

TECHNOLOGY BRIEF

Intel® Solid-State Drive 520 Series

Non-Volatile Memory Storage Solutions from Intel



Data security features in the Intel® Solid-State Drive 520 Series

Enhanced security features for your peace of mind



As Solid-State Drives become the storage of choice for PCs worldwide, professionals and consumers are requiring enhanced security features to help protect their data. Today's security environment requires multiple tiers of protection. While one tier helps protect against malicious software attacks, another tier addresses the physical protection of stored data in the event that a PC is lost or stolen.

Intel continues to support enhanced security features in its latest generation of Solid-State Drives (SSD). This technology brief describes how the Intel® SSD 520 Series uses the Advanced Encryption Standard (AES) and ATA drive password to help protect a user's data.

Encryption in the Intel SSD 520 Series

Encryption converts data to an unintelligible form. The only way to decrypt the data to its original form is by the use of a special key.

The Intel SSD 520 Series offers this encryption/decryption feature according to the Advanced Encryption Standard (AES). The AES encryption standard, defined in the Federal Information Processing Standards (FIPS) Publication 197, is widely accepted and used in the PC industry for encryption of user data.

Physical Security Layer of Protection

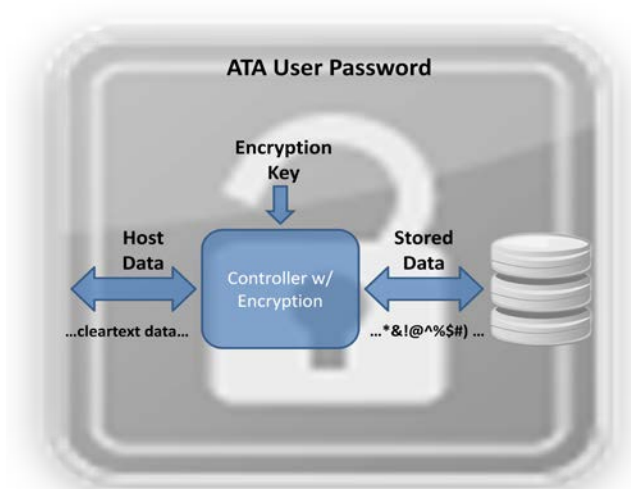
AES implementation in the Intel SSD 520 Series provides a hardware-based mechanism for encryption and decryption of user data without performance impact.

Encryption is only as good as the key used for the encrypting. The key is a packet of information that is used in the encryption process to encode/decode the data. If a person does not have this key, then the data cannot be deciphered and understood. The stronger the key, the more difficult it is for an attacker to break the key and decode the data. The AES implementation in the Intel SSD 520 Series drive uses a 128-bit key.

Each Intel SSD 520 Series has a unique key when it leaves the factory. The user can simply start using the SSD and data is encrypted with that unique key.

However, if the user prefers a new key, one can be generated by executing a Secure Erase or Enhanced Secure Erase on the SSD. Secure Erase and Enhanced Secure Erase are part of the security features in the ATA ACS2 specification, administered by Technical Committee T13 of the International Committee on Information Technology Standards (INCITS). Secure Erase can be performed using the Intel® Solid-State Drive Toolbox. Download the Intel SSD Toolbox, free of charge, at: www.intel.com/go/ssdtoolbox.

To complete the physical security layer of protection, encryption needs to be paired with an ATA user password (also known as the drive password). The drive password is a security feature of the ATA specification. Unlike encryption, which is automatically enabled on the Intel SSD 520 Series, the drive password must be set by the user via the BIOS configuration. (For more information on setting the drive password, check the computer documentation or contact the computer manufacturer customer support.) The drive password is required each time the drive is powered on, so authentication is required by the user to access data on the drive.



Added Peace of Mind

In the event that a PC without encryption and a drive password is accidentally lost or stolen, the data is not protected and anyone who can access the media can read out the data. The Intel SSD 520 Series is equipped with AES encryption that, when paired with a user-selected drive password, can give you an important security advantage. Encryption in the Intel SSD 520 Series works out-of-the box, and once you enable the drive password, you can have the confidence and peace of mind that your data is being safeguarded by these security measures.

Solid-State Computing Starts with Intel Inside®. For more information, visit www.intel.com/go/ssd

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT.

UNLESS OTHERWISE AGREED IN WRITING BY INTEL, THE INTEL PRODUCTS ARE NOT DESIGNED NOR INTENDED FOR ANY APPLICATION IN WHICH THE FAILURE OF THE INTEL PRODUCT COULD CREATE A SITUATION WHERE PERSONAL INJURY OR DEATH MAY OCCUR.

Intel may make changes to specifications and product descriptions at any time, without notice. Designers must not rely on the absence or characteristics of any features or instructions marked "reserved" or "undefined." Intel reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them. The information here is subject to change without notice. Do not finalize a design with this information.

The products described in this document may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request.

Contact your local Intel sales office or your distributor to obtain the latest specifications and before placing your product order.

Copies of documents which have an order number and are referenced in this document, or other Intel literature, may be obtained by calling 1-800-548-4725, or go to: <http://www.intel.com/design/literature.htm>

Intel and the Intel logo are trademarks of Intel Corporation in the U.S. and other countries.

*Other names and brands may be claimed as the property of others.

Copyright © 2012 Intel Corporation. All rights reserved.

Printed in USA 6/2012/SB/PDF

Please Recycle

327564-001US