsobjekten, Operatoren und Funktionen.

DocExpressions sind formatfrei und können beliebig umgebrochen bzw. eingerückt werden. Leerzeichen werden, außer in Zeichenkettenkonstanten, ignoriert.

25.3.1 Konstanten

25.3.1.1 Zahlen

Als numerische Konstanten wird die Ganzzahl (z.B. **123**) und die Gleitkommazahl (z.B. **0.123**) unterstützt.

25.3.1.2 Zeichenketten

Zeichenketten sind in einfache oder doppelte Anführungszeichen (, oder „) eingeschlossen.

Beispiel: **‘abc‘** oder **“abc“**

25.3.2 Attribute

Konfigurationsobjekte bestehen aus Attribute. Alle Attribute, die in einem Konfigurationsobjekt aktuell gesetzt sind, können über den Reiter **Admin** im **Quelltext** des Konfigurationsobjektes angezeigt werden. In der DocExpressions Syntax beginnen Attribute immer mit einem **$**-Zeichen, z.B. **$description**.

Attribute können dabei von unterschiedlichem Typ sein. Zeichenkette, Ganzzahl, Kommazahl, aber auch Array, Hash oder Datasource.

25.3.2.1 Array-Attribute

Um auf ein Element innerhalb eines Arrays zuzugreifen, muss der Index in eckigen Klammern stehen, z.B. **$docexpr_vars[1]**.

25.3.2.2 Hash-Attribute

Um auf ein Element innerhalb eines Hashes zuzugreifen, muss der Schlüsselwert in geschweiften Klammern stehen, z.B. **$metadata{‘Option2‘}**.

25.3.2.3 Datasource-Attribute

Datasource-Attribute verweisen auf Werte in anderen Konfigurationsobjekten. DocExpressions ermöglichen es, diesem Link zu folgen und auf die Werte in diesen anderen Objekten zuzugreifen.

Für den Verweis wird der Operator **->** verwendet. Links davon steht das Attribut, das auf ein anderes Objekt verweist. Rechts steht das Attribut, auf das verwiesen wird und auf das zugegriffen werden soll.

Beispiel: **$cert_ca->cert_subject:** Das Attribute **cert_ca** verweist auf die CA eines Zertifikats. In dem Beispiel wird somit das Subjekt der CA eines Zertifikates ermittelt.

25.3.3 Operatoren

Die einzelnen Werte und Attribute können mittels Operatoren verknüpft werden. Unterstützt werden folgende Operatoren:

Operator	Erklärung
+	Addition
-	Subtraktion
*	Multiplikation
&&	Logisches Und
||	Logisches Oder
->	Verweise auf ein anderes Konfigurationsobjekt
==	gleich (Zahl oder Zeichenkette)
!=	nicht gleich (Zahl oder Zeichenkette)
<	kleiner (Zahl)
>	größer (Zahl)
<=	kleiner gleich (Zahl)
>=	größer gleich (Zahl)
!	nicht

25.3.4 Funktionen

Funktionen wenden, ähnlich wie die DocExpressions selbst, eine Operation auf ihre Argumente an und liefern das Ergebnis zurück. Funktionsargumente stehen in runden Klammern, die Klammern müssen auch angegeben werden, wenn die Funktion keine Argumente hat.

Funktionen können eine beliebige Anzahl von Argumenten haben. Es müssen immer alle Argumente angegeben werden. Ausnahme sind Argumente, die Standardwerte haben (in der Auflistung unten mit eckigen Klammern [ ] gekennzeichnet). Solche Argumente können weggelassen werden. In diesem Fall werden die Standardwerte verwendet.

Argumente von Funktionen können auch wiederum DocExpressions sein. Sie können also beliebig geschachtelt werden.

25.3.4.1 Liste der verfügbaren Funktionen

Funktion	Erklärung
add(a, b) bzw. a + b	berechnet die Summe der Zahlen **a** und **b**
all(array, re [, throw()])	ist wahr, wenn alle Elemente von Array auf **re** matchen (sonst false/throw)
and(a, b) bzw. a && b	ist die logische Und-Verknüpfung von **a** und **b**
any(array, str [, throw()])	ist wahr, wenn wenigstens ein Element von **array** exakt **str** ist (sonst false/throw)
apply(array, expr)	erzeugt ein neues Array, wobei **expr** auf jedes Element angewendet wird (**$_** in **expr** ist aktuelles Element)
array_add(array, elem [, pos])	erzeugt ein neues Array mit Element an **pos**/am Ende
array_count(array, elem [, pos])	liefert die Anzahl der Elemente im Array
array_delete(array [, pos])	löscht das Element **pos** / das letzte
array_element(array, i1 [, i2])	liefert das Array Element **i** bzw. **i1**, **i2**
array_index_of(array, str)	liefert die Position von **str** im Array
array_sort(array)	liefert eine sortierte Kopie
attribute_value_byid(id, attribut, [default1], [default2])	liefert das Attribut des mit ID-bezeichneten Objekts. **default1** wird zurückgegeben, wenn das Attribut leer ist, **default2** wenn das Objekt nicht existiert. **default1/2** sind leere Strings, wenn nicht angegeben. Für die defaults kann auch ein **throw()** verwendet werden
base64decode(str)	dekodiert den base64-String
base64encode(str)	liefert String base64-kodiert
chr(i)	erzeugt das Unicode-Zeichen **i**
concat(str1, str2)	hängt **str2** an **str1** an
cond(c, wahr, falsch)	liefert den Wert von wahr /falsch, je nach **c**. Für wahr/falsch kann **throw()** verwendet werden.
datasource(attribut, data)	liefert den Wert **data** des Datasource-Attributs data
date(t [, delta])	liefert Datum zu **t** als dd.mm.yy (+ delta sec.)
datediff_days(t1 , t2)	liefert Differenz von **t1** und **t2** in Tagen
datetime(t [, delta])	liefert Datum + Zeit zu **t** als dd.mm.yy HH:MM:SS (+ delta sec.)
datetimetz(t [, delta])	liefert Datum + Zeit zu **t** als dd.mm.yy HH:MM:SS + TZ (+ delta sec.)
div(zaehler, nenner) bzw. zaehler / nenner	berechnet einen Quotienten.
docpath([id])	liefert den Array der Containerhierarchie (docpath[0] == root())
eq(x,y) bzw. x==y	ist ein Prädikat, das wahr liefert wenn zwei Zahlen oder Strings gleich sind (d.h 2.0 == 2)
exec_action(id),	starte Abfrage mit Aktion mit ID
ge(x,y) bzw. x >= y	ist ein Prädikat, das wahr liefert wenn **x >= y**
get_doctype([id])	bestimmt den doctype von ID (selbst)
get_id_byname(name [, type [, fail [, root]]])	liefert die ID von **name** mit Typ **type**, gesucht ab **root**. Fail kommt wenn nicht gefunden

