Guida alla cifratura dei dati

Versione 1.2 –03 marzo 2022

SOMMARIO

1. Premessa

I dati personali sono informazioni che identificano direttamente o indirettamente una persona fisica e che possono fornire informazioni sulle sue caratteristiche, quali i dati anagrafici, il codice fiscale, una targa, ma anche quei dati che rivelano lo stato di salute, le opinioni politiche, l'appartenenza sindacale ecc .

Viste le disposizioni di legge nazionali e le normative internazionali (*Regolamento Ue 679/2016* anche "*GDPR*", c.d. Codice Privacy e ss.mm.ii.), nonché le *Istruzioni generali per il trattamento dei dati personali, ai sensi dell'Articolo 32, comma 4 del Regolamento Europeo per la Protezione dei Dati (GDPR)* di Ateneo, il Settore Cybersecurity, Protezione Dati e Conformità invita gli utenti che abbiano la necessità di trasmettere o trattare tali dati a leggere il seguente documento, in modo da mettere in atto azioni di prevenzione sul trattamento dei dati personali propri o di terzi.

A tal proposito ricordiamo che come previsto dalle suindicate Istruzioni Generali dell'Ateneo, è richiesta obbligatoriamente l'adozione della cifratura per tutti i supporti esterni (es. chiavette USB, dischi Esterni) e per i computer portatili utilizzati per trattare dati personali per conto dell'Ateneo al fine di ridurre il rischio collegato al data breach in caso di smarrimento o furto del computer.

Per cifratura, si intende infatti un processo crittografico (utilizzato pertanto spesso come sinonimo di "crittografia") che tramite l'utilizzo di un algoritmo matematico agisce su una sequenza di caratteri, trasformandola e rendendola illeggibile agli utenti che non sono in possesso della chiave di decifratura. Tale processo rappresenta quindi una misura di sicurezza volta a garantire, in base alla metodologia utilizzata, la riservatezza e l'integrità delle informazioni cifrate.

La presente guida è, quindi, stata redatta con l'obiettivo di **descrivere alcuni strumenti da utilizzare al fine di cifrare i dati di cui si volesse preservare la confidenzialità** memorizzati su dispositivi di tipo Windows, MacOS o Linux o durante il loro trasferimento.
Per ulteriori approfondimenti ed indicazioni di tipo tecnico di maggior dettaglio rispetto a quelle fornite all'interno del presente documento, si rimanda alla *Guida alla cifratura dei dati* di Ateneo.

L'esecuzione di alcune delle operazioni descritte nel presente documento potrebbero richiedere il possesso di competenze di livello tecnico informatico e/o di privilegi di tipo amministrativo. In tal caso **potrebbe essere necessario richiedere supporto tecnico e/o operativo al referente tecnico preposto (referente di struttura o referente tecnico del servizio) prima di procedere**: il Settore Cybersecurity, Protezione Dati e Conformità, che ha curato la stesura del presente documento, non è infatti deputato a fornire assistenza operativa in tal senso.

Ulteriori informazioni utili in materia di sicurezza ICT e protezione di dati personali, in ogni caso, possono essere reperite nella sezione dedicata del portale di Ateneo raggiungibile a partire da https://work.unimi.it/servizi/security_gdpr/118582.htm

Si specifica, infine, che il Settore Cybersecurity, Protezione Dati e Conformità non risponde di alcun danno o malfunzionamento derivante dall'applicazione non corretta o non rispondente alle stesse. Si invitano i suoi destinatari delle presenti linee guida consultare periodicamente la sezione dedicata del sito di Ateneo in modo da verificare di disporre di documenti sempre aggiornati.

