CKS

Cryptographic Key Server

Founded in 1997 by Professor K.Y. Lam as an advanced security R&D house in Singapore, PrivyLink is geared to meet the strong industrial demands for high-assurance delivery channels in secure electronic transactions and homeland security systems. We have established ourselves as the key innovator of strong security solutions deployed in government departments, financial institutions and corporations. Our products offer adaptive end-to-end security protection for applications and data exchanged over fixed networks and mobile channels. In addition, we have been engaged by reputable organizations to provide consulting services, security review and system design.

For more information, please visit our website at
http://www.privylink.com/ or contact us by
email: sales@privylink.com.sg

CKS

Cryptographic Key Server

Proven solution for banks, government departments and enterprises

PrivyLink's Cryptographic Key Server or CKS has been in use in many banks, government departments and enterprises. Our customers require strong data protection and user authentication for many of their mission-critical and high-value applications. Besides security, they have chosen CKS for its cost-effectiveness and scalability.

PrivyLink

tamper resistant & scalable

Hardware Security Module

CKS supports a multitude of cryptographic algorithms for both symmetric (AES, 3DES etc.) and public key (up to 4096 bits) systems. Besides strong cryptographic algorithms, administration of cryptographic keys is equally important as poor key management can easily become the weakest link in data networks. CKS implements a well-defined hierarchy of roles and rights from super-users to root administrators. No individual is able to assess sensitive data alone. Cryptographic keys are categorized as per their usages, which include keys for encrypting and decrypting data and those for protecting other cryptographic keys.

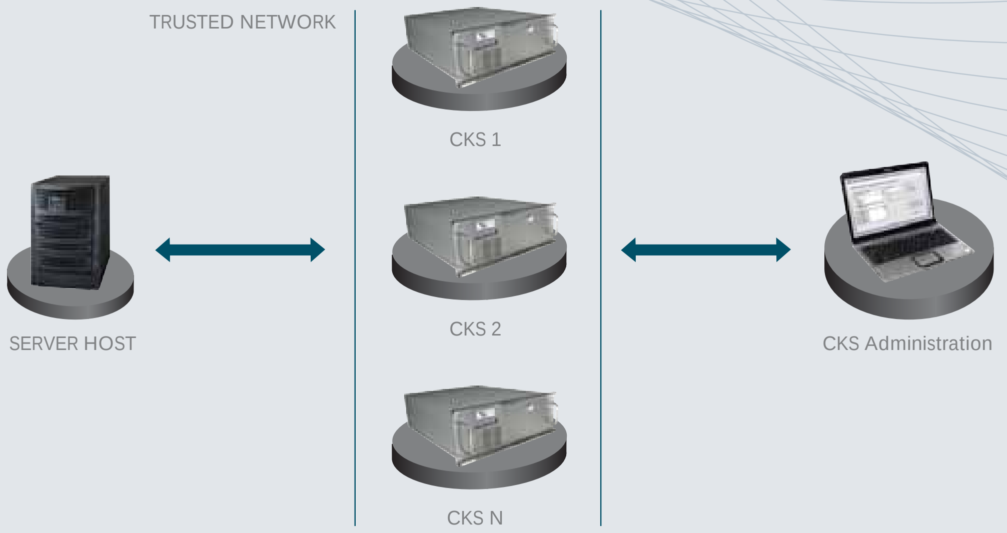
What is more, CKS carries out all these critical operations within a highly secure server that is tamper resistant against physical intrusions and other abnormalities. Upon detection of any attack or irregularity, data zeroization is performed to prevent any possible security compromise. In addition, event logging for auditing is fully supported.

In fact, CKS was the first hardware secure module product in Asia certified by US National Institute of Standards and Technology to meet the stringent Federal Information Processing Standards (FIPS).

Scalability & High Availability

CKS is administered by CKS Admin Console, an application software run from a remote workstation. A single or multiple CKS servers can be configured to serve a cluster of hosts. As a result, CKS can easily be scaled to meet application and enterprise related requirements.

For applications requiring high network resilience and system availability, two or more CKS could be configured to provide the required level of redundancy.



Applications

CKS is a powerful and dedicated cryptographic processor housed inside a tamper-resistant enclosure. Coupled with advanced key management and flexible system configuration, CKS can support a wide variety of mission-critical applications in various industrial sectors:

- Generation of digital certificates, RSA and symmetric keys
- Encryption and decryption of messages, keys and other data
- Signing and hashing operations
- Data encryption / decryption and key management for application servers hosted by certificate authorities, merchants and payment operators
- PIN generation and user authentication for e-banking applications and ATM systems
- Key management for payment cards
- PKI applications in e-commerce
- Secure electronic transactions over the Internet
- One-time-password generation for multi-factor authentication applications. The passwords can be generated from a combination of random number, bank secret key and transaction summary (i.e. transaction-specific)
- For use with PrivyLink's range of data security products such as RidgeVault^{TM} (biometric cryptography product) and Mobile-Payment.

Standard Compliance

CKS has been designed to comply with the following international standards:

- US NIST FIPS 140-1 Overall level 3 (Cert. No. 202)
- US NIST FIPS-46-3 3DES (Cert. No. 62) / DES (Cert. No. 123) Cryptographic Algorithm
- US NIST FIPS-180-1 Hashing Algorithm (Cert. No. 53)
- US NIST FIPS-197 AES Cryptographic Algorithm (Cert. No. 23)
- RSA Encryption (up to 4096 bits) & Digital Signature (PKCS#1)
- RFC 1321 MD5 Message Digest Algorithm
- ANSI X9.17 Pseudo Random Number Generator

Dimensions

Height	: 175mm
Width	: 482mm
Depth	: 538.5mm
Weight	: 29kg