Funktion	Erklärung
gt(x,y) bzw. x > y	ist ein Prädikat, das wahr liefert wenn **x > y**
hash_elementhash_element(hash, key)	liefert den Wert von **key** im **hash**
hash_fromarray(array)	erzeugt aus einem Array (key1, value1, key2, ...) einen Hash {key1 => value1, key2 =>...}
hash_fromarrays(key_array, value_array)	erzeugt aus zwei gleich großen Arrays einen Hash
hash_keys(hash)	liefert ein Array mit den Schlüsseln des Hashs
hash_toarrayhash_toarray(hash)	liefert ein Array mit den Schlüsseln und Werten des Hashs
hash_values(hash)	liefert ein Array mit den Werten des Hashs
host(cn)	liefert die ID des mit **cn** bezeichneten Host. Ist **cn** leer, wird der Host gesucht, auf dem die DocExpression ausgeführt wird
hosts()	liefert Array des Hosts (#0 ist immer Master)
is_a(type [, id])	ist wahr, wenn ID (selbst) den Typ **type** hat
is_unique(attribut [, wert [, root]])	ist wahr, wenn der Wert **val** für das Attribut (gesucht ab **root**) eindeutig ist
join(trenner, array)	wandelt Array in einen String, wobei die Werte mit dem Trenner (z.B. **“**,“) getrennt werden
lc(STRING)	wandelt **STRING** in **String**
le(x,y) bzw. x<=y	ist ein Vergleichsoperator für **x** und **y**
lt(x,y) bzw. x<y	ist ein Vergleichsoperator für **x** und **y**
master()	liefert die ID des Masters
matches(str, pattern, res)	liefert **res** wenn **str** auf das Muster **pattern** matcht (**res** darf kein **throw** sein)
matchesnot(str, pattern, res)	liefert **res** wenn **str** NICHT auf das Muster **pattern** matcht (**res** darf kein **throw** sein)
month(time)	liefert dem Monat (1..12) zum Zeitstempel **time**
mult(x,y) bzw. a * b	berechnet das Produkt von **a** und **b**
ne(x,y) bzw. a != b	ist das Prädikat zur Ungleichheit der Strings oder Zahlen **a** und **b**
not(a) bzw. !a	liefert logische Negierung von **a**
or(a,b) bzw. a || b	liefert logisches Oder von **a, b**
ord(c)	liefert den Unicode von **c**
parent([id])	liefert den nächsthöheren Container zu einer ID (default: selbst)
quote(arg)	liefert **arg** als String zurück
root()	liefert den Wurzelcontainer
sort(array)	sortiert das Array
split(trenner, string)	spaltet **string** am Trennzeichen in array: **“a,b,c“** -> **(a, b, c)** (siehe **join**)
streq(a,b)	vergleicht die Strings **a** und **b** (d.h. streq(„2.0“, „2“) ist falsch)
sub(x,y) bzw. x-y	bildet eine Differenz von **x** und **y**
subst(str, suche, ersetze)	ersetzt in **str** das erste Muster **suche** mit **ersetze**
substall(str, suche, ersetze)	ersetzt in **str** jedes Muster **suche** mit **ersetze**
throw(fehlermeldung)	wirft eine Exception mit der angegebenen Fehlermeldung

Funktion	Erklärung
time()n	Sekundengenauer UTZ-Zeitstempel (format yyyyMMDDhhmmssZ)
today()	liefert heutiges Datum als TT.MM.YYYY
uc(string)	wandelt **string** in **STRING**
year(dbzeit)	liefert das 4-stellige Jahr das zum Zeitpunkt gehört

25.4 Beispiel

Die folgende DocExpressions berechnet die Gültigkeitsdauer eines X.509-Zertifikats:

datediff_days(time(), ‚20280414152928Z') - 100

Die Funktion **datediff_days** berechnet die Differenz in Tagen.

Die Funktionsargumente sind die Funktion **time()**, die das aktuelle Datum und Uhrzeit liefert und eine Zeichenkettenkonstante, die in diesem Fall den Endzeitpunkt der CA angibt. Von der Differenz in Tagen, die die Funktion **datediff_days** berechnet, wird die Zahl **100** abgezogen.

Alle Zertifikate, die mit einer so berechneten Gültigkeit angelegt werden, laufen 100 Tage vor dem angegebenen Zeitpunkt, hier der 14.4.2028 um 15:29:28 GMT, ab, egal wann sie angelegt werden.

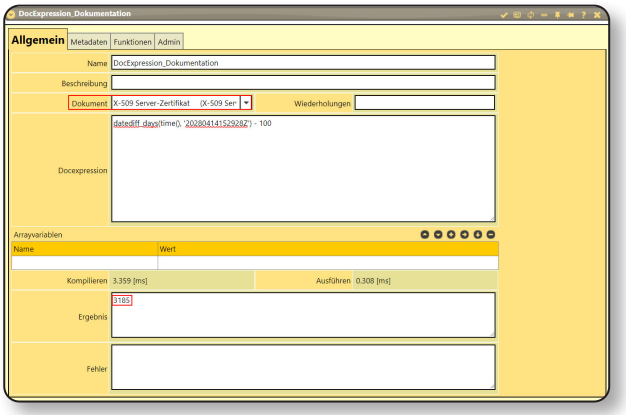


Abb. 25.03: *DocExpression testen*

Mit dem DocExpression Debugger kann die DocExpression getestet werden. Sie bezieht sich auf ein X.509-Zertifikat-Objekt, was aber in diesem Fall nicht nötig wäre, weil kein Attribut verwendet wird. Durch einen Klick auf die Schaltfläche **Übernehmen** wird die DocExpressions kompiliert und ausgeführt. Hat man sich vertippt, kommt im Feld Fehler eine Meldung. Sind die DocExpressions richtig eingegeben, wird im Feld Ergebnis das Resultat angezeigt. (Das angezeigte Ergebnis ist natürlich vom Zeitpunkt der Ausführung abhängig).

26 Certificate Enrollment Agent - Anhänge

26.1 Kommandozeilenoptionen

Option	Kurzform	Beschreibung
`--help`	`-h`	Hilfe anzeigen
`--debug <RUST_LOG-Einstellungen>`	`-d`	Log-Level setzen, bevor die Konfiguration geladen wird
`--config-name <Name>`	`-c`	Name der Konfigurationsdatei (ohne Endung/Pfad)
`--config <Pfad>`	`-C`	Vollständiger Pfad zur Konfigurationsdatei
`--home <Pfad>`	`-H`	Home-Verzeichnis (Standard: `$HOME` bzw. `%LOCALAPPDATA%\ECOS`)
`--no-env`	`-E`	Umgebungsvariablen nicht zur Konfiguration heranziehen
`--batch`		Keine interaktiven Rückfragen (z. B. Kennwort), stattdessen Abbruch bei fehlenden Angaben
`--tag <Tag>`	`-t`	Tag zur Auswahl der zu bedienenden Abonnenten (Push-Modus)
`--loop <Sekunden>`	`-l`	Daemon-Betrieb: alle <n> Sekunden erneut ausführen
`--background`	`-b`	Im Hintergrund ausführen (Linux)
`--print-config`	`-X`	Wirksame Konfiguration (inkl. Defaults) ausgeben und been-den
`--push`		Push-Modus: Zertifikate von der TMA per SSH auf Zielsysteme verteilen
`--new-agent-auth <Benutzer>`	`-n`	Neues Authentisierungszertifikat für den angegebenen Be-nutzer erzeugen
`--address <Host>`	`-a`	Hostname/IP-Adresse der TMA
`--port <Port>`	`-p`	Port der TMA
`--user <Benutzer>`	`-u`	Benutzer für die Anmeldung an der TMA
`--password <Kennwort>`	`-p`	Kennwort für die Anmeldung an der TMA
`--auth-cert <Datei.p12>`	`-A`	Authentisierungszertifikat (PKCS#12)
`--auth-password <Passphrase>`	`-S`	Passphrase für das Authentisierungszertifikat
`--server-ca <Datei.pem>`	`-s`	CA-Kette zur Prüfung des TLS-Server-Zertifikats der TMA
`--accept-invalid-cert`	`-I`	TLS-Server-Zertifikat der TMA nicht prüfen
`--pause-on-exit`		Vor Beenden auf Eingabe warten
`--install`	`-i`	Installation durchführen (Linux: systemd; Windows: Windows-Dienst)
`--reinstall`		Bestehende Installation entfernen und neu einrichten

