R&S®CryptoServer

Höchste Sicherheit für vertrauliche Daten und kryptografische Schlüssel

ROHDE&SCHWARZ

Sichere Kommunikation

Datenblatt | 01.01

R&S®CryptoServer
Auf einen Blick

R&S®CryptoServer wird als Hardware-Sicherheitsmodul (HSM) für die Absicherung von Transaktionen und Daten eingesetzt. R&S®CryptoServer entspricht höchsten internationalen Sicherheitsstandards, verfügt über Zertifizierungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und des US National Institute of Standards and Technology (NIST). Über Schnittstellen (APIs) wird R&S®CryptoServer in vorhandene IT-Systeme wie Public-Key-Infrastrukturen (PKI) von Ausweis- und Inspektionssystemen integriert und dort für Verschlüsselung und Signatur vertraulicher Daten genutzt.

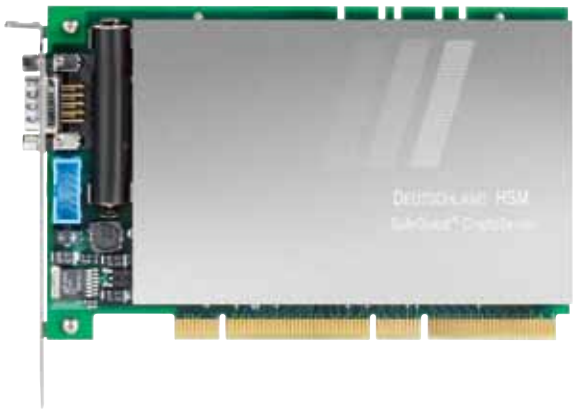
R&S®CryptoServer ist durch sein optimiertes Durchsatzverhalten und den geringen Administrationsaufwand besonders für den zentralen Einsatz, z.B. zur Initialisierung und Validierung von Zertifikaten einer PKI, zur Verschlüsselung von Datenbanken oder zur sicheren Authentisierung geeignet. Durch den hohen Sicherheitsstandard von R&S®CryptoServer ist das Hardware-Sicherheitsmodul (HSM) sowohl für hoheitliche Anwendungen, z.B. bei Polizei, Militär und Verwaltung, als auch für kommerzielle Anwendungen mit höchsten Sicherheitsanforderungen, z.B. bei Banken, einsetzbar.

Dieser hohe Sicherheitsstandard wird durch die Kombination von physischen Schutzmaßnahmen mit Software-Sicherheitstechniken ermöglicht. Selbst bei einem massiven mechanischen Angriff auf ein entwendetes HSM werden die gespeicherten Informationen vor Offenlegung bewahrt, da R&S®CryptoServer mit ausgefeilten Mechanismen zur Angriffserkennung sowie begleitenden Schutzmaßnahmen versehen ist. So wird im Falle eines unautorisierten Zugriffversuchs das gespeicherte Schlüssel- und Datenmaterial binnen Millisekunden gelöscht.

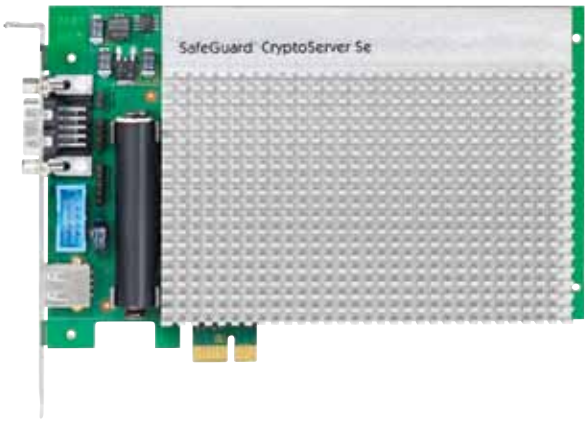
Hauptmerkmale

- Hardware-Sicherheitsmodul als Einsteckkarte (PCI/PCIe) für Server-Betrieb und als LAN-Appliance (Industrie-PC) für Betrieb als Netzwerk-Server
- Hochperformante Bereitstellung zeitgemäßer kryptografischer Methoden und Algorithmen (z.B. AES, Elliptische Kurven) für verschiedene Schlüssellängen
- Physische Sicherungstechniken für maximale Sicherheit (z.B. Manipulationsschutz, Speicherschutz, Notlöschen, physikalischer Zufall)
- Zugelassen durch BSI, ZKA und NIST
- Hochsicherer Datenspeicher

R&S®CryptoServer/Deutschland-HSM (PCI-Karte).



R&S®CryptoServer/SecurityServer Se (PCIe-Karte).