2. Gli strumenti descritti nelle presenti linee guida

In ambito informatico, **la crittografia può essere definita come una tecnica che converte i dati attraverso l'utilizzo di una chiave (password o pin) in un formato illeggibile al fine di minimizzare** il rischio di una loro accidentale diffusione. Per ottenere dai dati cifrati quelli originali è necessaria l'applicazione della chiave di decifratura segreta. Le chiavi di cifratura e decifratura possono coincidere.
Esistono vari strumenti per crittografare dati in accordo con il sistema operativo utilizzato. Tra i principali annoveriamo quelli trattati in questa guida, ovvero:

- *BitLocker Drive Encryption*: funzionalità integrata nei sistemi Microsoft Windows Vista e successivi;
- *FileVault*: tecnologia presente nel sistema operativo Mac OS X, e successivi;
- *VeraCrypt*: programma applicativo open source multipiattaforma disponibile per sistemi Windows, Mac OSX e Linux;
- *Kleopatra*: programma applicativo gratuito per cifrare file in sistemi Windows;

Le prime due soluzioni, *BitLocker Drive Enrcyption* e *FileVault*, possono essere utilizzate per la cifratura del disco, mentre le altre, *VeraCrypt* e *Kleopatra*, consentono la cifratura rispettivamente di volumi[1] e singoli file.

In calce al documento, sono inoltre riportate informazioni relative alla soluzione di Azure Information Protection che consente di classificare tramite etichettatura il livello di riservatezza di file e cartelle e, a seconda della tipologia di etichetta selezionata, cifrarne i dati.

3. Avvertenza

È opportuno sottolineare che **tutti gli strumenti di seguito descritti richiedono la disponibilità di chiavi di cifratura e/o decifratura (password, pin o *passphrase)* da conservare con estrema cura in un luogo sicuro e distinto da quello in cui sono conservati i dati cifrati. Nel caso in cui le suddette chiavi fossero smarrite non sarebbe più possibile recuperare i dati. Inoltre, è importante che la chiave di decifratura rimanga segreta perché chiunque ne entri in possesso può leggere i dati.**
Si raccomanda fortemente, inoltre, di **effettuare un backup dei dati da cifrare prima di intervenire su di essi.**

4. BitLocker Drive Encryption

Nei più recenti sistemi operativi Microsoft è integrata una funzionalità di protezione dei dati denominata ***BitLocker Drive Encryption* che permette di crittografare** l'intera partizione del sistema operativo o di una unità dati rimovibile.

Una volta cifrati, i dati possono essere decifrati soltanto da utenti che dispongono della chiave crittografica appropriata (ad esempio una password). Ne consegue che per cifrare un'unità di Windows è necessario accedere con un account da amministratore.

[1] Partizione o semplice cartella, salvata in locale sul PC oppure su un dispositivo esterno.

Quando viene abilitato BitLocker, **è necessario creare un PIN che sarà richiesto ogni volta che il computer viene acceso**. **Inoltre, viene generata una chiave di ripristino**, utilizzata per accedere al computer quando viene dimenticata la password.

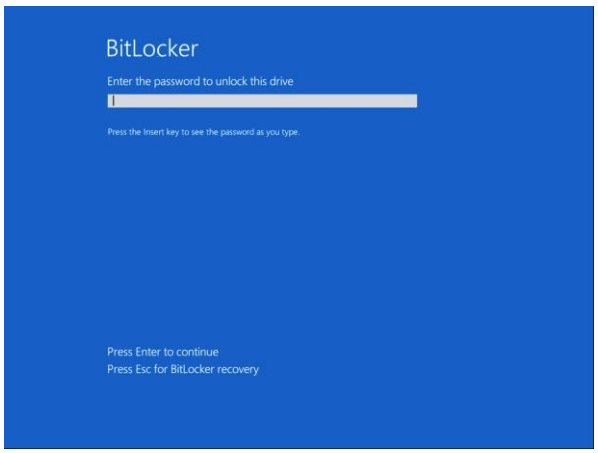


Figura 1- Richiesta inserimento password del BitLocker

3.1 Requisiti minimi e richieste addizionali

Per utilizzare il BitLocker il computer deve soddisfare alcuni requisiti:

- Sistemi operativi supportati:
  - Windows 10 nelle versioni Education, Pro, o Enterprice;
  - Windows 8 nelle versioni Professional o Enterprice;
  - Windows 7 nelle versioni Enterprice o Ultimate.
  - Per il sistema operativo Windows 7, il modulo TMP nella versione 1.2 o superiore deve essere installato, abilitato e attivato.
- Per il sistema operativo Windows 7, il modulo TMP nella versione 1.2 o superiore deve essere installato, abilitato e attivato.

