RankSecure
Cryptodata security specialist

FAQ – Ranksecure 'Pocket Rocket'

What is 'Ranksecure 'Pocket Rocket''?

Ranksecure 'Pocket Rocket' is a USB hardware encryption solution designed to provide real time, in-line encryption of ANY USB enabled mass storage device, regardless of size, including Blu-Ray and DVD/DVD/CD-R USB devices. Ranksecure 'Pocket Rocket' can and will encrypt data from a camera, smart phone, tablet, USB backup drives, 'thumb' drives, and much more.

Figures 1-3, from left clockwise: Photo of Ranksecure 'Pocket Rocket' module; the *Ranksecure 'Pocket Rocket'* *connected to a USB3.0/SATA hard drive; t*he *Ranksecure 'Pocket Rocket'* connected to a USB2.0 Thumb drive.

Ranksecure 'Pocket Rocket' + USB MSC = Connected Pair

Ranksecure 'Pocket Rocket' incorporates real-time USB- to-USB crypto module, which performs full disk encryption with AES ECB/CBC 256-bit strength to all connected USB MSC (Mass Storage Class) storage drives. VERY heavy duty protection indeed!

What is disk encryption?

Disk encryption is a technology which protects data by converting it into an unreadable format called cipher text. Without the correct deciphering key, the data will remain encrypted.

What is *Full Disk Encryption (FDE)*?

The term *"full disk encryption*" is often used to signify that all of the data on a disk is encrypted.

What is *Self Encrypting Drive (SED)*?

A self encrypting drive is the same as an FDE (full disk encrypting drive); the meaning is the same, only with a different name.

What are the Features and Benefits of *Ranksecure 'Pocket Rocket'*?

Glad you asked! There are many great features of Ranksecure 'Pocket Rocket':

Features & Benefits
- Ranksecure 'Pocket Rocket' is totally transparent
- No training required!
- USB1.1/2.0/3.0 compliant

- Easy to use for years to come
- Encrypts all USB MSC devices[1] including card readers
- Simple yet very effective key management
- A "Recovery Password" that performs two-factor authentication
- Encrypts Blu-Ray DVD, DVD RW, CD-R;
- Windows, MAC operating systems
- NO software or complicated drivers to install
- Simple to initialize and use
- Full disk encryption protects all of your data
- Both 512 bytes or 4K bytes sectors are protected
- Certified hardware AES ECB 256 bits strength
- Virtually impenetrable
- Slim, compact and ultra light weight form factor
- 60.7mm (H) x 19.6mm (W) x 10.1mm (H) with
- 11g (0.39 oz) weight

Why choose the Ranksecure 'Pocket Rocket' over FDE or SED?

Ranksecure 'Pocket Rocket' was designed to be convenient, portable, transparent and simple to use - all the while securing your valuable data. Its purpose is to encrypt data on the fly. If you travel, take Ranksecure 'Pocket Rocket' with you to protect your mobile data. If you don't travel, use Ranksecure 'Pocket Rocket' to protect your home and office data.

Convenience, simplicity and security. Unlike the limited selection of FDE and SED drives, which usually involves with using costly key management software, Ranksecure 'Pocket Rocket' works reliably with any drive with any geometry; and best of all, you get to control your own ciphering key.

How does Ranksecure 'Pocket Rocket' work?

Follow these three simple steps:

Insert the USB drive to the female connector (at the back) of the Ranksecure 'Pocket Rocket' device.

Insert the Ranksecure 'Pocket Rocket' to any host USB port. At first usage, you must properly initialize Ranksecure 'Pocket Rocket' by executing a code utility which is an .exe file.   The code utility will guide you through the simple initialization procedure.

After initialization, you can start using Ranksecure 'Pocket Rocket'.

The initialization procedure is:

Download the code utility and unpack it
Insert the USB drive to the Ranksecure 'Pocket Rocket' then insert the Ranksecure 'Pocket Rocket' to any host USB port
Execute the code utility then follow the two steps as guided
**Un-plug** then _**re-plug the Ranksecure 'Pocket Rocket'**_ along with the USB drive to allow Ranksecure 'Pocket Rocket' to save the settings
The OS detects the attached USB drive, and asks if you want to format the drive. Click YES and every cryptographic operation is now automatic and transparent.

What will happen if Ranksecure 'Pocket Rocket' isn't properly initialized?

The Ranksecure 'Pocket Rocket' is not fully functional other than detects your connected USB drive. Attempt to format the USB drive through the un-initialized Ranksecure 'Pocket Rocket' will produce an error message prompted by Windows as "The disk is write protected."

Do I need any training to use Ranksecure 'Pocket Rocket'?

NO! You don't have to learn or manage anything. After the initialization procedure is completed, simply insert the Ranksecure 'Pocket Rocket' along with USB drive into any host USB port. The OS detects the Attached USB storage drive and asks if you want to format the drive. Click YES and every cryptographic operation is automatic and transparent.

What is the "Key Management" of Ranksecure 'Pocket Rocket'?