R&S®CryptoServer

Wesentliche Merkmale und Vorteile

Leistungsstark, flexibel und hochverfügbar

- Hoher kryptografischer Durchsatz bei geringem Administrationsaufwand
- Flexible Integration in sicherheitskritische Anwendungen durch Standard-Schnittstellen
- Redundanter Einsatz für Ausfallsicherheit und Lastverteilung

▷ Seite 4

Professionelles Schlüssel- und Rollenmanagement

- Kryptografisches Mehr-Augen-Prinzip nach Shamir
- Sicheres Schlüssel-Backup
- Fernadministration kryptografischer Parameter mittels Secure Messaging

▷ Seite 5

Bestätigte Sicherheit durch internationale und deutsche Zertifizierungen

- Internationale Zertifizierungen (NIST, BSI, Common Criteria)
- Deutsche Zertifizierungen (BSI, SigG, ZKA)

▷ Seite 6

Kommerzielle und hoheitliche Einsatzbereiche

- Authentisierungsserver (Betriebsausweis, hoheitliche Dokumente, ePASS)
- Public-Key-Infrastrukturen
- Dokumentenmanagement und Archivierungslösungen
- Datenbank-Verschlüsselung
- Bargeldloser Zahlungsverkehr (ePayment)
- Elektronische Rechnungsstellung (eBilling)
- Zeitstempelanwendungen

▷ Seite 7

R&S®CryptoServer/SecurityServer CS (PCI-Karte).

Leistungsstark, flexibel und hochverfügbar

Hoher kryptografischer Durchsatz bei geringem Administrationsaufwand

Ob Schlüsselerzeugung, elektronische Signatur oder Datenverschlüsselung – R&S®CryptoServer vollzieht kryptografische Operationen in kürzester Zeit. Dazu wird R&S®CryptoServer entweder als PCI-/PCIe-Einsteckkarte oder als fertige 19"-LAN-Appliance verbaut. Die zu verschlüsselnden bzw. zu signierenden Daten werden von der Anwendung auf gesichertem Übertragungsweg an das HSM übermittelt, kryptografisch verarbeitet und zurückgesendet.

Der Aufwand für die Inbetriebnahme beschränkt sich auf die Basis-Administration (Benutzer, Berechtigungen, etc.) und das Einrichten der Schnittstellen, die von der Anwendung zur Kommunikation mit R&S®CryptoServer genutzt werden sollen.

Der geringe Administrationsaufwand während der Laufzeit ermöglicht einen raschen „Return-on-Investment".

Flexible Integration in sicherheitskritische Anwendungen durch Standard-Schnittstellen

Zur Integration in die abzusichernden Prozesse kann R&S®CryptoServer je nach Produktvariante flexibel über folgende Standard-Schnittstellen adressiert werden:

- PKCS#11
- Microsoft CryptoAPI und Cryptography Next Generation (CNG)
- Java Cryptography Extension (JCE)
- OpenSSL
- Cryptographic eXtended services Interface (CXI)

Die gewünschten Schnittstellen werden auf dem Host, auf dem die abzusichernde Anwendung läuft, eingerichtet und einem HSM zugewiesen. Da einige Anwendungen PKCS#11-Daten im Klarbetrieb übertragen, wurde der PKCS#11-Wrapper von R&S®CryptoServer um eine Übertragungsverschlüsselung erweitert.

R&S®CryptoServer/Deutschland-HSM und seine Untervarianten unterstützen keine der oben genannten Schnittstellen. Aufgrund der speziellen Sicherheitsanforderungen hoheitlicher eID- und PKI-Anwendungen wurde R&S®CryptoServer/Deutschland-HSM mit der speziellen, auf Java basierenden Schnittstelle „Java-eID" ausgestattet.

Redundanter Einsatz für Ausfallsicherheit und Lastverteilung

Bei Hochverfügbarkeitsanwendungen sollte R&S®CryptoServer redundant eingesetzt werden. Der redundante Einsatz ermöglicht schnellere Antwortzeiten durch Lastverteilung (z.B. wenn mit vielen zu signierenden Statusanfragen zur Zertifikatsprüfung zu rechnen ist) und Ausfallsicherheit durch Hot-Standby-/Cold-Standby-Szenarien.

In beiden Fällen wird der redundante Betrieb abhängig von der eingesetzten Standard-Schnittstelle implementiert: die Microsoft-Schnittstellen C-API und CNG sowie die JCE- und CXI-Schnittstellen unterstützen standardmäßig den redundanten Betrieb. Dazu wird an der Schnittstelle der Berechtigungsschlüssel von R&S®CryptoServer hinterlegt, der den Zugang zu jedem R&S®CryptoServer innerhalb des vorgesehenen Lastennetzes ermöglicht. Bei PKCS#11 und Java-eID hingegen kann die Redundanz individuell auf Anwendungsebene implementiert werden.