- Richieste addizionali:
  - Accedere al computer come Amministratore.

3.2 Avvertenza

Qualora si perdesse o si dimenticasse sia PIN che la chiave di recupero di BitLocker, i dati cifrati non saranno più reperibili, per cui è fortemente consigliabile effettuare un backup prima di configurare il BitLocker.

3.3 Attivazione e configurazione di BitLocker

Vengono di seguito riportati i passaggi per abilitare BitLocker e procedere alla cifratura dell'unità che si desidera proteggere (hard disk interno, chiavetta USB, disco removibile, ecc.).
Per le versioni da Windows Vista in poi e precedenti Windows 10 occorre:

1. Digitare nella barra di ricerca di Windows *Gestione BitLocker*, oppure aprire il **Pannello di controllo** > **Sistema e sicurezza** > **Crittografia unità BitLocker**;

2. Selezionare il dispositivo da crittografare e cliccare su **Attiva BitLocker**;

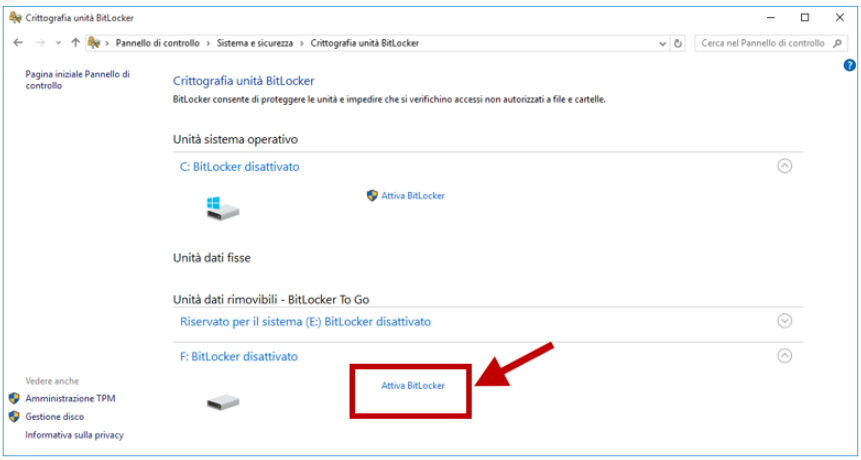


Figura 2 - Attivazione del BitLocker

3. Attendere il termine del processo per avviare BitLocker;

