integral™

Crypto

AES 256-BIT HARDWARE ENCRYPTED
USB FLASH DRIVES & SSD
Integral Crypto AES 256-bit hardware encrypted USB Drives

USB Flash Drive security is a challenge facing all IT departments and with many governments starting to impose hefty fines, encryption of sensitive data on USB drives is becoming compulsory.

Integral produce a range of AES 256-bit hardware encrypted USB Flash Drives that provide an easy to use, cost effective and highly secure solution that is designed to work with your end-point security.

Our Crypto Drive USB range is FIPS and CESG validated and all models have a zero footprint, so no software installation is required. All files transferred to the drive are automatically encrypted and are protected by a mandatory high-strength password. If the Crypto USB is ever lost or stolen, the drive will securely destroy all data after six failed password attempts.

Crypto Drives are used and trusted worldwide by government departments, global corporations and SMEs.

The Integral Crypto DUAL and DUAL+ offer an optional master password override, in addition to a high-strength user password. If a user forgets their password the Crypto DUAL and DUAL+ drives can be accessed with a master password by an IT administrator.

Crypto DUAL is also compatible with both Windows® and Mac® operating systems. Crypto DUAL+ includes the same features as the Crypto DUAL but in an expanded design, to allow for greater storage capacity, starting at 64GB and 128GB.

Crypto Drive range - User Features

AES 256-bit Hardware Encryption

AES 256-bit hardware encryption provides superior security over software encryption. Password comparisons are securely processed on the Crypto hardware.

Mandatory Encryption

All files transferred to the drive are encrypted. A user cannot save unprotected files.

Secure Entry

Encrypted data cannot be accessed without the correct high-strength 8-16 character alphanumeric password. An optional password hint can be set-up which cannot be the same as the password. Before use a high-strength password must be set.

Password Entry Count

The Crypto Drive records the failed entry count. e.g. if the Crypto is removed after 2 failed attempts and reinserted, the drive will resume with the 3rd attempt.

Brute-Force Password Attack Protection

Encrypted data is automatically erased after 6 failed password attempts. The data and encryption key are securely destroyed and the Crypto Drive is reset and can be reused.

Auto Lock

The Crypto drive will automatically encrypt all data and lock; when the drive is removed from the PC, when the screen-saver or “computer lock” function is activated.

Additionally for the Crypto Dual and Dual+ the drive will lock if left idle for more than 10 minutes.

www.integralmemory.com
An administrator can set up an optional master password on a drive. A user then sets a user password as normal. A warning is given to the user after the fifth failed password attempt to take the drive to the administrator to unlock the drive by using the master password. The user and master password cannot be the same.

Available on Crypto Dual and Crypto Dual+.

**Dual Password**

An administrator can set up an optional master password on a drive. A user then sets a user password as normal. A warning is given to the user after the fifth failed password attempt to take the drive to the administrator to unlock the drive by using the master password. The user and master password cannot be the same.

Available on Crypto Dual and Crypto Dual+.

**Rugged triple-layer waterproof design**

Protects the Crypto Drive against knocks, drops, break-in and submerging in water. The electronics are sealed in epoxy resin and then shielded by a steel inner case. The rubberised silicone outer casing provides a final layer of protection.

Up to 4 ft. water; conforms to IEC 60529 IPX8.

**Multilingual interface**

Simple multilingual interface for "out of the box" use with minimal support; ideal for global corporations.

**Zero Footprint**

Crypto Drive has a zero footprint - No software installation is required before use.

**Personal ID Function**

As an option, contact details can be added to the Crypto that can be viewed without compromising encrypted data.

**Serial Number**

The USB pin on each drive is etched with a unique 7-digit code. This allows a record to be kept of which drive has been allocated to a specific user.

**OS Compatibility**

The Integral Crypto is available in separate PC and Mac editions. The Integral Crypto Dual and Dual+ are compatible with PCs and Macs (Windows XP/Vista/7 & Mac OS X).

