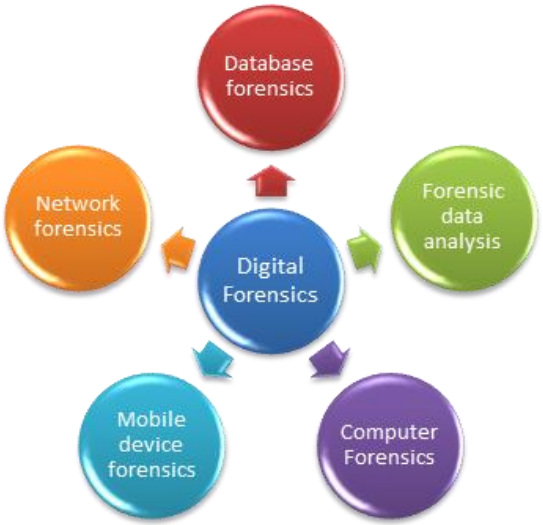
IPHONE ENCRYPTION

Litiano Piccin

11 ottobre 2014



MOBILE FORENSICS

Nella **Computer Forensics**, le evidenze che vengono acquisite sono dispositivi statici di massa; questa significa che possiamo ottenere la stessa immagine (bit stream) ogni volta.

Nella **Mobile Forensics** tutti dispositivi possono essere considerati come dispositivi dinamici salvo particolari modalità di acquisizione (fisica).

HACK IN BO
SICUREZZA ALL'OMBRA DELLE TORRI

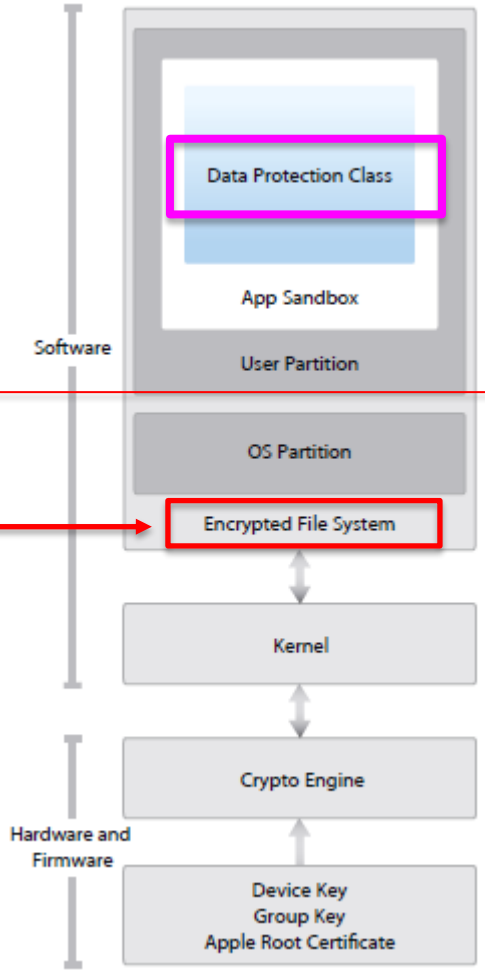
IPHONE ENCRYPTION

❑ *Data Protection*

❑ *File System Encryption*

SECURE ENCLAVE (5S)

UID (256 bit)



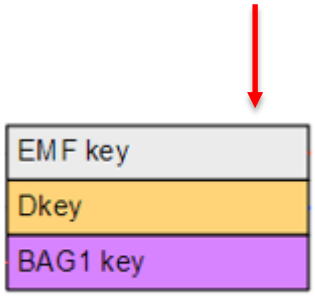
http://images.apple.com/iphone/business/docs/iOS_Security_Oct12.pdf

