



se.SAM™ P220 Industrie Krypto-Modul



- ▶ Geeignet und geprüft für den Einsatz in **Industrie, IT und Büro**
- ▶ **Langfristige** Verfügbarkeit
- ▶ Hohe Temperaturtoleranz von **-40°C bis +85°C**
- ▶ Treiberlos - „**Plug & Play**“ unabhängig vom Betriebssystem
- ▶ **Keine Bibliotheken** oder spezielle Software nötig
- ▶ **Isolierte Speicherbereiche** für den Schutz kryptographischer Schlüssel und Daten
- ▶ Kosteneffiziente Integration durch **geringe Einarbeitungszeit**



sematicon se.SAM™ P220

Das **se.SAM™ P220 Sicherheitsmodul** wurde speziell im Hinblick auf die Erfordernisse im Geräte- und Anlagenbau für die Industrie, Elektrotechnik und andere verwandte Bereiche entwickelt. Besonderer Wert wurde dabei auf Stabilität, Robustheit und einfache Handhabung gelegt.

Einfach integrierbar - treiberlos - „Plug & Play“

Der schnelle und mühelose Einsatz mittels Standard Mini PCI Express Schnittstelle und die Tatsache, dass weder Gerätetreiber noch Software für den Betrieb notwendig sind, ermöglichen die Einbindung in nahezu jedes System. Das Gerät steht direkt in der Anwendung oder Entwicklungsumgebung zur Verfügung.

Mit Sicherheit verschlüsselt

Mit modernster Technologie bietet **se.SAM™** 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 oder der Schutz Ihrer Messwerte vor unberechtigtem Zugriff? Mit unserem **se.SAM™ P220 Sicherheitsmodul** sind Sie bestens gerüstet!

Mit Sicherheit robust

Ein hoher Temperaturbereich sowie eine erweiterte Funkentstörung ermöglichen einen Einsatz in allen Klimabereichen sowie im Schaltschrank. Gegen mechanische Einflüsse und Hardware-Manipulation ist das Modul mit einer speziellen Vergusstechnik vollständig, ohne Lufteinschluss, geschützt.

Mit Sicherheit Qualität

Durch die Herstellung im eigenen Haus, unter Einhaltung unserer hohen Qualitätsstandards bei Fertigung und Entwicklung, können wir die langfristige Verfügbarkeit des Moduls sicherstellen. Somit sparen Sie bares Geld, da Ersatzteile langfristig lieferbar bleiben.

Integrierte Uhr für dynamisches Schlüsselmanagement

Durch die integrierte Echtzeituhr ist das Modul in der Lage auch ohne externe Stromversorgung selbstständig Schlüssel zu erstellen und mit anderen Modulen synchron zu halten. Somit ist die Offline-Prüfung von Einmalkennwörtern (OTP) oder Zertifikaten problemlos möglich. Die unabhängige Echtzeituhr kann natürlich auch in Ihre individuellen Anwendungen eingebunden werden.



Anwendungsbeispiel

Technische Spezifikation

Kryptographie

- ▶ Schlüsselspeicher: 10 symmetrische Schlüssel und 10 asymmetrische Schlüsselpaare mit Zertifikat
- ▶ 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, deaktivierbares Firmware-Update, kryptographischer Selbsttest, Secure Key Import, Key Usage Counter, integrierte präzise Echtzeituhr für automatisches Schlüsselmanagement

Zertifizierungen

- ▶ Common Criteria EAL6+ (Hardware und Betriebssystem des Krypto-Prozessors)
- ▶ Berücksichtigung der EU-Richtlinie 2014/32/EU und dem WELMEC Softwareleitfaden für Messgeräte (V7.2, 2015)

Anschluss

- ▶ Full-Size PCI Express Mini Card

Eigenschaften

- ▶ Größe (LxBxH): 50,95 x 30 x 6,3 mm
- ▶ Gewicht: bis 35g
- ▶ Temperaturbereich: -40°C bis +85°C
- ▶ Feuchtigkeitsbereich: 0%-100% (nicht kondensierend)
- ▶ Datenlesbarkeit: über 15 Jahre
- ▶ Immunität (ESD): 4 kV Kontaktentladung (Performance Criteria A), 8 kV Luftentladung (Performance Criteria A), EN55024:2010, EN61000-6-2:2005
- ▶ Immunität (EMI): 10V/m von 80 MHz bis 1 GHz (Performance Criteria A), 3V/m von 1GHz bis 2,7 GHz (Performance Criteria A), EN55024:2010, EN61000-6-2:2005
- ▶ Emission (EMR): EN55032:2012
- ▶ Zeitgenauigkeit: ±1 ppm @ 25°C
- ▶ Spannungsbereich: 3,3 V (DC)
- ▶ Stromaufnahme: bis zu 25 mA (unter Last)
- ▶ EU-Normen (CE): 2012/19/EU (WEEE), 2011/65/EU und 2015/863/EU (RoHS), 2014/30/EU (EMV)



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