VDEE – Virtual Disk Encryption Engine

In one minute you can protect your data from hackers, unauthorized personnel, Black Hats, White Hats, foreign actors and employers at home or in “Bring Your Own Device BYOD environments”.

A virtual container (silo) is created on your device and ALL data is automatically saved with strong encryption. There is NO change in device use. There is no integration with any other device applications.

If you lose your phone or tablet or notebook you are protected. If anyone can manage to get access into the device they cannot access data since you are the only one who knows the passphrases.

Email and all documents and files are automatically protected when the data files for related applications are in your virtual drive.

This paper is intended to examine a security pathway for the cloud.

Virtual Drive Encryption Engine - VDEE

Deconstruction in cryptography shows that all security boils down to key creation, safe key distribution and secure key management.

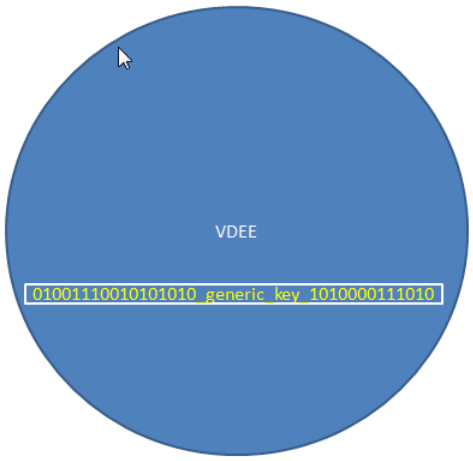
One Whitenoise key will create an infinite number of one-time-pads (tokens) and keys. VDEE provides a seamless pathway and a generic, no-risk method of distributing an initial WN key. This is single step that needs to be accomplished to access ALL Security-as-a-Service offerings as your needs grow.

It is known that many security technologies are actually manufactured and implemented in countries with whom we compete before being sent to western markets. This is a big risk.

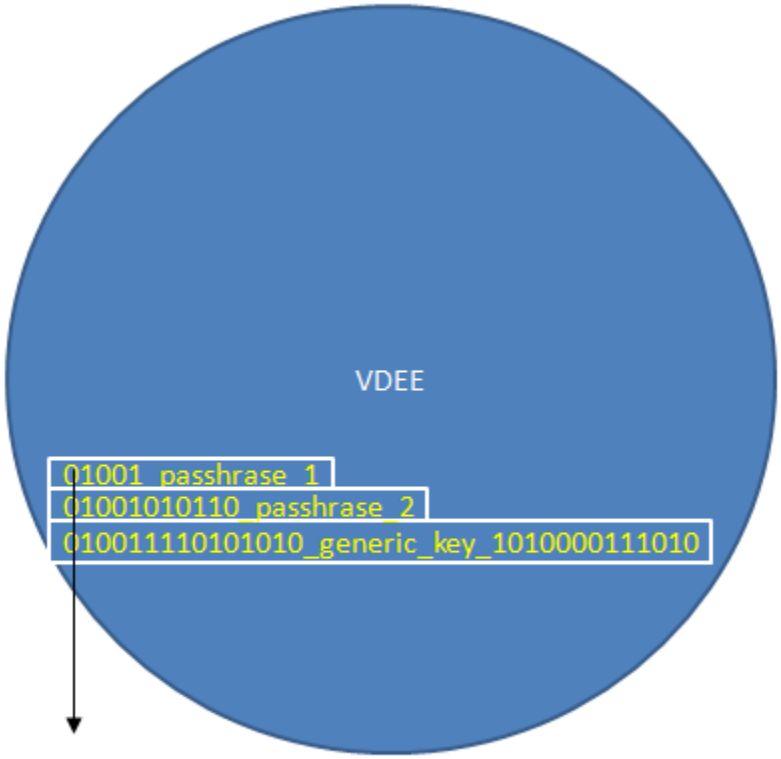
http://www.wnlabs.com/pdf/What_happened_to_you.pdf

To combat this security problem devices have firmware or applications that have a generic Master Key. All devices off the factory line are identical. This means that at this point there is **no** security offered because everything has the same key. This is the first and only key distribution required by Whitenoise to enable secure device, enterprise and cloud security.

Client downloads generic VDEE application and it is automatically installed. Note the generic master key. That is actually comprised of tens subkeys.



