safeStorage

> Allows access to simple encryption and decryption of strings for storage on the local machine.

Process: Main

This module protects data stored on disk from being accessed by other applications or users with full disk access.

Note that on Mac, access to the system Keychain is required and these calls can block the current thread to collect user input. The same is true for Linux, if a password management tool is available.

Methods

The `safeStorage` module has the following methods:

`safeStorage.isEncryptionAvailable()`

Returns `boolean` - Whether encryption is available.

On Linux, returns true if the secret key is available. On MacOS, returns true if Keychain is available. On Windows, returns true with no other preconditions.

`safeStorage.encryptString(plainText)`

- `plainText` string

Returns `Buffer` - An array of bytes representing the encrypted string.

This function will throw an error if encryption fails.

`safeStorage.decryptString(encrypted)`

- `encrypted` Buffer

Returns `string` - the decrypted string. Decrypts the encrypted buffer obtained with `safeStorage.encryptString` back into a string.

This function will throw an error if decryption fails.