R&S®CryptoServer wird in verschiedenen Versionen angeboten, als Einsteckkarte (PCI-/PCIe-HSM) und als komplette Server-Appliance im Rackformat (LAN-HSM).

Professionelles Schlüssel- und Rollenmanagement

Kryptografisches Mehr-Augen-Prinzip nach Shamir

Besonders bei Behörden und behördennahen Institutionen überwachen dedizierte Sicherheitsverantwortliche den korrekten Umgang mit sicherheitskritischen Funktionen wie dem Schlüsselmanagement. Daher wurde R&S®CryptoServer mit dem kryptografischen Vier- bzw. Sechs-Augen-Prinzip nach Shamir ausgestattet. Dieses stellt sicher, dass bestimmte Operationen nur dann ausgeführt werden können, wenn sich mindestens zwei bzw. drei Sicherheitsverantwortliche mit ihren persönlichen Schüsselteilen gegenüber R&S®CryptoServer authentisiert haben. Die persönlichen Schlüsselteile werden zu dem rollenspezifischen Schlüssel zusammengesetzt, der für den kryptografischen Zugang zu den Funktionen erforderlich ist.

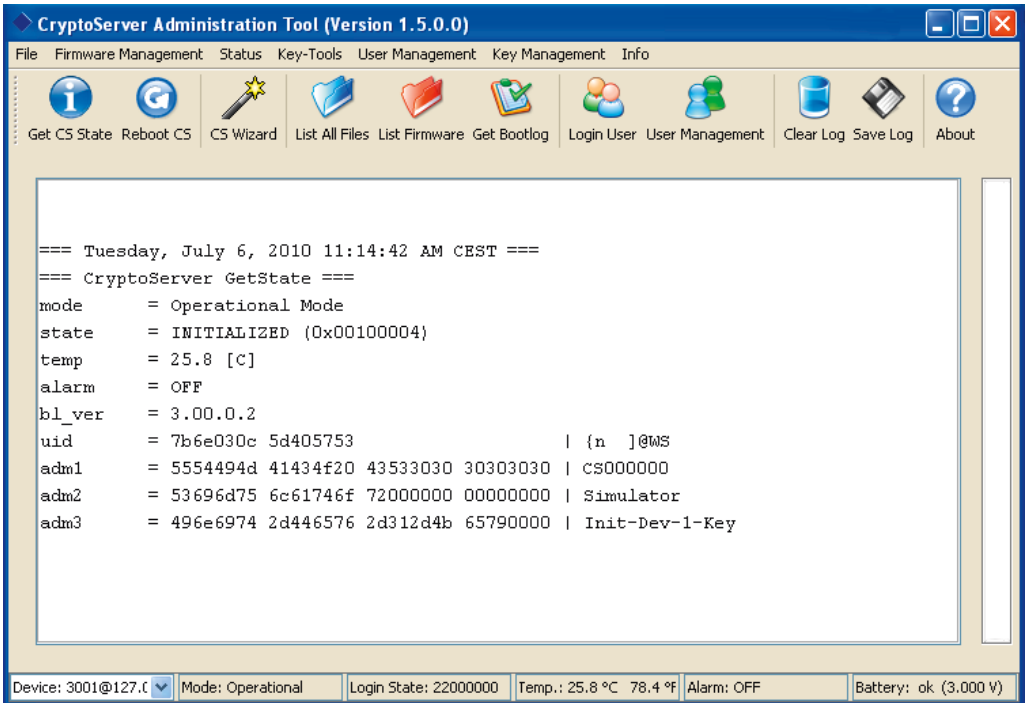
Sicheres Schlüssel-Backup

Um Schlüssel zu sichern, können diese im verschlüsselten Zustand von R&S®CryptoServer exportiert werden. Dies erfordert die Anwesenheit mehrerer Sicherheitsverantwortlicher, da die exportierten Schlüssel mit einem Transportschlüssel (KEK) nach dem kryptografischen Mehr-Augen-Prinzip gesichert werden. Die gesicherten Schlüssel werden anschließend entweder in einer sicheren Umgebung deponiert oder in ein Backup-Gerät importiert.

Fernadministration kryptografischer Parameter mittels Secure Messaging

Für die Administration sicherheitsrelevanter und kryptografischer Parameter wurde die Administrations-Software des R&S®CryptoServer mit einem speziell geschützten Management-Zugang ausgestattet. Dieser Zugang basiert auf Secure Messaging, einer Technik, bei der ein verschlüsselter Kanal zu R&S®CryptoServer aufgebaut wird. Administratoren und Sicherheitsverantwortliche erlangen über diesen Kanal den Fernzugriff auf R&S®CryptoServer.