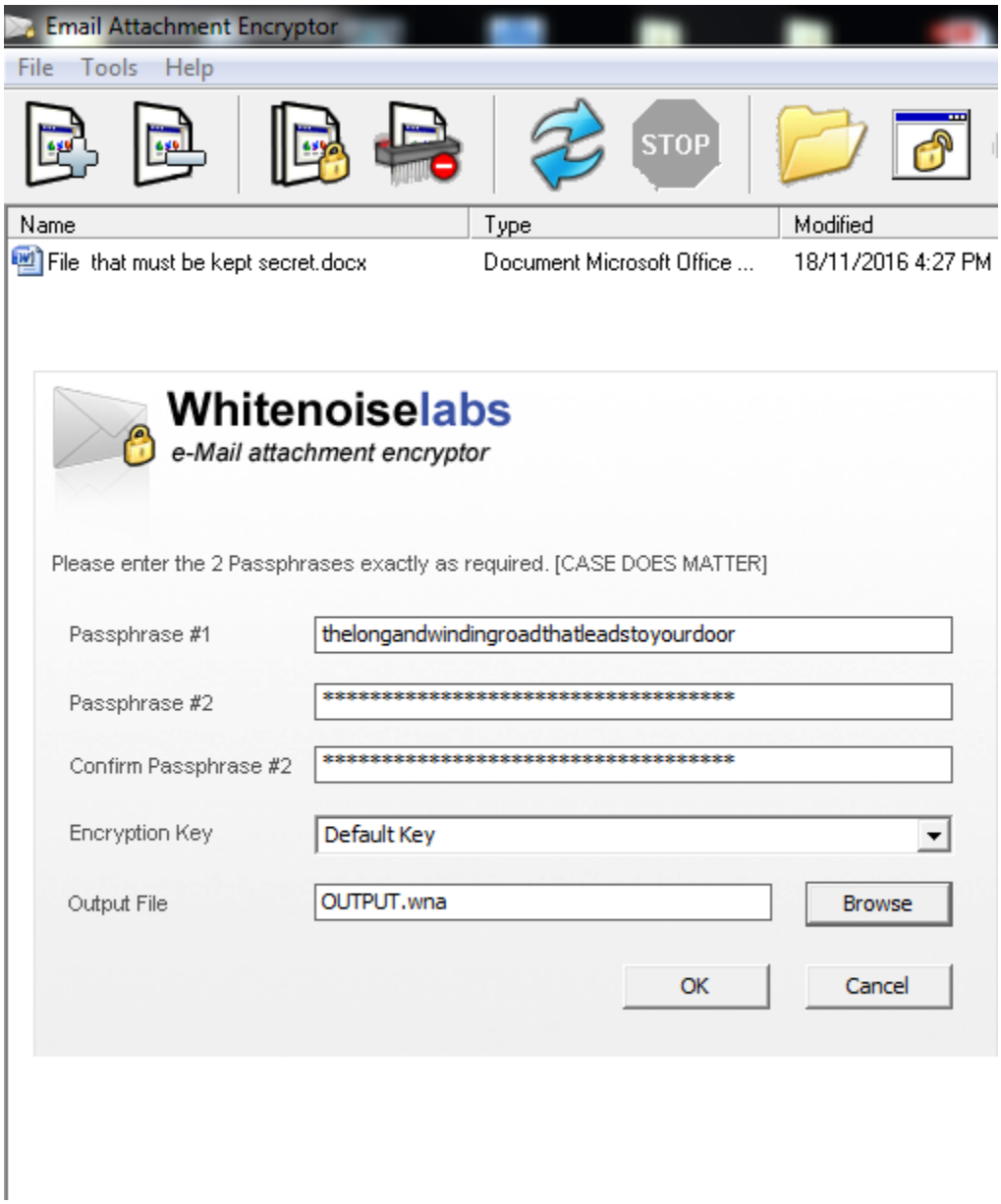
The client then makes the key unique to themselves by choosing two pass phrases of different prime number lengths i.e. 31 and 29 bytes. The pass phrases are their own private secret. They both authenticate the user and become subkeys in the structure to make your key stronger.



When passwords are used with existing technology the strength of the resulting perturbed key is weakened to the strength of the password because of the multiplicative process and integer factorization cryptography (i.e. RSA style).

With Whitenoise, client passphrases are converted to prime number binary equivalents and become subkeys to make the generic Master Key unique to the user and their private secret. This process actually strengthens the key and the unique client private key is greater than 25,000 bit strength. See the following presentation to learn how Whitenoise keys are made.)