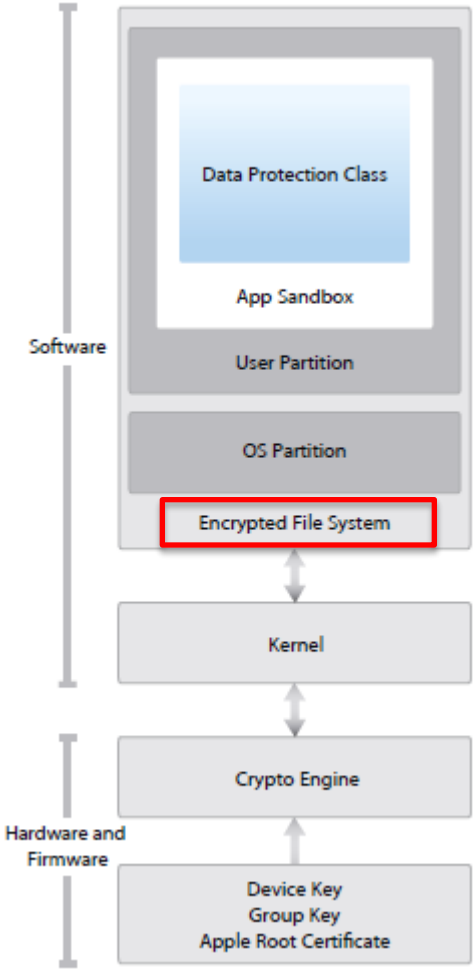
FILE SYSTEM ENCRYPTION

***File System Encryption**: since iPhone 3GS*, Apple offers 256-bit AES encoding hardware-based encryption to protect all data on the device. Disk encryption was designed to accomplish one thing:*

Instantaneous remote wipe.

Disk wiping work by simply erasing the 256-bit AES key used to encrypt the data (EMF, Dkey and BAG1 Key).



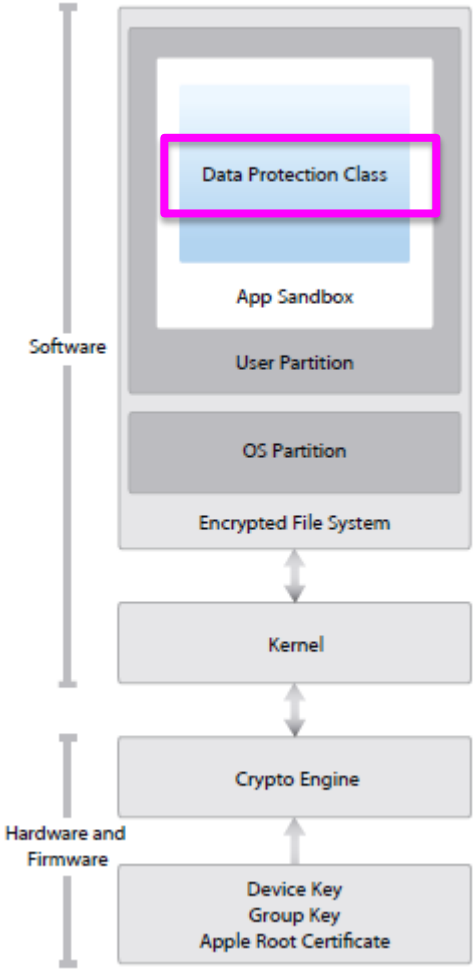


http://images.apple.com/iphone/business/docs/iOS_Security_Oct12.pdf

DATA PROTECTION

***Data Protection*: Apple develop a new encryption scheme that has the primary advantage of using the user's passcode or password to derive a key that is used to encrypt data on the device. When the phone is locked or turned off, the key is immediately erased**, *making data secured on the device inaccessible.*

