R&S®CryptoServer

Highest level of security for confidential data and cryptographic keys

ROHDE&SCHWARZ

Secure Communications

Data Sheet | 01.00

R&S®CryptoServer
At a glance

The R&S®CryptoServer is used as a hardware security module (HSM) for the protection of data and transactions. The R&S®CryptoServer meets highest international security standards and is certified by the German Federal Office for Information Security (BSI) and the US National Institute of Standards and Technology (NIST). Via interfaces (APIs), the R&S®CryptoServer is integrated into existing IT systems such as public key infrastructures (PKI) for ID and inspection systems, where it is used to encrypt and sign confidential data.

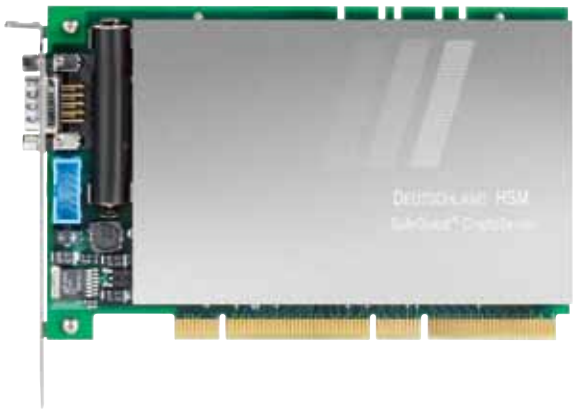
The R&S®CryptoServer's optimized throughput performance and low administrative overhead makes it especially suitable for centralized operations, i.e. to initialize and validate certificates of a PKI, to encrypt databases or for secure authentication. The R&S®CryptoServer's high security standard makes the HSM ideal for use in government applications such as used by the police, the military and public administration, and also for commercial applications with highest security requirements, such as banks.

This high security standard is achieved through a combination of physical protection measures and software security technologies. Even a stolen HSM is protected against concerted mechanical attack. The R&S®CryptoServer is equipped with a sophisticated attack detection mechanism and accompanying protection measures, so that stored data is not disclosed. If an attempt is made to obtain unauthorized access, stored key and data material is erased within milliseconds.

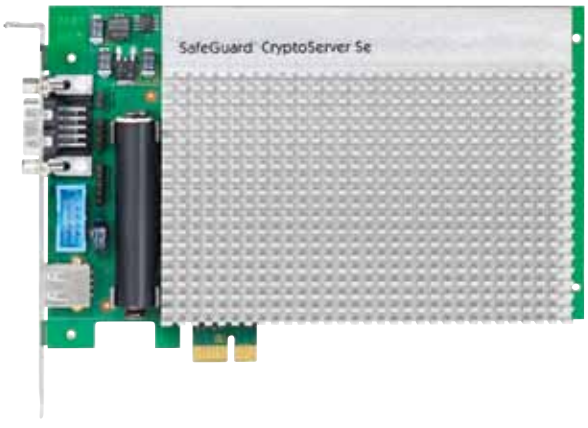
Key facts

- Hardware security module as a plug-in card (PCI/PCIe) for server operation and as a LAN appliance (industrial PC) for operation as a network server
- High-performance, state-of-the-art cryptographic methods and algorithms (e.g. AES, elliptic curves) for various key lengths
- Physical security mechanisms for maximum security (e.g. tamper protection, memory protection, emergency erasure, physical randomness)
- Certified by BSI, ZKA and NIST
- High-security memory

The R&S®CryptoServer/Deutschland HSM (PCI card).



The R&S®CryptoServer/SecurityServer Se (PCIe card).



R&S®CryptoServer
Benefits and key features

Powerful, flexible and high availability
- High cryptographic throughput with low administrative overhead
- Flexible integration in security-critical applications using standard interfaces
- Redundant use for fail-safe operation and load sharing

▷ page 4

Professional key and role management
- Cryptographic secret sharing according to Shamir
- Secure backup of keys
- Remote administration of cryptographic parameters using secure messaging

▷ page 5

Security confirmed by international and German certification
- International certification (NIST, BSI, Common Criteria)
- German certification (BSI, SigG, ZKA)

▷ page 6

Commercial and government applications
- Authentication server (company ID cards, government documents, ePASS)
- Public key infrastructures
- Document management and archiving solutions
- Database encryption
- Cashless payment transactions (ePayment)
- Electronic billing (eBilling)
- Time stamp applications

▷ page 7

The R&S®CryptoServer/SecurityServer CS (PCI card).

