



se.SAM™ N-200 Krypto-Appliance



- ▶ **Schlüssel in Hardware** für jedermann
- ▶ **Kostengünstige Krypto-Appliance** für IT, Cloud, Industrie und Embedded Entwicklung
- ▶ **Vielfältige IoT, IIoT und Embedded Anwendungen**
- ▶ **Ideal für den kryptographischen Schutz** von geistigem Eigentum, Firmware und Lizenzschlüsseln
- ▶ **Sicherer PKI-Betrieb**
- ▶ **Unbegrenzte Clients**, keine versteckten Kosten



sematicon se.SAM™ N-200

Mit modernster Technologie bietet die **se.SAM™ N-200** Krypto-Appliance umfangreichen Schutz für digitale Geheimnisse und verhindert unerlaubte Kopien. Neben einer weltweit einzigartigen Seriennummer kombiniert das Gerät viele kryptographische Funktionen zu einem Werkzeug - einfach zu handhaben und leicht verständlich. Egal welche Motivation Ihr Projekt antreibt: der Schutz Ihres geistigen Eigentums, die Echtheit Ihrer Daten, der Schutz Ihrer Messwerte vor unberechtigtem Zugriff oder der Betrieb einer PKI Umgebung?

Mit unserer **se.SAM™ N-200** Krypto-Appliance sind Sie bestens gerüstet!

Flexible Schnittstellen

Ausgerichtet auf eine besonders einfache Handhabung stellt die N-Serie eine breite Palette von Schnittstellen zur Verfügung, um die Anforderungen von IT, Industrie und der Embedded Welt zu erfüllen. Für viele Anwendungen ist dabei keine Client-Software notwendig.

Integrierte Krypto-Prozessoren

Je nach Modell verfügt die Appliance über zwei bis acht voneinander unabhängig konfigurierbare Krypto-Prozessoren, die mit einer Vielzahl an Schlüsseln arbeiten können. Somit können Test und Produktion voneinander getrennt auf einer Plattform betrieben werden.

Flexible Architektur

Der Betrieb der Appliance in einem hoch verfügbaren Cluster garantiert die Ausfallsicherheit für kritische Umgebungen.

Benutzer, Rollen und Zuständigkeiten

Die Schlüssel sowie deren Verwendung sind an Berechtigungen gebunden. Benutzer können lokal oder aus bestehenden Verzeichnisdiensten (z.B. Active Directory) eingebunden werden. Beim Zugriff auf besondere Schlüssel sowie bei der Konfiguration der Appliance besteht die Möglichkeit, durch die Nutzung des Vier-Augen-Prinzips die Sicherheit weiter zu erhöhen.

Backup und Disaster Recovery

Intelligente Prozesse erlauben ein einfach zu handhabendes Backup. Dieses kann automatisch erstellt und in Form von Dateien nach Ihren Vorgaben auf einem beliebigen Datenträger abgelegt werden.



{ json:api }



Technische Spezifikation

Unterstützte Krypto-Algorithmen

- ▶ Symmetrische Algorithmen: AES CBC, AES, CTR, AES ECB jeweils 128 und 256 bit, SHA1-HMAC, SHA256-HMAC, SHA384-HMAC, SHA512-HMAC, CMAC-128
- ▶ Asymmetrische Algorithmen: RSA 512 bis 4096, ECC-NIST-P/secp192r1 bis 521r1, ECC-Brainpool 160 bis 512, ECC Koblitz/secp160k1 bis 256k1, ECDSA, ECDH
- ▶ HASH Digest: SHA1, SHA-2-224 bis 512
- ▶ Schlüsselableitungen: HKDF
- ▶ Zusätzliche Funktionen: Secure Hardware-Counter, „Multi Source True Random Number Generator“, Schlüssel-ACLs, Secure Key Exchange, Lizenzschlüssel-Generator

Unterstützte Betriebssysteme

- ▶ Vollständig betriebssystemunabhängig
- ▶ Microsoft CNG KSP (verfügbar ab Q2/2021), Windows 10, Windows Server 2016/2019

Applikationsschnittstellen - APIs

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

Management

- ▶ Web-GUI mit optionaler LDAP oder Active Directory Anbindung
- ▶ NTP, SNMPv2 und Syslog
- ▶ Multi-Node Cluster Konfiguration

Lizenzierung

- ▶ Keine CALs oder Zusatzkosten für Basisschnittstellen
- ▶ Microsoft CNG ist separat kommerziell erhältlich

Sicherheitszertifizierungen

- ▶ Common Criteria EAL 6+ zertifizierter Crypto-Core (bis Secure-Processor-OS-Level)

Appliance Eigenschaften

- ▶ Standard 1HE 19 Zoll Rack-Appliance
- ▶ 2 Gigabit Ethernet Ports, VLAN 802.1q Support
- ▶ Größe (BxTxH): 437 x 287 x 43 mm, kurze Einbautiefe
- ▶ Gewicht: 4,3 kg
- ▶ Max 30W, 85BTU/h - 220-240V AC, 50-60Hz



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