In the screen shot below the first secret pass phrase (subkey) chosen is from well known lyrics. A second pass phrase is added. The resultant key used to encrypt the “File that must be kept secret” is strong and unbreakable.



This approach bypasses the problems attendant with foreign manufacturing and electronic key distribution altogether. You will share your private secret for each confidante in a different way i.e. during a private conversation.

At this stage a client should backup, save or escrow their private secret in a separate location known only to the client and not to any providers.

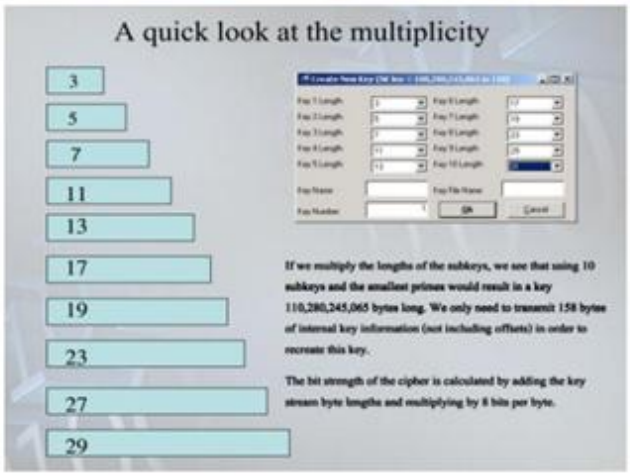
Creating your own unique, private, unbreakable, one-time-pad key

A Whitenoise keys is comprised of a variable number of prime number length subkeys that are populated with random data. Each corresponding bit is XOr'd between subkeys to create a deterministic but random key. Only the subkey structure and offsets need to be saved to recreate this key.

As seen in the graphic below the smallest key that can be made by Whitenoise using the smallest prime number length subkeys is 110 billion bytes long and is greater than 1600 bits in strength.

http://www.wnlabs.com/pdf/How_is_a_key_made.pdf

How do I calculate the length and strength of a Whitenoise key?



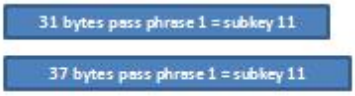
- the length of a Whitenoise key is calculated by multiplying the length of the subkeys in bytes.
- the strength of a Whitenoise key is calculated by adding the lengths of the subkeys in bytes and multiplying by 8 bits per byte.
- we only have to store 158 bytes of information

NOKIA

Multiplying the 10 smallest prime numbers together would create a key over 110 billion bytes long and we need to only store 158 bytes of key DNA information to recreate it exactly.

whitenoise technologies | TCS INNOVATION Labs

The users create their own keys by adding two pass phrases (subkeys).



Above we added two pass phrases to perturb the key and make it unique.

These two pass phrases serve first to authenticate the user because this is their private secret.

Adding the pass phrases (converted to binaries) as subkeys strengthens the user's resultant private, unique, unbreakable, one-time-pad key.

In our example:

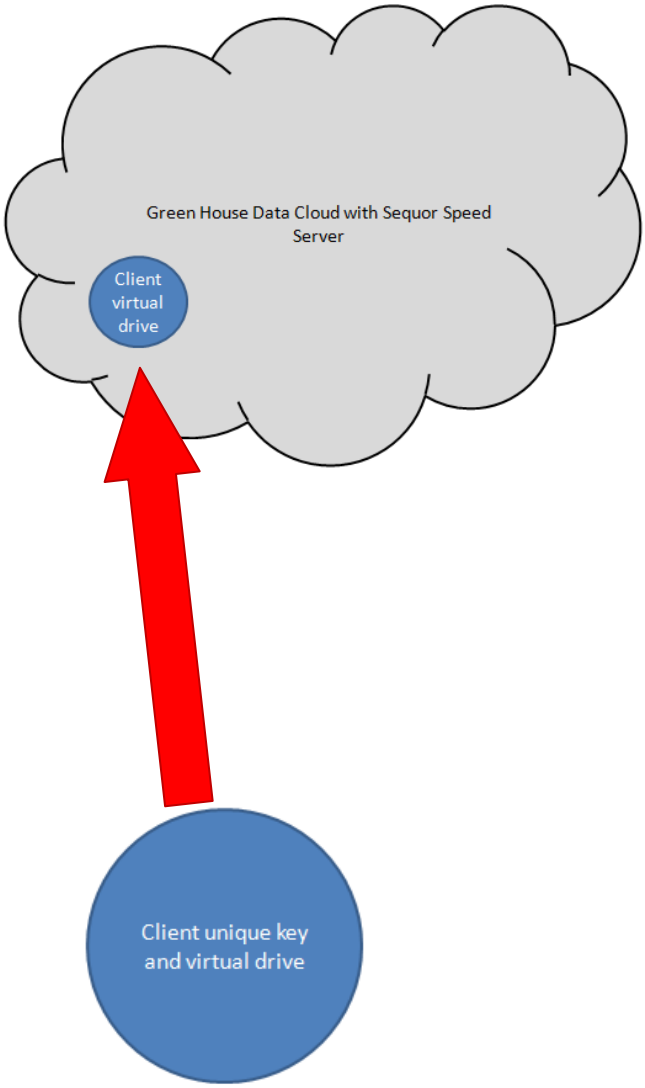
The key is now 31 X 37 X 110,280,245,065 = 126,491,441,089,555 bytes long.