Nur unter Windows verfügbar:

Option	Beschreibung
`--uninstall`	Windows-Dienst stoppen und entfernen (TMA-Registrierung bleibt bestehen)
`--start-service`	Windows-Dienst starten
`--stop-service`	Windows-Dienst stoppen
`--service`	Als Windows-Dienst ausführen (wird vom Service Control Manager gesetzt)
`--elevate`	Prozess mit administrativen Rechten (UAC) neu starten
`--use-local-machine`	Authentisierungszertifikat im Zertifikatspeicher des lokalen Computers ablegen und Registrierungswerte unter `HKEY_LOCAL_MACHINE` verwenden

26.2 Template-Variablen

Alle Templates verwenden die Handlebars-Syntax. Variablen werden mit doppelten geschweiften Klammern referenziert: `{{variablenname}}`. Bedingte Blöcke werden mit `{{#if ...}}...{{/if}}` und Schleifen mit `{{#each ...}}...{{/each}}` formuliert.

26.2.1 Hilfsfunktionen

Aufruf	Beschreibung
`{{datetime zeitstring format}}`	Formatiert einen ISO-8601-Zeitstring nach dem angegebenen chrono-Format.
`{{data wert}}`	Gibt einen Wert als `echo -e`-kompatiblen Escaped-String aus (Zeilenumbrüche, Sonderzeichen etc. werden maskiert).

26.2.2 Verzeichnisse und Bezeichnung

Aufruf	Beschreibung
`{{cert_dir}}`	Absoluter Pfad des Verzeichnisses auf dem Zielsystem, in dem die Zertifikatdateien gespeichert werden.
`{{alias_dir}}`	Alternativer Verzeichnispfad, der den label-Namen trägt und einen festen Verzeichnisnamen für das Zertifikatverzeichnis auf dem Zielsystem bereitstellt (z.B. als Symlink-Ziel).
`{{label}}`	Menschenlesbarer Bezeichner dieses Zertifikatseintrags, wie er in der Konfiguration definiert wurde. Kann beliebige Zeichen enthalten.
`{{label_ascii}}`	ASCII-sichere Version von label. Nicht-alphanumerische Zeichen werden durch _ ersetzt und der Wert wird auf die konfigurierte Maximallänge gekürzt. Geeignet für Dateinamen, Alias-Bezeichner und Umgebungsvariablen.

Beispiele:

`{{cert_dir}}`

```
# Verzeichnis anlegen und Zertifikat speichern
mkdir -p {{cert_dir}} || exit $?
cat - <<EOF > {{cert_dir}}/cert.pem
{{cert_pem}}
EOF
```

`{{alias_dir}}`

```
# Symlink mit festem Namen anlegen
ln -sfn {{cert_dir}} {{alias_dir}}
```

`{{label}}`

```
echo "Verarbeite Zertifikat: {{label}}"
```

`{{label_ascii}}`

```
# Als Dateiname verwenden
cp {{cert_dir}}/cert.pem /etc/ssl/certs/{{label_ascii}}.pem
```

26.2.3 Zertifikatidentität

Aufruf	Beschreibung
`{{fingerprint}}`	SHA-256-Fingerabdruck des Zertifikats im Doppelpunkt-getrennten Hex-Format (z.B. `AA:BB:CC:DD:...`). Wird typischerweise in `result_uptodate`-Regex-Templates genutzt, um zu prüfen, ob das richtige Zertifikat installiert ist.
`{{valid_until}}`	Ablaufdatum des Zertifikats als formatierter String (z.B. `2027-06-15T04:34:24Z`).
`{{id}}`	Eindeutiger Bezeichner des Zertifikats.

Beispiele:

`{{fingerprint}}`

```
# Fingerabdruck des installierten Zertifikats prüfen
openssl x509 -noout -fingerprint -sha256 -in {{cert_dir}}/cert.pem
# Erwarteter Wert für result_uptodate-Regex:
# (?i)sha256 Fingerprint={{fingerprint}}
```

{{valid_until}}

```
echo "Zertifikat gültig bis: {{valid_until}}"
```

{{id}}

```
echo "Zertifikats-ID: {{id}}"
```

26.2.4 Subject/Distinguished Name

Aufruf	Beschreibung
{{subject}}	Subject Distinguished Name wie er in der TMA-Konfiguration angegeben wurde, entsprechend RFC 4514 (z.B. `CN=beispiel-simulation-cert,OU=agent group 1,OU=AgentTest,O=firma`).
{{subject_compat}}	Subject DN im OpenSSL-kompatiblen Format. Nicht-ASCII-Zeichen werden korrekt kodiert (z.B. `/O=firma/OU=AgentTest/OU=agent group 1/CN=beispiel-simulation-cert`). Zu verwenden beim Aufruf von `openssl req -subj`.
{{subject_reverse}}	Subject DN mit umgekehrter Reihenfolge der RDN-Komponenten (RFC 4514-Stil, aber in reverse order z.B. `O=firma, OU=AgentTest, OU=agent group 1, CN=beispiel-simulation-cert`).

Beispiele:

{{subject}}

```
echo "Subject: {{subject}}"
```

{{subject_compat}}

```
openssl req -new -utf8 -nodes \
  -subj '{{subject_compat}}' \
  -newkey rsa:2048 \
  -keyout {{cert_dir}}/key.pem \
  -out {{cert_dir}}/req.pem \
  || exit $?
```

{{subject_reverse}}

```
echo "RFC-4514-Subject: {{subject_reverse}}"
```

26.2.5 Schlüsseltyp

Aufruf	Variable	Beschreibung
{{keytype}}		Kryptographischer Schlüsseltyp mit zugehörigen Parametern. Entweder RSA (mit key_size) oder EC (mit curve_name).
	{{keytype.RSA.key_size}}	RSA-Schlüssellänge in Bits (z.B. 2048, 4096). Nur vorhanden wenn keytype = RSA.
	{{keytype.EC.curve_name}}	Name der elliptischen Kurve (z.B. prime256v1, secp384r1). Nur vorhanden wenn keytype = EC.