4. Scegliere il metodo desiderato (password oppure *smart card*) per proteggere l'unità e cliccare su **Avanti**;

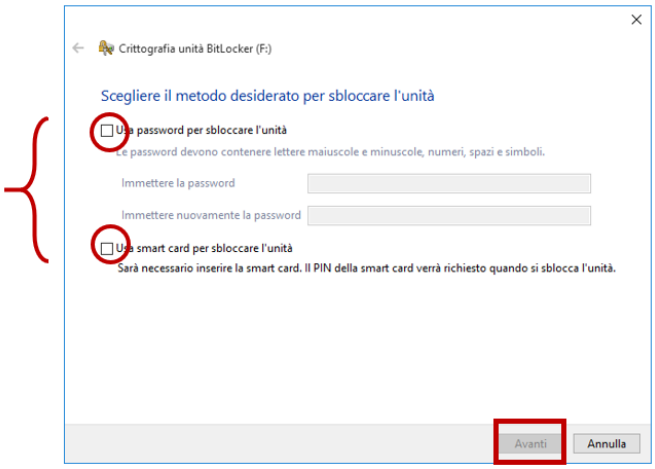
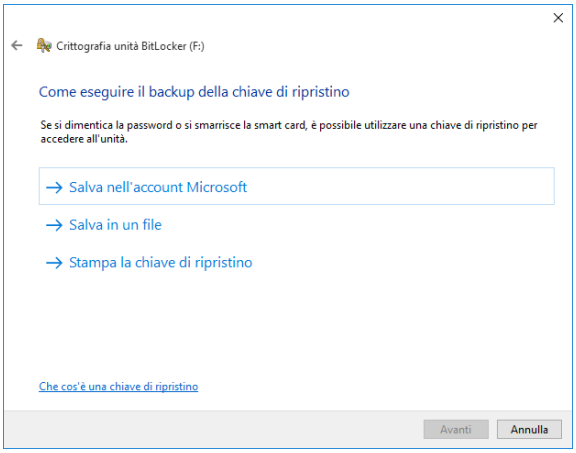


Figura 3 - Smart card o password per sbloccare il Bitlocker

5. Scegliere dove eseguire il backup della chiave di ripristino (delle tre opzioni è preferibile scegliere la prima) e cliccare su **Avanti**;



6. Figura 4 - Chiave di ripristino del BitLockerScegliere se applicare la crittografia soltanto allo spazio utilizzato del disco oppure all'intera unità (è preferibile scegliere questa seconda ipotesi) e cliccare su **Avanti**, quindi attendere il completamento dell'operazione.

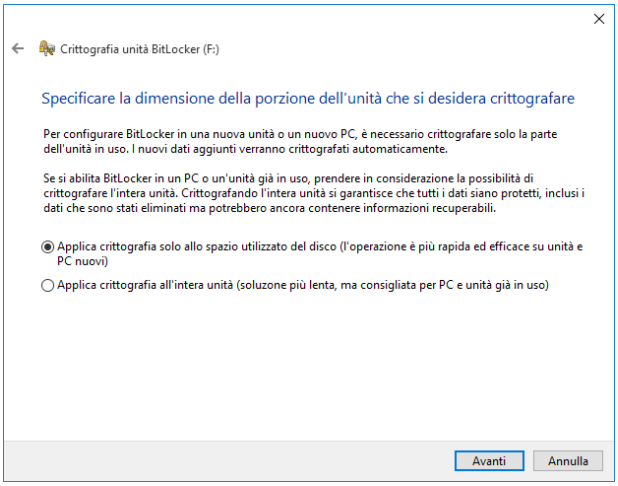


Figura 5 - Dimensione dell'unità da crittografare

In Windows 10, per attivare la funzionalità BitLocker è sufficiente cliccare col tasto destro sull'unità da proteggere, scegliere il comando **Attiva BitLocker** e seguire le istruzioni.

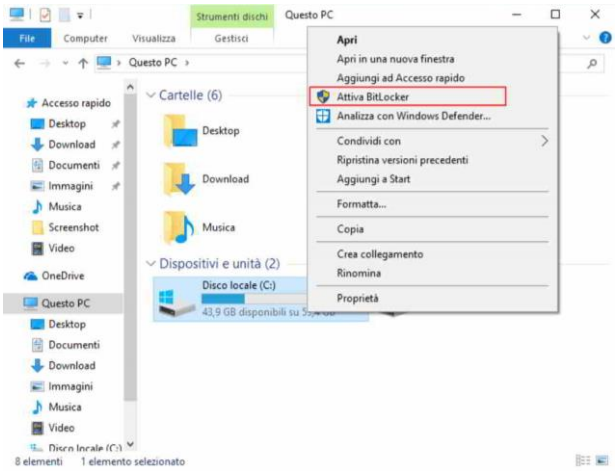


Figura 6 - Attivare Bitlocker su Windows10Maggiori informazioni sono reperibili nel sito ufficiale di Microsoft.

