The DigitalBank Vault SuperEncryption System is working offline , on ‘air gapped’ devices, that are permanently not connected to the internet.

All the encryption and decryption process is done completely offline. The question is how to transfer the encrypted files to your counterparts ? How can you communicate with your counterparts if the DBV system is offline?

The process is simple: you transfer the encrypted files to an online device and use whatever internet exchange solutions you have, for sending the encrypted files (gmail, whatsapp, telegram, signal, cloud storage, social media platforms and more).

The receiving party needs to then transfer the file from the online device, where the file has been received, and transfer it to the offline device, where the DBV system is installed.

Important to understand that only and exclusively encrypted files are reaching the online devices.

All encryption/decryption procedures are always executed on the offline device.

In case your online device is compromised by some kind of spyware, the hackers will never be able to decipher the encrypted files. In case your online device is stolen, lost or seized, any digital forensic analysis will not be able to decrypt the files retrieved.

How encrypted files are transferred from the offline device where the DBV system is installed, to online devices, for then sending the encrypted files to the communicating parties.

There are several transfer options for example through physical means such as USB sticks (DiskOnKey), SD memory cards, cables between devices , or by non-physical transfer solutions such Bluetooth (for files) or QR codes (for encrypted plaintext).

During transfers between devices, is always advisable to disconnect the online device from the internet, to use only new USB sticks or SD cards, never use used ones or ones that you do not know their origins.

The transfer between DBV offline devices used and the online ones, is manual and therefore time consuming , but make no mistakes about it, this is the only way to secure your encrypted files. Most online connected devices are already compromised by some kind of spyware or malware, that hack your data before you even encrypt it or immediately after you decrypt it.

This is the reason you confine the encryption/decryption process to offline devices, never connected to the internet. This is the same methodology used by the leading intelligence agencies in the World , today.

DigitalBank Vault is not supplying hardware, and therefore the user needs to buy the hardware(Windows Laptop or Android phone or tablet), he will then use it as the “offline device” where the DBV system will be installed.

DBV provides the set of software that will transform that offline device into the most secure encryption platform in the World.