About key file

The key file used by gcmc is such a thing:

> "The cipher key used for the actual encryption. "

It is such a thing.

> Apply a 256-bit (32-byte) cipher to AES-256 Keywrap.
>
> Encrypt the keywrapped key with AES-256-GCM.

In practice, when performing encryption and decryption, it is used as follows.

> Decrypt the key file and extract the contents (256-bit encryption key).
>
> Actual encryption and decryption are performed using the extracted cipher key.

AES-256-GCM decryption can detect such things:

> The key file has been tampered with (corrupted).
>
> The decryption password of the key file is incorrect.

When detected,

> Key file decryption
>
> Actual encryption, decryption

are not performed.

> Encryption is performed using a key that has never been used before.

That is the proper and ideal on cipher.

But actually doing this is too much.

However, password keys are too difficult to secure.

In terms of security, the key file is like the middle point between

> Random number generation key that has never been used for encryption and
>
> Password key.

Although it is far from "random number generation key that has never been used for encryption", it is much better than "password key".

It is something like this.