5. FileVault

FileVault è una tecnologia Apple per criptare i dati su MacOS e hardware Mac.
Tale tecnologia permette di cifrare tutti i dati sul disco di avvio, ma consente di cifrare anche i backup *Time Machine*. Gli utenti devono inserire la password ad ogni riavvio del computer, quando il computer viene riattivato dopo uno stand-by o screensaver.
Quando viene abilitato FileVault, è necessario creare una password che sarà richiesta ogni volta che il computer viene acceso. Inoltre, il sistema chiederà di generare una chiave di ripristino, utilizzata per accedere al computer quando viene dimenticata la password, oppure utilizzare l'account iCloud come una chiave.

4.1 Requisiti minimi e richieste addizionali

Per utilizzare il FileVault il computer deve soddisfare alcuni requisiti:

- Sistemi operativi supportati:
  - OS X Lion o versioni successive.
- Richieste addizionali:
  - Accedere al computer come Amministratore.

4.2 Avvertenza

Qualora di perdesse o si dimenticasse sia la password del proprio account che la chiave di recupero di FileVault, i dati cifrati non sarebbero più reperibili, per cui è fortemente consigliabile effettuare un backup prima di utilizzare FileVault.

4.3 Attivazione e configurazione di FileVault

Vengono di seguito riportati i passaggi per abilitare FileVault:

1. Scegliere menu Apple > Preferenze di Sistema, quindi cliccare su Sicurezza e Privacy e **cliccare su FileVault**;

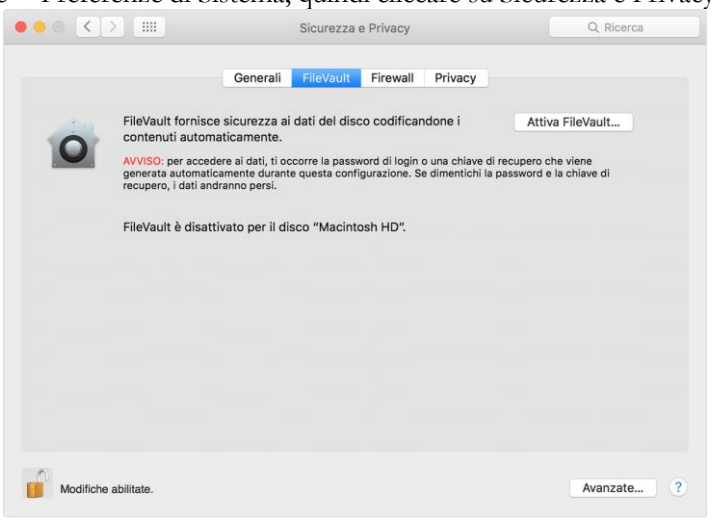


Figura 7 - Attivazione FileVault

Cliccare su  , quindi immettere un nome e relativa password di amministratore;

2. Cliccare su Attiva FileVault;

Se un messaggio avvisa che il computer deve riavviarsi, cliccare su **Riavvia**. Dopo il riavvio, eseguire il login e tornare al pannello **FileVault**.

Se sul Mac sono presenti account di altri utenti, cliccare su **Abilita utente** e inserire la password dell'utente. Gli account utente aggiunti dopo l'attivazione di FileVault vengono abilitati automaticamente.