Beispiel:

```
# RSA- oder EC-Schlüssel je nach konfiguriertem Typ erzeugen
openssl req -new -utf8 -nodes \
  -subj '{{subject_compat}}' \
  -keyout {{cert_dir}}/key.pem \
  -out {{cert_dir}}/req.pem \
  {{#if keytype.RSA}}
    -newkey rsa:{{keytype.RSA.key_size}} \
  {{else}}
    -newkey ec -pkeyopt 'ec_paramgen_curve:{{keytype.EC.curve_name}}' \
  {{/if}}
  || exit $?
```

26.2.6 Zertifikatdaten

Aufruf	Beschreibung
{{cert_name}}	Basisdateiname der Zertifikatdateien ohne Verzeichnis und Erweiterung.
{{cert_pem}}	End-Entity-Zertifikat im PEM-Format.
{{cert_key_pem}}	Kombiniertes PEM-Bundle aus Zertifikat und privatem Schlüssel (wird nach Verwendung aus dem Speicher gelöscht – Zeroize).
{{cert_pem_fullchain}}	Vollständige Zertifikatkette im PEM-Format: End-Entity-Zertifikat gefolgt von allen Intermediate-Zertifikaten.
{{cert_der}}	End-Entity-Zertifikat im DER-Binärformat.
{{cert_der_base64}}	End-Entity-Zertifikat im DER-Binärformat, Base64-kodiert. Kann direkt in Skripten verwendet werden, ohne weitere Kodierung.
{{cert_pkcs7}}	Zertifikat oder Zertifikatkette im PKCS#7 (CMS)-Format.
{{cert_pkcs12}}	Zertifikatbundle im PKCS#12-Format, typischerweise enthält es Zertifikat, privaten Schlüssel und Kette.

Beispiele:

`{{cert_name}}`

```
cp {{cert_dir}}/cert.pem /etc/ssl/certs/{{cert_name}}.crt
```

`{{cert_pem}}`

```
cat - <<EOF > {{cert_dir}}/cert.pem
{{cert_pem}}
EOF
```

`{{cert_key_pem}}`

```
cat - <<EOF > {{cert_dir}}/cert-with-key.pem
{{cert_key_pem}}
EOF
chmod 600 {{cert_dir}}/cert-with-key.pem
```

`{{cert_pem_fullchain}}`

```
cat - <<EOF > {{cert_dir}}/fullchain.pem
{{cert_pem_fullchain}}
EOF
```

`{{cert_der_base64}}`

```
# Zertifikat als DER-Datei speichern
echo '{{cert_der_base64}}' | base64 -d > {{cert_dir}}/cert.der
```

Für HTTP-Skripte muss die Base64-Kodierung benutzt werden, um Binärdaten in ein Skript einzufügen.

Beispiel: Zertifikat im DER-Format per PUT hochladen

```
PUT https://1.2.3.4/api/v2.0/attachment-url
base64,{{cert_der_base64}}
```

{{cert_pkcs12}}

```
# PKCS#12 in Java-Keystore importieren
echo {{cert_pkcs12}} | base64 -d > {{cert_dir}}/bundle.p12
keytool -importkeystore \
  -srckeystore {{cert_dir}}/bundle.p12 \
  -srcstoretype PKCS12 \
  -destkeystore /opt/app/keystore.jks \
  -deststoretype JKS
```

26.2.7 CA-Zertifikate

Aufruf	Variable	Beschreibung
{{ca_pem_fullchain}}		Vollständige CA-Zertifikatskette im PEM-Format: alle Intermediate-CAs und die Root-CA.
{{ca}}		Array aller CA-Zertifikatsvariablen, beginnend bei der ausstellenden CA bis hin zur Root-CA. Die Elemente werden mit {{#each ca}} iteriert.
	{{ca_pem}}	CA-Zertifikat dieses Eintrags im PEM-Format.
	{{ca_der}}	CA-Zertifikat im DER-Binärformat.
	{{ca_der_base64}}	CA-Zertifikat im DER-Binärformat, Base64-kodiert.
	{{alias}}	Menschenlesbarer Bezeichner für dieses CA-Zertifikat (z.B. für Keystore-Import).
	{{id}}	Eindeutiger Bezeichner dieses CA-Zertifikats.
	{{fingerprint}}	SHA-256-Fingerabdruck dieses CA-Zertifikats im Doppelpunkt-Hex-Format.
	{{crl_pem}}	Von dieser CA ausgestellte Certificate Revocation List (CRL) im PEM-Format.
	{{crl_der}}	CRL im DER-Binärformat.
	{{crl_der_base64}}	CRL im DER-Binärformat, Base64-kodiert.

Beispiele:

{{ca_pem_fullchain}}

```
cat - <<EOF > {{cert_dir}}/ca.pem
{{ca_pem_fullchain}}
EOF
# Als vertrauenswürdige CA installieren
cp {{cert_dir}}/ca.pem /usr/local/share/ca-certificates/{{label_ascii}}.crt
update-ca-certificates
```

{{ca}}

```
# Jede CA einzeln in den System-Trust-Store importieren
{{#each ca}}
cat - <<EOF > /usr/local/share/ca-certificates/{{alias}}.crt
{{ca_pem}}
EOF
{{/each}}
update-ca-certificates
```

```
# Einzelnen CA-Fingerabdruck prüfen
{{#each ca}}
echo "CA {{alias}}: {{fingerprint}}"
{{/each}}
```

26.2.8 CRL

Aufruf	Beschreibung
{{crl_pem_fullchain}}	Vollständige Certificate Revocation List-Kette aller CAs im PEM-Format.

Beispiel:

{{crl_pem_fullchain}}

```
cat - <<EOF > {{cert_dir}}/crl.pem
{{crl_pem_fullchain}}
EOF
```

26.2.9 Privater Schlüssel

Aufruf	Beschreibung
{{key_pem}}	Privater Schlüssel im PEM-Format (wird nach Verwendung aus dem Speicher gelöscht – Zeroize).
{{key_der}}	Privater Schlüssel im DER-Binärformat (wird nach Verwendung aus dem Speicher gelöscht – Zeroize).
{{key_der_base64}}	Privater Schlüssel im DER-Binärformat, Base64-kodiert (wird nach Verwendung aus dem Speicher gelöscht – Zeroize). Kann direkt in Skripten verwendet werden, ohne weitere Kodierung.

Beispiele:

`{{key_pem}}`

```
cat - <<EOF > {{cert_dir}}/key.pem
{{key_pem}}
EOF
chmod 600 {{cert_dir}}/key.pem
```

`{{key_der_base64}}`

```
# Schlüssel als DER-Datei speichern
echo '{{key_der_base64}}' | base64 -d > {{cert_dir}}/key.der
chmod 600 {{cert_dir}}/key.der
```

Für HTTP-Skripte muss die Base64-Kodierung benutzt werden, um Binärdaten in ein Skript einzufügen.

Beispiel: Schlüssel im DER-Format per PUT hochladen

```
PUT https://1.2.3.4/api/v2.0/attachment-url
base64,{{key_der_base64}}
```

26.2.10 Serververbindung (TMA-Abruf)

Die folgenden Variablen beschreiben den Server auf der TMA (Trusted Management Appliance), von dem das Zertifikat per SCP oder SFTP abgerufen werden kann.

