

Konfigurierte Vertrauensdienste (Certificate Authorities)

Standardkonfiguration RELAY-3_7-3_23-CFG-71 (vom 05.04.2022) für OCSP/CRL-Relays ab Governikus SC 3.7

Das OCSP/CRL-Relay ist eine Komponente der Governikus Service Components. Als Validierungskomponente führt es nach einem XKMS-Request eine vollständige Zertifikatsprüfung durch. Überprüft werden der Vertrauenspfad (Zertifikatspfad), die Signaturen der Zertifikate der Kette bis zum Wurzelzertifikat, der Sperrstatus des Signaturzertifikats oder Siegelzertifikats (online beim ausstellenden Trustcenter) und ob der Signierzeitpunkt innerhalb des Gültigkeitsintervalls des Zertifikats liegt. Die Prüfergebnisse werden als XKMS-Response an die anfragenden Clients zurückgesendet. Die Interpretation der Prüfergebnisse obliegt dabei immer der anfragenden Instanz.

Das OCSP/CRL-Relay benötigt eine Konfigurationsdatei (Standardkonfiguration), in der Root- und Zwischenzertifikate, technische Daten zur Verbindungskonfiguration und Informationen zur Qualität der Zertifikate (Staat, in dem das Trustcenter ansässig ist, Überwachungsqualität des Trustcenters, Zertifikatsniveau, Gültigkeitsmodell der Zertifikatsprüfung etc.) hinterlegt sind. Die Standardkonfiguration gliedert sich in vier Bereiche:

- **Bereich 1:** Vertrauensdiensteanbieter, die qualifizierte Zertifikate für elektronische Signaturen oder Siegel ausstellen. Die Bundesnetzagentur ist dabei die zuständige Aufsichtsbehörde und als solche mit dem Aufbau und der Überwachung einer sicheren und zuverlässigen Infrastruktur für qualifizierte elektronische Signaturen bzw. Siegel betraut. Die Übersicht der Vertrauensdiensteanbieter befindet sich auf den Seiten der [Bundesnetzagentur](#),
- **Bereich 2:** Konfigurierte Zertifizierungsstellen, die fortgeschrittene Zertifikate, Authentisierungs- und/oder Verschlüsselungszertifikate herausgeben, soweit sich diese auf qualifizierten Signaturkarten befinden,
- **Bereich 3:** Konfigurierte Zertifizierungsstellen der deutschen Verwaltung, die fortgeschrittene Zertifikate herausgeben (zum Beispiel eine Landes-PKI unterhalb der PKI-1-Verwaltung),
- **Bereich 4:** Sonstige konfigurierte Zertifizierungsstellen.

Die Standardkonfiguration wird kurzfristig aktualisiert und bereitgestellt, sobald sich Änderungen in den Bereichen 1 bis 3 ergeben. Dieses gilt auch, wenn ein neuer Vertrauensdiensteanbieter, der qualifizierte Zertifikate für elektronische Signaturen oder Siegel ausstellt, von der Bundesnetzagentur den Status Vertrauensdiensteanbieter nach der eIDAS-Verordnung verliehen hat, soweit dieser nicht nur Zertifikate oder Siegel an geschlossene Nutzergruppen herausgibt. Angestrebt wird die Bereitstellung einer aktualisierten Standardkonfiguration, bevor die Änderungen wirksam werden, um eine unterbrechungsfreie Prüfung der Zertifikate zu gewährleisten. Die im Bereich 4 konfigurierten Zertifizierungsstellen werden nur aktualisiert, wenn eine Bereitstellung aufgrund von Änderungen in den Bereichen 1 bis 3 notwendig wird.

Bereich 2: Konfigurierte Zertifizierungsstellen für fortgeschrittene Signaturzertifikate, Authentisierungs- und/oder Verschlüsselungszertifikate

Die folgenden Diensteanbieter geben fortgeschrittene Signaturzertifikate, Authentisierungs- und/oder Verschlüsselungszertifikate heraus, die sich auf qualifizierten Signaturkarten befinden. Mit den Konfigurationen in diesem Bereich wird sichergestellt, dass alle Zertifikate, die sich auf qualifizierten Signaturkarten (herausgegeben von deutschen Vertrauensdiensteanbietern) befinden, auch vom OCSP/CRL-Relay geprüft werden können.

Name des Trustcenters	Name der Zertifizierungsstelle (gemäß CN)
Bundesnotarkammer (BNotK)	PCA der ZS der BnotK

Name des Trustcenters	Name der Zertifizierungsstelle (gemäß CN)
	SCA des ZDA BnotK SCA BnotK VHN CA beN OSCI CA
Deutscher Sparkassen Verlag GmbH	S-TRUST Authentication and Encryption CA 2005 S-TRUST Authentication and Encryption Class 3 CA
DGN Deutsches Gesundheitsnetz Service GmbH	dgnservice CA
D-Trust GmbH	D-Trust CA D-Trust Advanced (Card) CA D-Trust Advanced Card Class 3 CA D-TRUST Limited Basic CA
medisign GmbH	DEMDs CA für Ärzte DEMDs CA für Psychotherapeuten DEMDS CA für Zahnärzte MED-ZOD2-CA MESIG.HBA-qCA
Trust Center der Deutschen Telekom AG	NKS CA TeleSec PKS CA

Bereich 3: Konfigurierte Zertifizierungsstellen der deutschen Verwaltung für fortgeschrittene Signaturzertifikate