Powerful, flexible and high availability

High cryptographic throughput with low administrative overhead

Key generation, electronic signature and data encryption – the R&S®CryptoServer quickly executes all cryptographic operations. It is available as a PCI/PCIe plug-in card and as a 19" LAN appliance. The data that is to be encrypted or signed is sent to the HSM, cryptographically processed and then transmitted back over a secure transmission path.

The setup is confined to basic administration (user, authorizations, etc.) and setup of the interfaces that the application will use to communicate with the R&S®CryptoServer.

The low adminstrative overhead means a fast return on investment.

Flexible integration in security-critical applications using standard interfaces

To integrate the R&S®CryptoServer into the processes that need to be protected, it can be flexibly addressed over the following standard interfaces (variant-dependent):

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

The desired interfaces will be set up on the host where the application runs. Each interface is assigned to an HSM. Since some applications transmit PKCS#11 data in plain mode, encrypted transmission has been added to the R&S®CryptoServer's PKCS#11 wrapper.

Since government applications require specific security methods, R&S®CryptoServer/Deutschland HSM and its subvariants support none of the above mentioned interfaces. A specific, Java-based interface is used instead. This interface, called "Java eID", serves government eID and PKI applications.

Redundant use for fail-safe operation and load sharing

Applications that have high availability requirements should use redundant R&S®CryptoServers. Redundant use results in load sharing which means faster response times (e.g. when many status queries requiring a signature are expected for certificate checks) and fail-safe operation using hot/cold standby scenarios.

In both cases, implementation of redundant operation depends on the standard interface used: The C-API and CNG Microsoft interfaces and the JCE and CXI interfaces support redundant operation as standard. The R&S®CryptoServer stores an authorization key on the interface which allows each R&S®CryptoServer to be accessed within the load-balancing network. In the case of PKCS#11 and Java eID, redundancy can be individually implemented at the application level.

The R&S®CryptoServer is available as a plug-in card (PCI/PCIe HSM) and as a complete server appliance in rack format (LAN HSM).

Professional key and role management

Cryptographic secret sharing according to Shamir

Especially in the case of government authorities and similar institutions, security personnel monitor whether security-critical functions, such as key management, are handled correctly. For this reason, the R&S®CryptoServer supports cryptographic secret sharing according to Shamir (also known as the four-eyes or six-eyes principle). This principle ensures that certain operations can only be performed when at least two (or three) security administrators have been authenticated using their personal R&S®CryptoServer key parts. The personal key parts are combined to form the role-specific key required for cryptographic access to the functions.