Zur zusätzlichen Absicherung kann R&S®CryptoServer so konfiguriert werden, dass der Secure-Messaging-Kanal nur unter Verwendung von persönlichen Authentisierungsinformationen aufgebaut werden kann. Diese persönlichen Informationen sind zum Beispiel auf der Smartcard gespeichert, so dass Administratoren und Sicherheitsverantwortliche immer ein angeschlossenes Kartenlesegerät zur Authentisierung für die Fernadministration benötigen.



Das mitgelieferte R&S®CryptoServer Administration Tool (CAT) ermöglicht das Sicherheitsmanagement über eine komfortable Bedienoberfläche.

Bestätigte Sicherheit durch internationale und deutsche Zertifizierungen

Internationale Zertifizierungen (NIST, BSI, Common Criteria)[1)]

R&S®CryptoServer ist mit modernen Erkennungs- und Schutzmaßnahmen gegen physische Angriffe ausgestattet. Damit erfüllt R&S®CryptoServer den US-amerikanischen Standard FIPS PUB 140-2 Level 3 mit dem Zusatz Level 4 für „Physical Security“. Dieser Zusatz ist in den implementierten Schutzmaßnahmen gegen diverse Seitenkanalangriffe (wie Abstrahlungs- und Energieverbrauchsmessungen), dem frühzeitigen Erkennen physischer Angriffe sowie dem sofortigen Einleiten der Notlöschmaßnahmen begründet.

Neben den kryptografischen Algorithmen ist die Güte des Zufalls für die Schlüsselgenerierung ein wesentliches Kriterium für hochsichere Kryptogeräte. Das BSI gibt mit den AIS-Dokumenten international anerkannte Kriterien für Zufallszahlen vor. R&S®CryptoServer erzeugt Zufallszahlen physisch gemäß BSI AIS 31 Klasse P2, deterministisch nach BSI AIS 20 Klasse K4 und entspricht damit jeweils der höchsten Klasse dieser Kriterien.

R&S®CryptoServer wird derzeit für eine Zertifizierung nach Common Criteria EAL4+ vorbereitet.

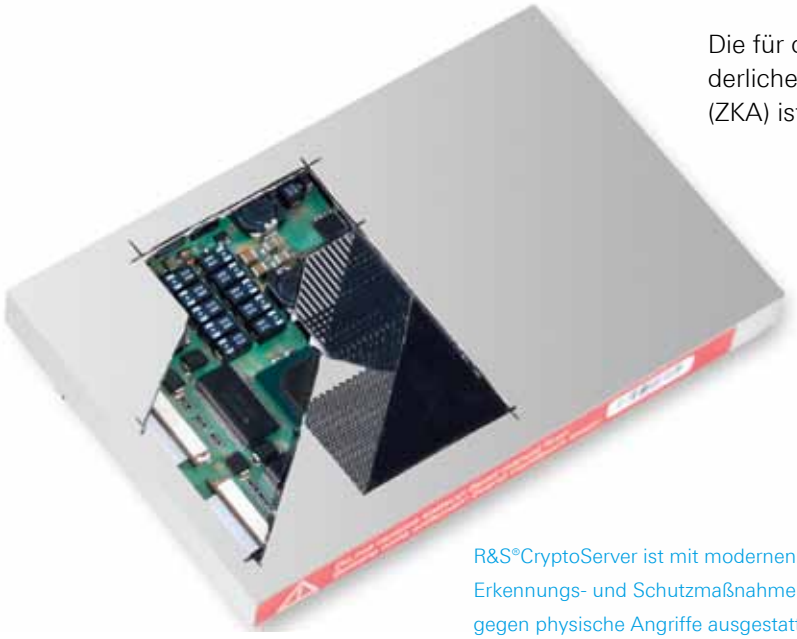
Deutsche Zertifizierungen (BSI, SigG, ZKA)[1)]

R&S®CryptoServer/Deutschland-HSM erfüllt die Sicherheitsanforderungen des BSI für die Verarbeitung von vertraulichen Informationen bis VS-Vertraulich und ist daher die erste Wahl für die hoheitlichen Projekte der Bundesrepublik Deutschland.

R&S®CryptoServer/QES-HSM ist für die qualifizierte elektronische Signatur bzw. Massensignatur nach dem deutschem Signaturgesetz (SigG) vorgesehen. R&S®CryptoServer/QES-HSM wird für eine Bestätigung nach SigG vorbereitet.

Die für den Einsatz bei Banken und Kreditinstituten erforderliche Zulassung durch den zentralen Kreditausschuss (ZKA) ist vorhanden.

[1)] Zertifizierungen abhängig von der Variante des R&S®CryptoServer.



R&S®CryptoServer ist mit modernen Erkennungs- und Schutzmaßnahmen gegen physische Angriffe ausgestattet.

