
# DigitalBank VAULT ENCRYPTION

*DigitalBank Vault Limited*

# WELCOME TO THE UNCONVENTIONAL


*You cannot hack what isn't there!*

*DATA THAT CANNOT BE READ IS OF NO USE TO A CYBER CRIMINAL*

**The DigitalBank Vault One Time Pad Encryption System**

The DigitalBank Vault Encryption System is based on
the One Time Pad Encryption Concept.

DigitalBank Vault provides governments, organizations, institutions, and private corporations with personal, individual, private, impenetrable cyber defense systems for each individual or department, within an organization, for securing in an absolute way classified databases &confidential information (in transit) from internal and external threats.

*The DBV One Time Pad Encryption System help you encrypt in an uncrackable way :*
any type of files in order to locally or cloud store them, and for transferring
encrypted files outside the perimeter of your institution,
covering also any form of internal and external communication (voice, video, text).

DBV Technologies allows Multi Platforms, Multi-level, & Multi-Signature scenarios.
Therefore there are no ways to alter docs, switching, or tempering files.

The DigitalBank Vault ®  Cyber Defense Technology is far beyond military-level Encryption.
DigitalBank Vault Encryption is near to quantum-safe cryptography.

**OUR ENCRYPTION SYSTEM'S METHODOLOGY**
NO Information ever stored
NO Internet connection
NO Servers
NO Third Parties Involved
NO Encryption Keys Stored or Exchanged


**THE DIGITALBANK VAULT ULTIMATE ENCRYPTION MACHINE**

*Absolute security, hardware-based encryption.*

The encryption of sensitive and/or classified information for being transmitted and/or stored is an integral part of a financial institution's cybersecurity methodology.

Our capabilities offer you absolute cybersecurity in the encryption/decryption process.

This is an air-gapped (offline) laptop, designed in our laboratories and running our proprietary OS, is immune to any type of Spyware, Malware, Online or Offline Attacks, and any type of Digital Forensics Analysis.

The DBV Operating System installed on this hardware has no capabilities of storing any information, keys, data, files, or folders.


*Why do we say that the encryption systems we offer are immune to Spyware, Malware, Online or Offline Attacks, and any type of Digital Forensics Analysis?*

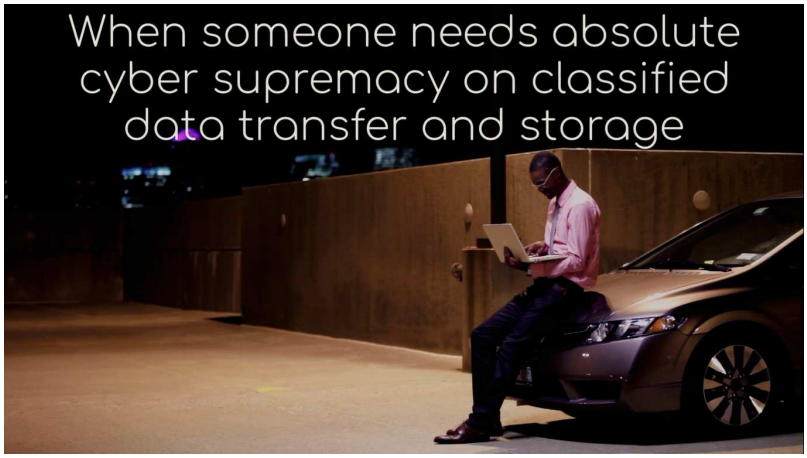
Let's start from the offline hardware itself: we use different brands of laptops, but we take them apart, replace different parts (like memory chips, etc..), remove Internet (Ethernet) and WiFi Connections, block all ports leaving just the SD card operating ( for the transfer or encrypted/decrypted data), we also make sure that the entire internal part if "sealed" with marble strength, by using advanced epoxy raisin, this seal prevents anyone to 'play' with the internal parts and inject any potential transmitting gadget.

Our Own Firmware: on this " rugged" laptop we are then installing our own proprietary OS, developed by us, that, of course, is not Windows, iOS, Linux, or any other type of know OS.

The DBV Operating System has no capabilities of storing any information, data, or files. After each use, the system will run 9 consecutive "erasing" cycles, which will include the complete overwrite with junk data, of all the memories in the laptop will then encrypt this junk data with random encryption, then it is erasing this memory.

This is done for 9 times, in order to be sure that no readable data of any kind is left. This feature prevents any laboratory from extracting valuable data from the device with digital forensic tools.

In case the laptop is stolen or sized, they will get an 'empty' device. Then at the shutdown, the system is re-installing itself to "factory settings", it means that when you then restart the laptop, you received a brand new device.




For adding an additional layer of security, we are able to supply to each client a slightly different OS, it is enough that a few lines of coding will be changed and the cyber weapon developed to attack our OS, will not be able to function, because they designed it for one specific OS.

Please also note that the hardware device is working only and exclusively offline, therefore an Online Attack is impossible. An Offline attack is not feasible too, because of all the above mentioned. The only working port is the SD card one, and as explained above, any attack vector has been neutralized.