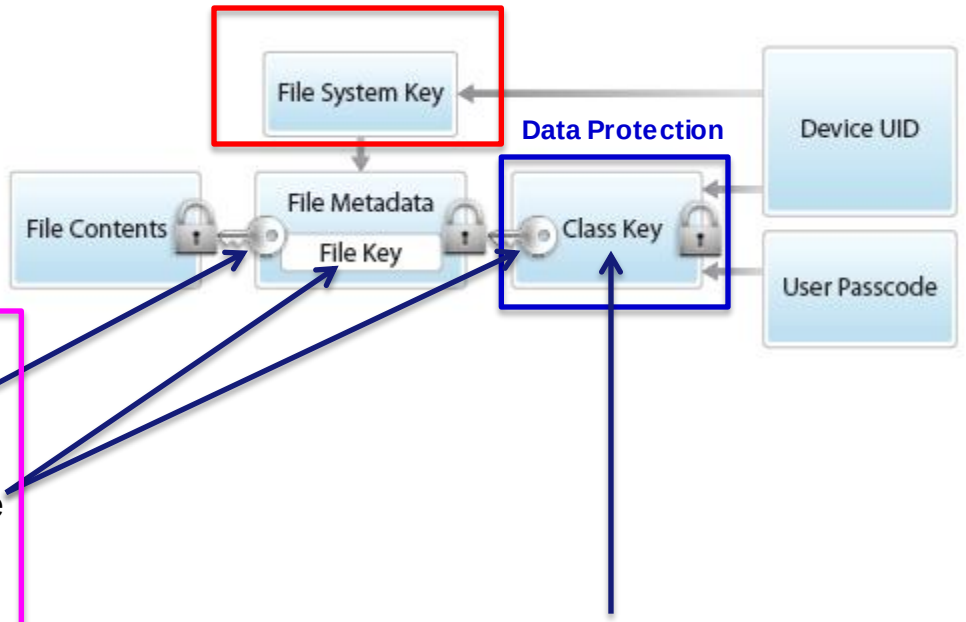
Data protection is a feature available for devices that offer hardware encryption, including iPhone 3GS and later, all iPad models, and iPod touch (3rd generation and later).



http://images.apple.com/iphone/business/docs/iOS_Security_Oct12.pdf

HACK IN BO
SICUREZZA ALL'OMBRA DELLE TORRI

File System Encryption (EMF)



DATA ENCRYPTION

FILE

Contenuto del file criptato con una **chiave** unica.

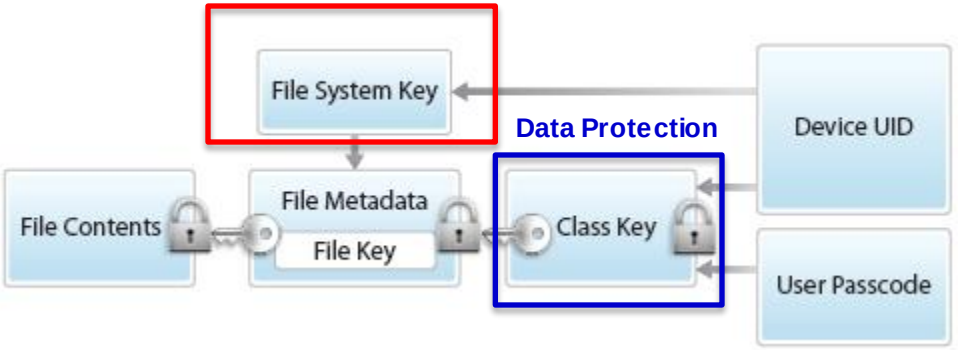
La **chiave** viene criptata con una "CLASS KEY" e inserita nei metadati del file.

I Metadati sono criptati con una "File System Key"

La "CLASS KEY" è protetta da un HARDWARE UID e dalla password dell'utente.

