

mtG-CARA: PKI made in Germany

Kompatibilität / Schnittstellen / Protokolle

mtG-CARA ist kompatibel mit folgenden Schlüsselmedien:

Smart Cards	Alle Smart Cards mit Microsoft Crypto Service Provider Interface oder PKCS#11 Interface, z.B.: <ul style="list-style-type: none">➤ TCOS 2.0 oder höher (T-Systems, ITSEC E4 hoch zertifiziert)➤ HiPath Scurity CardOS V4.2 und höher (Siemens, CC EAL 4+ bzw. ITSEC E4 hoch zertifiziert)➤ Gemalto Classic TPC IS mit GemSAFE Card CSP ab Version 4➤ STARCOS SPK2.3 (Giesecke & Devrient, ITSEC E4 hoch zertifiziert)
USB Tokens	Alle Tokens mit Microsoft Crypto Service Provider Interface oder PKCS#11 Interface, z.B.: <ul style="list-style-type: none">➤ Gemalto USB eSeal Token V1 (integriert ist Gemalto Classic TPC IS)➤ CrypToken M2048 und CrypToken MX2048JCOP (Marx Data)

mtG-CARA unterstützt folgende Schnittstellen zur Kartenpersonalisierung:

Online (SOAP)	➤ Schnittstelle zu Atron / Winter AG
Offline (CSV und andere Formate)	Schnittstellen zu <ul style="list-style-type: none">➤ Giesecke & Devrient➤ PPC Card Systems➤ T-Systems Enterprise Services



Dolivostraße 11
64293 Darmstadt
Tel +49 6151 8193-0
Fax +49 6151 8193-43
security.vertrieb@mtg.de

mtG-CARA: PKI made in Germany

Kompatibilität / Schnittstellen / Protokolle

mtG-CARA ist unterstützt folgende eHealth Spezifikationen und Schnittstellen:

CAMS (Card Application Management System)	➤	PKI Schnittstelle auf Basis von CMP zwischen KV-KAMS und X.509-/CVC-CA, V 2.1, Giesecke & Devrient
Elektronische Gesundheitskarte (eGK)	➤	alle aktuellen Spezifikationen der gematik GmbH zu Zertifikaten der eGK
Heilberufsausweis (HBA)	➤	alle aktuellen Spezifikationen der gematik GmbH zu Zertifikaten des HBA
Security Module Card (SMC)	➤	alle aktuellen Spezifikationen der gematik GmbH zu Zertifikaten der SMC

mtG-CARA unterstützt folgende Technische Richtlinien zu digitalen Ausweisen:

TR-03110	➤	Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC) and Password Authenticated Connection Establishment (PACE), BSI
TR-03111	➤	Elliptic Curve Cryptography Based on ISO 15946, BSI



media transfer AG

Dolivostraße 11
64293 Darmstadt
Tel +49 6151 8193-0
Fax +49 6151 8193-43
security.vertrieb@mtg.de

www.mtg.de

mtG-CARA: PKI made in Germany

Kompatibilität / Schnittstellen / Protokolle

mtG-CARA ist kompatibel mit folgenden Authentifizierungs- und Verschlüsselungsanwendungen:

