SmartLock

Purpose

SmartLock is a program that allows the user to encrypt and decrypt files using **windows hello** capabilities. **Windows Hello** is a technology developed by Microsoft that introduces biometric security features in Windows operation system.

Technologies

SmartLock is developed in **C#** using Microsoft Visual Studio. It makes use of the credential and cryptography libraries developed by Microsoft. Below is a summarizing table with all the technologies used.

Technology	Library in C#
Windows Hello asymmetric encryption	Windows.Security.Credentials
AES symmetric encryption	System.Security.Cryptography
SHA256 hash one way function	System.Security.Cryptography
BASE64 encoding/decoding	System.Convert
JSON data storage	System.Text.Json

Technical Details

Encryption key

In order to achieve encryption without always needing a password, an encryption key is produced in such a way that will be possible to retrieve it using either Windows Hello or a user password. The encryption key is used to encrypt and decrypt the user data. It is important to store it in a secure way because with access to it the encrypted user data are exposed.

For the storage of the encryption key, AES encryption is used. The user password is salted using a random predefined string and turned into a secret key. Then the AES encryption transformation is used on the encryption key using the secret key and a random predefined IV (initialization vector). The resulted bytes are encoded into a BASE64 string which is stored. Performing the same procedure backwards, requires the user password and results into the encryption key.

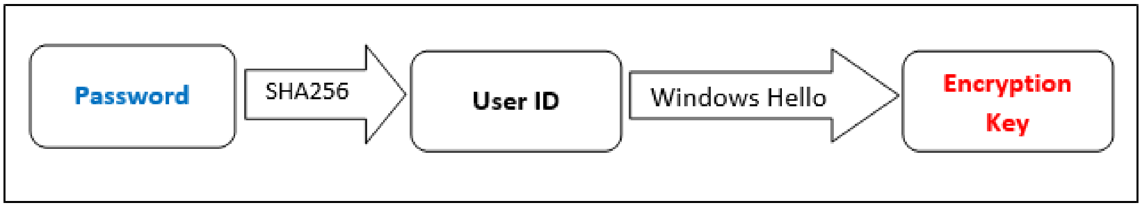


Image 1: Generation of encryption key

User password

At the initial execution of the application a user password is required to produce the encryption key. Using the user password, a user ID is created. Each unique password produces a single unique ID. The ID is then used to generate the encryption key through windows hello.

The password can be used to access the encryption key and thus decrypt or encrypt data. For this reason, it is important to be kept secret by the user. It is recommended to be noted down in a notebook (offline) and stored in a safe place. It will be only needed in case data decryption cannot be achieved through windows hello and a backup decryption way is necessary. SmartLock allows only data decryption using the user password but it can also be used to encrypt them due to the fact that the encryption key is accessed. This functionality is scope of this application.

User ID

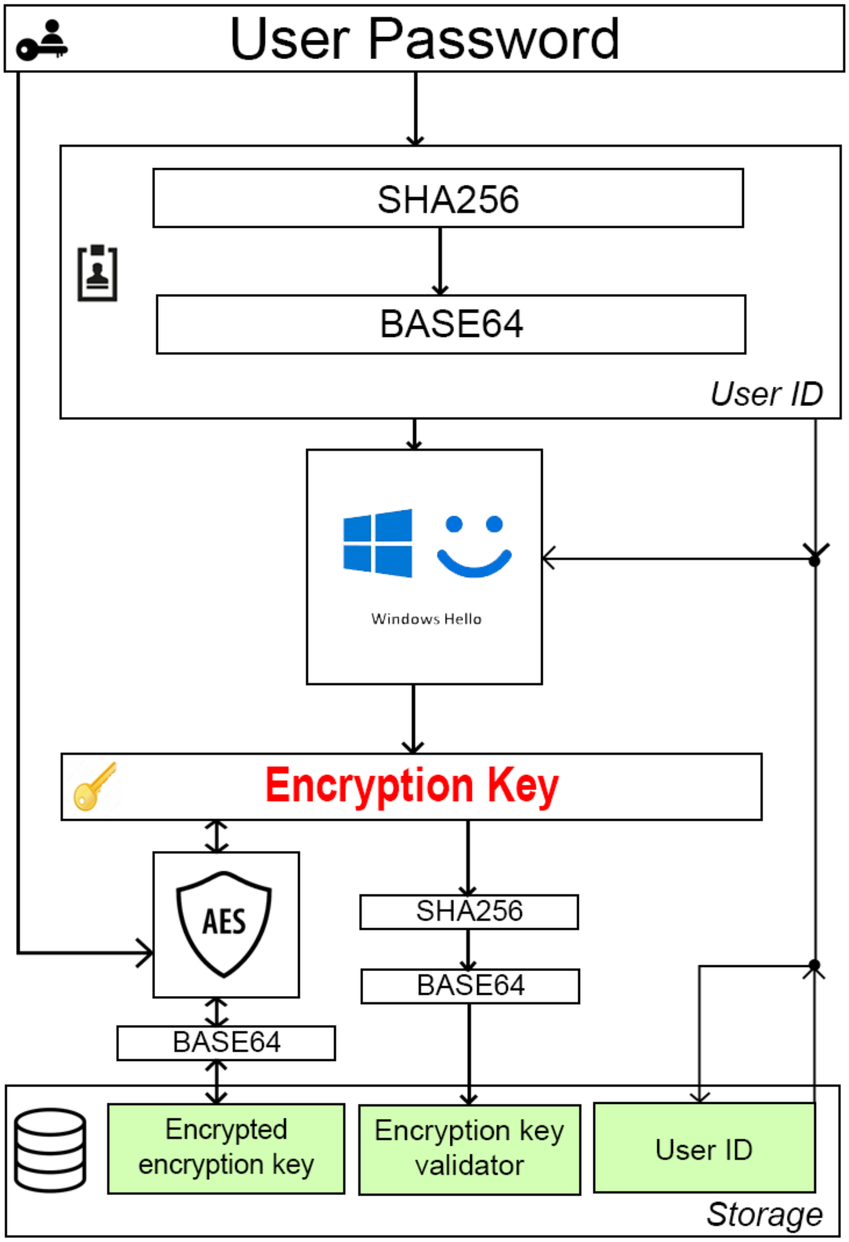
The user ID is a BASE64 encoded string of the SHA256 hash of the user password. Given the user ID an asymmetric encryption key pair is produced through Windows Hello. Using this key pair, the user ID is signed with the private key generating the encryption key. The same user ID can result in different key pairs and thus different encryption key, depending on the Windows Hello user authorization. As mentioned before, each unique user password produces a single unique user ID, but each user ID will produce a different key pair for each Windows Hello user. So, there is no way for a user to access the encryption key of another user in the same operation system.

The user ID is stored locally to avoid requiring the user password every time in order to generate it. The conversion from the user password to the user id is a one-way function so there is no possibility to generate the user password knowing only the user id.

Encryption Key Validation

During the initial generation of the encryption key, a fingerprint of the key is stored locally. This fingerprint is a BASE64 encoded string of the SHA256 hash of key and it is used to validate if everything is correctly configured. On subsequent application executions, the encryption key generated through Windows Hello, must be the same with the one produced on the initial run to avoid data corruption. For this reason, on each execution, the stored fingerprint is compared against the one created on runtime and it is a mandatory to be equal for the application to continue.

Encryption Scheme


User Password
SHA256
BASE64
User ID
Windows Hello
Encryption Key
AES
SHA256
BASE64
BASE64
Encrypted encryption key
Encryption key validator
User ID
Storage