



# se.SAM™ P220 Industrial Crypto-Module



- ▶ Suitable and tested for **industry, IT and office** operation
- ▶ **Long-term** availability
- ▶ **Extreme temperature ranges**  
-40°C to +85°C
- ▶ **Driverless - "Plug & Play"**  
OS-independent
- ▶ **No libraries** or special software necessary
- ▶ **Isolated storage areas** for protection of cryptographic keys and data
- ▶ **Cost-efficient integration** by **short training periods**



# sematicon se.SAM™ P220

The **se.SAM™ P220** Crypto-Module has been especially designed to meet the requirements of device and plant construction in industry, electronic engineering and other related areas. Special attention was paid to stability, robustness and particular easy handling.

## Easy to integrate - driverless - "Plug & Play"

The fast and effortless use of the standardised Mini PCI Express interface enables the module's integration into nearly every system - requiring neither device drivers nor software for operation. The device can be utilised directly in the application or development environment.

## Securely encrypted

By means of state-of-the-art technology, **se.SAM™** 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 or to protect your measurement values against unauthorised access?

With your **se.SAM™ P220** Crypto-Module you are excellently prepared!

## Securely resilient

A wide temperature range and an extended radio interference suppression enable the module's application in all climatic areas and control cabinets, too. The module is fully encapsulated with a special sealing compound, without air inclusion, resisting mechanical influences and hardware manipulation.

## Securely qualitative

Due to in-house production complying with our high quality standards in development and manufacturing, the module's availability is ensured in the long run. We help our customers save money, as spare parts can be delivered on a long-term basis.

## Integrated clock for dynamic key management

Due to the integrated real-time clock, the module is able to create keys and keeps them synchronised with other modules even without external power supply. The offline verification of one-time passwords (OTP) or certificates is thus possible without any problem. The independent real-time clock can of course also be incorporated into your individual applications.



application example

## Technical specifications

### Cryptography

- ▶ Key storage: 10 symmetric keys and 10 asymmetric key pairs with certificate
- ▶ 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, firmware update, which can be disabled, cryptographic self-test, Secure Key Import, Key Usage Counter, integrated precise real-time clock for automatic key management

### Certifications

- ▶ Common Criteria EAL6+ (hardware and operating system of the crypto-processor)
- ▶ Compliant to EU-directive 2014/32/EU and the WELMEC Software Guide for Measuring Instruments (V7.2, 2015)

### Connection

- ▶ Full-Size PCI Express Mini Card

### Appliance features

- ▶ Size (LxWxH): 50,95 x 30 x 6,3 mm
- ▶ Weight: up to 35g
- ▶ Temperature range: -40°C to +85°C
- ▶ Humidity rating: 0% - 100% (without condensation)
- ▶ Data memory retention: over 15 years
- ▶ Immunity (ESD): 4 kV contacted discharge (Performance Criteria A), 8 kV air discharge (Performance Criteria A), EN55024:2010, EN61000-6-2:2005
- ▶ Immunity (EMI): 10V/m from 80 MHz to 1 GHz (Performance Criteria A), 3V/m from 1GHz to 2,7 GHz (Performance Criteria A), EN55024:2010, EN61000-6-2:2005
- ▶ Emission (EMR): EN55032:2012
- ▶ Accuracy of time: ±1 ppm @ 25°C
- ▶ Voltage: 3,3 V (DC)
- ▶ Power supply: up to 25 mA (under load)
- ▶ EU-directives (CE marking): 2012/19/EU (WEEE), 2011/65/EU and 2015/863/EU (RoHS), 2014/30/EU (EMC)