IBM FlashCore Module
Cryptographic Erase
For use with the IBM FlashSystem 9100 and the IBM Storwize V7000

Matt Smith
Statement on Cryptographic Erasure

IBM® FlashCore Modules (FCMs) are storage devices that come in 4.8TB, 9.6TB and 19.2TB capacities. They are a 2.5” drive form factor device and use second generation 3D triple-level cell (TLC) flash memory on which to store data.

This paper details the cryptographic erasure of data stored on these devices when used in an IBM FlashSystem® 9100 (9846-AF7, 9846-AF8, and 9848-AF7, 9848-AF8, 9848-UF7, 9848-UF8) or IBM Storwize® V7000 (2076-724, 2076-U7B)

The cryptographic erasure process described within this paper is designed to meet the requirements set out in NIST SP 800-88, Appendix D available at:


Each FCM is a Self-Encrypting Drive (SED), where a unique media encryption key (MEK) exists on the device itself and is used to encrypt any data written to the drive. To read data back from device the same unique key is required to decrypt the data.

In the IBM FlashSystem 9100 and IBM Storwize V7000 products, where FCMs are being used, a unique MEK is created when the FCM device is added to a RAID array. Data written to and read from the device will use this and only this key to encrypt and decrypt data.

The generation of the MEK is done using an SP 800-90A dynamic random bit generator (DRBG), and encryption is performed using XTS-AES-256. IBM has obtained FIPS 140-2 certification for the IBM FlashCore® Modules as shown at:


When the FCM is used in the IBM FlashSystem 9100 or IBM Storwize V7000 it uses two partitions. The first partition is used to store encrypted client data. A smaller, second 1GB partition is used to store unencrypted system configuration data for recovery. No client data is stored on the second partition.

To achieve a cryptographic erase, the MEK and the wrapped key structure where the MEK is stored must be overwritten to ensure the encrypted data on the drive cannot be decrypted. The process for doing this is detailed in the following section.

One of the steps in the cryptographic erasure process is to add the FCM device into the new array. As part of adding the FCM device into a new array, a new MEK is generated using a DRBG and placed in the same location as the old keys. If the generation of a new key fails,
then the device will not be added into the array and should not be considered as cryptographically erased.

To ensure the integrity of an MEK, the FCM device does not support escrow or injection of the MEK at or below the level of the sanitization operation. An MEK is generated internally to the FCM device and never leaves it. FCMs do not support export of a MEK for key escrow. FCMs do not support import of a random number from outside the FCM to be used as a MEK (i.e. key inject).

The FCM devices should only be cryptographically erased within a supported IBM FlashSystem 9100 or IBM Storwize V7000 using the process described. There is no direct support for cryptographic erase via the FCM device NVMe interface.

This paper only covers FCMs. Other drives found within an IBM FlashSystem 9100 or IBM Storwize V7000 do not have FIPS 140-2 certification. If the Easy Tier® function is used between FCMs and other drives, consider that the other drives are not certified to the same level but may still contain client data.

### Process for Cryptographic Erasure

The process described is for mass cryptographic erasure of multiple FCMs that are already in use in a Storage Pool. Before starting you should ensure that all FCMs are shown as online otherwise we won't be able to delete the MEKs.

Using the GUI, ensure that encryption is enabled as shown in Figure 1.

![Figure 1 Ensure encryption is enabled](image)

Navigate to the Pools screen and locate the Storage Pool (or Pools) that contain the FCMs. Select the Delete option to remove the FCMs from the Pool as shown in Figure 2 on page 3.
Using the same screen, select the Create option, ensuring encryption is enabled. This will create a new Storage Pool into which you can add the FCM devices as shown in Figure 3.

Then select the Storage Pool you've just created and click Add Storage. FCM devices are classified as internal storage, so select Internal and add the same set of FCM devices that you removed from the previous Storage Pool into this new Storage Pool as shown in Figure 4 on page 4.
A dialog will appear that shows the FCM devices being added to the pool. Assuming that the task completes successfully, this will have written new MEKs to the FCMs over the location of the old keys and the cryptographic erase will be complete as shown in Figure 5.
You can validate the steps above by using the Audit Log. You'll see an entry for remove pool (rmmdiskgrp), followed by an entry for create pool (mkmdiskgrp) and then an entry for adding the FCMs to the pool (mkdistributedarray) as shown in Figure 6.

![Audit Log](image)

**Figure 6  Validating the steps using the Audit Log**

It's not possible to confirm using the GUI that the set of FCM devices that have been removed were the set of FCMs that were added back into the pool. However, if you're doing a mass cryptographic erase of all FCMs in the system, then you can add them all back into the new pool and confirm that the `-drivecount` parameter on the command `mkdistributedarray` matches the number of drives in the system.

**Authors**

This paper was produced at IBM Hursley, UK.

**Matt Smith** is a FlashSystem Offering Manager with responsibility for the FlashSystem V9000 and FlashSystem 9100.

Thanks to the following people for their contributions to this project:

Bill Scales  
**IBM Hursley**

Paul Cashman  
**IBM Hursley**

Brent Yardley  
**IBM Oregon**

This project was managed by:

**Jon Tate**  
**IBM ITSO**

**Now you can become a published author, too!**

Here's an opportunity to spotlight your skills, grow your career, and become a published author—all at the same time! Join an IBM Redbooks residency project and help write a book in your area of expertise, while honing your experience using leading-edge technologies. Your efforts will help to increase product acceptance and customer satisfaction, as you expand your network of technical contacts and relationships. Residencies run from two to six weeks in length, and you can participate either in person or as a remote resident working from your home base.

Find out more about the residency program, browse the residency index, and apply online at:
Stay connected to IBM Redbooks

- Find us on Facebook:
  http://www.facebook.com/IBMRedbooks
- Follow us on Twitter:
  http://twitter.com/ibmredbooks
- Look for us on LinkedIn:
  http://www.linkedin.com/groups?home=&gid=2130806
- Explore new Redbooks publications, residencies, and workshops with the IBM Redbooks weekly newsletter:
- Stay current on recent Redbooks publications with RSS Feeds:
  http://www.redbooks.ibm.com/rss.html
Notices

This information was developed for products and services offered in the US. This material might be available from IBM in other languages. However, you may be required to own a copy of the product or product version in that language in order to access it.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user’s responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:
IBM Director of Licensing, IBM Corporation, North Castle Drive, MD-NC119, Armonk, NY 10504-1785, US

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you provide in any way it believes appropriate without incurring any obligation to you.

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Statements regarding IBM’s future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to actual people or business enterprises is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided “AS IS”, without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.
Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at “Copyright and trademark information” at http://www.ibm.com/legal/copytrade.shtml

The following terms are trademarks or registered trademarks of International Business Machines Corporation, and might also be trademarks or registered trademarks in other countries.

<table>
<thead>
<tr>
<th>Easy Tier®</th>
<th>IBM FlashSystem®</th>
<th>Storwize®</th>
</tr>
</thead>
<tbody>
<tr>
<td>IBM®</td>
<td>Redbooks®</td>
<td></td>
</tr>
<tr>
<td>IBM FlashCore®</td>
<td>Redbooks (logo)®</td>
<td></td>
</tr>
</tbody>
</table>

The following terms are trademarks of other companies:

Other company, product, or service names may be trademarks or service marks of others.