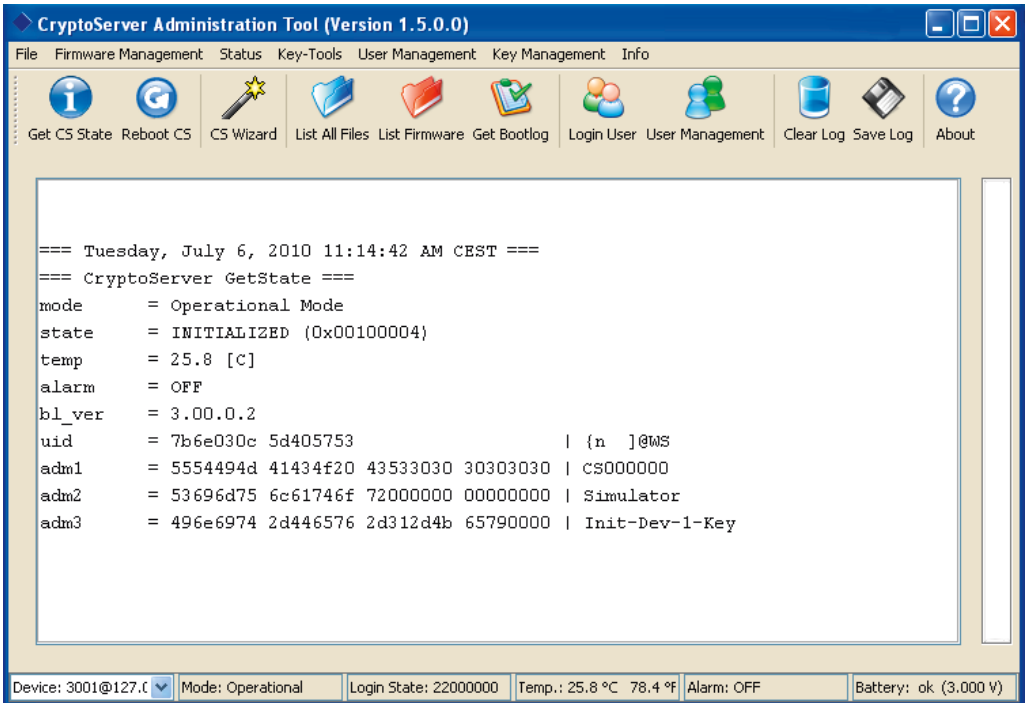
Secure backup of keys

To protect the keys, the R&S®CryptoServer can export them in an encrypted form. Several security administrators must be present, since the exported keys are protected using a transport key (KEK) in line with the four-eyes or six-eyes principle. Then, the protected keys are either deposited in a secure environment or imported into a backup device.

Remote administration of cryptographic parameters using secure messaging

For the administration of security-relevant and cryptographic parameters, the R&S®CryptoServer administration software has a specially-protected management access. This access is based on secure messaging, a technology which sets up an encrypted channel to the R&S®CryptoServer. Applications and security administrators can remotely access the R&S®CryptoServer over this channel.

As a further protective measure, the R&S®CryptoServer is configured such that the secure messaging channel can only be set up using personal authentication information. This personal information can be stored on the Smart Card, so that security administrators always need a connected card reader to provide authentication for remote administration.



The R&S®CryptoServer administration tool (CAT) supplied with the device provides a convenient user interface for security management.

Security confirmed by international and German certification

International certification (NIST, BSI, Common Criteria)

The R&S®CryptoServer comes with state-of-the art detection and protection measures to prevent physical attacks. It meets the US standard FIPS PUB 140-2 Level 3 and the additional Level 4 for physical security. Level 4 security is based on the implemented protection measurements to prevent side channel attacks (such as RF leakage and energy consumption measurements), early detection of physical attacks, and the immediate implementation of emergency erasure measures.

In addition to the cryptographic algorithms, the high entropy of the randomness generator for the keys is a major criterion for high-security crypto devices. Documents from the German BSI define international recognized criteria for random number generation. The R&S®CryptoServer generates random numbers in line with BSI AIS 31 (class P2). The postprocessing of these random numbers is done in line with BSI AIS 20 (class K4).

The R&S®CryptoServer is currently being prepared for certification in line with Common Criteria EAL4+.

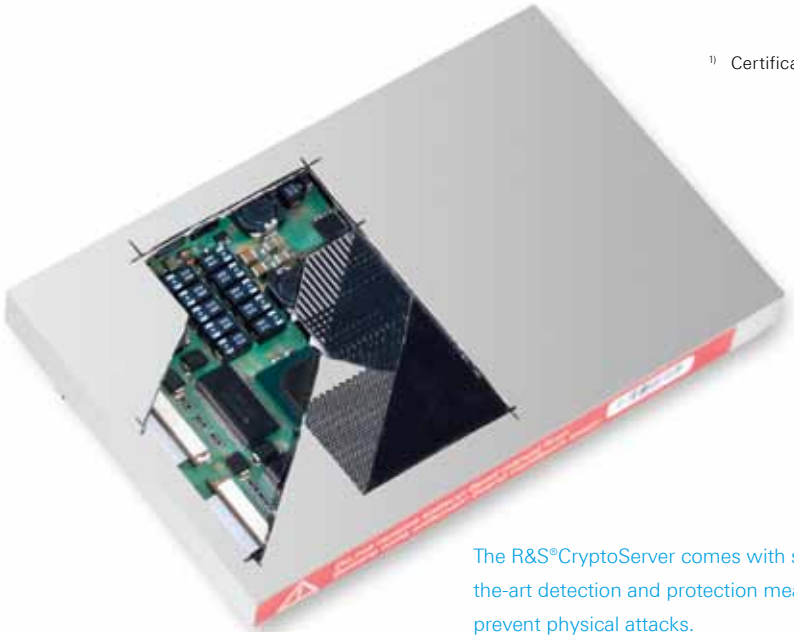
German certification (BSI, SigG, ZKA)[1)]

The R&S®CryptoServer/Deutschland HSM meets the BSI security requirements for processing sensitive (classified) information up to "German confidential" (VS-V), making it the first choice for government projects in Germany.

The R&S®CryptoServer/QES HSM is being prepared for qualified electronic signature and mass generation of signatures in line with the German Electronic Signature Act (SigG).

Approval required for use in banks and credit institutions (ZKA) has already been granted.

