advenica

SecuriRAM®

Self-erasing USB drive

USB flash drives are often used to transfer information between systems. Lack of rutines for how to use the drives introduces a risk of sensitive information getting in the wrong hands or that malware is spread between the systems. SecuriRAM changes the user behaviour to use drives as a transport media instead of storage.

USB memory for Data in Motion

SecuriRAM is a self-erasing USB drive made for transporting a limited amount of information. Its unique feature is the ability to completely erase all its content, either manually by the user or automatically after 24 hours of inactivity.

This enables companies and organisation to take control and be pro-active, limit unintentional distribution of information. With each erasure the risk of spreading virus and malicious code is significantly decreased. Typical use cases include;

Information transfer from protected to untrusted system

By performing a secure erase on SecuriRAM once the information has been transferred to the untrusted system, any existing malware will be completely erased and the device can immediately be re-used.

Information transfer from one protected system to another

Avoid inserting an "unclean" device in the protected system by performing a secure erase on SecuriRAM as soon as the intended information has been transferred. It will also eliminate the risk of exposing sensitive information to another user.

Information distribution within a protected system

When distributing data encryption keys, private keys or documents within a protected system, SecuriRAM can be securely erased directly after the information has been received to avoid unnecessary risk of exposure.

Receiving information from another person

When handing over an ordinary USB memory stick to another person that is sharing for instance an electronic presentation, possible sensitive file content can be copied to the other persons computer. By performing a secure erase on SecuriRAM before it is handed over, the risk is eliminated.

Usage

Unlike ordinary USB memory sticks, SecuriRAM information transfer is performed in a protected and controlled manner. By pressing its two buttons, SecuriRAM erases all data permanently within seconds, by zeroisation. Due to the secure erase, SecuriRAM can be re-used for all purposes, over and over again.

Benefits

- The secure erase returns SecuriRAM to an unclassified state.
- Anyone within the trusted environment may reuse SecuriRAM once a secure erase has been performed.
- Promotes a more secure behaviour with small memory size and time limited storage.
- No costs for the destruction of USB flash drives and CDR media.

Technical description

- Secure erase is performed by an internal, battery-powered processor.
- SecuriRAM uses volatile memory where every bit of information is possible to permanently erase.
  Ordinary USB memory sticks use flash memory for storage. Because of inherent properties with this technology and the "wear level algorithm" used, some data may stay permanently on chip level.
- The secure erase is achieved by over-writing the complete memory (including file table) with zeroes, a procedure called zeroisation.
- After a secure erase, the SecuriRAM is in the same state as when it left the factory.
- SecuriRAM reports a unique ID to the operating system, including its serial number, for use by a third party white listing service.
- The automatic erase timer is renewed by inserting SecuriRAM in a powered USB port.
- The 24-hour automatic erase timer can be customized on request, an action that is performed during production.

Secure erase activation

The secure erase function is activated when:

- The user presses both buttons.
- The battery voltage is low and SecuriRAM is not connected to a powered USB port.
- The automatic erase is activated after 24 hours.

Erasing USB drives

Complete erase of a USB drive, where no information remain in any part of the memory limits possible technologies. Meaning that it must not be possible to recover a single bit of information, not even in laboratory environment.

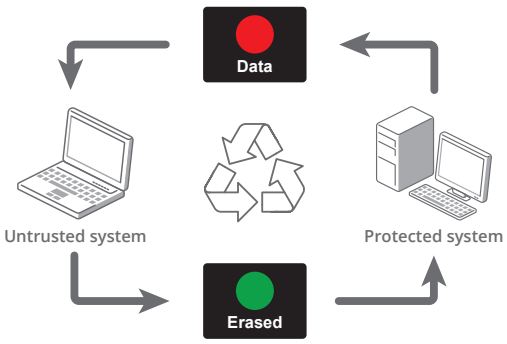
Flash memory technology

Ordinary USB sticks use flash memory. Unfortunately, with the flash memory technology it is not possible to erase all bits of data on chip level. This is because the flash memory is being worn with every write that is performed, and at some stage some memory cells will fail permanently. To accommodate this problem the flash memory chips contain more memory than is actually possible to read from and write to.

With a manufacturer specific "wear level algorithm", all memory cells are used in a way that levels the wear. This algorithm basically counts the number of writes that has been performed to every block in the memory, and when a threshold is reached the blocks are marked as "do not use anymore". These blocks of memory cells are not possible to read from the flash memory's interface, but in a laboratory environment it is possible to read information stored in every cell. This is the reason why ordinary USB sticks cannot be used with sensitive data and then securely erased. Not even excessive over-writing will solve the problem.

Memory technology in SecuriRAM

The only solution is to use another memory technology, where each and every memory cell is possible to write to from the memory's interface. The SDRAM memory technology used in SecuriRAM is one of the best memory technologies for this purpose.



Technical specification

Parameter	*Value*
Memory capacity	64 MByte
USB standard	2.0
File format	FAT
Automatic erase	24 hours
Temperature range	-10°C - +60°C
Size (incl. USB contact)	30 x 73 x 13 mm
Order code	BSF-SR13956A

Doc. no.: 13945v2.0

ISO 9001 CERTIFIED
ISO 14001 CERTIFIED