hiddn | CMS

Protocols
TLS 1.2 protocol

Version
2.0.1

Operating systems
Windows 7 and 10

Package includes
CMS licence, Crypto Officer smart card User smart cards, Smart card reader

MODELS

CMS

PRODUCT FEATURES

With Hiddn's CMS the IT department can easily administrate users, keys and authentication policies.

Card Management System
Hiddn's CMS is a software application that allows the IT administrator to generate encryption keys and certificates, and to manage the various user profiles and encryption devices in an organisation.

Crypto Officer administrates the Hiddn SafeDisk using a separate Crypto Officer card.

Use case
A typical use case for the SafeDisk & CMS encryption suite is for organisations with very strict safety requirements for carrying sensitive information, e.g. a national security agency or a health care unit.

With Hiddn's CMS the SafeDisk can be customized to meet your individual or organisational demands.

CMS – managing security
When starting with a new Hiddn SafeDisk from the factory, or a zeroized module, initialization must be performed by an IT administrative having the Crypto Officer role. The initialization process is carried out once by

inserting a card loaded with the Crypto Officer initialization data. After a successful initialization the crypto module is ready for use with a User Card.

RECOMMENDED USE

Backup
Regular backups, of the computer systems and the CMS are a must for mission critical systems. Daily backups are recommended and occasional restores to check the integrity of the backups.

Secure management
It is recommended to install the CMS on a protected PC, preferably on a laptop with SafeDisk installed.

TECHNICAL SPECIFICATIONS

Operating Systems	Windows 7 and 10
DEK transfer	Transport Layer Security (TLS)
Protocols	TLS 1.2
System requirements	100 MB or more available

ADDITIONAL FEATURES

Administrator role
The administrator can define PIN and PUK policies and facilitate key escrow, a proactive solution anticipating the future need for access to keys.

Transportation of Data Encryption
KeyThe Hiddn SafeDisk uses a Data Encryption Key (DEK) to encrypt/decrypt data on a disk. The DEK is transferred to the Hiddn SafeDisk from a User smart card after the user has been authenticated. Transport Layer Security (TLS) is used to provide a secure and authenticated transfer of the DEK, and in this lies the use of a number of additional keys and digital certificates. Before the Hiddn SafeDisk can receive a DEK from a User Card, it must first be initialized by a Crypto Officer smart card. The initialization procedure will load onto the Hiddn SafeDisk a set of keys including a Key Encryption Key (KEK) that is used to decrypt the DEK received from a User Card, since the DEK itself is encrypted. Along with the keys, certificates are also loaded onto the Hiddn SafeDisk used to prove the authentication and ownership of the keys.

After the Hiddn SafeDisk has been initialized, a User Card can be produced containing a signed and encrypted file containing the DEK (keyfile) in addition to the TLS keys and the certificates corresponding to those on the Hiddn SafeDisk. Now, when the User smart card is processed by the Hiddn SafeDisk, a secure TLS link will be established over which the signed keyfile can be transferred.

hiddn | CMS

Protocols
TLS 1.2 protocol

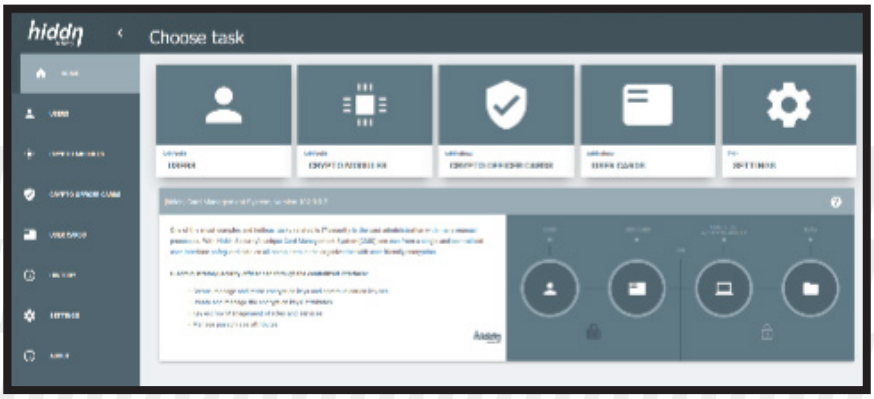
Version
2.0.1

Operating systems
Windows 7 and 10

Package includes
CMS licence, Crypto Officer smart card User smart cards, Smart card reader

MODELS

CMS



SECURITY FEATURES

HIDDN'S ADVANTAGE
DESIGNED, DEVELOPED AND ASSEMBLED IN NORWAY

GDPR-PROOF GUARANTEE

APPROVED SUPPLIER TO THE NORWEGIAN ARMED FORCES

Smart cards
Hiddn's smart cards are effectively small, secure computing devices that contain advanced key management and transfer technology. The smart cards are tamper-proofed in accordance with Common Criteria-principles for physical security (CC EAL5+).

SafeDisk - Crypto Officer card
The Crypto Officer smart card activates the Crypto Officer role and is used to initialize the Hiddn SafeDisk, and later to update relevant Critical Security Parameters (CSP). The Crypto Officer card is issued with a reference to a specific user in the CMS application.

SafeDisk - User Card
SafeDisk stores its data encryption keys on a User Card. This User Card also contains certificates required to authenticate the user. The User Card is protected by the user's PIN (or Password). For the user to access data on the encrypted storage device, two factors must exist; User Card and PIN/PUK.

Strong Two-factor Authentication
The Smart card and PIN / PUK are the two factors required to be granted access to the data. Something you have and something you know.

Hiddn's technology
The unique feature of Hiddn's solution is that the encryption key is actively deleted from the SafeDisk when the system is shut down. Instead, it is stored on a separate, tamper-proof smart card. This provides an unmatched level of security which has been approved and applied by various military, governmental and national security agencies to store highly sensitive information.