1) Certification depends on the R&S®CryptoServer variant.



The R&S®CryptoServer comes with state-of-the-art detection and protection measures to prevent physical attacks.

Commercial and government applications

The R&S®CryptoServer is a hardware security module used to execute cryptographic functions such as encryption, signature and hash. It helps ensure the confidentiality, integrity and authenticity of data in IT systems. Secret keys are required to identify persons, objects and processes that are especially sensitive. These keys are generated and stored securely in the R&S®CryptoServer.

The R&S®CryptoServer can be used flexibly and offers maximum security for:

- Electronic identities in commercial and government environments (eID, PKI)
- Document management/archiving, database encryption
- Cashless payment transactions (ePayment)
- Electronic billing (eBilling)
- Electronic allocation systems
- Time stamp applications

One of the R&S®CryptoServer's main applications within eID systems is to provide trustworthy electronic identities. For both the German biometric passport and the new German electronic ID, the R&S®CryptoServer is used for secure:

- production and personalization of government documents
- confidential maintenance of revocation lists
- operation of government and commercial eID servers
- authorization checks within inspection systems

Electronic passport checking is subject to strict security guidelines. Only officially authorized persons are allowed to access the biometric data stored in the documents. For example, the R&S®CryptoServer can be used as a hardware security module in an ICAO PKI as defined by the International Civil Aviation Organization (ICAO). More details on the operation of the R&S®CryptoServer as a hardware security module of a national control system can be found in the BSI technical guideline TR-03129 "PKIs for Machine Readable Travel Documents".

Since 2007, biometric data has been stored in German passports.

New electronic ID with ePass, eID and eSign functions (photo: © German Federal Ministery of the Interior).

Glossary

Term	Description
AES	Advanced Encryption Standard
AIS	Guidance and Interpretation of Scheme Issues
API	Application Programming Interface
BSI	German Federal Office for Information Security
CA	Certificate Authority of a 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 in line with Common Criteria
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
eID	Electronic IDs
FIPS	(US) Federal Information Processing Standard
HU	Height Unit
HSM	Hardware Security Module
ICAO	International Civil Aviation Organization
JCE	Java Cryptographic Extension
KEK	Key Encryption Key
LAN	Local Area Network
MD5	Message-Digest algorithm 5
MRTD	Machine Readable Travel Documents
NIST	(US) National Institute of Standards and Technology
PCI	Peripheral Component Interconnect
PCIe	Peripheral Component Interconnect Express
PKCS#11	Public Key Cryptography Standard #11
PKI	Public Key Infrastructure
PP	Protection Profile
QES	Qualified Electronic Signature
RIPEMD	RACE Integrity Primitives Evaluation Message Digest
RSA	Rivest Shamir Adleman
SHA	Secure Hash Algorithm
SigG	German Electronic Signature Act
SSCD	Secure Signature Creation Device
VA	Validation Authority for certificates
VS-V (VS-Vertraulich)	German confidential (for classified documents)
ZKA	German Central Credit Committee

Specifications

Specifications				
	Commercial applications		**Government applications**	**Qualified Electronic Signature in line with SigG**
R&S®CryptoServer [1] variant	SecurityServer Se	SecurityServer CS	Deutschland HSM	QES HSM
Performance/throughput				
Number of RSA signatures per second (2048 bit/4094 bit)	1250/250	80/10	80/10	80/10
Number of EC signatures per second (224 bit/256 bit)	1300/1100	1200/1000	1200/1000	–
Hardware				
Available format				
PCI Express plug-in card (167.65 mm long, 111.15 mm high)	●	–	–	–
PCI plug-in card (167 mm long, 107 mm high)	–	●	●	–
LAN appliance (rack format, 2 HU) (446 mm wide, 88 mm high, 510 mm deep)	●	●	●	●
Operating temperature range (plug-in card)	+10 °C to +45 °C	+10 °C to +35 °C		
Storage temperature range	–14 °C to +66 °C			
Cryptographic functions				
Symmetric algorithms	AES, DES, 3DES		AES	
Asymmetric algorithms	ECDSA, ECDH, RSA, DH, DSA		ECDSA, RSA	RSA
Hash algorithms	SHA-1, SHA-2 family, RIPEMD-160, MD5			
Random number generation	true random numbers in line with AIS 31 class P2, pseudo random numbers in line with FIPS 186-2 and AIS 20 class K4		true random numbers in line with AIS 31 class P2, pseudo random numbers in line with FIPS 186-2 and AIS 20 class K4 additionally: BSI qualification	
Certification/conformance				
ZKA	–	●	–	–
BSI	–	–	up to "German confidential" (VS-V) [2]	–
Signature law (SigG)	–	–	–	● [3]
Common Criteria	–	–	EAL4+ in line with PP CM Enhanced [2][3]	EAL4+ in line with PP SSCD [3]
FIPS 140-2	Level 3 [3]	Level 3 + Level 4 "Physical Security"	–	–
Functional features				
R&S®CryptoServer administration tool (CAT)	●	●	●	●
Emergency erase button	●	●	●	●
Active erasure/overwriting of memory contents in case of physical attack	–	●	●	●
Backup of keys	●	●	●	–
Multi client capability	●	●	●	–
PKCS #11 wrapper	●	●	–	–