Kommerzielle und hoheitliche Einsatzbereiche

R&S®CryptoServer ist ein Hardware-Sicherheitsmodul für die Ausführung kryptografischer Funktionen wie Verschlüsselung, Signatur und Hash. Es stellt Vertraulichkeit, Integrität und Authentizität von Daten in IT-Systemen sicher. Dazu sind geheime Schlüssel erforderlich, die unter anderem der Identifikation von Personen, Objekten und Prozessen dienen und naturgemäß besonders schützenswert sind. Diese Schlüssel werden innerhalb R&S®CryptoServer erzeugt sowie sicher und dauerhaft gespeichert.

R&S®CryptoServer ist flexibel nutzbar und bietet in einer Vielzahl von Einsatzbereichen ein Maximum an Sicherheit:

- Elektronische Identitäten im kommerziellen und hoheitlichen Umfeld (eID, PKI)
- Dokumentenmanagement/Archivierung, Datenbank-Verschlüsselung
- Bargeldloser Zahlungsverkehr (ePayment)
- Elektronische Rechnungsstellung (eBilling)
- Elektronische Vergabesysteme
- Zeitstempelanwendungen

Die vertrauenswürdige Bereitstellung elektronischer Identitäten innerhalb von eID-Systemen ist eine Schwerpunkt-Anwendung von R&S®CryptoServer. Sowohl für den deutschen Reisepass mit Biometrie-Funktion als auch für den neuen elektronischen Personalausweis der Bundesrepublik Deutschland sichert R&S®CryptoServer:

- die Produktion und Personalisierung der hoheitlichen Dokumente
- die vertrauliche Datenpflege von Sperrlisten
- die Bereitstellung hoheitlicher und kommerzieller eID-Server
- die Berechtigungsprüfung im Kontrollsegment

Die Kontrolle des elektronischen Reisepasses unterliegt strengen Sicherheitsrichtlinien. Nur offiziell berechtigte Personen dürfen auf biometrische Daten, die in den Dokumenten gespeichert sind, zugreifen. R&S®CryptoServer ist z.B. für den Einsatz in einer durch die International Civil Aviation Organization (ICAO) definierten ICAO-PKI als Hardware-Sicherheitsmodul vorgesehen. Weitere Informationen zum Betrieb von R&S®CryptoServer als Hardware-Sicherheitsmodul eines nationalen Kontrollsystems sind in der Technischen Richtlinie TR-03129 „PKIs for Machine Readable Travel Documents“ des BSI enthalten.

Im deutschen Reisepass werden seit 2007 biometrische Daten gespeichert.

Neuer elektronischer Personalausweis mit ePass-, eID- und eSign-Funktion (Foto: © Bundesministerium des Inneren).

Glossar

Begriff	Beschreibung
AES	Advanced Encryption Standard
AIS	Anwendungshinweise und Interpretationen zum Schema
API	Application Programming Interface, Programmierschnittstelle
BSI	Bundesamt für Sicherheit in der Informationstechnik
CA	Certificate Authority einer PKI
CAT	R&S®CryptoServer Administration Tool
CC	Common Criteria for Information Technology Security Evaluation
CNG	(Microsoft) Cryptographic Next Generation (Interface)
EAL	Evaluation Assurance Level nach Common Criteria
ECDH	Eliptic Curve Diffie-Hellman
ECDSA	Eliptic Curve Digital Signature Algorithm
eID	elektronische Identitäten
FIPS	(US) Federal Information Processing Standard
HE	Höheneinheit
HSM	Hardware-Sicherheitsmodul
ICAO	International Civil Aviation Organization
JCE	Java Cryptographic Engine
KEK	Key Encryption Key
LAN	Local Area Network
MD5	Message Digest Algorithm 5
mRTD	Machine-Readable Travel Documents
NIST	National Institute of Standards and Technology (USA)
PCI	Peripheral Component Interconnect
PCIe	Peripheral Component Interconnect Express
PKCS#11	Public Key Cryptography Standard #11
PKI	Public Key Infrastructure
PP	Protection Profile
QES	Qualifizierte elektronische Signatur
RIPEMD	RACE Integrity Primitives Evaluation Message Digest
RSA	Rivest Shamir Adleman
SHA	Secure Hash Algorithm
SSCD	Secure Signature Creation Device (deutsch: SSEE)
SSEE	Sichere-Signatur-Erstellungseinheit
SigG	Gesetz der Bundesrepublik Deutschland über Rahmenbedingungen für elektronische Signaturen
VA	Validierungsdienst für Zertifikate (Validation Authority)
VS	Verschlusssache
VS-V	VS-Vertraulich
ZKA	Zentraler Kreditausschuss der Bundesrepublik Deutschland

