The PKCS #8 Ciphered Private Key format

Introduction

Description of the PKCS #8 format (encrypted version)

Conclusion

Introduction

PKCS #8 is a part of the PKCS standard (Public Key Cryptography Standards). It defines a 'syntax' allowing the storage of private key information.

The PKCS #8 syntax can only be considered a key block when dealing with a ciphered private key. In such a format, a key will be ciphered by a symmetric algorithm which can be triple-DES or AES. The (symmetric) key that ciphers the data is generated by a key derivation scheme (pbkdf2, for example) from a password.

More generally, PKCS #12 binds PKCS #8 private keys to X.509 certificates. But this can be highly complex.

PKCS #8 key block format comes in two versions: a non-encrypted and an encrypted version. The non-encrypted version is comparable to the PKCS #1 key block format and has little interest as a key block format. Therefore, we will only present the encrypted version format.

Description of the PKCS #8 Format (Encrypted Version)

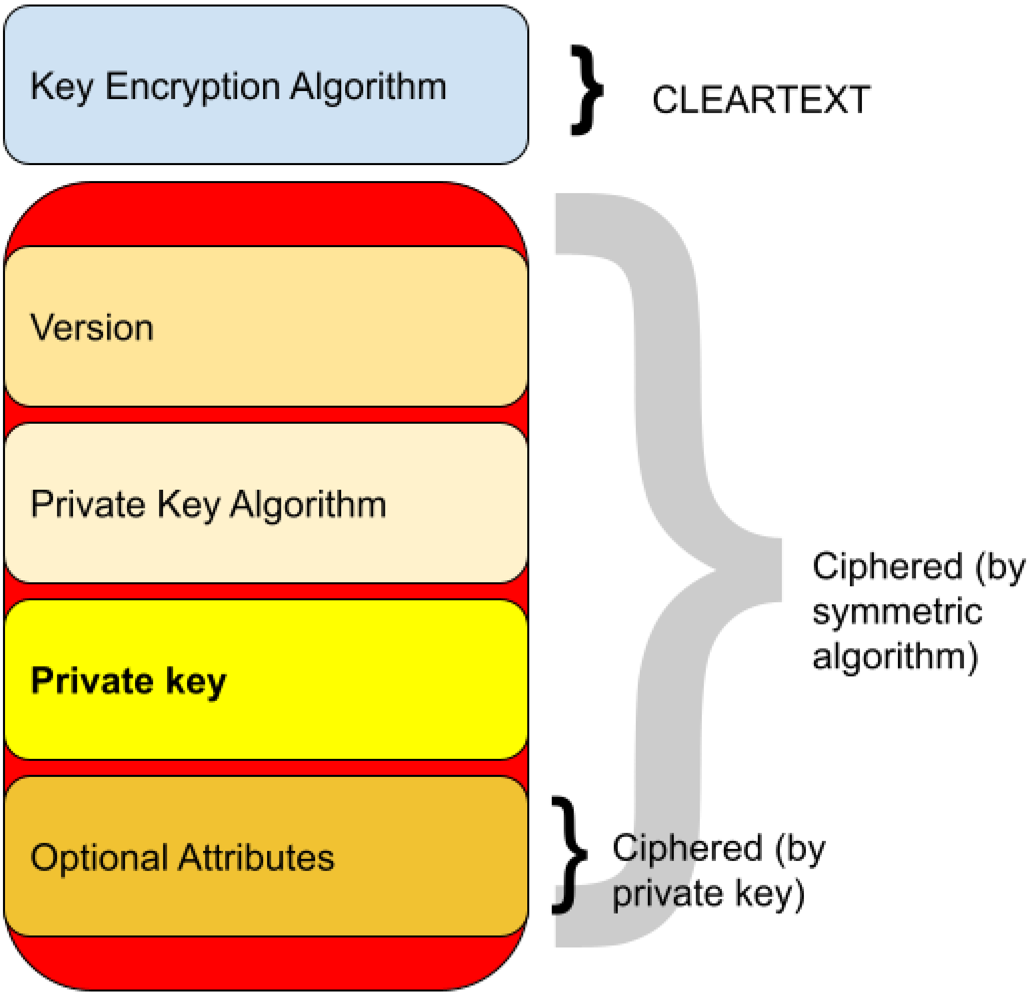
The PKCS #8 format contains a header in cleartext and a block of encrypted data. Its header is quite simple. It includes the **key encryption algorithm** used for encrypting the data. There is no macing mechanism to bind the header and the encrypted data. However, some optional attributes are ciphered with the private key, which means that this can be used as a validation mechanism by using the corresponding public key part.

The data are BER-encoded; hence the length of the fields may vary.

The encrypted data contains four blocks:

- **The version**: The syntax version number (usually '`0`' until the norm evolves)

- **The private Key Algorithm**: The type of algorithm that the private key stored will be used for (typically PKCS #1's `rsaEncryption`).
- **The private key** itself: The storage format will depend on the utilization and nature of that private key. For `rsaEncryption`, this is the BER value of an RSA private key.
- **Optional attributes**: Extended information, which may vary and are encrypted with the private key



Conclusion

The PKCS #8 format - encrypted version is a key block format that does not follow the TR-31 logic. A new version has been proposed but is still a draft.

While the PKCS#8 format may not be as robust as other formats, it is used every day for exchanging private keys. The PFX format utilized by Microsoft is similar to PKCS #8. Typically, the key encryption mechanism derives its ciphering key from a password.