Our Own Encryption Software: The One Time Pad Encryption Software installed within our Offline OS is able to encrypt and decrypt any type of files, folders, extensions, voice, text audio messages, and more.

Data for decryption is imported and data encrypted is also exported through the SD card port. No encryption keys ever leave the “air-gapped” device, and no encryption keys are ever stored on the device.

No files either encrypted or decrypted are left on the device.

**No Storage=Nothing to Hack.**


**THE DIGITALBANK VAULT PRO ENCRYPTION PLATFORM**
*High-security, hardware-based encryption.*

**Defending mobile devices for high-level officials and decision-makers**

DBV Premium is the latest innovation from DigitalBank Vault Limited
a complete universal encryption platform in the format of a microSD card or USB
with impressive performance capabilities.

As part of the unique Crypto security architecture, encryption is performed
in a hardware processor integrated into the microSD card/ USB.

The integrated Flash memory is also controlled and protected by this processor.

The  DBV Premium is compatible with all high-performance Windows PC and Laptops.

**You simply insert the SD card/USD into the PC – it will remain invisible to others**
**AND WILL LEAVE NO TRACE ON YOUR PC.**

*If your mobile phone should fall into the wrong hands or be stolen,*
*no one can access the data stored on the card.*

## WITH the DBV Premium, you own the smallest high-security Encryption Platform in the World.


**THE DIGITALBANK VAULT ENCRYPTION PRO SOFTWARE SYSTEM**

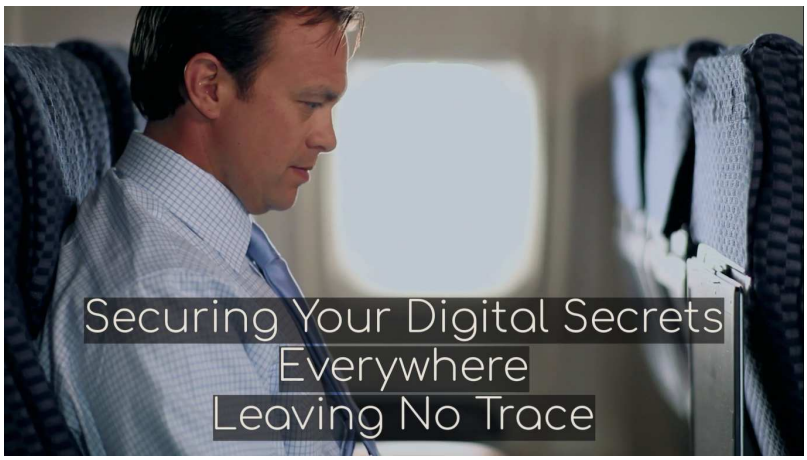
One Time Pad PRO Encryption System that can be downloaded to all
Operating systems and devices:
Windows, Apple/Mac iOS, Linux, Android smartphones, iPhones.

The DBV PRO Encryption App can be used with all online devices.
**However, we strongly advise to install and use the DBV Encryption System on dedicated devices, used for encryption/decryption purposes only and kept always offline, while transferring encrypted files to and from the offline device, by USB or SD Cards.**

Each User receives a dedicated set of encryption algorithms.

This Unique Version of the Encryption system can be then
distributed by the user to his network of contacts (in the forms of applications)
for enabling ultra-secure communications between managers, partners, workers, clients.

All Users of the DigitalBank Laptop or SD cards will receive a large package of downloads of their unique encryption systems, so that they can distribute it to their contacts and be able to exchange encrypted files with them.



DigitalBank
VAULT
ENCRYPTION

# When you don't trust anymore, anyone, within your organization
# It's Time to Use Your Personal Unique Encryption System

**The Uniqueness of the DigitalBank Vault One Time Pad Encryption System:**

1) No Encryption Keys stored anywhere (on any device used or server) at any given time.

2) No Encryption Keys exchanged between the communicating parties.

3) The user is the only one responsible for creating the encryption keys. One Time Pad Encryption Keys are generated Offline, on the spot by the user with NO third-party involvement.

4) Individual, Private, and Unique encryption system for each and every user :
Dedicated Set Of OTP Encryption Algorithms for each individual institution and multiple versions for each department, creating customized corporate networks for ultra-secure internal communication and privately-owned encryption systems for each manager.

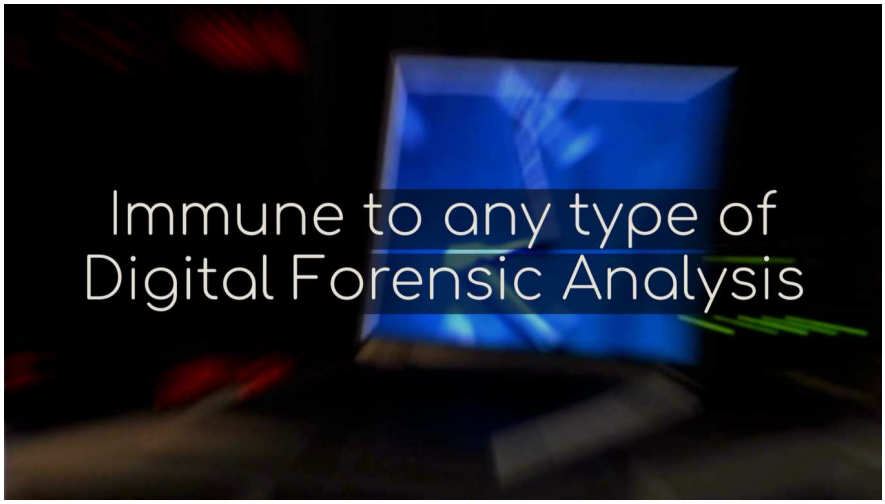
5) The unique versions of the Encryption system (in the forms of applications) can be then distributed by the user to his network of contacts for enabling ultra-secure communications between managers, partners, workers, clients.

