



se.SAM™ N-200 Crypto-Appliance



- ▶ **Keys in hardware** for everyone
- ▶ **Economic crypto-appliance** for IT, cloud, industry and embedded development
- ▶ **Manifold IoT, IIoT and embedded applications**
- ▶ **Ideal for the cryptographic protection** of intellectual property, firmware and license keys
- ▶ **Secure PKI operation**
- ▶ **Unlimited clients, no hidden costs**



sematicon se.SAM™ N-200

By means of state-of-the-art technology, the **se.SAM™ N-200** Crypto-Appliance provides extensive protection of digital secrets against unauthorised copies. In addition to a world-wide unique serial number, a variety of cryptographic functions is combined in just one tool - easy to handle and to understand. No matter what the motivation behind your project is: to protect your intellectual property, to guarantee the authenticity of your data, to protect your measurement values against unauthorised access or to operate a PKI environment?

With our **se.SAM™ N-200** Crypto-Appliance you are excellently prepared!

Flexible interfaces

By focusing on particular easy handling, the N-Series offers a wide range of interfaces to meet the requirements of IT, industry and embedded environments. For many applications, no client-software is necessary.

Integrated crypto-processors

Depending on the type, the appliance disposes of two to eight crypto-processors, which can be configured independently of each other and are able to work with a variety of keys. Test and production can be operated separately on one platform.

Flexible architecture

The appliance's operation in a high-availability cluster ensures system stability for critical environments.

Users, roles and authorisations

The keys and their use are limited to certain permissions. Users can be integrated locally or from already existing directories, e.g. Active Directory. During the process of accessing special keys and configuring the appliance, the dual control principle can be put into use to increase security even further.

Backup and disaster recovery

Intelligent processes allow an easy-to-handle backup. This can be created automatically and stored on any data carrier in the form of files according to your requirements.



{ json:api }



Technical specifications

Supported crypto-algorithms

- ▶ Symmetric algorithms: AES CBC, AES, CTR, AES ECB each with 128 and 256 bit, SHA1-HMAC, SHA256-HMAC, SHA384-HMAC, SHA512-HMAC, CMAC-128
- ▶ Asymmetric algorithms: RSA 512 to 4096, ECC-NIST-P/secp192r1 to 521r1, ECC-Brainpool 160 to 512, ECC Koblitz/secp160k1 to 256k1, ECDSA, ECDH
- ▶ HASH digest: SHA1, SHA-2-224 to 512
- ▶ Key derivation function: HKDF
- ▶ Additional functions: Secure Hardware-Counter, "Multi Source True Random Number Generator", Key-ACLs, Secure Key Exchange, License Key-Generator

Supported operating systems

- ▶ Completely OS-independent
- ▶ Microsoft CNG KSP (available from Q2/2021), Windows 10, Windows Server 2016/2019

Application interfaces - APIs

- ▶ RESTful JSON API
- ▶ TCP/TLS RAW Socket
- ▶ MQTT
- ▶ Node-RED
- ▶ Microsoft CNG Key Storage Provider (optional)

Management

- ▶ Web-GUI with optional LDAP or Active Directory connection
- ▶ NTP, SNMPv2 and Syslog
- ▶ Multi-Node Cluster configuration

Licensing

- ▶ No CALs or additional costs for basis-interfaces
- ▶ Microsoft CNG is commercially available as well

Security certifications

- ▶ Common Criteria EAL 6+ certified crypto-core (up to Secure-Processor-OS-Level)

Appliance features

- ▶ Standard 1HE 19 inch rack appliance
- ▶ 2 Gigabit Ethernet Ports, VLAN 802.1q Support
- ▶ Size (LxWxH): 437 x 287 x 43 mm, low installation depth
- ▶ Weight: 4,3 kg
- ▶ Max 30W, 85BTU/h - 220-240V AC, 50-60Hz



sematicon AG • Schatzbogen 56 • 81829 Munich
office@sematicon.com • +49 (89) 413 293 000 • www.sematicon.com