Billions of credentials are leaked and exposed online every year causing immense damage to organisations and individuals alike.

Cyber-criminals are capable of leveraging stolen credentials to further their illicit activities.

Why SecuriPass?

SecuriPass is the industry’s first Enterprise Solution to provide a hardware-based solution with Common Criteria certified hardware that securely encrypts and verifies your Enterprise Credentials which prevents any SecuriPass protected credentials from being tampered with while at-rest and from being usable and readable by unauthorized parties after a leak have occured.

SecuriPass spots a highly portable and scalable USB 2.0 Security Key form factor that can be clustered and automatically load-balanced.

SecuriPass also features an easy yet secure Web API for easy integration into existing Enterprise Applications and Infrastructures and also leverages a quorum of administrators to securely and easily administrate the SecuriPass solution over a remote network connection without needing to be physically present at the data center.

SecuriPass Use Cases

The SecuriPass solution is highly flexible and scalable and maybe applied in a wide range of industry setting.

E-Commerce, Banks & Financial Institutions
- PIN and password encryption at-rest requirements.
- Secure verification requirements within certified hardware.

Data, Email and Identity Service Providers
- Strong credential protection against cyber-criminals attacking huge data stores containing sensitive credentials.
- Highly cost-effective and scalable-friendly solution to provide low cost protection and aid in achieving compliance to privacy regulations (i.e. GDPR, PDPR, HIPAA).
SecuriPass Technical Specifications

Cryptographic Algorithm
• Data Encryption with AES-256
• Data Integrity with HMAC-SHA256
• Hardware Root of Trust ID with RSA-2048 (ROCA-Resistant)

Supported Operating Environment
• Windows
• VMWare

Physical Characteristics
• Length: 4.3 cm
• Weight: 5 grams

Tamper Protection Characteristics
• Tamper Resisting Secure Element
• Tamper Evident matt black body

Hardware Connectivity
• USB 2.0 over USB-CCID connection

Application Programming Interface
• HTTPS POST Web API

Throughput (per module)
• Credential Enrollment at 160 credentials / minute
• Credential Verification at 80 credentials / minute

Availability and Scalability
• Automatic load-balancing and clustering of modules for enhanced experience
Management
• Proprietary Secure Remote Administration protocol
• M-out-of-N administrator

Security Compliance
• Common Criteria EAL 5+ certified Secure Element