(ES Dkey per la maggior parte dei file)

File System Encryption (EMF)



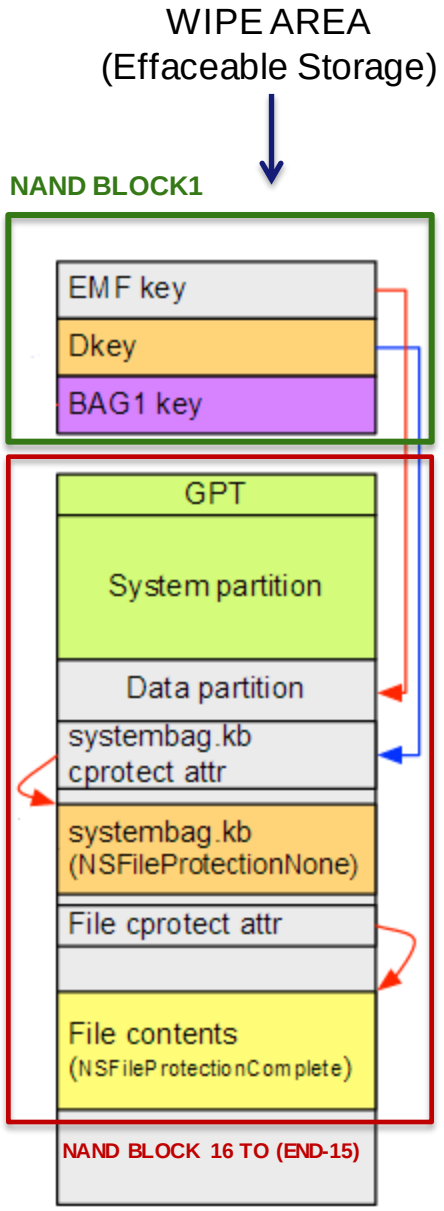
DATA ENCRYPTION

- Ogni file è criptato con una chiave diversa.
- La chiave che cripta il file è criptata con la chiave del DATA PROTECTION.
- Il risultato delle criptazione della chiave che cripta il file viene salvato nei metadati del file.
- Il metadato che descrive il file viene criptato con la chiave di criptazione del File System.

DATA ENCRYPTION: FILE SYSTEM ENCRYPTION

File System encryption protects the raw File System. If you were to remove and dump the contents of the NAND chip inside an iOS device, you'd find that the entire **File System portion of the NAND is encrypted.**

The encryption key used to encrypt the "DATA USER" File System is named "*EMF*" stored into the block 1 of the NAND.



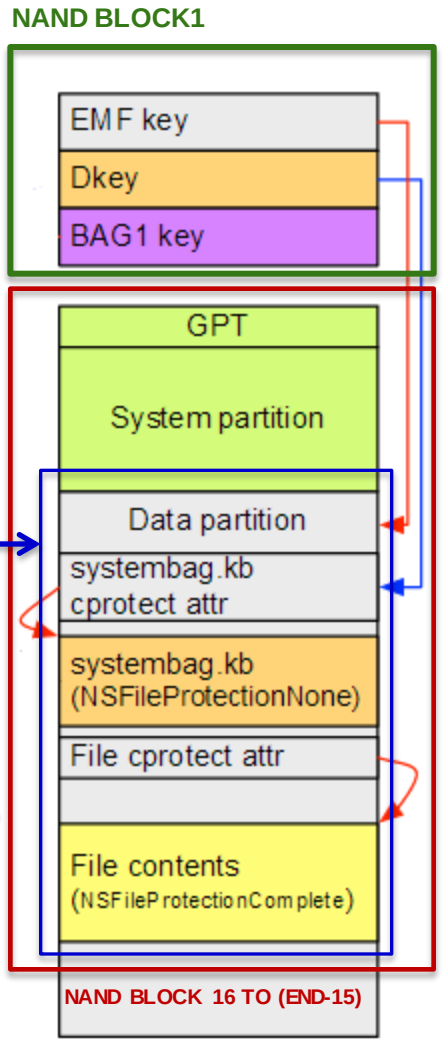
https://code.google.com/p/iphone-dataprotection/wiki/EncryptionKeys

DATA ENCRYPTION: FILE SYSTEM ENCRYPTION

Starting from iPhone 3GS, iDevices contain a cryptographic chip that performs hardware encryption of the filesystem.

