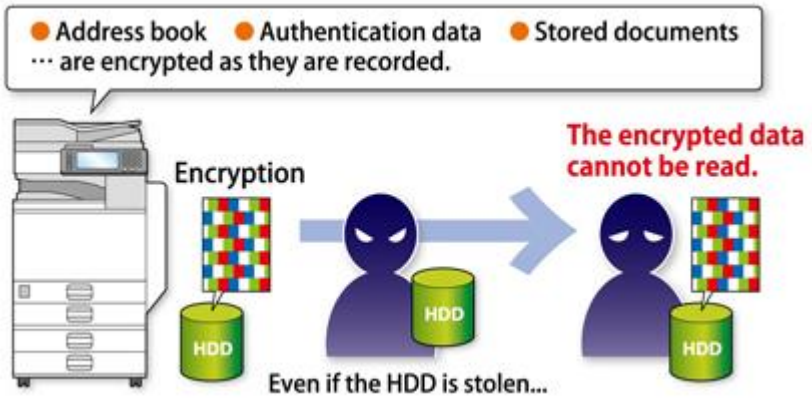
Hard Disk Security Functions

Hard disk drive (HDD) encryption

Address books, authentication information, and accumulated documents stored in a multifunction copiers are encrypted as they are stored. This function prevents information from being leaked even if the hard disk drive is physically removed.



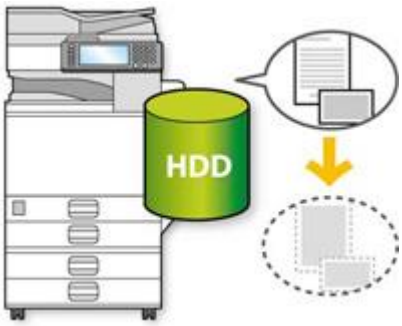
Data to be encrypted

The following data stored in the non-volatile memory or hard disk drive of the multifunction copiers are encrypted:

- ・Address book
- ・User authentication data
- ・Stored documents
- ・Temporarily stored documents
- ・Logs
- ・Network interface settings
- ・Configuration

DataOverwriteSecurity System (DOSS)

When a document is scanned by an MFP or a scanner or when data is received from a PC, some data may be stored on the hard disk drive or memory device. For example, temporary image data, data the user has chosen to save, or device configuration data may be stored. When the data is no longer needed this function actively erases it by overwriting it.



Event-driven:

The image data stored in the device during the copying and printing processes is overwritten and erased each time a job is executed.

Overwrite all:

All data, including the user information registered in the multifunction copier, is erased at one time when the multifunction copier is to be transferred to another department or to be decommissioned.

Method of erasing:

NSA	Data is overwritten twice with random numbers and once with zeros.
DoD	Data is overwritten by a random number, then by its complement, and then by another random number.
Random Numbers	Data is overwritten multiple times with random numbers. The number of overwrites can be selected from 1 to 9.
BSI/VSITR*	Data is overwritten 7 times with the following patterns: 0x00, 0xFF, 0x00, 0xFF, 0x00, 0xFF, 0xAA.
Secure Erase*	Data is overwritten using an algorithm that is built in to the hard disk drive.
Format*	The hard disk is formatted. Data is not overwritten.

*These methods are available for Overwrite all function.

Our device supports the above erasing methods to enable customers to select the erasing method which follows customers' security policies. The results of each erasing method except for Format are the same.

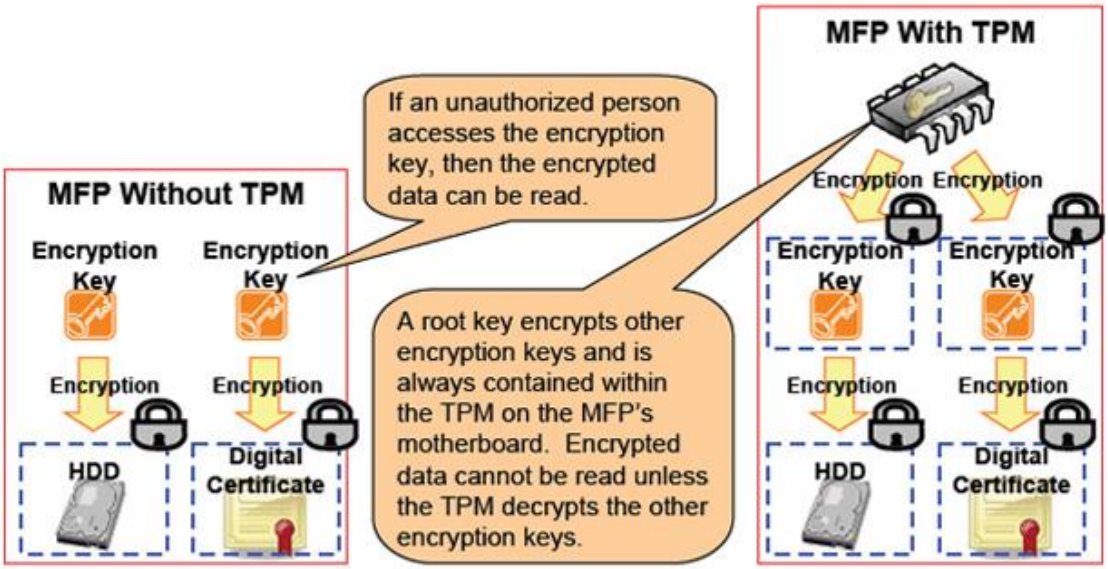
Encryption key protection via TPM

Ricoh MFPs employ a Trusted Platform Module (TPM) which is a tamper-proof hardware security module that performs cryptographic functions and securely stores cryptographic data. Ricoh uses the TPM to store the root encryption key that protects the hard disk data encryption key and the digital certificate of the MFP, and to perform a trusted boot operation which validates MFP firmware authenticity before permitting the MFP to operate.
The root key and cryptographic functions are always contained within the TPM and cannot be altered from outside. This provides a high level assurance of the validity of the MFP's firmware, device identity, and hard disk security. This is another good example of how Ricoh's MFP products are designed with our customers' security interests at the forefront.

Ricoh Products Equipped with Trusted Platform Module (TPM)

Link to this Ricoh document for HDD security:

http://www.ricoh.com/security/products/mfp/function/#eraseBox


MFP With TPM
If an unauthorized person accesses the encryption key, then the encrypted data can be read.
MFP Without TPM
Encryption Key
Encryption Key
Encryption
Encryption
HDD
Digital Certificate
A root key encrypts other encryption keys and is always contained within the TPM on the MFP's motherboard. Encrypted data cannot be read unless the TPM decrypts the other encryption keys.
Encryption
Encryption
Encryption Key
Encryption Key
Encryption
Encryption
HDD
Digital Certificate