

[hiddn]TM **Crypto Adapter**

Description & Application Note

GENERAL

The **[hiddn]**TM **Crypto Adapter** is unique and provides for cost efficient encryption/decryption of thumb drives, external drives, and other USB-connected storage media!

The **[hiddn]**TM **Crypto Adapter** connects to your computer via USB. The two-factor authentication in the form of a smartcard storing all encryption keys and a PIN-code, allows for robust and easy to use protection of all your externally stored data. The **[hiddn]**TM **Crypto Adapter** is the perfect solution for transportation of data between the office and home, for travelling with sensitive data, and for working between office branches.

The **[hiddn]**TM **Crypto Module (CM)** is providing the hardware encryption, and is certified with FIPS 140-2 Level 3 and Common Criteria EAL4+ and incorporated into all **[hiddn]**TM **Crypto Adapter** units. This provides for compliant and assured data protection for all needs.



The cost of losing data is now reduced to the minimal cost of losing a low-priced thumb drive, as the **[hiddn]**TM **Crypto Adapter** demolishes the need for expensive encryption thumb drives as it encrypts unlimited capacities of any USB-connected storage media!

PRODUCT DESCRIPTION – CONFIGURATIONS & FEATURES

The **[hiddn]**TM **Crypto Adapter (CA)** can be preconfigured and/or configured to allow smartcards to be used with any **CA** within an organization (e.g. company, project, unit, etc.). Each smartcard has its unique encryption key(s) preventing USB storage media encrypted with one smartcard from being read/decrypted with another – at no point are encryption keys stored on the storage media itself or in the computer processing the data. This opens up for volume deployment of multiple **CAs** within an organization for full-disk encryption of all corporate and private USB storage devices! In the pre-configured configurations, the smartcards are programmed with sets of matching random generated keys for added security.

Organisations can configure the smartcards themselves via the optionally available **[hiddn]**TM **Key Management System (KMS)** which is normally operated (in a secure environment) by the

organisation's IT Manager, Security Manager or Personnel Manager(s) providing encryption key generation, user/smartcard/unit logging and key escrow.

The **[hiddn]™ Crypto Adapter enables a safe USB-environment** – it runs on any computer and, unlike many other “special” encryption USB devices, does not require admin-rights for the user to operate.

Standalone **[hiddn]™ Crypto Adapters (CA)** can be deployed anywhere, and e.g. one CA located in the conference room can be accessed by all authorized employees using their individual smartcards and PIN-codes. Since the CA requires no management resources, it saves costs and improves efficiency.

Deployment of **[hiddn]™ Crypto Adapters** introduces a **security culture**. By only allowing for USB storage devices to be connected through a **[hiddn]™ Crypto Adapter**, the organization is assured that these are fully encrypted at all times, regardless of content or intended usage.



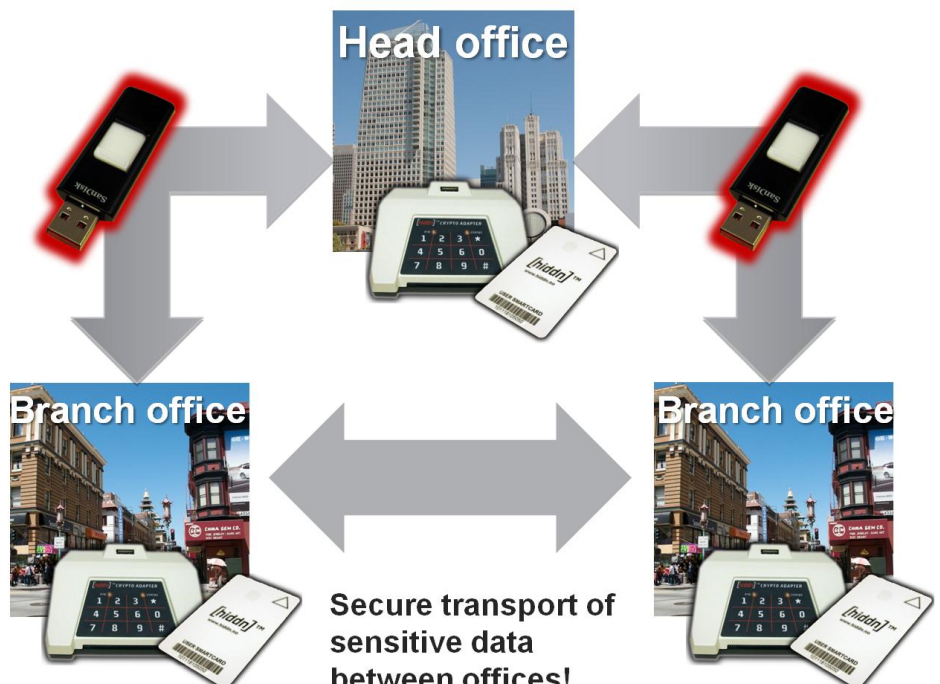
Bring your storage media and smartcard to the meeting room



Sharing of infrastructure made efficient and cost effective!

Why allow unencrypted memory sticks at all and why let employees choose what is encrypted, when you can encrypt all whilst at the same time remain efficient and productive!?

Encryption of all USB storage devices with one Crypto Adapter – data protection in practice!