Aufruf	Beschreibung
{{server_host}}	Hostname oder IP-Adresse des TMA-Servers.
{{server_port}}	Portnummer des TMA-Servers.
{{server_username}}	Benutzername zur Authentifizierung am TMA-Server.
{{server_filename}}	Primärer Dateiname auf dem TMA-Server (erste Datei bei Einzelabruf).
{{server_url}}	Primäre URL für Serveroperationen auf der TMA (z.B. SCP- oder SFTP-URL, erste URL).
{{server_filenames}}	Geordnete Liste aller Dateinamen auf dem TMA-Server, wenn mehrere Dateien übertragen werden.
{{server_urls}}	Geordnete Liste aller URLs für Serveroperationen auf der TMA, wenn mehrere Endpunkte verwendet werden.

Beispiele:

`{{server_host}}`

```
scp {{server_username}}@{{server_host}}:{{server_filename}} {{cert_dir}}/cert.pem
```

`{{server_port}}`

```
scp -P {{server_port}} {{server_username}}@{{server_host}}:{{server_filename}} {{cert_dir}}/cert.pem
```

`{{server_filename}}`

```
sftp {{server_username}}@{{server_host}}:{{server_filename}}
```

`{{server_filenames}}`

```
{{#each server_filenames}}
scp {{../server_username}}@{{../server_host}}:{{this}} {{../cert_dir}}/
{{/each}}
```

`{{server_urls}}`

```
{{#each server_urls}}
echo "Datei verfügbar unter: {{this}}"
{{/each}}
```

26.2.11 Remote-Dateizugriff (Push-Modus)

Diese Variablen werden zusammen mit den `#!get`- und `#!put`-Direktiven in Templates verwendet.

Aufruf	Beschreibung
`{{target_scp_url}}`	SCP-URL-Template für den Dateitransfer zum Zielsystem im **Push**-Modus.
`{{target_sftp_url}}`	SFTP-URL-Template für den Dateitransfer zum Zielsystem im **Push**-Modus.

Beispiele:

`{{target_scp_url}}`

```
# Datei per SCP vom Zielsystem holen
#!get {{target_scp_url}}/{{cert_dir}}/cert.pem
# Datei per SCP auf das Zielsystem übertragen
#!put {{target_scp_url}}/{{cert_dir}}/cert.pem {{data cert_pem}}
```

`{{target_sftp_url}}`

```
# Datei per SCP vom Zielsystem holen
#!get {{target_sftp_url}}/{{cert_dir}}/cert.pem
# Datei per SFTP auf das Zielsystem übertragen
#!put {{target_sftp_url}}/{{cert_dir}}/cert.pem {{data cert_pem}}
```

26.2.12 Systeminformationen

Aufruf	Beschreibung
{{hostname}}	Kurzname (Hostname) des Rechners, auf dem das Zertifikat ausgerollt wird.
{{fqdn}}	Vollqualifizierter Domainname (FQDN) des Zielsystems.
{{starttime}}	Startzeitpunkt der Enrollment-Operation im Format `YYYY-MM-DD-HH:MM:SS.ffffff`.

Beispiele:

`{{hostname}}`

```
echo "Deploye Zertifikat auf Host: {{hostname}}"
```

`{{fqdn}}`

```
# FQDN im Subject Alternative Name verwenden
openssl req -new -utf8 -nodes \
  -subj '{{subject_compat}}' \
  -addext "subjectAltName=DNS:{{fqdn}}" \
  -newkey rsa:2048 \
  -keyout {{cert_dir}}/key.pem \
  -out {{cert_dir}}/req.pem \
  || exit $?
```

`{{starttime}}`

```
echo "Enrollment gestartet um: {{starttime}}"
# Logverzeichnis mit Zeitstempel
mkdir -p /var/log/enrollment/{{starttime}}
```

26.2.13 Benutzerdefinierte Eigenschaften

Aufruf	Beschreibung
{{properties.<schlüssel>}}	Benutzerdefinierte Schlüssel-Wert-Paare aus der Deployment-Konfiguration. Die Werte werden nach Verwendung aus dem Speicher gelöscht (Zeroize). Der Zugriff erfolgt über den konfigurierten Eigenschaftsnamen als Pfad.

Beispiele:

`{{properties.<schlüssel>}}`

```
# Beispiel: Eigenschaft "app_password" im Template nutzen
echo "Anwendungspasswort: {{properties.app_password}}"

# Beispiel: Eigenschaft "target_path" für Zieldatei
cp {{cert_dir}}/cert.pem {{properties.target_path}}/server.crt
```

26.2.14 Vollständiges Template-Beispiel

Das folgende Beispiel zeigt ein `post_deploy`-Script, das mehrere Variablen kombiniert:

```
#!/bin/sh
set -e

echo "=== Zertifikat-Deployment auf {{fqdn}} ==="
echo "Label:       {{label}}"
echo "Startzeitpunkt: {{starttime}}"

# Zertifikat und Schlüssel in Anwendungsverzeichnis kopieren
install -m 644 {{cert_dir}}/cert.pem    /etc/myapp/tls/server.crt
install -m 644 {{cert_dir}}/ca.pem      /etc/myapp/tls/ca.crt
install -m 600 {{cert_dir}}/key.pem     /etc/myapp/tls/server.key

# CRL ablegen
install -m 644 {{cert_dir}}/crl.pem     /etc/myapp/tls/crl.pem

# CA-Zertifikate einzeln in den Trust-Store importieren
{{#each ca}}
install -m 644 - /usr/local/share/ca-certificates/{{alias}}.crt <<EOF
{{ca_pem}}
EOF
{{/each}}
update-ca-certificates

# Anwendung neu starten
systemctl restart myapp

echo "=== Deployment abgeschlossen. Gültig bis: {{valid_until}} ==="
```

26.2.15 Beispielwerte

Die folgende Liste zeigt Beispiele (nicht vollständig) für diverse Variablen:


```
cert_dir: "/home/cert-enrollment-agent/.ecos-tma/certs/3f45e9f85f7c252d4aa8eb-
7596c64ef1",
alias_dir: "/home/cert-enrollment-agent/.ecos-tma/certs/beispiel-simulation-cert",
label: "beispiel-simulation-cert",
label_ascii: "beispiel_sim",
fingerprint: "B1:F3:39:ED:E3:52:F8:E0:6F:F3:79:2B:B2:A7:63:BC:BE:78:BB:BF:14:5F:FA:55:08:4B
:23:58:3C:93:D7:CB",
valid_until: "2027-05-04T08:52:18Z",
id: "3f45e9f85f7c252d4aa8eb7596c64ef1",
subject_compat: "/O=firma/OU=AgentTest/OU=agent group 1/CN=beispiel-simulation-
cert",
subject_reverse: "O=firma, OU=AgentTest, OU=agent group 1, CN=beispiel-simulation-
cert",
subject: "CN=beispiel-simulation-cert,OU=agent group 1,OU=AgentTest,O=firma",
keytype: None,
cert_name: "agent-beispiel-simulation-beispiel-simulation-cert",
cert_pem: "",
cert_key_pem: "",
cert_pem_fullchain: "",
cert_der: [],
cert_pkcs7: [],
cert_pkcs12: [],
ca: [],
ca_pem_fullchain: "",
crl_pem_fullchain: "",
key_pem: "",
key_der: [],
server_host: "",
server_port: 0,
server_username: "",
server_filename: "",
server_url: "",
server_filenames: [],
server_urls: [],
target_scp_url: "scp://{target_ssh_user}:{target_ssh_password}@@{target_ssh_priv-
key}@{target_ssh_host}:{target_ssh_port}",
target_sftp_url: "sftp://{target_ssh_user}:{target_ssh_password}@@{target_ssh_
privkey}@{target_ssh_host}:{target_ssh_port}",
hostname: "myhost",
fqdn: "myhost.example.com",
starttime: "2026-06-15-08:32:03.914137",
```

```
properties: {
    "target_ssh_host": "10.1.2.3",
    "target_ssh_user": "username",
    "target_ssh_port": "22",
    "target_ssh_password": "",
    "target_ssh_privkey": "-----BEGIN PRIVATE KEY-----\nMIIE..."
},
```

