



CryptoServer CP5 VS-NfD*

*Classified – for official use only (de: Verschlussache – nur für den Dienstgebrauch)

CryptoServer
The Root of Trust HSM



Governments and government-like organizations like NATO declare as “classified information” such information that they consider particularly sensitive. Increased caution is required when handling such data, especially with regard to confidentiality and integrity, even at the entry-level classifications “VS-NfD”, “EU restricted” and “NATO restricted”.

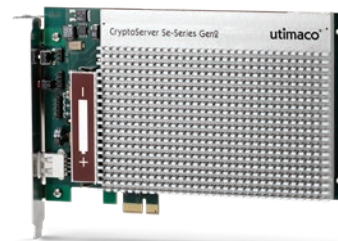
The most important features and advantages for public authorities:

- CryptoServer CP5 VS-NfD is the only VS-NfD HSM approved by the BSI
- UTIMACO is an official participant in the qualified BSI approval process for encryption solutions
- UTIMACO works with a network of partners who offer and implement a wide range of VS-NfD-compliant solutions

SecurITy

made
in
Germany

Trust Seal
www.teletrust.de/itsmig



utimaco[®]



Product Highlights

- The data security standards for public authorities require the use of appropriate measures for ensuring the seamless protection of all sensitive data. One of the most efficient ways to do this is to use encryption tools that securely store and use keys in a VS-NfD HSM.



- CryptoServer CP5 VS-NfD is a hardware security module that is suitable for a variety of use cases, such as certificate issuing for, and signing of classified documents. The German Federal Office for Information Security (BSI) has approved "CryptoServer CP5 VS-NfD" according to the Qualified Certification Procedure – **the product is the only VS-NfD hardware security module approved by the BSI. It allows to secure data classified up to "VS-NfD", "EU restricted" and "NATO restricted"**.
- CryptoServer CP5 VS-NfD is available as a PCIe plug-in card or as a network-attached appliance.



Key Features

- Secure key storage and processing within the security boundary of the HSM
- Extensive key management with key authorization
- Key authorization API and tool (acc. PP EN 419 221-5)
- "m of n" quorum authentication (e.g. 3 out of 5)
- 2-factor authentication based on smartcards
- Role-based access control and separation of duties
- Multi-tenancy support
- Remote management
- Dedicated software simulator for evaluation and integration testing
- Supported operating systems: Windows and Linux
- A variety of integrations with PKI applications, etc.
- Integrated load balancing and HA functionality
- Flexible backup options
- All features included in product price



HSM Functionalities

Cryptographic algorithms

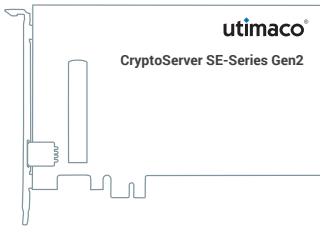
- RSA, ECDSA with NIST and Brainpool curves
- ECDH with NIST and Brainpool curves
- AES
- CMAC, HMAC
- SHA2, SHA3
- Hash-based deterministic random number generator (DRG.4 according to AIS 31)
- True Random Number Generator (PTG.2 according to AIS 31)
- Up to 3,000 RSA or 2,500 ECDSA signature operations when processing in bulk mode
- All algorithms included in the product price

Application programming interfaces (APIs)

- PKCS#11
- Microsoft Cryptography API: Next Generation (CNG)
- Cryptographic eXtended services Interface (CXI) – UTIMACO's high performance interface ensures easy integration of cryptographic functionality into client applications



Technical specifications PCIe card



Physical Dimensions

- **Form factor:** Half-length, full-height single lane PCI Express card
- **Compatibility:** PCIe 1.1, PCIe 2.0 and PCIe 3.0 slots
- **Height:** 111.15 mm ("full" height)
- **Weight:** 400 g



Electrical

- **Power Supply:** 3.3 V DC via PCI Express bus
- **Normal energy consumption:** 5 W, max. 10 W
- **Heat dissipation:** 34 BTU/h



Operating Environment

- **Operating temperature:** +10°C to +35°C (+50°F to +95°F)
- **Storage temperature:** -10°C to +55°C (+14°F to +131°F)
- **Relative humidity:** 10% to 95%, non-condensing
- **MTBF:** 360,000 hours at 25°C / 77°F



Connectivity

- **Interface:** PCI express bus; USB interface for pin pad



Security and Compliance

- **Bullet Security:** Common Criteria certified; classified VS-NfD, RESTREINT UE / EU RESTRICTED, NATO RESTRICTED
- **Safety:** IEC/EN 60950-1; CB certificate; UL
- **Emissions:** CE, FCC Class B
- **Environmental:** RoHS II, WEEE



Technical specifications Network appliance



Physical Dimensions

- **Form factor:** 19" 1U
- **Width:** 446 mm excluding brackets
- **Depth:** 533.4 mm excluding handles
- **Height:** 44 mm
- **Weight:** 10 kg



Electrical

- **Power Supply:** Dual Hot Swap Power Supplies: 2 x 100 ~ 240 V AC, 50 ~ 60 Hertz, 300 W
- **Normal energy consumption:** 45 W / 66 VA, max. 50 W / 70 VA
- **Heat dissipation:** max. 171 BTU/h



Operating Environment

- **Operating temperature:** +10°C to +40°C (+50°F to +104°F)
- **Storage temperature:** -10°C to +55°C (+14°F to +131°F)
- **Relative humidity:** 10% to 95%, non-condensing
- **MTBF:** 100,000 hours at 25°C / 77°F, environment GB, GC – Ground Benign, Controlled



Connectivity

- **Interfaces:** 2 RJ45, 1 Gb/s network connections; USB interfaces for pin pad and USB stick



Security and Compliance


- **Bullet Security, Safety, Emissions and environmental directives:** as with the PCIe version






EMEA

UTIMACO IS GmbH

 Germanusstraße 4
52080 Aachen,
Germany

 +49 241 1696 200

 hsm@utimaco.com

Americas

UTIMACO Inc.


 900 E Hamilton Ave.,
Suite 400
Campbell, CA 95008,
USA


 +1 844 UTIMACO

 hsm@utimaco.com

APAC

UTIMACO IS Pte Limited

 50 Raffles Place,
Level 19,
Singapore Land Tower,
Singapore 048623

 +65 6631 2758

 hsm@utimaco.com

For more information about UTIMACO HSM products, please visit:

hsm.utimaco.com

© UTIMACO IS GmbH 05/20

UTIMACO® is a trademark of UTIMACO GmbH. All other named Trademarks are Trademarks of the particular copyright holder. All rights reserved. Specifications are subject to change without notice.