

## Paranoia2 - Overview

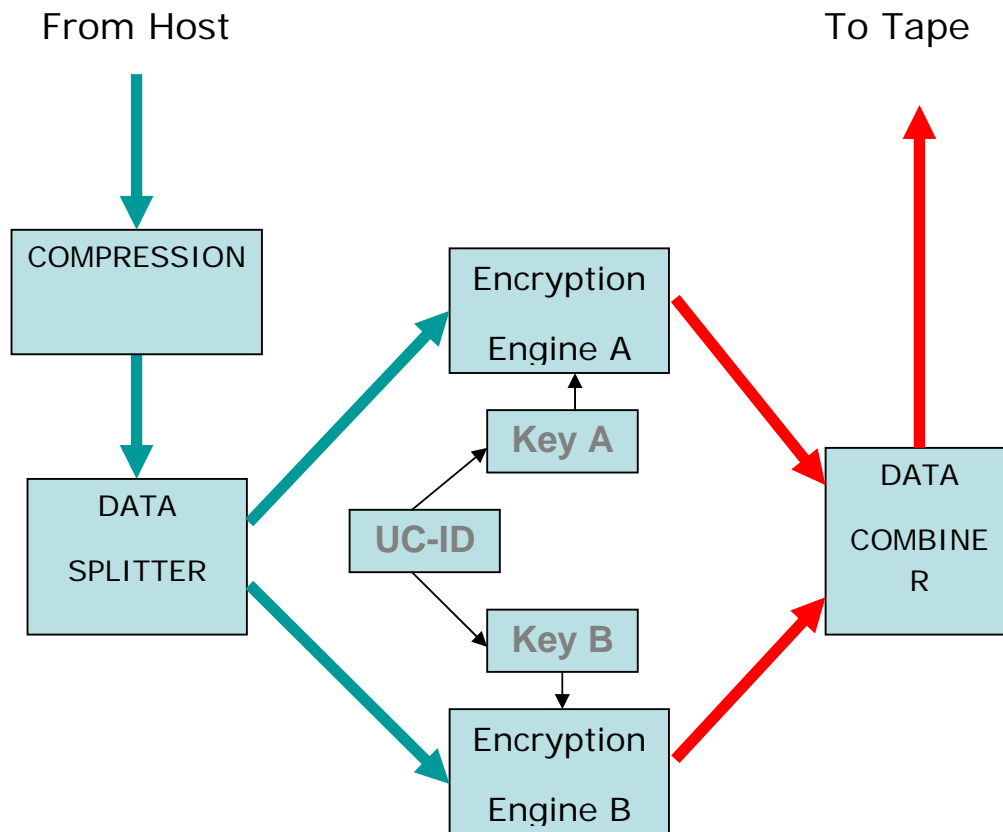
---

- A simple to use in-line, dedicated encryption appliance for removable media based on a proven second generation design.
- Available for SCSI and Fibre Channel devices
- Operationally non-intrusive - no changes to your existing operation procedures are required
- Dual encryption engines
- Unique customer ID chip (UC-ID)
- GUI configuration & management software
- Network based management option available
- On-board pre-compression to ensure tape capacity is retained
- Does not use an operating system as these are targets for malicious attacks, viruses and hacking.

### How do we encrypt data?

---

- When set in secure mode the data is first compressed as once encrypted the data will be uncompressible.
- The data is then split into two streams, each stream is then fed into a dedicated encryption engine.
- The 2 encrypted data streams are then merged together and written to tape.
- The read process is the reverse of the write process.



## Paranoia2 – Encryption Keys

- The Keys consist of 3 parts:
- 2 x user soft keys are entered into the Paranoia unit and cannot be read from the unit even by the manufacturer.
- 1 x hardware key which is unique to each customer (UC-ID).
- Each of the soft keys is blended with the hardware key to deliver the final encryption keys.
- The 2 encryption engines are then loaded with the 2 separate encryption keys.