26.3 Fehlersuche und Logging

Meldung (sinngemäß)	Ursache	Lösung
"Address of TMA not known"	Es liegt weder `--address` noch eine vorherige Registrierung vor.	`--address` angeben oder zunächst `--install`/`--new-agent-auth` ausführen
"User to access TMA not known"	Bei der Registrierung fehlt `--user` (`--new-agent-auth`/`--install`).	`--user <Konto>` angeben
"Not supported: ... in deployment ..."	Nicht unterstützte Kombination aus Modus, Ziel-OS und Deployment-Methode (siehe **18.4.2.2 Deployment-Methoden**)	Deployment-Methode (Deploymentinfo für Agent) bzw. Modus (Abonnentenkonto für Agent) anpassen
"Script ... did not succeed. Did not find success regex ..."	Das konfigurierte Regex-Feld für ein Skript hat in dessen Ausgabe nicht gepasst.	Skript-Ausgabe und Regex (Deploymentinfo für Agent) prüfen
"Command ... failed with ..."	Ein Skript bzw. ein externer Befehl (z. B. `useradd`, `systemctl`) ist fehlgeschlagen.	Exit-Code und Ausgabe des Befehls prüfen (Logdatei bzw. `journalctl`)

27 Support

Bei technischen Fragen zu unseren Produkten stehen wir Ihnen gerne zur Verfügung. Bitte halten Sie die Seriennummer Ihres-ECOS Produkts bereit.

27.1 Technischer Support

Tel: +49 (6133) 939-300

E-Mail: support@ ecos.de

27.2 Störungsannahme

Mo-So 0.00-24:00 Uhr.

27.3 Bearbeitungszeiten von Supportfällen

Mo-Fr* 8:00 – 18:00 Uhr

*außer an gesetzlichen Feiertagen

27.4 Hardware-Tests

Senden Sie Hardware-Tests bitte mit einer kurzen Beschreibung und Ihren Kontaktinformationen an:

hwtest@ecos.de

27.5 Meldung von Security-Vorfällen

Melden Sie Security-Vorfälle bitte mit einer ausführlichen Beschreibung und Ihren Kontaktdaten an:

support@ecos.de

27.6 Updates

Informationen zu Updates erhalten Sie mit den ECOS Release Notes. Unsere Release Notes können Sie auch per Newsletter beziehen.

28 Abbildungen

Einführung 11

Teil I - Inbetriebnahme 13

1 Installation und Inbetriebnahme der Appliance 14
Abb. 1.01: Start der Installation 15
Abb. 1.02: Auswahl der Festplatte 15
Abb. 1.03: Angabe der IP-Adresse 15
A**bb.** 1.04: Angabe der Gateway-Adresse 15
Abb. 1.05: Die Installation ist abgeschlossen 15
Abb. 1.06: Anmeldung an der Administrationsoberfläche 16
Abb. 1.07: Ersteinrichtung - Administratorkonto einrichten 16
Abb. 1.08: Ersteinrichtung - Lizenzvereinbarung 17
Abb. 1.09: Ersteinrichtung - Lizenz einspielen 17
Abb. 1.10: Ersteinrichtung - Netzwerkeinrichtung 17
Abb. 1.11: Ersteinrichtung - PKI-Dienste auswählen 18
Abb. 1.12: Ersteinrichtung - Root-CA konfigurieren 18
Abb. 1.13: Ersteinrichtung - Sub-CA konfigurieren 19
Abb. 1.14: Ersteinrichtung - ACME-Dienst einrichten 20
Abb. 1.15: Ersteinrichtung - CMP-Dienst einrichten 21
Abb. 1.16: Ersteinrichtung - EST-Dienst einrichten 21
Abb. 1.17: Ersteinrichtung - SCEP-Dienst einrichten 22
Abb. 1.18: Ersteinrichtung - OCSP-Dienst einrichten 23
Abb. 1.19: Ersteinrichtung - Übersicht der Ersteinrichtung 23

2 Aufbau der Administrationsoberfläche - Standardansicht 25
Abb. 2.01: Hauptansicht der Administrationsoberfläche 25
Abb. 2.02: Header-Menü der Administrationsoberfläche 26
Abb. 2.03: Untermenü Benutzer 26
Abb. 2.04: Anzeige der Suchergebnisse 27
Abb. 2.05: Übersicht der Suchergebnisse 27
Abb. 2.06: Sitemap-Anzeige 28
Abb. 2.07: Containeransicht **de**r Administrationsoberfläche 28
Abb. 2.08: Weitere Optionen für Container 29
Abb. 2.09: Tabelleneinstellungen 30
Abb. 2.10: Filtereinstellungen 31
Abb. 2.11: Kontextmenü in Tabellen 31

3 Aufbau der Expertenansicht 33
Abb. 3.01: Aufbau der Administrationsoberfläche in der Expertenansicht 33
Abb. 3.02: Navigationsbaum 34
Abb. 3.03: Navigationsbaum - Kontextmenü 35
Abb. 3.04: Konfigurationsobjekt - Ansicht 37
Abb. 3.05: Konfigurationsobjekt - Untereinander anzeigen 37
Abb. 3.06: Kontextmenü eines Konfigurationsobjekts 38

Abb. 3.07: Tabellenfilter ... 39
Abb. 3.08: Tabellen - Kontextmenü einer Tabellenspalte ... 41
Abb. 3.09: Aktionen der Aktionsleiste ... 42
Abb. 3.10: Reiter „Admin“ ... 42
Abb. 3.11: Reiter „Log“ ... 43