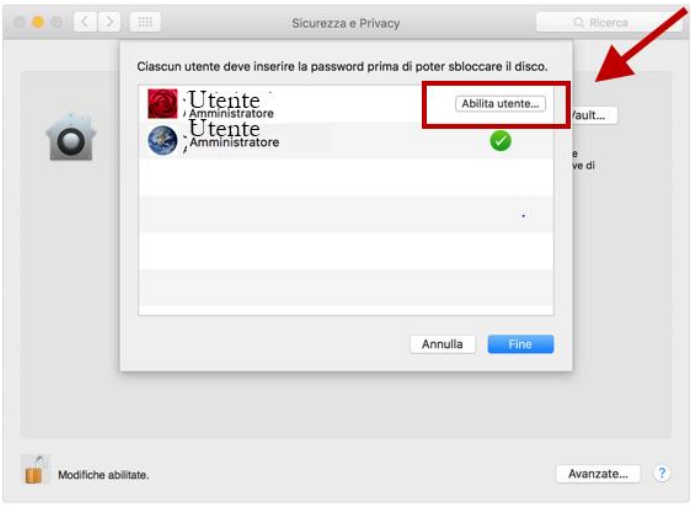


Figura 8 - Abilitazione utente su FileVault

3. Scegliere come sbloccare il disco e reimpostare la password di login se dimenticata (sono disponibili due opzioni), poi cliccare su **Continua** e successivamente su **Riavvia**.

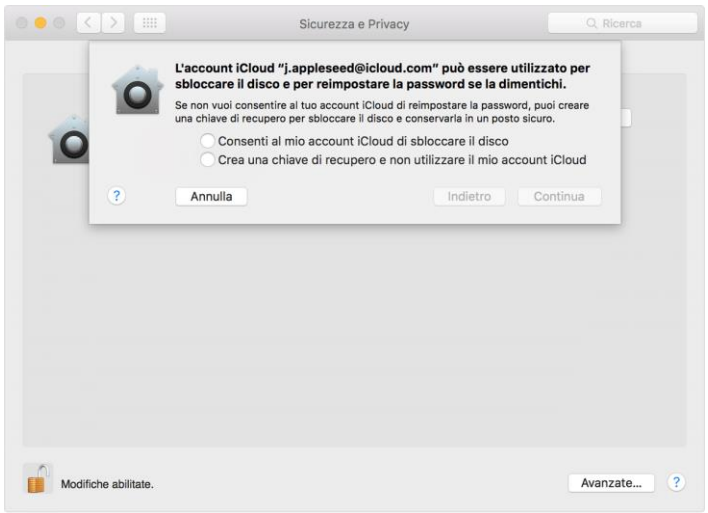


Figura 9 - Accesso ad iCloud

Maggiori informazioni sono reperibili nel sito ufficiale della Apple.

6. VeraCrypt

VeraCrypt è un programma applicativo *opensource* multipiattaforma, disponibile per Windows, MacOSX e Linux.

È un software utilizzato per creare e mantenere cifrato un volume, cioè un supporto di memorizzazione dei dati. I dati sono automaticamente cifrati prima di essere salvati e sono decifrati dopo che sono caricati, senza alcun intervento dell'utente.

Le principali caratteristiche di VeraCrypt sono:

- creazione di contenitori di file cifrati;
- cifrare interi volumi o partizioni;
- cifrare l'intero sistema operativo;
- può essere eseguito in modalità portatile, consentendo l'utilizzo dalla chiavetta USB senza alcuna installazione.

5.1 Requisiti minimi e richieste addizionali

Per utilizzare VeraCrypt il computer deve soddisfare alcuni requisiti:

- Sistemi operativi supportati:
    - Windows Xp e successivi (e.g. Vista, 7, 8 e 8.1,10);
    - Windows Server (2003, 2008, 2012);
    - MacOsX Lion e successivi;
    - Linux x86 (32-bit e 64 bit, kernel 2.6 o compatibile);
    - FreeBSF x86 (32-bit e 64 bit, dalla versione 11).

- Richieste addizionali:
    - Accedere al computer come Amministratore.

5.2 Avvertenza

Qualora si perdesse o si dimenticasse sia la password del proprio account che la chiave di recupero di VeraCrypt, i dati cifrati non sarebbero più reperibili, per cui è fortemente consigliabile effettuare un backup prima di utilizzare VeraCrypt.

5.3 Installazione di VeraCrypt

Il seguente tutorial si riferisce al sistema operativo Windows 10, per sistemi operativi diversi si consiglia di consultare la documentazione presente nel sito di VeraCrypt: https://www.veracrypt.fr.

