

# Technische Spezifikationen

icoya EDI Signature Server Appliance

## Plattformen

Linux (Red Hat Enterprise Linux  
32/64-Bit, glibc 2.3)  
MS-Windows 2000 Server  
MS-Windows 2003 Server

## Smart Cards

TCOS 2.0 Signaturkarten  
nach SigG  
SECCOS (nur Windows)  
MICARDO 2.1 (nur Windows)  
CardOS 4.3  
Starcos 3.0

## Kartenleser

CCID kompatibler Reader  
USB und serielle Kartenleser  
(B1 kompatibel)  
z.B. SCM Microsystems SPR132,  
SPR332, SPR532

## Signaturformate

Adobe PDF (1024/1536/2048 bit)  
XML-Signature, XMLDSIG  
PKCS#7  
RAW

## Funktionen

- Signaturerstellung
- Signaturprüfung
- Erstellung von Zeitstempeln (auch in Verbindung mit Signaturprüfung und Erstellung)
- Zertifikatsprüfung OCSP
- Qualifizierte Signatur nach deutschem Signaturgesetz
- Selbstüberwachende Systemsoftware (Unveränderbarkeit gesichert durch Code Signatur)
- Abhörsichere PIN-Eingabe ohne Tastatur über Web-Browser (plattformunabhängig)
- Workflow-gesteuerte Erstellung von RSA/DSA Zertifikaten für fortgeschrittene Signatur
- CA-Verwaltung
- Integrierter Verifikationsserver für die automatische Erstellung von Prüfprotokollen
- Skalierbarkeit durch parallelen Chipkartenbetrieb mit bis zu 1440 Signaturkarten für die qualifizierte digitale Signatur
- Mehrere Mandanten (Mandantenfähigkeit)
- Signatur von EDI Daten: XCBL, EANCOM, EDIFACT, ebXML, IDoc und weitere
- Integrierte Firewall
- Signaturprüfung und Zertifikatsprüfung mit frei verfügbarer Prüfsoftware icoya Scan Processor

## Kryptographische Verfahren Smartcards

SHA1 mit RSA (1024 bit) Smartcards , z.B. D-TRUST, SignTrust, Telesec, Verisign

SHA1 mit RSA (1536 bit) Smartcards , z.B. S-TRUST, Verisign

SHA1 mit RSA (512 bit) Smartcards , z.B. Schlumberger/Axalto Cryptoflex 32k

SHA1 mit RSA (768 bit) Smartcards , z.B. Schlumberger/Axalto Cryptoflex 32k

SHA1 mit RSA (1024 bit) Smartcards , z.B. Schlumberger/Axalto Cryptoflex 32k

SHA1 mit RSA (2048 bit) Smartcards , z.B. Schlumberger/Axalto Cryptoflex 32k

## Kryptographische Verfahren, fortgeschrittene digitale Signatur und Verschlüsselung

SHA1/MD5/MD2/RIPE-MD160/SHA-224/SHA-256/SHA-384/SHA-512 mit RSA (1024 bit)

SHA1/MD5/MD2/RIPE-MD160/SHA-224/SHA-256/SHA-384/SHA-512 mit RSA (2048 bit)

SHA1/MD5/MD2/RIPE-MD160/SHA-224/SHA-256/SHA-384/SHA-512 mit RSA (4096 bit)

SHA1/MD5/MD2/RIPE-MD160/SHA-224/SHA-256/SHA-384/SHA-512 mit RSA (8096 bit)

SHA1/SHA-224/SHA-256/SHA-384/SHA-512 mit DSA (1024 bit)

SHA1/SHA-224/SHA-256/SHA-384/SHA-512 mit DSA (2048 bit)

SHA1/SHA-224/SHA-256/SHA-384/SHA-512 mit DSA (4096 bit)

SHA1/SHA-224/SHA-256/SHA-384/SHA-512 mit DSA (8096 bit)

## Option: Hochsichere ECC-Signatur und Verschlüsselung nach Vorgabe US-MIL und NSA Standards

SHA1/MD5/MD2/RIPE-MD160/SHA-224/SHA-256/SHA-384/SHA-512 mit ECC (307 bit)

## Schnittstellen

Netzwerkschnittstelle (HTTPS mit Zertifikat, SSH mit Zertifikat)

Dateischnittstelle mit Prioritätsstufen (Windows-Share, SMB, NFS)

LDAP Zugriffskontrolle

OCSP

SSH2

S/MIME, SMTP / SSMTP (Secure Simple Mail Transmit Protocol) (Optional)

XML-RPC

SOAP, Web Services

DataMatrix ECC200 2D-Barcode

**Kontakt:**  
struktur AG

Kronenstr. 22A  
70173 Stuttgart / Germany

T. +49-711-89 66 56 0  
F. +49-711-89 66 56 10

E-Mail: [info@struktur.de](mailto:info@struktur.de)  
Web: [www.icoya.de](http://www.icoya.de)