Every Ranksecure 'Pocket Rocket' comes with a code utility that allows user to initialize their Ranksecure 'Pocket Rocket'. The Ranksecure 'Pocket Rocket' may not be used without being initialized through the establishment and confirmation of the "Recovery Password."

The "Recovery Password" generates the Data Encryption Key (DEK) needed to authenticate the Ranksecure 'Pocket Rocket'. This "Recovery Password" generates the same DEK programmed to the *Ranksecure 'Pocket Rocket'*.

If the DEK was incorrect or missing, the Ranksecure 'Pocket Rocket' will not allow access to the encrypted data on the USB drive. Without the correct recovery password, the resulting encrypted drive appears to be an unformatted drive. This is true even if the encrypted drive has been moved to a different platform. Attempts to surface scan the entire drive sectors/platters in order to access the encrypted data will be futile.

Can Ranksecure 'Pocket Rocket' encrypt Blue-Ray DVD, DVD RW and/or CD-R media?
Yes. Ranksecure 'Pocket Rocket' can encrypt/decrypt generic USB interfaced or bridged interfaced media (such as USB2.0/SATA or USB3.0/SATA) Blu-Ray DVD, DVD RW and CD-R media real-time. All the encryption and decryption must be done using USB interface devices.

What happens when a Ranksecure 'Pocket Rocket' encrypted Blue-Ray DVD, DVD RW and/or CD-R media is lost or stolen?
The encrypted media will be seen as a brick (brand new media without being previously formatted) without the presence of the Ranksecure 'Pocket Rocket'. The only way to gain access to the media will be to connect it to Ranksecure 'Pocket Rocket', and load in the correct recovery password.

What happens when a Ranksecure 'Pocket Rocket' is lost or stolen?
If the Ranksecure 'Pocket Rocket' is ever damaged, lost or stolen, simply purchase another Ranksecure 'Pocket Rocket'. Install the Ranksecure 'Pocket Rocket' in the same fashion and use the same "Recovery Password" to generate the same DEK to allow operation over the encrypted media that was previously encrypted with the lost or damaged Ranksecure 'Pocket Rocket'.

Does Ranksecure 'Pocket Rocket' support 4KB/sector drives?
Yes, Ranksecure 'Pocket Rocket' *supports both* standard 512 bytes per sector drive and 4K bytes per sector drives without regard to capacity of the drive.

Does Ranksecure 'Pocket Rocket' support drive capacity over 2TB (2 Terabytes)?

Yes. Ranksecure 'Pocket Rocket' supports drives greater than 2TB per drive. See additional comments in 'What is the likelihood of an Ranksecure 'Pocket Rocket' malfunction' answer on the next page.

Does Ranksecure 'Pocket Rocket' support various file systems?

Sure. Ranksecure 'Pocket Rocket' supports all file systems including FAT, FAT32, NTFS, Linux and MAC OS. Note that certain file systems in MAC OS may not be compatible with other file systems as seen in a PC Windows environment.

Does Ranksecure 'Pocket Rocket' feature Anti-Malware?

Yes. Ranksecure 'Pocket Rocket' features "Write-Protect Entire Storage" and "Safeguard Boot Sector" that prevent malicious virus, worms and spyware from Implanting to your USB drive.

Is Ranksecure 'Pocket Rocket' compatible with various operating systems?

Yes – the Ranksecure 'Pocket Rocket' supports popular MAC OS (10.6 and 10.7), Windows (7, Vista, XP 32/64-bit & Windows 10). This represents over 98% of the operating systems available today.

Can someone hack into the data encrypted with Pocket-Rocket?

These hardware algorithms are certified to provide reliable security. At full strength, it is virtually impossible to access the encrypted data by guessing or deriving the correct AES Key. All data at rest on the disk drive is encrypted, which means that the data on that drive is safe even if attackers try to boot from their own disk, or to move your disk to an unprotected machine.

If the Ranksecure 'Pocket Rocket' malfunctions, will I lose my data?

No, as long as you maintain your own Recovery Password as mentioned above. Go out and purchase a new Ranksecure 'Pocket Rocket' device and initialize it as you did previously. You should have no problems recovering your encrypted data.

What's the likelihood of a Ranksecure 'Pocket Rocket' malfunction?

Extremely unlikely. Each RankSecure family microchip is tested using a zero tolerance manufacturing policy and complies with international quality assurance standards prior to being shipped. But being an electronic device, however, there may be occasions that a chip might malfunction after some period of time, or at some unique unpredictable circumstances. This problem can be resolved by simply replacing the defective Ranksecure 'Pocket Rocket' with the a new unit. A malfunctioning *Pocket Rocket* unit can easily be replaced, and the encrypted contents of the disk drive will be intact and accessible (as long as the original DEK is intact).

Can I exchange the Ranksecure 'Pocket Rocket' encrypted files over the public Internet?

Great question! Not using this current product release. If this type of support is required, please contact us thru email and we can provide you with a solution.

Do I need to establish a separate "encrypted folder" under file directory as required by some software solutions?