The NAND chip is a flash memory organized as the following:

- Block 1 : contains the following encryption keys:
  - **EMF** : used to encrypt the **DATA PARTITION**.
  - **Dkey**: used to encrypt the master key of the protection class "NSFileProtectionNone" (the majority of files)
  - **BAG1**: used with the passcode to produce the encryption keys for the other master keys (for files like Mails...).
- Block 16 to (END-15): contains the HFS+ filesystem.

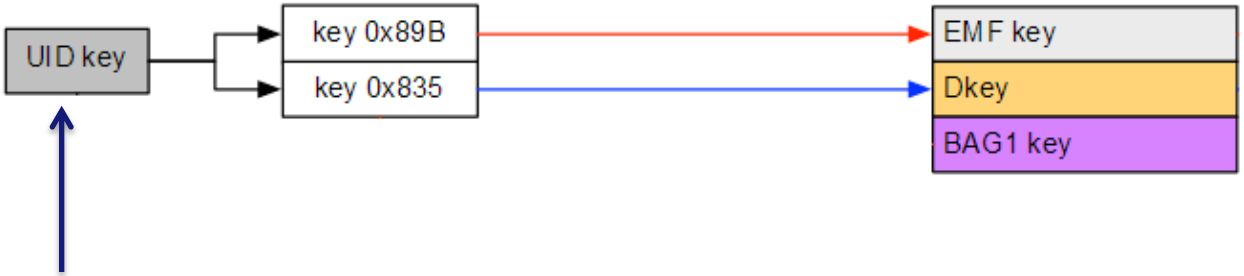


https://code.google.com/p/iphone-dataprotection/wiki/EncryptionKeys

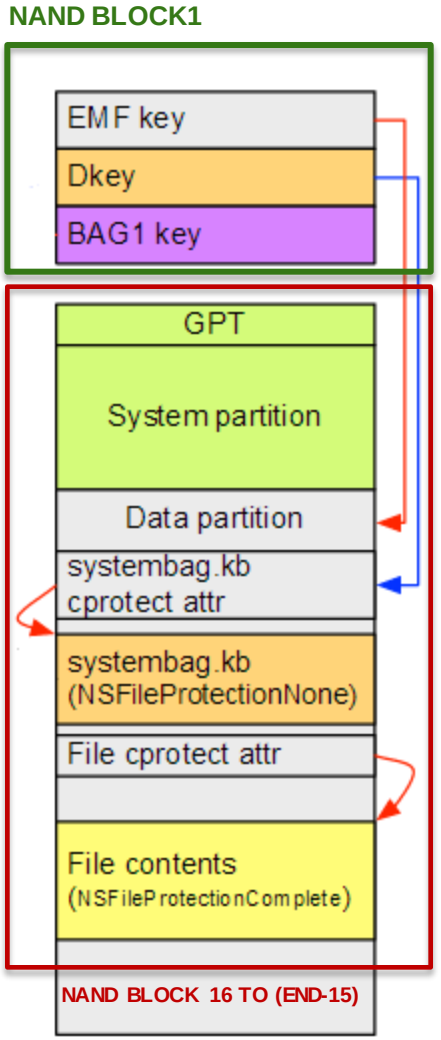
HACK IN BO
SICUREZZA ALL'OMBRA DELLE TORRI

DATA ENCRYPTION: FILE SYSTEM ENCRYPTION

EMF and Dkey keys are automatically extracted from Block 1 of the NAND in order to decrypt the the HFS+ filesystem "Data Partition".



UID key: hardware key (256 bit) embedded in the application processor AES engine, unique for each device. This key is not accessible by the CPU. The UID is also not available via JTAG or from any kind of debug interface.



https://code.google.com/p/iphone-dataprotection/wiki/EncryptionKeys

DATA ENCRYPTION: PROTECTION CLASS

"This technology is designed with mobile devices in mind, taking into account the fact that they may always be turned on and connected to the Internet, and may receive phone calls, text, or emails at any time.