**User Manual**

User manual stored on drive.

**FIPS 140-2 Level 2 Validated**

- Cert No: 1424 FIPS 197 Cert No: 1137

Individually and stringently tested for data encryption and protection to the Federal Information Processing Standards (FIPS) managed by NIST (National Institute of Standards and Technology).

**CESG Claims Tested Mark (CCTM)**

- Cert No: 2011 05 0097

Crypto Drives have been awarded the CESG Claims Tested Mark (CCTM) by CESG, the UK Government’s National Technical Authority for Information Assurance. Public sector buying confidence is assured.

**Unique ID (Optional)**

Crypto Drives can be personalised with a designated company identifying name or number. This will allow a Network Administrator to block access to unrecognised USBs for security purposes, whilst allowing the Integral encrypted Flash Drive to function as the ‘official’ company drive.

**Customisation (Optional)**

Customisation Available - Your own serial number etching, Flash Drive and GUI can be customised to suit your brand (subject to minimum order quantities).

www.integralmemory.com
# Integral Encrypted USB Product Range

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Available Capacities</strong></td>
<td>2GB, 4GB, 8GB, 16GB, 32GB</td>
<td>2GB, 4GB, 8GB, 16GB, 32GB</td>
<td>2GB, 4GB, 8GB, 16GB, 32GB</td>
<td>2GB, 4GB, 8GB, 16GB, 32GB</td>
<td>64GB, 128GB</td>
<td>64GB, 128GB</td>
<td>64GB, 128GB</td>
<td>64GB, 128GB</td>
</tr>
<tr>
<td>AES 256-bit hardware encryption</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>FIPS Validation</td>
<td>140-2 Level 2</td>
<td>140-2 Level 2</td>
<td>197</td>
<td>197</td>
<td>197</td>
<td>197</td>
<td>140-2 Level 2</td>
<td>140-2 Level 2</td>
</tr>
<tr>
<td>CESG Claims Tested Mark (CCTM)</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Mandatory encryption of all files</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Zero Footprint - No software required</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Compatible with Endpoint security software</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Works on Windows without administrator privileges</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Works on Mac OS X without administrator privileges</td>
<td>-</td>
<td>✓</td>
<td>-</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Secure Entry - Password Mandatory</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>High-Strength Password Enforcement</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Brute-Force Password Attack Protection</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Auto-Lock</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Password Entry Count</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Personal ID Function</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Rugged triple-layer waterproof design</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>User manual stored on drive</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Multi-lingual Interface</td>
<td>24 Languages</td>
<td>6 Languages</td>
<td>24 Languages</td>
<td>6 Languages</td>
<td>26 Languages</td>
<td>26 Languages</td>
<td>26 Languages</td>
<td>26 Languages</td>
</tr>
<tr>
<td>Dual Password</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Dual OS - PC &amp; Mac compatible</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>4 Channel access (faster read &amp; write speeds)</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Serial Number Etching</td>