The loss of an unprotected memory stick or theft of unencrypted backup data can be **devastating to business**, and being able to assure customers

and clients that their data is at all times safeguarded is of major importance. Data breaches increasingly grab media headlines, and legislation is introduced globally to ensure the interests of customers and clients are maintained.

To comply with the growing need for protection of externally stored data, organizations purchase expensive “special” encryption memory sticks and hard drives. However, these “special” memory sticks normally require training, management, access to SW/your own Laptop and support and, if lost, represent a significant cost compared to normal low cost USB memory sticks when they are replaced.

Why pay more for single units when one Crypto Adapter can replace them all and turn any of your USB storage media into fully encrypted storage media? Easily store encrypted data on any USB storage device and transport data safely to and from locations;

The [hiddn]TM CA Home & Office application note (ref. below) is an example deployment allowing for personnel to move between Crypto Adapters with only their personal smartcard and USB storage media of their own choice – more free and a far more secure manner of work.

APPLICATIONS

[hiddn]TM Crypto Adapter @ Home & Office – Enabling a safe USB-environment

The [hiddn]TM Crypto Adapter @ Home & Office application example provides for hassle-free protection of all data stored on any USB storage device! No longer worry over lost or stolen memory sticks or sensitive backup data and avoid paying excess for “special” encryption memory sticks – one [hiddn]TM Crypto Adapter turns all your USB storage devices fully encrypted and protected.

- How many memory sticks do you have lying around in your office?
- Have you ever lost any?
- Do employees store sensitive corporate data on memory sticks to bring home?
- How can you be sure they take necessary precautions to protect yours and your customers’ and clients’ data?
- What do your customers think of this? Expect?
- Do you backup your Laptop regularly, and is this backup encrypted?

Mobility and Security Combined – seamless integration.

The mobile and flexible **CA** provides the organization with effortless and standalone protection for all USB storage devices; from the small memory sticks to the high capacity corporate USB based backup drives. **CAs** can be deployed wherever protection is required, whether inside or outside the office providing **easy, cost-efficient and secure protection of sensitive data on USB storage units.**

Employees or third party personnel can easily and safely move between any number of **CA** only carrying their encrypted USB storage media and personal smartcard, and when travelling outside of the organization’s infrastructure, simply bring along a **CA** and remain protected regardless of computer used!

The [hiddn]™ Crypto Adapter is ideal for:

- Corporate Environments
- Small businesses
- Creative professions (art, advertising, film, writing, etc.) protecting IPR/works
- Healthcare
- Government
- Defence
- Lawyers
- Other
- Law enforcement (forensics, court data, etc.)
- Finance
- Offshore (secure transportation of data offshore/onshore)
- Insurance
- Home Office Environments (also protecting private data)
- Sales material (bids, price lists, etc.)



Mobility and security go hand in hand with the [hiddn]TM Crypto Adapter, and the need to carry a Laptop is now redundant, improving efficiency and easing everyday business life.



Lawyers can visit clients assuring them that all data shared remains confidential, doctors can bring patient records outside of the office without worrying over data protection, the CEO can visit the branch office carrying quarterly reports on encrypted memory sticks, and anyone else with a need to share sensitive data no longer have to worry – cost-efficient and reliable encryption for all.

For further application notes, user manuals, where to buy (global dealer network), etc., please visit www.hiddn.no.

For ordering information, table of benefits and features, please see below.

ORDERING INFORMATION

The following standard CA configurations are available:

Configuration / Deliverable	Description
[hiddn]™ Crypto Adapter	Single unit – stand-alone – 1 set of pre-configured smartcards
[hiddn]™ Crypto Adapter - SOHO	Two (2) units – paired – 2 sets of pre-configured smartcards
[hiddn]™ Crypto Adapter – Enterprise V	Five (5) units – matched – 5 sets of pre-configured smartcards
[hiddn]™ Crypto Adapter – Enterprise X	Ten (10) units – matched – 10 sets of pre-configured smartcards
[hiddn]™ Crypto Adapter – Enterprise	Single unit – 1 set (2 un-programmed cards) of smartcards
[hiddn]™ Crypto Adapter – Enterprise KMS	Customised no. of units and sets of un-programmed cards (>50 for both) with KMS for configuration of own smartcards within an organisation

If you want to make an order and/or you need another configuration, please contact our sales representatives, ref. www.hiddn.no, or send an email to: sales@hdd.no.

BENEFITS & FEATURES

More secure than software:	No encryption keys are stored on the storage media, all keys stored in the smartcard
Easy to audit:	Without the physical smartcard present, the media is inaccessible
Lower Total cost of ownership:	No annual licensing fees, no updates, and zero end-of-life disposal cost of the storage media
Works with all PCs:	Invisible to all Operating Systems, File Systems, and computer software/hardware
Security by best approach:	Passed international certification at the highest commercially viable level
Strong & secure encryption:	AES 256-bit encryption algorithm
Authentication:	Smartcard with encrypted key transfer and PIN-code. No encryption keys stored on storage media
Performance:	Transparent and real-time encryption with no delay @ 40MB/s (limited by USB-protocol)
Plug and play:	No drivers or software required

For more details: www.hiddn.no