Windows Smart Card Logon	Windows Smart Card Logon wird vollständig unterstützt (Client Zertifikate und Domain Controller Zertifikat)
IPSec Devices	<p>Alle IPSec Geräte bzw. Anwendungen, die Zertifikate und Sperrlisten gemäß X.509 sowie das SCEP Protokoll oder Zertifikatsrequest per PKCS#10 unterstützen, z.B.:</p> <ul style="list-style-type: none"> ➤ CISCO Router mit IOS 12.3 und höher ➤ Juniper Router mit ScreenOS 5.4 und höher ➤ Watchguard Router mit OS 5.1.1 SP1 und höher
Web Server/SSL Server	<p>Unterstützt werden alle SSL Server, die einen standardkonformen Zertifikatsrequest im Format PKCS#10 erzeugen, z.B.:</p> <ul style="list-style-type: none"> ➤ Apache (+ MOD SSL, + Raven, + SSLeay) ➤ BEA WebLogic ➤ iPlanet Enterprise Server 4.1 ➤ Lotus Domino ➤ Microsoft Internet Information Server ➤ Netscape Enterprise/Fast Track ➤ Novell ConsoleOne ➤ Tomcat
Web Browser/SSL Client	<p>Unterstützt werden alle Browser, die einen standardkonformen Zertifikatsrequest im Format PKCS#10 oder Netscape SPKAC erzeugen, z.B.:</p> <ul style="list-style-type: none"> ➤ Microsoft IE 5.01+ ➤ Netscape Communicator 4.51+ ➤ Mozilla 1.0+ einschließlich Firefox ➤ Opera 8.52+ ➤ Apple Safari 1.0+ ➤ Red Hat Linux Konqueror
e-Mail Clients	<p>Unterstützt werden alle e-Mail Clients, die X.509-Zertifikate im Format PKCS#12 importieren oder selbst einen standardkonformen Zertifikatsrequest im Format PKCS#10 oder Netscape SPKAC erzeugen, z.B.:</p> <ul style="list-style-type: none"> ➤ Microsoft Outlook 99+ ➤ Netscape Communicator 4.51+ ➤ Mozilla 1.0+



media transfer AG

Dolivostraße 11
64293 Darmstadt
Tel +49 6151 8193-0
Fax +49 6151 8193-43
security.vertrieb@mtg.de

www.mtg.de

mtG-CARA: PKI made in Germany

Kompatibilität / Schnittstellen / Protokolle

mtG-CARA unterstützt folgende Schnittstellen und Protokolle:

PKCS#10/7	Zertifikatsrequest und -response gemäß: <ul style="list-style-type: none"> ➤ PKCS #10: Certification Request Syntax Standard, RSA Laboratories ➤ PKCS #7: Cryptographic Message Syntax Standard, RSA Laboratories
PKCS#11	Zugriff auf Schlüsselspeicher gemäß: <ul style="list-style-type: none"> ➤ PKCS #11: Cryptographic Token Interface Standard, RSA Laboratories
PKCS#12	Auslieferung von Schlüsselpaar und Zertifikat gemäß: <ul style="list-style-type: none"> ➤ PKCS #12: : Personal Information Exchange Syntax Standard, RSA Laboratories
Microsoft CAPI (CSP)	Zugriff auf Schlüsselspeicher gemäß: <ul style="list-style-type: none"> ➤ Cryptographic Service Provider (CSP) stellt kryptografische Funktionen gem. Microsofts Cryptographic Application Programming Interface (CAPI) zur Verfügung
SCEP	Sicheres Protokoll zur Ausgabe von Zertifikaten an Router und Gateways: <ul style="list-style-type: none"> ➤ Cisco Systems' Simple Certificate Enrollment Protocol, IETF Internet-Draft, 2008
CMP	Sicheres Protokoll für Ausgabe und Management von Zertifikaten: <ul style="list-style-type: none"> ➤ RFC 4210 : Internet X.509 Public Key Infrastructure Certificate Management Protocol
SMTP	Protokoll für Mail Transfer: <ul style="list-style-type: none"> ➤ RFC 2821 : Simple Mail Transfer Protocol
SOAP	Protokoll zur Client-/Serverkommunikation: <ul style="list-style-type: none"> ➤ SOAP Version 1.2 , Series of W3C Recommendations
TSL/TCL	Signierte Liste zur Verteilung von Zertifikaten und Sperrlisten : <ul style="list-style-type: none"> ➤ Trust-service Status List nach ETSI TS 102 231 V2.1.1 (2006-03)



Dolivostraße 11
64293 Darmstadt
Tel +49 6151 8193-0
Fax +49 6151 8193-43
security.vertrieb@mtg.de