<td>Available on request</td>
<td>Available on request</td>
<td>Available on request</td>
<td>Available on request</td>
<td>Available on request</td>
<td>Available on request</td>
<td>Available on request</td>
<td>Available on request</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>2GB</td>
<td>INFD02GCRYPTO140-2</td>
<td>32GB</td>
<td>INFD32GCRYPTO140-2</td>
<td>2GB</td>
<td>INFD02GCRYPTO197</td>
<td>16GB</td>
<td>INFD16GCRYPTO197</td>
<td>4GB</td>
<td>INFD04GCRYPTO140-2</td>
<td>4GB</td>
<td>INFD04GCRYPTO197</td>
<td>4GB</td>
<td>INFD04GCRYPTO197</td>
<td>8GB</td>
<td>INFD08GCRYPTO197</td>
<td>8GB</td>
<td>INFD08GCRYPTO197</td>
<td>16GB</td>
<td>INFD16GCRYPTO197</td>
<td>16GB</td>
<td>INFD16GCRYPTO197</td>
</tr>
<tr>
<td>4GB</td>
<td>INFD04GCRYPTO140-2</td>
<td>4GB</td>
<td>INFD04GCRYPTO197</td>
<td>4GB</td>
<td>INFD04GCRYPTO197</td>
<td>4GB</td>
<td>INFD04GCRYPTO197</td>
<td>4GB</td>
<td>INFD04GCRYPTO197</td>
<td>128GB</td>
<td>INFD128GCRYPTO197</td>
<td>128GB</td>
<td>INFD128GCRYPTO197</td>
<td>128GB</td>
<td>INFD128GCRYPTO197</td>
<td>128GB</td>
<td>INFD128GCRYPTO197</td>
<td>128GB</td>
<td>INFD128GCRYPTO197</td>
<td>128GB</td>
<td>INFD128GCRYPTO197</td>
</tr>
<tr>
<td>8GB</td>
<td>INFD08GCRYPTO140-2</td>
<td>8GB</td>
<td>INFD08GCRYPTO197</td>
<td>8GB</td>
<td>INFD08GCRYPTO197</td>
<td>8GB</td>
<td>INFD08GCRYPTO197</td>
<td>8GB</td>
<td>INFD08GCRYPTO197</td>
<td>8GB</td>
<td>INFD08GCRYPTO197</td>
<td>8GB</td>
<td>INFD08GCRYPTO197</td>
<td>8GB</td>
<td>INFD08GCRYPTO197</td>
<td>16GB</td>
<td>INFD16GCRYPTO197</td>
<td>16GB</td>
<td>INFD16GCRYPTO197</td>
<td>16GB</td>
<td>INFD16GCRYPTO197</td>
</tr>
<tr>
<td>16GB</td>
<td>INFD16GCRYPTO140-2</td>
<td>16GB</td>
<td>INFD16GCRYPTO197</td>
<td>16GB</td>
<td>INFD16GCRYPTO197</td>
<td>16GB</td>
<td>INFD16GCRYPTO197</td>
<td>16GB</td>
<td>INFD16GCRYPTO197</td>
<td>16GB</td>
<td>INFD16GCRYPTO197</td>
<td>16GB</td>
<td>INFD16GCRYPTO197</td>
<td>16GB</td>
<td>INFD16GCRYPTO197</td>
<td>32GB</td>
<td>INFD32GCRYPTO197</td>
<td>32GB</td>
<td>INFD32GCRYPTO197</td>
<td>32GB</td>
<td>INFD32GCRYPTO197</td>
</tr>
<tr>
<td>32GB</td>
<td>INFD32GCRYPTO140-2</td>
<td>32GB</td>
<td>INFD32GCRYPTO197</td>
<td>32GB</td>
<td>INFD32GCRYPTO197</td>
<td>32GB</td>
<td>INFD32GCRYPTO197</td>
<td>32GB</td>
<td>INFD32GCRYPTO197</td>
<td>32GB</td>
<td>INFD32GCRYPTO197</td>
<td>32GB</td>
<td>INFD32GCRYPTO197</td>
<td>32GB</td>
<td>INFD32GCRYPTO197</td>
<td>32GB</td>
<td>INFD32GCRYPTO197</td>
<td>32GB</td>
<td>INFD32GCRYPTO197</td>
<td>32GB</td>
<td>INFD32GCRYPTO197</td>
</tr>
</tbody>
</table>

www.integralmemory.com
Protect your data with an encrypted Integral Crypto SSD

The Integral Crypto SSD is the ideal solution for data protection. When the system is shut down, 256-bit full disk encryption is instigated.

If a PC or laptop with an Integral Crypto SSD installed is lost or stolen, sensitive data is secure and cannot be accessed without the high-strength password.

Crypto SSD is the no-fuss and highly-secure solid state encryption solution for many industries including: finance, legal, health, education and government.

A direct replacement for a laptop’s Hard Drive/SSD. Fits easily into any desktop PC using a fitting kit*.