Name des Trustcenters	Kontextinformation	Name der Zertifizierungsstelle (gemäß CN)
CA der Bundesdruckerei unter der PKI-1-Verwaltung	Die Zertifizierungsstelle gibt Softtoken heraus.	PPKI CA OSCI CA
CA der Freien Hansestadt Bremen	Die Zertifizierungsstelle gibt Softtoken heraus.	Freie Hansestadt Bremen SubCA Freie Hansestadt Machine SubCA SubCA-Machine SubCA-User
CA des Freistaates Bayern unter der PKI-1-Verwaltung	Die Zertifizierungsstelle gibt Softtoken heraus.	Bayerische VPKI Class3 Issuing CA
	Die Zertifikate befinden sich auf einer Signaturkarte.	Bayerische VPKI Smartcard Issuing CA
CA der Hessen-PKI unter der PKI-1-Verwaltung	Die Zertifizierungsstelle gibt Softtoken heraus.	CA-1-HessenHZD
CA IVBB Deutsche Telekom unter der PKI-1-Verwaltung	Die Zertifizierungsstelle gibt Softtoken heraus.	CA IVBB Deutsche Telekom AG
Deutsche Rentenversicherung Bund	Die Zertifikate befinden sich auf Mitarbeiterausweisen der Deutschen Rentenversicherung Bund.	NQ 70 Mitarbeiter CA NQ DRV MA Sig P-CA NQ DRV 11 MA CA NQ DRV 13 MA CA NQ DRV RT CA
Deutschland Online Infrastruktur CA unter der PKI-1-Verwaltung	Die Zertifizierungsstelle gibt Softtoken heraus. Die Zertifikate werden auch auf Netkey 3.0 Karten der TeleSec aufgespielt.	DOI CA

Bereich 4: Sonstige konfigurierte Zertifizierungsstellen

Die in diesem Bereich konfigurierten Zertifizierungsstellen werden nur aktualisiert, wenn eine Bereitstellung aufgrund von Änderungen in den Bereichen 1 bis 3 notwendig wird, es sei denn, die Aktualisierung einer der hier aufgeführten Zertifizierungsstellen wurde gesondert vertraglich vereinbart.

Name des Trustcenters	Kontextinformation	Name der Zertifizierungsstelle (gemäß CN)
Authega	Die Zertifizierungsstelle gibt Softtoken heraus.	AuthegaEFRESOFTCA
Bundesnotarkammer (BnotK)	Die Zertifizierungsstelle gibt Softtoken heraus.	OSCI CA beA Card CA beA MA CA beA OSCI CA beA Token CA
Bundeszahnärztekammer	Unbekannt	
DFN Deutsches Forschungsnetz	Die Zertifizierungsstelle gibt Softtoken heraus.	DFN-Verein Certification Authority 2 DFN-Verein Global Issuing CA Deutscher Bundestag CA - G02 Fraunhofer Service CA - G02 Fraunhofer User CA - G02 KIT-CA MPG CA - G02 RUB-Chipcard CA G2 TU Dortmund Chipcard CA 2 TU Dresden CA TU Ilmenau CA G2
D-Trust GmbH	Die Zertifizierungsstelle gibt Softtoken heraus.	D-TRUST Advanced Class 1 CA D-TRUST Advanced Class 2 CA D-TRUST Advanced Class 3 CA D-TRUST Encryption Class 2 CA D-TRUST Service Class 3 CA D-TRUST Application-Certificates CA
European Patent Office	Zertifikat auf der Signaturkarte des europäischen Patentamtes	European Patent Office CA European Patent Office Intermediate CA.cer
Governikus GmbH & Co KG	Die Zertifizierungsstelle gibt Softtoken heraus.	Governikus CA
medisign GmbH	Die Zertifizierungsstelle gibt fortgeschrittene Zertifikate auf Signaturkarten heraus.	Medisign CA
Trust Center der Deutschen Telekom AG	Die Zertifizierungsstelle gibt Softtoken heraus.	Shared Business CA Business CA TeleSec Business CA
procilon GROUP	Die Zertifizierungsstelle gibt Softtoken heraus.	procilon GROUP Customer CA – OSCI

Konfigurierte Zertifizierungsstellen, die den Sperrstatusdienst eingestellt haben

Die folgenden Zertifizierungsstellen liefern keine Sperrinformationen mehr für Zertifikate. Eine entsprechende Meldung wird vom Relay übermittelt.

Name des Trustcenters	Name der Zertifizierungsstelle (Root oder CA)
Bundesnetzagentur	3R-CA 1:PN 4R-CA 1:PN
Deutsche Post Signtrust und DMDA GmbH (inkl. Vorgänger)	SCA DP Com, O = SCA Deutsche Post Signtrust und DMDA GmbH SCA des ZDA Signtrust SCA DP Com
Deutscher Sparkassen Verlag GmbH	Alle Aussteller
Deutsche Rente	DRV QC * CA
TrustCenter GmbH	TC Trust accredited

Name des Trustcenters	Name der Zertifizierungsstelle (Root oder CA)
DATEV eG Zertifizierungsstelle	CA DATEV CA E:SECURE CA ENCAUTH CA ZDA DATEV
Steuerberaterkammern*	CA STBK B CA STBK P CA HSTBK HB CA STBK F CA STBK M CA STBK H CA STBK HD CA STBK N CA STBK SB CA STBK L CA STBK S
Wirtschaftsprüferkammer	CA WPK B
Patentanwaltskammer	CA DPAK
Rechtsanwaltskammern*	CA RAK BA CA RAK B CA RAK D CA RAK F CA HansRAK HH CA RAK KO CA RAK K CA RAK M CA RAK N

*Zur Vereinfachung der Darstellung sind hier nur die Kammern allgemein aufgeführt.