Technische Daten

Technische Daten	Kommerzielle Anwendungen		Hoheitliche Anwendungen	Qualifizierte elektronische Signatur nach SigG
Variante des R&S®CryptoServer [1]	SecurityServer Se	SecurityServer CS	Deutschland-HSM	QES-HSM
Leistung/Durchsatz				
Max. Anzahl RSA-Signaturen pro Sekunde (2048 bit/4094 bit)	1250/250	80/10	80/10	80/10
Max. Anzahl EC-Signaturen pro Sekunde (224 bit/256 bit)	1300/1100	1200/1000	1200/1000	–
Hardware				
Verfügbarer Formfaktor				
PCI-Express-Einsteckkarte (167,65 mm lang, 111,15 mm hoch)	●	–	–	–
PCI-Einsteckkarte (167 mm lang, 107 mm hoch)	–	●	●	–
LAN-Appliance (Rackformat, 2 HE) (446 mm breit, 88 mm hoch, 510 mm tief)	●	●	●	●
Betriebstemperaturbereich (Einsteckkarte)	+10 °C bis +45 °C	+10 °C bis +35 °C		
Lagertemperaturbereich	–14 °C bis +66 °C			
Kryptografische Funktionen				
Symmetrische Algorithmen	AES, DES, 3DES		AES	
Asymmetrische Algorithmen	ECDSA, ECDH, RSA, DH, DSA		ECDSA, RSA	RSA
Hash-Algorithmen	SHA-1, SHA-2-Familie, RIPEMD-160, MD5			
Zufallserzeugung	echte Zufallszahlen nach AIS 31 Klasse P2, Pseudo-Zufallszahlen nach FIPS 186-2 und AIS 20 Klasse K4		echte Zufallszahlen nach AIS 31 Klasse P2, Pseudo-Zufallszahlen nach FIPS 186-2 und AIS 20 Klasse K4, zusätzlich: BSI-Qualifikation	
Zulassung/Konformität				
ZKA	–	●	–	–
BSI	–	–	bis VS-Vertraulich [2]	–
Signaturgesetz (SigG)	–	–	–	● [3]
Common Criteria	–	–	EAL4+ nach PP CM Enhanced [2][3]	EAL4+ nach PP SSCD [3]
FIPS 140-2	Level 3 [3]	Level 3 + Level 4 „Physical Security“	–	–
Funktionale Merkmale				
R&S®CryptoServer Administration Tool (CAT)	●	●	●	●
Notlösch-Schalter	●	●	●	●
Aktives Löschen/Überschreiben der Speicherinhalte beim physischen Angriff	–	●	●	●
Schlüssel-Backup	●	●	●	–
Mandantenfähigkeit	●	●	●	–
PKCS#11-Wrapper	●	●	–	–

[1] Rohde&Schwarz SIT GmbH ist exklusiver Vertriebspartner von Utimaco Safeware AG für hoheitliche eID-Projekte in Deutschland. R&S®CryptoServer und seine Varianten entsprechen den gleichnamigen SafeGuard™ CryptoServer-Produkten.

[2] Zulassungen sind abhängig von der gewählten R&S®CryptoServer/Deutschland-HSM-Untervariante (siehe Bestellangaben).

[3] Zulassung/Bestätigung in Arbeit.