*Supplied separately

Product Features

- Full 256-bit AES Hardware Encryption
- Dual password – User and Administrator override
- Hardware tied to computer when encryption is set
- Brute-force attack protection
- Anti-cloning when encryption is set
- Offers better protection than software encryption, as the data is hardware encrypted on the SSD drive
- No performance degradation when encryption is activated (compared to conventional SSD)
- High-speed sustained data transfer. Read and Write times up to 240MB/s
- No moving parts, greater resistance to shock and vibration
- Noise free, no spin or seek time
- Cuts boot time in half
- Weighs less than conventional HDD
- Uses 1/10 of the power of a normal spinning disk HDD
- Extends laptop battery life
- Super low power consumption during operation and sleep modes

Technical Features

- MLC-NAND Flash Technology
- SATA II 2.5"
- SATA Revision 2.6 compliant
- TRIM option
- S.M.A.R.T. option
- Power management supported
- 128MB DDR Cache Buffer
- CE and FCC certified and RoHs compliant
- Compatible with XP, Vista and 7

Specifications

<table>
<thead>
<tr>
<th>PERFORMANCE &amp; INTERFACE</th>
<th>Read</th>
<th>240MB/s (max)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Write</td>
<td>220MB/s (max)</td>
</tr>
<tr>
<td>Interface</td>
<td>SATA II (SATA 1.5Gbps and 3Gbps)</td>
<td></td>
</tr>
<tr>
<td>RELIABILITY</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wear levelling</td>
<td>Static &amp; Dynamic</td>
<td></td>
</tr>
<tr>
<td>MTBF</td>
<td>1,000,000 hours</td>
<td></td>
</tr>
<tr>
<td>ECC</td>
<td>48/32/28 bit per 2KB</td>
<td></td>
</tr>
<tr>
<td>Data Retention</td>
<td>10 years</td>
<td></td>
</tr>
<tr>
<td>POWER CONSUMPTION</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Power requirement</td>
<td>5V</td>
<td></td>
</tr>
<tr>
<td>Read Mode</td>
<td>1.4W*</td>
<td></td>
</tr>
<tr>
<td>Write Mode</td>
<td>4.7W*</td>
<td></td>
</tr>
<tr>
<td>Sleep Mode</td>
<td>0.2W</td>
<td></td>
</tr>
<tr>
<td>ENVIRONMENTAL</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operating Temp</td>
<td>0° - +70°C</td>
<td></td>
</tr>
<tr>
<td>Non - Operating Temp</td>
<td>-40° - +85°C</td>
<td></td>
</tr>
<tr>
<td>Humidity</td>
<td>RH=95% under 55°C</td>
<td></td>
</tr>
<tr>
<td>Vibration</td>
<td>20G (80-2000Hz)</td>
<td></td>
</tr>
<tr>
<td>Shock</td>
<td>1,500G (0.5msec)</td>
<td></td>
</tr>
<tr>
<td>PHYSICAL</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Length</td>
<td>100.1mm</td>
<td></td>
</tr>
<tr>
<td>Width</td>
<td>69.9mm</td>
<td></td>
</tr>
<tr>
<td>Height</td>
<td>9.3mm</td>
<td></td>
</tr>
<tr>
<td>Weight</td>
<td>76(g)</td>
<td></td>
</tr>
<tr>
<td>WARRANTY</td>
<td>2 Years</td>
<td></td>
</tr>
</tbody>
</table>

www.integralmemory.com
**Crypto SSD - User Features**

**AES 256-bit Hardware Encryption**
AES 256-bit hardware encryption provides superior security over software encryption. Password comparisons are securely processed on the Crypto SSD.

**Total Drive Encryption**
All data stored on the Crypto SSD is encrypted (including the Operating System).

**Secure Entry**
Encrypted data cannot be accessed without the correct high-strength 8-16 character alphanumeric password. An optional password hint can be set-up which cannot be the same as the password. Before use a high-strength password must be set.