No. All data written to the disk drive via the Ranksecure 'Pocket Rocket' is automatically encrypted without exception.

If I back my data up to an external drive, is that backed up data encrypted?

Yes, as long as you backup your data using another Ranksecure 'Pocket Rocket'. If your backup drive is USB enabled, protect that data with the Ranksecure 'Pocket Rocket'.

Should I expect a lengthy login procedure and complex GUI that other systems require?

No, not at all. Ranksecure 'Pocket Rocket' has been carefully designed not to change the user's regular computing behavior, nor does it require learning a complex GUI. The user is not required to memorize frequently used and cumbersome log on procedures.

RankSecure's prime objectives include building a secure product that will make the user's life a little more enjoyable. You need only to present your Ranksecure 'Pocket Rocket' every time you attempt to access your encrypted disk. Period.

Terminologies used in this document

There are several terminologies that are generally used and some specific to the Ranksecure 'Pocket Rocket' and it's time to get familiarized with those so that when confusion occurs, this could be the best paragraph to reference to.

USB MSC – USB Mass Storage Class; In general, it refers to a storage device under USB protocol;

AES - Advanced Encryption Standard as published in FIPS 197;

ECB - Electronics Code Book, is a confidentiality mode that features, for a given DEK, the assignment of a fixed cipher text block to each plaintext block, analogous to the assignment of code words in a codebook. Essentially the same DEK is applied to every plaintext data block independently.

CBC - Cipher Block Chaining, is a confidentiality mode whose encryption process features the combining ("chaining") of the plaintext blocks with the previous cipher text blocks. The CBC mode requires an IV (Initialization Vector) to combine with the first plaintext block, in addition to using a given DEK. The security level of a CBC implementation is quadruple trillions times more than that of an ECB.

DEK - Data Encryption Key, a 256-bit key responsible for data encryption and decryption based on AES ECB or CBC mode of operation.

Default DEK - Default Data Encryption Key, a 256-bit key embedded during the manufacturing process. This default DEK can be changed or replaced upon entering the "Recovery Password."

Initialization - a process required to initialize the *Ranksecure 'Pocket Rocket'* dongle by asking the user to enter and confirm the "Recovery Password," which allows the user to regain access to encrypted data in the event that Ranksecure 'Pocket Rocket' is lost, stolen, or may have malfunctioned. If the Ranksecure *'Pocket Rocket'* dongle wasn't properly initialized, the Ranksecure *'Pocket Rocket'* connected USB drive won't be able to get formatted. A system warning message of "This device is write-protected" will prompt when a user performs the action of "FORMAT" through an un-initialized *Ranksecure 'Pocket Rocket'*.

Recovery Password – an essential part of the *Ranksecure 'Pocket Rocket'* key management. A recovery password is responsible for generating the DEK value to regain access to the encrypted data, in the event that your Ranksecure 'Pocket Rocket' is lost, stolen, or may have malfunctioned. The same recovery password generates the same DEK. This "Recovery Password" should be kept with confidentiality.

Start Programming – a part of the "Recovery Password" process that writes the new DEK value to the Ranksecure *'Pocket Rocket'* to replace the old DEK value. Note that a new DEK value can be equivalent to the old DEK value.

Write-Protect Entire Storage – Using Ranksecure *'Pocket Rocket'*, the *"write-protect entire storage"* feature disables all write operations to the connected USB drive, making the USB drive "read-only" which effectively rejects any virus, spyware or malware intrusion. While this feature is turned ON, all contents of the drive remain encrypted. There isn't any extra driver to install. See also *"Safeguard Boot Sector."*

Safeguard Boot Sector Using *Ranksecure 'Pocket Rocket'* , the *"Safeguard Boot Sector"* feature disables all write operations to the boot sector of a connected USB thumb drive and card reader storage media, making it "read-only" which effectively rejects any virus, spyware or malware intrusion. While this feature is turned ON, write operation is only permitted to the other sectors with written data being encrypted. More, the Ranksecure 'Pocket Rocket' blocks the "autorun.ini" type malware so that the malware won't be

able to implant itself to the *Ranksecure 'Pocket Rocket'* built-in CD-ROM (***Ranksecure 'Pocket Rocket'_CD***) that contains all software code utilities. There isn't any extra driver to install. See also "***Write-Protect Entire Storage.***"

Firmware Update – a process that replaces your existing firmware using a newer version. This is only required whenever there is a newer version release that resolves known compatibility issue or enhances the security operation. There isn't any extra driver to install.

Note: Some composite device such as Western Digital's My Book Studio Edition 4TB is equipped with more than one interface. The WD 4TB drive comes with an extra HID/SES interface in addition to the USB MSC interface. The Ranksecure 'Pocket Rocket' supports current WD 4TB drive under Windows 7 32/64-bit platform. However, we have not exhausted our testing of other brands and cannot guarantee full compatibility with other 4TB drives. If an incompatibility issue occurs, please inform us and send us your configuration data as we will be pleased to try to resolve the technical difficulties for you.