Teil II - Standardansicht ... 44

4 Dashboards ... 45
Abb. 4.01: Dashboard der TMA ... 45

5 CA-Management ... 46
Abb. 5.01: CA-Management im Seitenmenü ... 46
Abb. 5.02: Übersicht CA-Zertifikate ... 47
Abb. 5.03: Kontextmenü für CA-Zertifikate ... 48
Abb. 5.04: Neue CA: Wizard starten ... 49
Abb. 5.05: Übergeordnete Zertifizierungsstelle auswählen ... 49
Abb. 5.06: CA-Kennwort angeben ... 50
Abb. 5.07: Policy & CPS ... 51
Abb. 5.08: CDP, OCSP-URI & CA-Aussteller ... 51
Abb. 5.09: Metadaten hinzufügen ... 52
Abb. 5.10: Speicherort festlegen ... 53
Abb. 5.11: CA-Zertifikat wird ausgestellt ... 53
Abb. 5.12: Upload erfolgreich ... 53
Abb. 5.13: CA-Kennwortanforderung festlegen ... 54
Abb. 5.14: Policy auswählen oder erstellen ... 55
Abb. 5.15: CRL Gültigkeitsdauer festlegen ... 55
Abb. 5.16: Metadaten ... 55
Abb. 5.17: Smartcard-/HSM-Optionen ... 56
Abb. 5.18: Angabe des CA-Kennworts ... 56
Abb. 5.19: Übersicht der CA-Zugangspunkte ... 57
Abb. 5.20: Übersicht der Zertifikate ... 57
Abb. 5.21: Kontextmenü der Zertifikate ... 59
Abb. 5.22: Start des Assistenten ... 59
Abb. 5.23: CA auswählen ... 60
Abb. 5.24: Schlüsseleinstellungen ... 60
Abb. 5.25: Signatureinstellungen ... 62
Abb. 5.26: Alternative Namen angeben ... 62
Abb. 5.27: Metadaten hinzufügen ... 63
Abb. 5.28: Speicherort für Schlüssel ... 63
Abb. 5.29: Zertifikatausstellung und Download ... 64
Abb. 5.30: Start des Assistenten ... 65
Abb. 5.31: CA auswählen ... 65
Abb. 5.32: Schlüsseleinstellungen ... 66
Abb. 5.33: Metadaten festlegen ... 67
Abb. 5.34: Speicherort für Schlüsselmaterial ... 67
Abb. 5.35: Zertifikat ausgestellt ... 67

Abb. 5.36: Übersicht der Richtlinien ... 69
Abb. 5.37: Neue Richtlinie erstellen ... 70
Abb. 5.38: Neue Richtlinie: Standardwerte bestimmen ... 71
Abb. 5.39: Neue Richtlinie: Validierungsregeln ... 71
Abb. 5.40: Neue Richtlinie: Bedingungen ... 72

6 RA-Management ... 73
Abb. 6.01: RA-Management im Seitenmenü ... 73
Abb. 6.02: Übersicht RA-Management ... 73
Abb. 6.03: CSR genehmigen: Eigentümer & Container ... 74
Abb. 6.04: CSR genehmigen: CA auswählen ... 75
Abb. 6.05: CSR genehmigen: Metadaten hinzufügen ... 75
Abb. 6.06: CSR genehmigen: Übersicht ... 75
Abb. 6.07: CSR ablehnen: Begründung ... 76

7 Benutzerverwaltung ... 77
Abb. 7.01: Benutzerverwaltung im Seitenmenü ... 77
Abb. 7.02: Übersicht Benutzerverwaltung ... 77
Abb. 7.03: Benutzer anlegen: Kontaktinformationen ... 78
Abb. 7.04: Benutzer anlegen: Authentifizierung ... 78
Abb. 7.05: Benutzer anlegen: Zeit/Sprache ... 79
Abb. 7.06: Benutzerkonto sperren ... 80
Abb. 7.07: Benutzerrolle anlegen ... 80
Abb. 7.08: Benutzerrolle zuweisen ... 81
Abb. 7.09: Übersicht Benutzerrollen ... 81

8 PKI-Dienste ... 82
Abb. 8.01: Übersicht Zugangspunkte ... 82

9 Globale Einstellungen ... 83
Abb. 9.01: Globale Einstellungen im Seitenmenü ... 83
Abb. 9.02: Netzwerkeinstellungen ... 83
Abb. 9.03: Organisation ... 84
Abb. 9.04: Übersicht Metadatenverwaltung ... 84
Abb. 9.05: Metadatenschlüssel erstellen ... 84
Abb. 9.06: Optionen hinzufügen ... 85
Abb. 9.07: Metadaten hinzufügen ... 85
Abb. 9.08: Lizenzinformationen ... 85

10 Dokumentation ... 86
Abb. 10.01: Dokumentation: Kapitelansicht ... 86

11 Self-Service-Portal ... 87
Abb. 11.01: Übersicht des Self-Service-Portals ... 87
Abb. 11.02: Schnellfilter oberhalb der Tabelle ... 88
Abb. 11.03: Zertifikatrequest wurde abgelehnt ... 88
Abb. 11.04: Neues Zertifikat anfordern ... 89

Abb. 11.05: CSR-Assistent: Typ des Zertifikats ... 89
Abb. 11.06: CSR-Assistent: Name & Kennwort ... 89
Abb. 11.07: CSR-Assistent: Subjekt & Verwendungszweck ... 90
Abb. 11.08: CSR-Assistent: Übersicht ... 90
Abb. 11.09: CSR-Assistent: Antrag wurde gestellt ... 91
Abb. 11.10: CSR importieren ... 91

Teil III - Expertenansicht ... 92

12 Das ECOS Appliance-Objekt ... 93
Abb. 12.01: ECOS Appliance-Objekt - Reiter Allgemein ... 93
Abb. 12.02: ECOS Appliance-Objekt - Reiter Netzwerk ... 94
Abb. 12.03: Reiter „Aktionen“ - Netzwerktool ping ... 95
Abb. 12.04: Reiter „Aktionen“ - Netzwerktool traceroute ... 95
Abb. 12.05: Reiter „Aktionen“ - Netzwerktool dns ... 96
Abb. 12.06: Reiter „Aktionen“ - Netzwerktool tcpdump ... 97
Abb. 12.07: Reiter „Aktionen“ - Manuelles Update ... 97
Abb. 12.08: Reiter Aktionen - Konfigurationsexport ... 98
Abb. 12.09: Reiter „Aktionen“ - Restart System/Dienste ... 98
Abb. 12.10: Reiter „Aktionen“ - Uhrzeit ... 99
Abb. 12.11: Reiter „Aktionen“ - Backup ... 99
Abb. 12.12: Reiter „Info“ ... 100
Abb. 12.13: ECOS Appliance als Container ... 100
Abb. 12.14: Route (statisch) ... 101
Abb. 12.15: Routing-Regel ... 101

13 Netzwerkkonfiguration ... 102
Abb. 13.01: Netzwerk-Interface konfigurieren ... 102
Abb. 13.02: Host-Name konfigurieren ... 102
Abb. 13.03: Port konfigurieren ... 103
Abb. 13.04: Netzwerke konfigurieren ... 104

14 Grundlegende Dienste ... 105
Abb. 14.01: HTTPS-Administration einrichten ... 105
Abb. 14.02: Konfiguration des Backup Keys ... 107
Abb. 14.03: Dienst: Backup ... 108
Abb. 14.04: Wartungsdienst einrichten ... 109
Abb. 14.05: Lokale Wartung konfigurieren ... 110
Abb. 14.06: Dienst: Smartcard-Enrollment ... 110
Abb. 14.07: Dienst: Software-Update ... 111
Abb. 14.08: Reiter „Aktionen“ - Manuelles Update ... 112
Abb. 14.09: Software-Update-Image - Reiter Allgemein ... 113
Abb. 14.10: Software-Update-Image - Reiter Download ... 113
Abb. 14.11: Software-Update-Quelle ... 113
Abb. 14.12: Dienst: Software-Update-Server ... 114
Abb. 14.13: Dienst: Software-Update ... 114

