# What is Apple's Secure Enclave and how does it protect iPhone and Mac?

iPhones and Macs have a Touch ID or Face ID that uses its own processor to handle users' biometric information. It's called the Secure Enclave, it's basically a complete computer and it offers a wide range of security features.

iPhones and Macs have a Touch ID or Face ID that uses its own processor to handle users' biometric information. It's called the Secure Enclave, it's basically a complete computer and it offers a wide range of security features.

Secure Enclave starts separately from the rest of the device. It runs its own small kernel, the operating system or programs running on the device cannot access this section directly. It has 4MB of flash memory, used exclusively for storing elliptic 256-bit personal keys. These keys are unique to your device and are never synced to the cloud or even the device's main operating system cannot be seen directly. Instead, the system requires Secure Enclave to decrypt the information using the keys.

## Why does Secure Enclave exist?

Secure Enclave makes it difficult for many hackers to decrypt sensitive information without accessing your device. Because Secure Enclave is a separate system and the main operating system never sees these decryption keys, it is difficult to decrypt the data without proper access.

Please note, biometric information is not stored on the Secure Enclave; 4MB is not enough storage space for all that data. Instead, Enclave stores the encryption keys used to lock that biometric data.

Third-party programs can also create and store keys in the Enclave to lock data, but applications never have access to those keys. Instead, applications that require Secure Enclave encrypt and decrypt data. This means any

information encrypted with the Enclave is extremely difficult to decode on any other device.

**Below is a reference to Apple documentation for developers:**

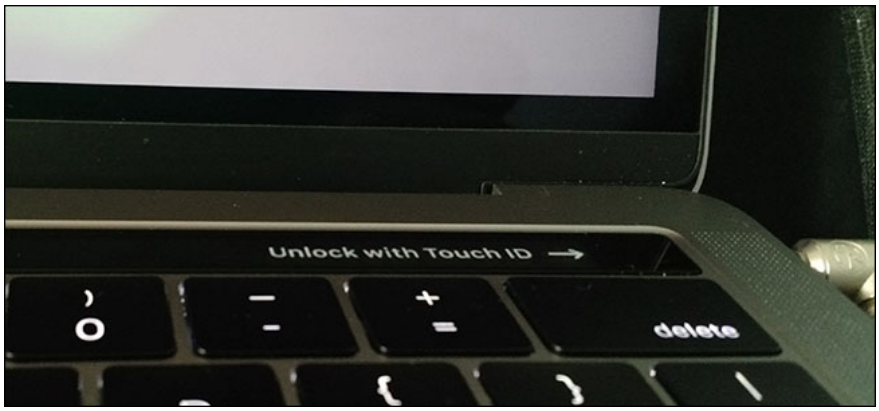
When storing a private key in Secure Enclave, the user instructs Secure Enclave to create a key, securely store it, and perform operations with it. You only receive the output of these operations, such as encrypted data or cryptographic signature verification results.

Secure Enclave cannot import keys from other devices: it is specifically designed to create and use keys on your phone or computer. This makes it difficult to decode the information on any device.

## Secure Enclave hacked?

Secure Enclave is complicated and makes it hard for hackers to access the device using this system. But nothing is absolutely safe. In the summer of 2017, hackers revealed that they had decrypted the Secure Enclave firmware, understanding how the Enclave works. However, it is worth noting that hackers have yet to find a way to retrieve the encryption keys stored in the Enclave: they only decrypt the software.

## Delete the Enclave before selling a Mac




The keys in the Secure Enclave on iPhone will be deleted when performing a factory reset. In theory, it will also be deleted when reinstalling MacOS, but Apple advises users to delete Secure Enclave on a Mac if they use anything except the official macOS installer.

See more:

1. Secure iPhone after jailbreak
2. 6 secure ways on iPhone
3. Security "security" for iPhone. How many methods do you know?

You finished reading the article "**What is Apple's Secure Enclave and how does it protect iPhone and Mac?**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.