

# mtG-CARA: PKI made in Germany

## Technische Daten

unterstützte Betriebssysteme	<ul style="list-style-type: none"> <li>➤ SUN Solaris 9 und 10</li> <li>➤ Linux mit 2.6er Kernel</li> <li>➤ Windows 2000/XP/2003</li> <li>➤ (weitere auf Anfrage)</li> </ul>
Anforderung Prozessorleistung	➤ mindestens 2 GHz
Anforderungen Hauptspeicher	➤ mindestens 1 GB RAM
Anforderung Plattenspeicher	➤ mindestens 20 GB (abhängig von Anzahl Zertifikate)
Anwendungsplattform	<ul style="list-style-type: none"> <li>➤ Java 5 Run Time Environment</li> <li>➤ Apache 1.3 Webserver</li> <li>➤ Tomcat 5.5/6.x Servlet Engine</li> </ul>
Datenbanken	<ul style="list-style-type: none"> <li>➤ Oracle 10 (empfohlen für ausfallsichere Umgebungen)</li> <li>➤ Postgres 8</li> </ul>
unterstützte Standards für Zertifikate	<ul style="list-style-type: none"> <li>➤ Zertifikate gemäß X.509 v3 / RFC 3280</li> <li>➤ CV Zertifikate (mit/ohne Message Recovery gemäß ISO-9796-2)</li> <li>➤ ISIS-MTT V1.1</li> </ul>
Unterstützte Schlüsselspeicher	<ul style="list-style-type: none"> <li>➤ Software Key Store</li> <li>➤ Smart Card</li> <li>➤ USB Token</li> </ul>
unterstützte Standards für Sperrlisten (CRL)	<ul style="list-style-type: none"> <li>➤ X.509 v1 und v2</li> <li>➤ indirekte CRLs</li> <li>➤ Delta CRLs</li> </ul>
Zertifikatsfeatures	<p>Zertifikatsprofile für:</p> <ul style="list-style-type: none"> <li>➤ Signatur</li> <li>➤ Authentifizierung</li> <li>➤ Verschlüsselung</li> <li>➤ Windows Logon inkl. Domain Controller</li> <li>➤ Web (SSL) Server Applikationen</li> <li>➤ IPSec Router und Gateways</li> <li>➤ Zertifikate gemäß gematik Spezifikationen (eGK, HBA, SMC)</li> <li>➤ Zertifikate für CSCA/CVCA Hierarchien (ePass, ePA)</li> <li>➤ Definition beliebiger anderer Profile möglich</li> </ul>



media transfer AG  
 Dolivostraße 11  
 64293 Darmstadt

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

# mtG-CARA: PKI made in Germany

## Technische Daten

PKI Features	<ul style="list-style-type: none"> <li>➤ CA-Hierarchien in beliebiger Tiefe</li> <li>➤ unterstützte Zeichensätze: PrintableString, IA5String, UTF-8</li> <li>➤ CA-Erzeugung für interne oder externe Signatur</li> <li>➤ synchrones Zertifikatsmanagement (logische Kopplung zusammengehöriger Zertifikate bei allen Verwaltungsvorgängen und Sperrung)</li> </ul>
Directory Features	<ul style="list-style-type: none"> <li>➤ Unterstützung aller Produkte mit LDAP v3 Interface, z.B. OpenLDAP, Netscape Directory Server oder Siemens DirX</li> <li>➤ parallele Veröffentlichung in mehrere LDAP-Verzeichnisse</li> <li>➤ Struktur des LDAP-Verzeichnisses frei definierbar</li> <li>➤ Veröffentlichung konfigurierbarer LDAP-Attribute mit dem Zertifikat</li> </ul>
Mandantenfähigkeit	<ul style="list-style-type: none"> <li>➤ mehrere virtuelle CAs (VCA) können parallel und unabhängig voneinander auf einem System verwaltet und betrieben werden</li> <li>➤ pro VCA können hierarchisch strukturierte Verwaltungsstrukturen etabliert werden (sog. Domänen)</li> </ul>
Skalierbarkeit/Ausfallsicherheit	<ul style="list-style-type: none"> <li>➤ mtG-CARA kann sowohl als Single Server System als auch als verteilte Umgebung mit Einzelkomponenten auf jeweils separater Hardware aufgesetzt werden. Jede Komponente für sich kann mehrfach vorhanden sein.</li> </ul>
Kryptographie	<ul style="list-style-type: none"> <li>➤ Hashverfahren: SHA-1, SHA-256, SHA-512, MD5, RIPEMD160, RIPEMD256 (weitere auf Anfrage)</li> <li>➤ Verschlüsselungsalgorithmen: RSA, RSA mit ISO 9696-2, EC, DSA;</li> <li>➤ Schlüsselgrößen: bis 4096 Bit</li> </ul>
HSM Support	<ul style="list-style-type: none"> <li>➤ LUNA SA (SafeNet, netzwerkfähig, FIPS-3 zertifiziert)</li> <li>➤ TCOS 2.0 oder höher (T-Systems, E4 hoch zertifiziert)</li> <li>➤ weitere PKCS#11-fähige Devices auf Anfrage</li> </ul>



media transfer AG  
Dolivostraße 11  
64293 Darmstadt

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