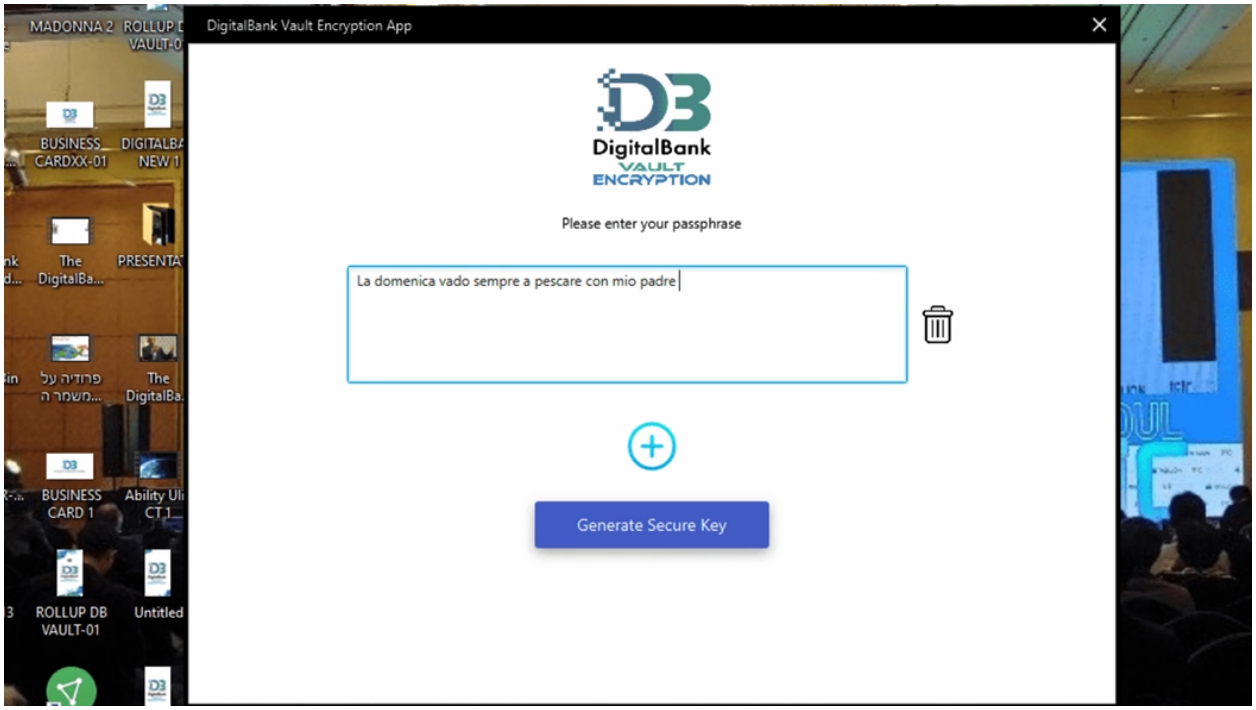

The Passphrase used on the DigitalBank Vault SuperEncryption system, is not a password, and it does not grant ‘entrance’ to a platform. This is a secret phrase invented by you, that is creating on the spot, with the combination of our algorithm, the encryption keys, used for encrypting and decrypting the files.

You can change the passphrase as much as you want, each time the passphrase changes, it will create new encryption keys.

Best is to use unpredictable phrases, randomly chosen, but most important is to remember them or take note of them, because you will need them for decrypting the information just encrypted.

The question is ‘ how do I exchange the secret phrase with a counterpart I am communicating with, that has the same encryption system version, and needs to decrypt the file sent out to them?’ How can the communicating party that is receiving the encrypted message can decrypt it?

First of all they need the same exact version you have. The DBV systems are unique and personal systems, programmed for each individual client, so that each client gets a different version of the system: it works and looks the same, but encrypts in a different way because we slightly change the encryption algorithms to each client.

To each client, we supply a number of licenses of the same version, so that he can share them with the parties he is in contact with, so that they will be able to communicate. In this way, we create a closed communication network between parties.

So ‘ how does the communicating party get the right passphrases to use for decrypting/encrypting the files exchanged ?’

This is called in the intelligence community “ Pre Shared Secret”. You need to pre-fix beforehand , a list of passphrases to be used between you. It can be changed daily, hourly or on every encrypted file exchanged.

It can also be random, like for example, you decide with your counterpart that today's passphrase is the daily title of the " New York Times" , or the last tweet that Barack Obama tweeted yesterday, or the last Facebook post of a known VIP, or your own last post on Linkedin.

How do you fix this pre-shared secret in a 'secret' way, without taking the risk of being exposed? You can to find ways to convey it to the communicating parties : either a face to face meeting, where you pre- arrange the passphrase methods to be used, or you create a long text message with all the instructions on how to work out the passphrases to be used, and send it to the other party, then just telling them over the phone to use for this first time only your email address as a passphrase, so that they can decrypt instantly the encrypted text and copy all the passphrases programmed.

There are hundreds of creative ways to exchange passphrases and fix random pre-shared secrets. For security reasons we will not disclose them here, this is classified information we release to the buyers of the DBV systems.

The important fact to remember is that nobody besides you and your close circle of people, you choose to be in contact with, does not have the same system as yours, so that even if someone intercept your passphrase , they cannot use it anyway, because even if they bought from us a system, is not similar, and by typing your passphrases , it will never decrypt your files, because the encryption algorithms are totally different on each system supplied.