PROTEG™ Secure Access Module (SAM)

Empower your data security with our cutting-edge Secure Access Module (SAM) - delivering unparalleled cryptographic performance, robust tamper resistance, and seamless integration for ultimate data protection and trust in every transaction.

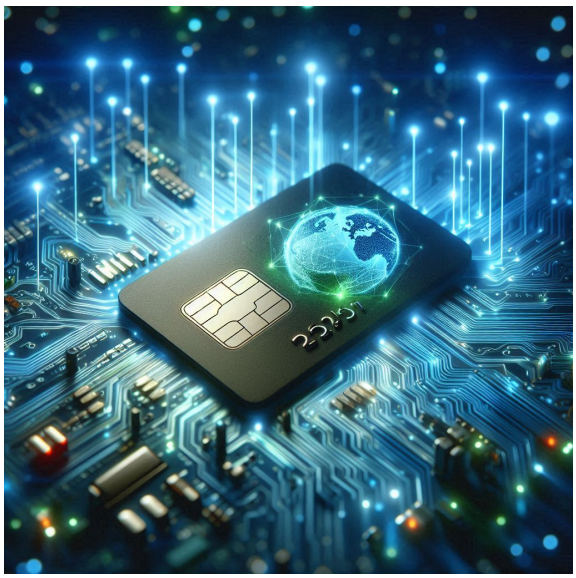
A Secure Access Module (SAM) is a critical component used to enhance security in various applications, especially in environments where cryptographic operations are essential, such as in payment systems, national ID, smart cards/RFID tags issuance, and secure access control.

Cryptographic Processing : Proteg™ SAM provides robust cryptographic processing capabilities, such as encryption and decryption, digital signature generation and verification, and secure key management. Using SAMs with Hardware Security Module (HSM) enhances security through centralized key management and secure local operations.

Secure Storage : Proteg™ SAM provides secure storage for sensitive information like cryptographic keys and certificates, coupled with tamper-resistant design to thwart physical and logical tampering attempts.

Authentication and Access Control : Proteg™ SAM ensures mutual and user authentication, establishing secure communication channels and enforcing role-based access control policies.

Interoperability : Proteg™ SAM supports industry-standard protocols and interfaces, such as ISO/IEC 7816, GlobalPlatform, and PKCS standards, ensuring broad compatibility and interoperability with smart cards and secure elements.



Performance : Designed for high-speed cryptographic operations, Proteg™ SAM minimizes performance impact while maintaining low power consumption, essential for battery-operated devices.

Compliance : Proteg™ SAM complies with regulatory standards like Common Criteria, and FIPS 140-2. This ensures that our SAM meets stringent security requirements.

Integration : Proteg™ SAM provides flexible integration options, including various form factors and API support, make it indispensable for securing sensitive operations across a wide range of applications.

Incore and the Proteg logo are trademarks of Incore Innovation Sdn Bhd. All other product or service names are the property of their respective owners. © 2024 Incore Innovation Sdn Bhd.

Date of Release: July 2024
Document Number: PROTEGSAM2024R1

PROTEG™ Secure Access Module (SAM)

Key Cryptographic Functions

- Digital signing ensures document authenticity and integrity with Elliptic Curve Digital Signature Algorithm (NIST P-256), verifying the sender's identity and confirming no alterations.
- Strong encryption secures data with advanced algorithms, making unauthorized access or deciphering extremely difficult.
- Key derivation function for deriving cryptographic keys from shared secrets.
- Hash-based Message Authentication Code (HMAC) for integrity and authenticity verification.
- Hashing converts data into a fixed-size string, ensuring data integrity by detecting changes or tampering.

TECHNICAL DATA

Algorithms	RSA (up to 2048-bit), ECC (Elliptic Curve Cryptography), AES (128/192/256-bit), DES/3DES, SHA-1, SHA-256, and HMAC.
Key Management	Secure key generation, storage, and management, including key wrapping and unwrapping
Standard Interfaces	ISO/IEC 7816 smart card interface, I2C, SPI, and USB
Communication Protocols	ISO 14443 (for contactless communication), ISO 7816 (for contact-based communication), and APDU commands.
Standards and Certifications	Common Criteria (CC) EAL 6+, FIPS 140-2, EMVCo
Security Features	Secure storage, mutual authentication, secure boot, tamper detection
Temperature and Environmental Tolerance	Operates reliably within a temperature range of -25°C to +85°C and can be stored between -40°C and +125°C, with humidity tolerance from 10% to 90% during operation and 5% to 95% in storage, both non-condensing. It features robust ESD protection and is designed to withstand standard mechanical shock and vibration, ensuring dependable performance across various environmental conditions.
Physical Size	Available in various form factors such as SIM-sized cards, chip modules, or embedded solutions.
Power Consumption	Optimized for low power consumption, suitable for battery-operated devices.
Hardware Specification	A secure microcontroller with dedicated cryptographic coprocessors, non-volatile memory for storing cryptographic keys and certificates, and physical security measures like active shields and sensors to detect and resist tampering attempts.

Incore and the Proteg logo are trademarks of Incore Innovation Sdn Bhd. All other product or service names are the property of their respective owners. © 2024 Incore Innovation Sdn Bhd.

Date of Release: July 2024
Document Number: PROTEGSAM2024R1