6) Fully Independent & Anonymous Encryption System (No Servers involved)

7) Compatible with all platforms: Windows, Linux, Mac iOS, Android, and iPhones.

8) Working both Online and Offline.

9) Work in all languages.




**The Uniqueness of the DigitalBank Vault One Time Pad Encryption System:**

10) The Only OTP Encryption system that allows the encryption of any file's extensions, entire folders, videos, images, audio, and text messages by using the unbreakable OTP (one-time pad) encryption solution. Video tutorial about the OTP Encryption: https://youtu.be/FlIG3TvQCBQ

11) Full Integration: No changes needed for the user's cybersecurity structure. Complementary encryption tech that can be used in synergy with the current cybersecurity systems of the user and his organization: No need to make any changes to the user's current cybersecurity structure.

12) The Uncrackable Encrypted files can be securely shared by any communication means already in use, such as Gmail, Whatsapp, Facebook Messenger, Telegram, Signal, LinkedIn, SMS, and more…

13) OTP encrypted data can be stored securely on any server or cloud storage services: such as Google Drive, Amazon, Dropbox, and else.

14) Immune to any type of digital forensic analysis: DigitalBank Vault Fully Air-Gapped Encryption Devices (laptops) 100% Offline, Immune to any type of Online or Offline Attack.

15) The Encryption System can be used Offline, installed by the user himself on his own dedicated devices permanently not connected to the internet (air-gapped).

16) Multi-Signature Encryption System:
An unlimited number of signatories can encrypt one single file, or for decrypting the file.

DigitalBank Vault Encryption

# DigitalBank Vault Offline One Time Pad Encryption Systems

## PRICING PLANS

| PLAN FEATURES | $5000 per month | $8000 per month | $12000 per month |
|---|---|---|---|
| *10 Private Encryption Software Systems* | ✓ | ✓ | ✓ |
| *200 App Downloads to distribute* | ✓ | ✓ | ✓ |
| *10 Hardware DV Mobile SD Card* | ✗ | ✓ | ✓ |
| *5 DB Encryption Machines(Laptop)* | ✗ | ✗ | ✓ |
| *Unlimited Encryption Apps Downloads to distribute* | ✗ | ✗ | ✓ |
| www.DigitalBankVault.com | **PRO** | **PREMIUM** | **ULTIMATE** |

**PRO PLAN:** Offers the Cross-Platform Software Solution Only, to be installed on any Android, Apple iOS, Windows, and Linux. The OTP Encryption works offline and without any server. The package includes 10 Unique Encryption Systems, dedicated versions with different sets of Encryption Algorithms, and 200 Downloads to share.

**PREMIUM PLAN:** Includes 5 Hardware Encryption Systems in the form of SD cards to be used on Android Smartphones, transforming your mobile device into a powerful ultra-secure encryption machine. It comes with 200 Downloads Cross-Platform Apps to share

**ULTIMATE PLAN:** 5 DigitalBank Vault Encryption Machines in a Laptop configuration. It comes with an unlimited number of Encryption Apps downloads to share with your selected connecting parties.

## COMPANY REGISTRATION

*DigitalBank Vault Limited*
*Irish Square, Upper Denbigh Road,*
*St Asaph Denbighshire LL17 0RN, UK*
*Company number 1198855a1*
*(Limited Liability Registered in England & Wales)*
*https://beta.companieshouse.gov.uk/company/11988551*

## WEBSITE

*https://www.digitalbankvault.com/*
*DigitalBank Vault ® One Time Pad Encryption Cyber-Technologies. DigitalBank Vault® provides Unbreakable Digital Anti Surveillance & Anti Interception technologies: above military-grade encryption systems for ultra-secure communication (voice, video & text messaging) with impenetrable file transfers & storage solutions*

## KEYLESS , OFFLINE, SERVERLESS ENCRYPTION

*Impenetrable Keyless & Serverless One Time Pad Encryption of DigitalBank Vault ® based on the DBV Science of Emptiness*

## THE DEVELOPMENT TEAM & CEO

*The development team is composed of top-level cybersecurity engineers coming from the leading cyber offensive software companies and are constantly up to date on the behavioral and technical evolution of methods of attack from professional hackers, cyber terrorists, computerized industrial espionage organizations, and units of cyber warfare.*

*CEO & Founder : Moty Weissbrot*

*https://www.linkedin.com/in/moty-weissbrot-42bb06162/*