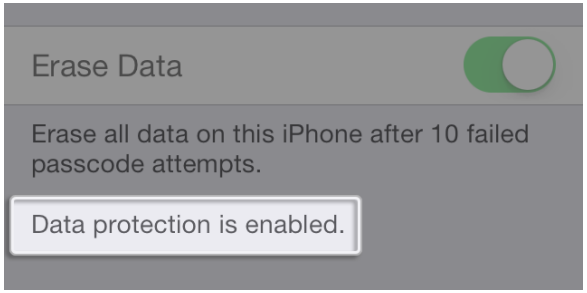
Data Protection allows a device to respond to events such as incoming phone calls without decrypting sensitive data and downloading new information while locked. These individual behaviours are controlled on a per-file basis by assigning each file to a class, as described in the "Classes" section later in document.

(24/09/2014)

DATA ENCRYPTION: PROTECTION CLASS

Data protection is available for devices that offer hardware encryption, including iPhone 3GS and later, all iPad models, and iPod touch (3rd generation and later).

Enable data protection by configuring a passcode for your device.



http://support.apple.com/kb/ht4175

HACK IN BO
SICUREZZA ALL'OMBRA DELLE TORRI

DATA ENCRYPTION: PROTECTION CLASS

HIGHT

Availability	File Data Protection
When unlocked	NSFileProtectionComplete
While locked	NSFileProtectionCompleteUnlessOpen
After first unlock	NSFileProtectionCompleteUntilFirstUserAuthentication
Always	NSFileProtectionNone

LOW

METADATI FILE

EMF + F(Bag1 key + Passcode)

EMF + Dkey

iOS Security October 2012

DATA ENCRYPTION: PROTECTION CLASS

NSFileProtectionComplete.

The class key is protected with a key derived from the user passcode and the device UID. The decrypted class key is discarded, rendering all data in this class inaccessible until the user enters the passcode again or unlocks the device using Touch ID.

NSFileProtectionCompleteUnlessOpen.

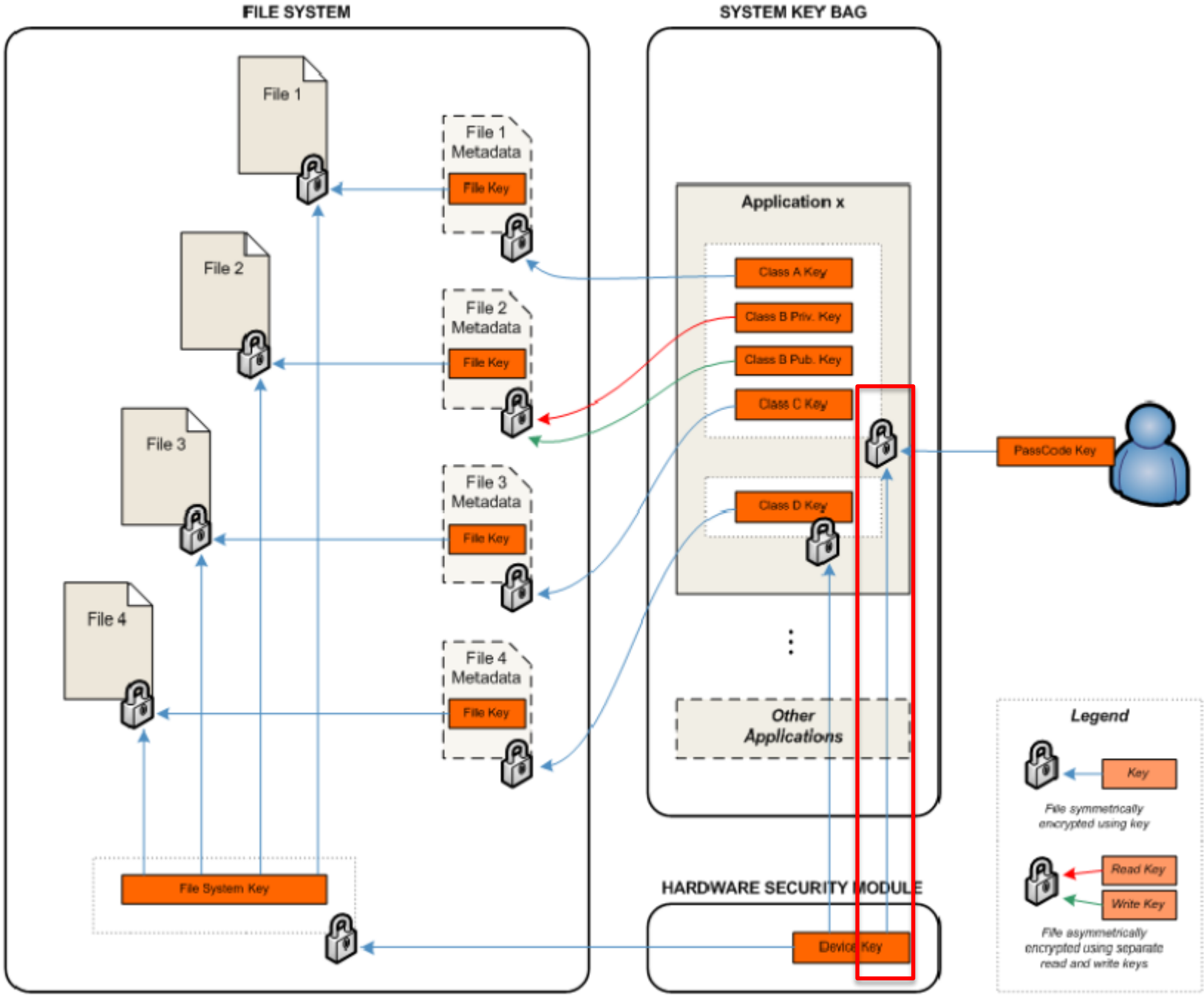
Some files may need to be written while the device is locked. A good example of this is a mail attachment downloading in the background.