15 Benutzerverwaltung (Experte) 115
Abb. 15.01: Privileg in Benutzerrolle 115
Abb. 15.02: Authentisierungsmethoden im Benutzer-Objekt 116

16 Zertifikate 118
Abb. 16.01: CA-Zertifikat-Objekt - Reiter Allgemein 118
Abb. 16.02: CA-Zertifikat-Objekt - Reiter Erweitert 120
Abb. 16.03: Zertifikat-Objekt - Reiter Allgemein 121
Abb. 16.04: Zertifikat-Objekt - Reiter Weitere Namen 122
Abb. 16.05: Zertifikat-Objekt - Reiter Verwendung 122
Abb. 16.06: CRL Distribution Point 123
Abb. 16.07: Zertifikat-Objekt - Reiter Smartcard 125
Abb. 16.08: Konfiguration eines HSM 127

17 Zertifikat-Enrollment mit Standardprotokollen 128
Abb. 17.01: Ablauf des Zertifikat-Enrollments 128
Abb. 17.02: CA-Zertifikat - CA-Typ bestimmen 129
Abb. 17.03: TLS-Serverzertifikat - Verwendungszweck 129
Abb. 17.04: Container: Abonnentengruppe - Reiter Allgemein 130
Abb. 17.05: CA-Abonnentenverknüpfung 130
Abb. 17.06: Dienst: ACME-Server - Reiter Allgemein 131
Abb. 17.07: Dienst: ACME-Server - Reiter ACME 132
Abb. 17.08: ACME-Abonnentenkonto - Reiter Allgemein 133
Abb. 17.09: ACME-Abonnentenkonto - Reiter Stammdaten 133
Abb. 17.10: ACME-Abonnentenkonto - Reiter Bestellungen 133
Abb. 17.11: Dienst: CMP-Server - Reiter Allgemein 134
Abb. 17.12: CMP-Abonnentenkonto - Reiter Allgemein 135
Abb. 17.13: CMP-Abonnentenkonto - Reiter Weitere Namen 135
Abb. 17.14: CMP-Abonnentenkonto - Reiter Authentisierung 135
Abb. 17.15: Dienst: EST-Server - Reiter Allgemein 136
Abb. 17.16: EST-Abonnentenkonto - Reiter Allgemein 137
Abb. 17.17: EST-Abonnentenkonto - Reiter Weitere Namen 137
Abb. 17.18: EST-Abonnentenkonto - Reiter Authentisierung 137
Abb. 17.19: Dienst: SCEP-Server - Reiter Allgemein 139
Abb. 17.20: SCEP-Abonnentenkonto - Reiter Allgemein 139
Abb. 17.21: SCEP-Abonnentenkonto - Reiter Weitere Namen 140
Abb. 17.22: SCEP-Abonnentenkonto - Reiter Authentisierung 140
Abb. 17.23: CA-Zertifikat - CA-Typ bestimmen 142
Abb. 17.24: ACME-Providerkonto - Reiter Allgemein 142
Abb. 17.25: ACME-Providerkonto - Reiter Stammdaten 143
Abb. 17.26: ACME-Providerkonto - Reiter Bestellungen 143
Abb. 17.27: ACME-Providerkonto - Reiter ACME-Aktionen 143
Abb. 17.28: CMP-Providerkonto - Anmeldung mit Zugangsdaten 144
Abb. 17.29: CMP-Providerkonto - Anmeldung mit Zertifikat 144

18 Zertifikat-Enrollment mit dem Certificate Enrollment Agent 146
Abb. 18.01: Zertifikat-Enrollment mit dem Certificate Enrollment Agent 146

Abb. 18.02: Dienst: Certificate Enrollment Agent - Reiter Allgemein 147
Abb. 18.03: Dienst: Certificate Enrollment Agent - Reiter Download 148
Abb. 18.04: Abonnentenkonto für Agent - Reiter Allgemein 148
Abb. 18.05: Abonnentenkonto für Agent - Reiter Weitere Namen 149
Abb. 18.06: Abonnentenkonto für Agent - Reiter Authentisierung 150
Abb. 18.07: Starten des Windows-Installers 153
Abb. 18.08: Zertifikatplan für Agent - Reiter Allgemein 157
Abb. 18.09: Deploymentinfo für Agent - Reiter Allgemein 158
Abb. 18.10: Deploymentinfo für Agent - Shell-Skript 161

19 Verzeichnissynchronisation 166
Abb. 19.01: Verzeichnissynchronisation im Navigationsbaum 166
Abb. 19.02: Verzeichnisdienst - Typ ECOS System 166
Abb. 19.03: LDAP - Reiter „Suchanfrage“ 167
Abb. 19.04: Verzeichnismap einrichten 167
Abb. 19.05: Verzeichnissynchronisation einrichten 168
Abb. 19.06: Manuelle Synchronisation anstoßen 168

20 Hochverfügbarkeit 169
Abb. 20.01: Container der Master-Appliance 169
Abb. 20.02: Einrichten der Master-Appliance 169
Abb. 20.03: ECOS System Connectors für eine Master-Appliance 170
Abb. 20.04: Aktivieren des Software-Update-Servers 170
Abb. 20.05: Duplizieren des Appliance-Objekts 171
Abb. 20.06: Slave-Appliance einrichten 171
Abb. 20.07: Appliance-Objekt für Basiskonfiguration 171
Abb. 20.08: Container der Basiskonfiguration 172
Abb. 20.09: Vererbung der Basiskonfiguration einrichten 172
Abb. 20.10: Einrichten der Appliance als HA-Basiskonfiguration 173
Abb. 20.11: Einrichten der HA-Konfiguration 173
Abb. 20.12: Konfiguration von Master zu Slave übertragen 173
Abb. 20.13: Verbindungen zum Master 174

21 Abfragen 175
Abb. 21.01: Abfrage - Reiter „Allgemein“ 175
Abb. 21.02: Abfrage - Reiter „Abfrage“ 175
Abb. 21.03: Datum auswählen 176
Abb. 21.04: Abfrage für ablaufende Zertifikate 176
Abb. 21.05: Keine automatische Suche 177
Abb. 21.06: Abfrage - Reiter „Felder“ 177
Abb. 21.07: Felder aus einer CA übernehmen 177
Abb. 21.08: Felder formatieren 178
Abb. 21.09: Abfrage - Reiter Hervorhebungen 178
Abb. 21.10: Abfrage mit Aktion - Reiter „Abfrage“ 179
Abb. 21.11: Abfrage mit Aktion - Reiter „Aktion“ 179

22 Berechtigungen 180
Abb. 22.01: Berechtigungen verteilen 181

Teil IV - Anhänge 183

23 Fehlerbeseitigung 184

24 Schlüsselverwendungszwecke 187

25 DocExpressions 190
Abb. 25.01: DocExpression Debugger 191
Abb. 25.02: DocExpression Debugger - Reiter „Funktionen“ 191
Abb. 25.03: DocExpression testen 196

26 Certificate Enrollment Agent - Anhänge 197

27 Support 211