

Everywhere you turn today you can see USB flash drives in use. Employees are becoming more and more mobile. With the increased use of USB flash drives, the risk of sensitive information walking out your front door and into the wrong hands is increasing dramatically. Even if the memory content has been thoroughly over-written, there is a risk that some, or all, of the data can be recovered.



Unlike ordinary USB flash drives, 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.

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.

## 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.

## Information transfer from one protected system to another

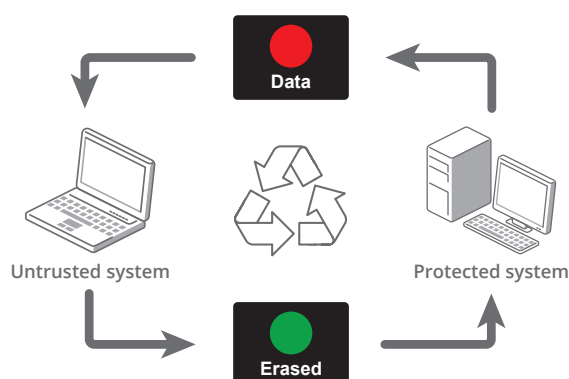
Avoid inserting an “unclean” device in the protected system by performing a secure erase on SecuriRAM as soon as the intended information has been transferred. It will also eliminate the risk of exposing sensitive information to another user.

## Information transfer from protected to untrusted system

When an ordinary USB flash drive is used in an untrusted system there is a risk of contamination (malware). By

## Travel with sensitive information

In case of an emergency, all data on the SecuriRAM can be quickly and securely erased by simultaneously pressing the two buttons. There is no need for tools or other equipment to destroy the device.



## 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 flash drive 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.

### About Advenica

Advenica is a leading European provider of cybersecurity. Advenica develops, manufactures and sells advanced cybersecurity solutions that prevent intrusions, theft and data leakage at information exchanges and therefore enables interaction between and within nations, organisations and systems with high security requirements. Cybersecurity made easy. Read more at [www.advenica.com](http://www.advenica.com).

### 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 flash drives 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.

### 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.

*Further details available upon request.*

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