

mtG-OCSP: PKI made in Germany

Technische Daten

unterstützte Betriebssysteme	<ul style="list-style-type: none">➤ SUN Solaris 9 und 10➤ Linux mit 2.6er Kernel➤ Windows 2000/XP/2003➤ (weitere auf Anfrage)
Anforderung Prozessorleistung	<ul style="list-style-type: none">➤ mindestens 1 GHz
Anforderungen Hauptspeicher	<ul style="list-style-type: none">➤ mindestens 1 GB RAM
Anforderung Plattenspeicher	<ul style="list-style-type: none">➤ 35 MB für das System, ansonsten abhängig von Anzahl Zertifikaten
Anwendungsplattform	<ul style="list-style-type: none">➤ Java 5 Run Time Environment➤ Apache 1.3 Webserver➤ Tomcat 5.5/6.x Servlet Engine
Transportprotokoll	<ul style="list-style-type: none">➤ HTTP, optional HTTPS
unterstützte Standards	<ul style="list-style-type: none">➤ ISIS-MTT-Specification, Common ISIS-MailTrust Specification For PKIApplications, T7 & TeleTrust, Version 1.1, 16. März 2004➤ ISIS-MTT-Specification, Optional Profile, SigG-Profile, Common ISISMaiTrust Specification For PKI-Applications, T7 & TeleTrust, Version 1.1, 16. März 2004➤ RFC 2560: Online Certificate Status Protocol - OCSP
Konfigurationsmöglichkeiten	<ul style="list-style-type: none">➤ Einstellung der verwendeten Schlüssellängen und Algorithmen➤ Einstellung der Verwendung von optionalen Extensions➤ Verwendung abgesicherter Verbindungen (optional / zwingend)➤ Clientauthentifizierung notwendig (optional / zwingend)➤ Gültigkeitszeitraum der Antwort



media transfer AG
Dolivostraße 11
64293 Darmstadt

Tel +49 6151 8193-0
Fax +49 6151 8193-43
security.vertrieb@mtg.de

mtG-OCSP: PKI made in Germany

Technische Daten

Bezug der Statusinformationen	<ul style="list-style-type: none">➤ Option 1 (Unterstützung der extensions certHash und requestedCertificate): mtG-OCSP liest Zertifikate und Statusinformationen aus einer Datenbank (Oracle 10, Postgres 8, andere auf Anfrage)➤ Option 2 (Unterstützung der extension crlID): CRL Auswertung
Mandantenfähigkeit	<ul style="list-style-type: none">➤ paralleler Einsatz für verschiedene CA Instanzen➤ pro CA kann eine eigene Signaturerstellungseinheit mit einem eigenen Signaturzertifikat konfiguriert werden➤ ein Signer kann auch für mehrere CAs verwendet werden
Skalierbarkeit/Ausfallsicherheit	<ul style="list-style-type: none">➤ per Standard-Load-Balancer Lastverteilung auf verschiedene OCSP-Responder➤ OCSP-Responder sind identisch konfiguriert und beziehen ihre Informationen aus der gleichen Quelle➤ annähernd lineare Skalierung
Kryptographie	<ul style="list-style-type: none">➤ Hashverfahren: SHA-1, SHA-256, SHA-512, MD5, RIPEMD160, RIPEMD256 (weitere auf Anfrage)➤ Verschlüsselungsalgorithmen: RSA, RSA mit ISO 9696-2, EC, DSA➤ Schlüsselgrößen: bis 4096 Bit
HSM Support	<ul style="list-style-type: none">➤ LUNA SA (SafeNet, netzwerkfähig, FIPS-3 zertifiziert)➤ TCOS 2.0 oder höher (T-Systems, E4 hoch zertifiziert)➤ weitere PKCS#11-fähige Devices auf Anfrage



media transfer AG
Dolivostraße 11
64293 Darmstadt

Tel +49 6151 8193-0
Fax +49 6151 8193-43
security.vertrieb@mtg.de