The key is (3 + 7 + 11 + 13 + 17 + 19 + 23 + 27 + 29 + 31 + 37 bytes) times 8 bits per byte =

397 X 8 bits per byte = 3176 bit strength

We will now examine upgrading to enterprise and cloud security solutions in the event you ever need it.

- **Example: secure data storage in the cloud**

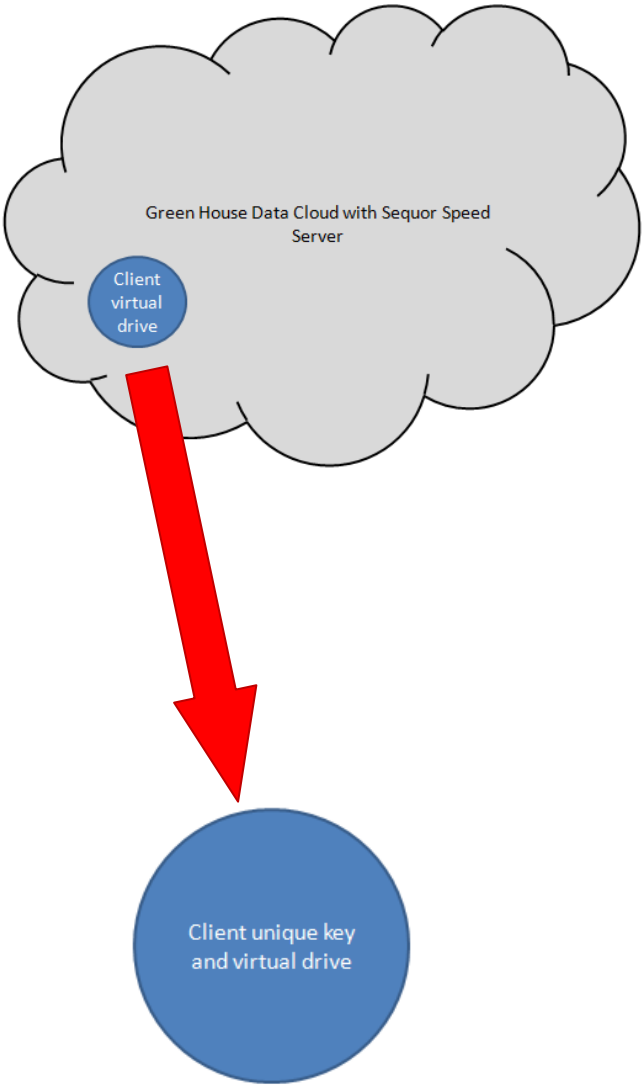


A virtual drive unique to the client is created in the GHD cloud.

The client uploads data over the existing SSL connection with the knowledge that the data uploaded is doubly encrypted with their unique private key and the SSL session key. Their data is store in the cloud is encrypted with ONLY their private key. The cloud host has no knowledge of the client key.

--

- **Example: Swap out generic key or private key from VDEE with unique key for openSSL and TLS-DIVA-PKI for other services.**



A virtual drive unique to the client is created in the GHD cloud.

The client downloads the client app and a unique key for TLS-DIVA-upgrade to be enabled to receive network security services. This key exchange goes over the existing SSL connection with a modified DH exchange. This is necessary for functions where a secure key is known by both the server and the client.

http://www.wnlabs.com/products/harddrive.php

http://www.wnlabs.com/pdf/Rapid_Factorization_of_semiprimes.pdf