[1] Rohde&Schwarz SIT GmbH is the exclusive sales partner of Utimaco Safeware AG for official eID projects of the German government. The R&S®CryptoServer and its variants are identical to the SafeGuard™ CryptoServer products of the same name.
[2] Approvals depend on the selected R&S®CryptoServer/Deutschland HSM subvariant (see ordering information).
[3] Approval/certification pending.

Ordering information

Designation	Type	Order No.
R&S®CryptoServer/SecurityServer Se Certification in line with FIPS 140-2 Level 3 pending. Can be used for applications and market segments with medium to high physical security requirements (such as large organizations and companies). The SE models are based on PCI Express cards.		
Hardware security module, PCIe card model, performance level: 100 RSA signatures (1024 bit) per second	SecurityServer Se10 PCIe	5414.1280.02
Hardware security module, PCIe card model, performance level: 500 RSA signatures (1024 bit) per second	SecurityServer Se50 PCIe	5414.1280.03
Hardware security module, PCIe card model, performance level: 4000 RSA signatures (1024 bit) per second	SecurityServer Se400 PCIe	5414.1280.04
Hardware security module, PCIe card model, performance level: 10000 RSA signatures (1024 bit) per second	SecurityServer Se1000 PCIe	5414.1280.05
Hardware security module, LAN appliance model, performance level: 100 RSA signatures (1024 bit) per second, contains one pinpad and three Smart Cards	SecurityServer Se10 LAN	5414.1280.06
Hardware security module, LAN appliance model, performance level: 500 RSA signatures (1024 bit) per second, contains one pinpad and three Smart Cards	SecurityServer Se50 LAN	5414.1280.07
Hardware security module, LAN appliance model, performance level: 4000 RSA signatures (1024 bit) per second, contains one pinpad and three Smart Cards	SecurityServer Se400 LAN	5414.1280.08
Hardware security module, LAN appliance model, performance level: 10000 RSA signatures (1024 bit) per second, contains one pinpad and three Smart Cards	SecurityServer Se1000 LAN	5414.1280.09
R&S®CryptoServer/SecurityServer CS Certified in line with FIPS 140-2 Level 3 (with Level 4 for "Physical Security"), certified by the ZKA (German Central Credit Committee). Can be used for applications and market segments with high physical security requirements (such as banks, financing and authorities). The CS models are based on PCI cards.		
Hardware security module, PCI card model, performance level: 100 RSA signatures (1024 bit) per second	SecurityServer CS10 PCI	5414.1297.02
Hardware security module, PCI card model, performance level: 500 RSA signatures (1024 bit) per second	SecurityServer CS50 PCI	5414.1297.03
Hardware security module, LAN appliance model, performance level: 100 RSA signatures (1024 bit) per second, contains one pinpad and three Smart Cards	SecurityServer CS10 LAN	5414.1297.06
Hardware security module, LAN appliance model, performance level: 500 RSA signatures (1024 bit) per second, contains one pinpad and three Smart Cards	SecurityServer CS50 LAN	5414.1297.07

The R&S®CryptoServer front panel (LAN appliance).

The R&S®CryptoServer rear panel (LAN appliance).