NSFileProtectionCompleteUntilFirstUserAuthentication.

This class behaves in the same way as Complete Protection, except that the decrypted class key is not removed from memory when the device is locked.

NSFileProtectionNone.

This class key is protected only with the UID, and is kept in Effaceable Storage. This is the default class for all files not otherwise assigned to a Data Protection class.


FILE SYSTEM
SYSTEM KEY BAG
File 1
File 1 Metadata
File Key
File 2
File 2 Metadata
File Key
File 3
File 3 Metadata
File Key
File 4
File 4 Metadata
File Key
File System Key
Application x
Class A Key
Class B Priv. Key
Class B Pub. Key
Class C Key
Class D Key
PassCode Key
Other Applications
HARDWARE SECURITY MODULE
Device Key
Legend
Key
File symmetrically encrypted using key
Read Key
Write Key
File asymmetrically encrypted using separate read and write keys

DATA ENCRYPTION: PROTECTION CLASS

When a Protection Class is used each individual file is encrypted with a unique key. When any file on the File System is deleted, the unique key for that file is discarded, which make the file unrecoverable.

- **File system's wiping consists of rewriting the EMF, Dkey and BAG1 Key.**
- **Files deletion consists of deleting the associated Key (cprotect).**

DATA ENCRYPTION: KEYBAGS

The keys *for services and* ***keychain Data Protection*** *classes are collected and managed in keybags.*

iOS uses the following keybags:

- ***System****: is where the wrapped class keys used in normal operation of the device are stored .*
- ***Backup****: is created* ***when an encrypted backup is made by iTunes*** *and stored on the computer to which the device is backed up.*
- ***Escrow****: is used for iTunes syncing and Mobile Device Management (MDM).* ***This keybag allows iTunes to back up and sync without requiring the user to enter a passcode****, and it allows an MDM server to remotely clear a user's passcode. It is stored on the computer that's used to sync with iTunes, or on the MDM server that manages the device.*
- ***iCloud****: is similar to the Backup keybag.*

QUESTION?

Litiano Piccin
CIFI-CHFI-ACE-AME
litiano@studiopiccin.it