Bestellangaben

Bezeichnung	Typ	Bestellnummer
R&S®CryptoServer/SecurityServer Se Zertifizierung nach FIPS 140-2 Level 3 in Arbeit, einsetzbar für Anwendungen und Marktsegmente die mittlere bis hohe physische Sicherheit erfordern (wie große Organisationen und Unternehmen) Die Modelle der Se-Serie basieren auf PCI-Express-Karten.		
Hardware-Sicherheitsmodul, Modell: PCIe-Karte, Performance Level: 100 RSA-Signaturen (1024 bit) pro Sekunde	SecurityServer Se10 PCIe	5414.1280.02
Hardware-Sicherheitsmodul, Modell: PCIe-Karte, Performance Level: 500 RSA-Signaturen (1024 bit) pro Sekunde	SecurityServer Se50 PCIe	5414.1280.03
Hardware-Sicherheitsmodul, Modell: PCIe-Karte, Performance Level: 4000 RSA-Signaturen(1024 bit) pro Sekunde	SecurityServer Se400 PCIe	5414.1280.04
Hardware-Sicherheitsmodul, Modell: PCIe-Karte, Performance Level: 10000 RSA-Signaturen (1024 bit) pro Sekunde	SecurityServer Se1000 PCIe	5414.1280.05
Hardware-Sicherheitsmodul, Modell LAN-Appliance, Performance Level: 100 RSA-Signaturen (1024 bit) pro Sekunde, enthält 1 Pinpad und 3 Smartcards	SecurityServer Se10 LAN	5414.1280.06
Hardware-Sicherheitsmodul, Modell LAN-Appliance, Performance Level: 500 RSA-Signaturen (1024 bit) pro Sekunde, enthält 1 Pinpad und 3 Smartcards	SecurityServer Se50 LAN	5414.1280.07
Hardware-Sicherheitsmodul, Modell LAN-Appliance, Performance Level: 4000 RSA-Signaturen (1024 bit) pro Sekunde, enthält 1 Pinpad und 3 Smartcards	SecurityServer Se400 LAN	5414.1280.08
Hardware-Sicherheitsmodul, Modell LAN-Appliance, Performance Level: 10000 RSA-Signaturen (1024 bit) pro Sekunde, enthält 1 Pinpad und 3 Smartcards	SecurityServer Se1000 LAN	5414.1280.09
R&S®CryptoServer/SecurityServer CS Zertifiziert nach FIPS 140-2 Level 3 (mit Level 4 für "Physical Security"), bestätigt durch ZKA (Zentraler Kreditauschuss), einsetzbar für Anwendungen und Marktsegmente die hohe physische Sicherheit erfordern (wie Banken, Finanzen und Behörden) Die Modelle der CS-Serie basieren auf PCI-Karten.		
Hardware-Sicherheitsmodul, Modell: PCI-Karte, Performance Level: 100 RSA-Signaturen (1024 bit) pro Sekunde	SecurityServer CS10 PCI	5414.1297.02
Hardware-Sicherheitsmodul, Modell: PCI-Karte, Performance Level: 500 RSA-Signaturen (1024 bit) pro Sekunde	SecurityServer CS50 PCI	5414.1297.03
Hardware-Sicherheitsmodul, Modell LAN-Appliance, Performance Level: 100 RSA-Signaturen (1024 bit) pro Sekunde, enthält 1 Pinpad und 3 Smartcards	SecurityServer CS10 LAN	5414.1297.06
Hardware-Sicherheitsmodul, Modell LAN-Appliance, Performance Level: 500 RSA-Signaturen (1024 bit) pro Sekunde, enthält 1 Pinpad und 3 Smartcards	SecurityServer CS50 LAN	5414.1297.07

Frontansicht des R&S®CryptoServer (LAN-Appliance).

Rückansicht des R&S®CryptoServer (LAN-Appliance).