Designation	Type	Order No.
R&S®CryptoServer/Deutschland HSM BSI approved (VS-V), can be used to produce government eID documents (such as electronic passports). All models are based on PCI cards.		
Hardware security module, PCI card model, performance level: 125 ECC signatures (256 bit) per second	Deutschland HSM/1 CS10 PCI	5414.1300.02
Hardware security module, PCI card model, performance level: 1000 ECC signatures (256 bit) per second	Deutschland HSM/1 CS50 PCI	5414.1300.03
Hardware security module, LAN appliance model, performance level: 125 ECC signatures (256 bit) per second, contains one pinpad and three Smart Cards	Deutschland HSM/1 CS10 LAN	5414.1300.06
Hardware security module, LAN appliance model, performance level: 780 ECC signatures (256 bit) per second, contains one pinpad and three Smart Cards	Deutschland HSM/1 CS50 LAN	5414.1300.07
R&S®CryptoServer/Deutschland HSM [1] CC evaluated and BSI approved (VS-V), can be used for blocking services for governmental eID applications, for example. All models based on PCI cards.		
Hardware security module, PCI card model, performance level: 125 ECC signatures (256 bit) per second	Deutschland HSM/2 CS10 PCI	5414.1300.12
Hardware security module, PCI card model, performance level: 1000 ECC signatures (256 bit) per second	Deutschland HSM/2 CS50 PCI	5414.1300.13
Hardware security module, LAN appliance model, performance level: 125 ECC signatures (256 bit) per second, contains one pinpad and three Smart Cards	Deutschland HSM/2 CS10 LAN	5414.1300.16
Hardware security module, LAN appliance model, performance level: 780 ECC signatures (256 bit) per second, contains one pinpad and three Smart Cards	Deutschland HSM/2 CS50 LAN	5414.1300.17
R&S®CryptoServer/Deutschland HSM [1] CC evaluated and EAL4+ certified, can be used for eID applications, electronic allocation systems and control systems. All models based on PCI cards.		
Hardware security module, PCI card model, performance level: 125 ECC signatures (256 bit) per second	Deutschland HSM/3 CS10 PCI	5414.1300.22
Hardware security module, PCI card model, performance level: 1000 ECC signatures (256 bit) per second	Deutschland HSM/3 CS50 PCI	5414.1300.23
Hardware security module, LAN appliance model, performance level: 125 ECC signatures (256 bit) per second, contains one pinpad and three Smart Cards	Deutschland HSM/3 CS10 LAN	5414.1300.26
Hardware security module, LAN appliance model, performance level: 780 ECC signatures (256 bit) per second, contains one pinpad and three Smart Cards	Deutschland HSM/3 CS50 LAN	5414.1300.27
R&S®CryptoServer/QES HSM [1] [2] CC EAL4+ certified as secure signature creation device (SSCD) and certified by SigG (German Electronic Signature Act). Can be used for central mass signature applications, based on PCI cards.		
Hardware security module, LAN appliance model, performance level: 80 RSA signatures (2048 bit) per second, contains one pinpad and three Smart Cards	QES HSM CS50 LAN	5414.1316.07
R&S®CryptoServer accessories		
Pinpad	R&S®CryptoServer Pinpad	5414.1322.02
Smart Card	R&S®CryptoServer Smart Card	5414.1322.03
Large external backup battery for the R&S®CryptoServer PCI and PCIe	R&S®CryptoServer Backup Battery PCI/PCIe	5414.1322.04
Small on-board spare battery for the R&S®CryptoServer PCI and PCIe	R&S®CryptoServer Spare Battery PCI/PCIe	5414.1322.05
Large on-board spare battery for the R&S®CryptoServer LAN	R&S®CryptoServer Spare Battery LAN	5414.1322.06

[1] Certification/approval pending.
[2] Delivery time for QES/HSM available upon request.

Service you can rely on

- Worldwide
- Local and personalized
- Customized and flexible
- Uncompromising quality
- Long-term dependability

About Rohde&Schwarz

Rohde&Schwarz is an independent group of companies specializing in electronics. It is a leading supplier of solutions in the fields of test and measurement, broadcasting, radiomonitoring and radiolocation, as well as secure communications. Established more than 75 years ago, Rohde&Schwarz has a global presence and a dedicated service network in over 70 countries. Company headquarters are in Munich, Germany.

Environmental commitment

- Energy-efficient products
- Continuous improvement in environmental sustainability
- ISO 14001-certified environmental management system

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

Regional contact

- Europe, Africa, Middle East
  +49 89 4129 123 45
  customersupport@rohde-schwarz.com
- North America
  1 888 TEST RSA (1 888 837 87 72)
  customer.support@rsa.rohde-schwarz.com
- Latin America
  +1 410 910 79 88
  customersupport.la@rohde-schwarz.com
- Asia/Pacific
  +65 65 13 04 88
  customersupport.asia@rohde-schwarz.com

PD 5214.4642.32 | Version 01.00 | November 2010 | R&S®CryptoServer

5214464232