**Dual Password**
As an option an Administrator can setup a user password and a master override password. If the user forgets their password, the Crypto SSD can be unlocked by the Administrator and the user password reset.

**Rugged Design**
The electronics are sealed in tamper-free epoxy resin and then shielded by a steel outer case.

**Brute-Force Password Attack Protection**
Encrypted data is automatically erased after the default 6 failed password attempts (password attempts configurable to a maximum of 20). The data and encryption key are securely destroyed and the Crypto SSD is reset and can then be reused.

**FIPS 197 Certified**
Independently and stringently tested for data encryption and protection to the Federal Information Processing Standards (FIPS) managed by NIST (National Institute of Standards and Technology).

**High-speed Read/Write**
The Crypto SSD has both high encryption and the main benefit of a standard SSD; a high-speed sustained data transfer rate. Read and Write times are up to 240MB/s.

**AES 256-bit Hardware Encryption**
Using a Crypto SSD in place of a traditional HDD can cut your desktop computer or laptop's boot time in half.

**Multilingual interface**
Simple multilingual interface for “out of the box” use with minimal support; ideal for global corporations.

---

**Product Ordering Information**

<table>
<thead>
<tr>
<th>CAPACITY</th>
<th>PRODUCT</th>
<th>PART NUMBER</th>
</tr>
</thead>
<tbody>
<tr>
<td>32GB</td>
<td>Crypto SSD</td>
<td>INSSD32GS25MCRYPTO</td>
</tr>
<tr>
<td>64GB</td>
<td>Crypto SSD</td>
<td>INSSD64GS25MCRYPTO</td>
</tr>
<tr>
<td>128GB</td>
<td>Crypto SSD</td>
<td>INSSD128GS25MCRYPTO</td>
</tr>
<tr>
<td>256GB</td>
<td>Crypto SSD</td>
<td>INSSD256GS25MCRYPTO</td>
</tr>
</tbody>
</table>

1GB = 1,000,000,000 bytes. Formatted capacity is less. Custom ID and pre-loaded content are available on request.

www.integralmemory.com
Solid State Encrypted Solutions

Head Office
Integral Memory Plc
Unit 6 Iron Bridge Close
Iron Bridge Business Park
London
NW10 0UF
England
Tel: +44 20 8451 8700
Fax: +44 20 8459 6301
www.integralmemory.com

USA
Integral Memory Inc
503 Faulconer Dr
Suite 1A
Charlottesville, VA 22903
USA
Tel: 434-200-8685
Toll Free: 855-436-2797 (855-4ENCRYPT)
Fax: 434-200-8424
www.integralmemoryusa.com
salesusa@integralmemory.com

France
Integral Europe SARL
38 Ter Rue de Verdun
92150 Suresnes
France
Tel: +33 1 41 44 73 00
Fax: +33 1 41 44 07 18
www.integralmemory.com
salesfr@integraleurope.com

Spain
Integral Memory España, S.A.
Calle Juan Perez Zuniga, 32
28027 Madrid
Spain
Tel: +34 91 406 29 32
Fax: +34 91 377 55 40
www.integralmemory.com
sales@integraleurope.com

Dubai
Office Number 1
High Bay Building
Dubai Silicon Oasis Authority
PO Box 341128
Dubai, UAE
Tel: +971 4 326 3446
Fax: +971 4 326 3447
www.integralmemory.com
salesmea@integralmemory.com

Netherlands
Integral Memory plc
Burgemeester Brandstraat 2
2841 XC Middelburg
The Netherlands
Tel: +31 18 23 77240
Fax: +31 18 23 77241
www.integralmemory.com
sales@integraleurope.com

Representative Offices
Poland
M: +48 60 244 3002
piotr.chrzanowski@integralmemory.com

Portugal
Tel: +35 1 210 819 012
M: +35 1 912 441 144
sobrinho.pires@integraleurope.com

Australia & New Zealand
Tel: +61 243 424 861
M: +61 406 061 437
duncan.way@integralmemory.com

INCRYPT0411