## Justification – Cost benefits

- The cost of a unit against the cost of a loss:
  - A Paranoia2 unit costs less than £7 per day amortised over 3 years
  - Cost of a loss: Bank of New York Mellon have provided free credit monitoring and fraud insurance for over 4.5 million customers – this is estimated to be costing them over \$100K per day, this is without all the other associated costs. See tech 404 data loss calculator
- How do you justify insurance:
  - Every company must have insurance to trade. Without insurance the implications of an accident at work and the subsequent litigation would be financially catastrophic to the business.
- Compliance and passing the audit
  - Compliance is an oft maligned word amongst IT staff who may not have a vision of the business as a whole. They may not understand that if the company fails to comply or fails an audit the consequences could be severe indeed; imagine if the company can no longer process payments from VISA/MasterCard etc. – what effect would that have on your business?
- Who goes to prison if data is lost or stolen? See the article below:

## House of Lords backs data loss law change

By Nick Heath

Published: [28 April 2008](#) 16:04 BST

<http://management.silicon.com/government/0,39024677,39208916,00.htm>

Losing personal data took a step closer to becoming a criminal offence after the House of Lords backed a change in the law.

Peers supported an amendment to the criminal justice and immigration bill which would make it a criminal offence to carelessly release or lose personal data.

Full Disclosure campaign silicon.com is aiming to make businesses and government take data security more seriously. Read more here.

The amendment, proposed by Liberal Democrat Lady Miller, would make it an offence for anyone to "intentionally or recklessly disclose information" or "repeatedly and negligently" allows information to be disclosed.

The amendment must be sanctioned by the House of Commons before it can become part of the bill.

It follows calls by the Information Commissioner Richard Thomas for the criminalisation of reckless data loss earlier this year.

A Ministry of Justice spokesman said it would consider its position on making data loss a criminal offence following the Lords vote.

He said: "The government has previously acknowledged that it needs to improve trust and confidence in the arrangements to protect personal data and is currently in the process of doing this."

In light of this development, he added the government will now look at the most appropriate course of action.

The move towards outlawing the reckless loss of data follows silicon.com's campaign for full disclosure.

The issue of public data loss shot into the public eye with the HMRC's loss of 25 million people's details on two CDs, which sparked a host of revelations about missing data in government.

Last week a government-sponsored report revealed the number of security breaches had fallen by a third in the past two years but that spending on security defences had tripled over the past six years.

-----  
Copyright © silicon.com 2005

## Questions you may be asked on Paranoia2

### Q. Will the unit slow down my backup?

A. With the Paranoia2 unit this will depend on the encryption algorithm you are using and the type of data. Using Paranoia2 with older technology tapes such as DLT, DDS and LTO-1 may even increase the backup speed.

### Q. Can I use the unit with an auto loader/library/robot?

A. Yes. The Paranoia2 family can handle autoloaders.

### Q. Do I need one Paranoia2 unit for each tape drive?

A. This depends on current data throughput you are currently achieving to each tape drive you wish to encrypt. The design allows for 4 tape drives and a library to be connected to the Paranoia2. We would normally recommend that Paranoia2 is installed on a one-to-one basis, this is to deliver a “business as usual” approach to encrypting data at rest.

### Q. Can I read my tapes on any Paranoia2 Unit?

A. The Paranoia2 unit incorporates unique customer ID chip technology. So a tape written within your organization cannot be read by another company even if they have gained access to your user keys and one of your tapes.

### Q. We need to have two different people to hold half of the key each. Is this possible?

A. Yes. Using Paranoia2 you can elect to have two separate key holders, one for each of the encryption engines. These can be loaded in at any time and are held in the Paranoia2 unit.

### Q. What happens if my unit fails, have I lost all of my data?

A. No. The electronics are standard, **just your key chip is unique**. One of our engineers can replace the Paranoia2 and swap your key chip into the new unit. You then set the encryption mode, enter your user keys, and you carry on as before.

### Q. Can the user keys be read out of the Paranoia units?

A. No. The user key cannot be retrieved from the Paranoia2 unit.

### Q. Can you help me manage my user keys?

A. Yes. We have a range of key management options available for Paranoia2 to integrate seamlessly into your environment.

### Q. What happens if the unique key chip fails?

A. All units ship with a spare key chip. Should this ever need to be used you should notify us and a replacement spare can be produced and shipped to you quickly.

### Q. If my unit is stolen can the thieves read my data?

A. No. The Paranoia2 units will retain the keys and setup for a short time to cope during a short power outage. But, if the power is lost for more than 5 minutes the Paranoia2 resets the keys and configuration setting to factory defaults