Bezeichnung	Typ	Bestellnummer
R&S®CryptoServer/Deutschland-HSM BSI (VS-V) zugelassen, einsetzbar zur Produktion hoheitlicher eID-Dokumente (z.B. elektronischer Reisepass) Alle Modelle basieren auf PCI-Karten.		
Hardware-Sicherheitsmodul, Modell: PCI-Karte, Performance Level: 125 ECC-Signaturen (256 bit) pro Sekunde	Deutschland-HSM/1 CS10 PCI	5414.1300.02
Hardware-Sicherheitsmodul, Modell: PCI-Karte, Performance Level: 1000 ECC-Signaturen (256 bit) pro Sekunde	Deutschland-HSM/1 CS50 PCI	5414.1300.03
Hardware-Sicherheitsmodul, Modell LAN-Appliance, Performance Level: 125 ECC-Signaturen (256 bit) pro Sekunde, enthält 1 Pinpad und 3 Smartcards	Deutschland-HSM/1 CS10 LAN	5414.1300.06
Hardware-Sicherheitsmodul, Modell LAN-Appliance, Performance Level: 780 ECC-Signaturen (256 bit) pro Sekunde, enthält 1 Pinpad und 3 Smartcards	Deutschland-HSM/1 CS50 LAN	5414.1300.07
R&S®CryptoServer/Deutschland-HSM [1] CC evaluiert und BSI (VS-V) zugelassen, einsetzbar z.B. für Sperrdienste hoheitlicher eID-Anwendungen Alle Modelle basieren auf PCI-Karten.		
Hardware-Sicherheitsmodul, Modell: PCI-Karte, Performance Level: 125 ECC-Signaturen (256 bit) pro Sekunde	Deutschland-HSM/2 CS10 PCI	5414.1300.12
Hardware-Sicherheitsmodul, Modell: PCI-Karte, Performance Level: 1000 ECC-Signaturen (256 bit) pro Sekunde	Deutschland-HSM/2 CS50 PCI	5414.1300.13
Hardware-Sicherheitsmodul, Modell LAN-Appliance, Performance Level: 125 ECC-Signaturen (256 bit) pro Sekunde, enthält 1 Pinpad und 3 Smartcards	Deutschland-HSM/2 CS10 LAN	5414.1300.16
Hardware-Sicherheitsmodul, Modell LAN-Appliance, Performance Level: 780 ECC-Signaturen (256 bit) pro Sekunde, enthält 1 Pinpad und 3 Smartcards	Deutschland-HSM/2 CS50 LAN	5414.1300.17
R&S®CryptoServer/Deutschland-HSM [1] CC evaluiert und EAL4+ zertifiziert, einsetzbar für eID-Anwendungen, eVergabe-Systeme und Kontrollsysteme Alle Modelle basieren auf PCI-Karten.		
Hardware-Sicherheitsmodul, Modell: PCI-Karte, Performance Level: 125 ECC-Signaturen (256 bit) pro Sekunde	Deutschland-HSM/3 CS10 PCI	5414.1300.22
Hardware-Sicherheitsmodul, Modell: PCI-Karte, Performance Level: 1000 ECC-Signaturen (256 bit) pro Sekunde	Deutschland-HSM/3 CS50 PCI	5414.1300.23
Hardware-Sicherheitsmodul, Modell LAN-Appliance, Performance Level: 125 ECC-Signaturen (256 bit) pro Sekunde, enthält 1 Pinpad und 3 Smartcards	Deutschland-HSM/3 CS10 LAN	5414.1300.26
Hardware-Sicherheitsmodul, Modell LAN-Appliance, Performance Level: 780 ECC-Signaturen (256 bit) pro Sekunde, enthält 1 Pinpad und 3 Smartcards	Deutschland-HSM/3 CS50 LAN	5414.1300.27
R&S®CryptoServer/QES-HSM [1] [2] CC EAL4+ zertifiziert als Sichere Signaturerstellungseinheit (SSEE) und SigG bestätigt (Gesetz über Rahmenbedingungen für elektronische Signaturen). einsetzbar für zentrale Massensignatur-Anwendungen, basiert auf PCI-Karten		
Hardware-Sicherheitsmodul, Modell LAN-Appliance, Performance Level: 80 RSA-Signaturen (2048 bit) pro Sekunde, enthält 1 Pinpad und 3 Smartcards	QES-HSM CS50 LAN	5414.1316.07
R&S®CryptoServer/Zubehör		
Pinpad	R&S®CryptoServer Pinpad	5414.1322.02
Smartcard	R&S®CryptoServer Smartcard	5414.1322.03
Große externe Stützbatterie für R&S®CryptoServer PCI und PCIe	R&S®CryptoServer Stützbatterie PCI/PCIe	5414.1322.04
Kleine On-Board-Ersatzbatterie für R&S®CryptoServer PCI und PCIe	R&S®CryptoServer Ersatzbatterie PCI/PCIe	5414.1322.05
Große On-Board-Ersatzbatterie für R&S®CryptoServer LAN	R&S®CryptoServer Ersatzbatterie LAN	5414.1322.06

[1] Zulassung/Bestätigung in Arbeit.
[2] Lieferzeit für QES-HSM auf Anfrage.

Service Ihres Vertrauens

- Weltweit
- Lokal und persönlich
- Flexibel und maßgeschneidert
- Kompromisslose Qualität
- Langfristige Sicherheit

Rohde&Schwarz

Der Elektronikkonzern Rohde&Schwarz ist ein führender Lösungsanbieter in den Arbeitsgebieten Messtechnik, Rundfunk, Funküberwachung und -ortung sowie sichere Kommunikation. Vor mehr als 75 Jahren gegründet ist das selbstständige Unternehmen mit seinen Dienstleistungen und einem engmaschigen Servicenetz in über 70 Ländern der Welt präsent. Der Firmensitz ist in Deutschland (München).

Der Umwelt verpflichtet

- Energie-effiziente Produkte
- Kontinuierliche Weiterentwicklung nachhaltiger Umweltkonzepte
- ISO 14001-zertifiziertes Umweltmanagementsystem

Certified Quality System
ISO 9001

Rohde&Schwarz SIT GmbH
Am Studio 3 | D-12489 Berlin
+49 30 65884-223 | Fax +49 30 65884-184
E-Mail: info.sit@rohde-schwarz.com
www.sit.rohde-schwarz.com

www.rohde-schwarz.com

Kontakt

- Europa, Afrika, Mittlerer Osten
  +49 89 4129 123 45
  customersupport@rohde-schwarz.com
- Nordamerika
  1 888 TEST RSA (1 888 837 87 72)
  customer.support@rsa.rohde-schwarz.com
- Lateinamerika
  +1 410 910 79 88
  customersupport.la@rohde-schwarz.com
- Asien/Pazifik
  +65 65 13 04 88
  customersupport.asia@rohde-schwarz.com

PD 5214.4642.31 | Version 01.01 | Oktober 2010 | R&S®R&S®CryptoServer
Daten ohne Genauigkeitsangabe sind unverbindlich | Änderungen vorbehalten

5214464231