Prima di utilizzare il software VeraCrypt, scaricabile dalla sezione *Download* del sito del produttore, è opportuno verificare la versione stabile compatibile con il proprio sistema operativo.

Dopo aver scaricato l'*installer*, provvedere ad avviare l'eseguibile.

Accettati i termini della licenza effettuare l'installazione, seguendo le indicazioni fornite dal software.

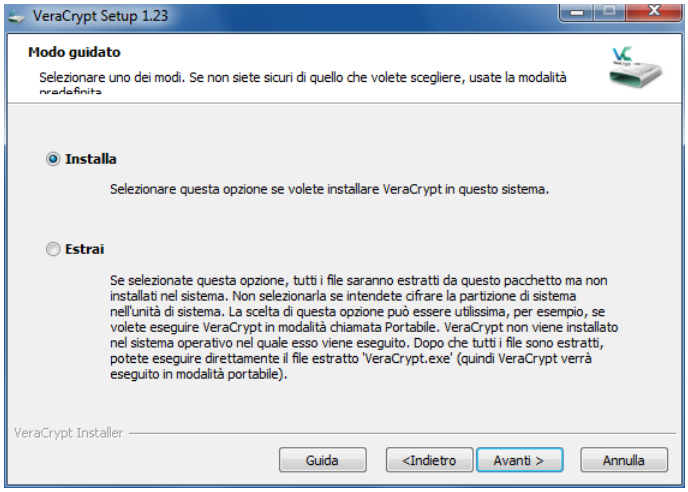


Figura 10 - Setup di VeraCrypt

La parte finale dell'installazione consiste nel definire la posizione dove installare il programma.

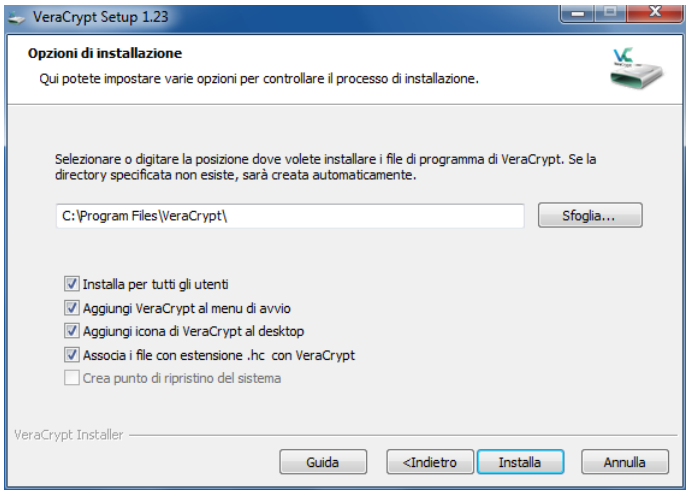


Figura 11 - Opzioni di setup di VeraCrypt

5.4 Configurazione di VeraCrypt

Di seguito vengono riportate le operazioni principali da eseguire per creare, montare ed utilizzare un volume VeraCrypt.

5.4.1 Creazione di un volume VeraCrypt

1. Dopo aver aperto il software cliccare su **Create Volume**;

2. A questo punto sono disponibili tre diverse opzioni:

   - **Create an encrypted file container** permette di cifrare un disco all'interno di un file ed è raccomandato per i principianti;

   - **Encrypt a non-system partition/drive** permette di cifrare unità interne/esterne e dà anche la possibilità di creare un volume nascosto;
   - **Encrypt the system partition or entire system drive** permette di cifrare l'intero sistema operativo (quindi per avere accesso al computer sarà necessario inserire la password corretta prima dell'inizializzazione del computer).

In questa guida si è scelto di mostrare come creare un volume VeraCrypt all'interno di un file, quindi occorre selezionare la prima opzione e cliccare su **Next**.

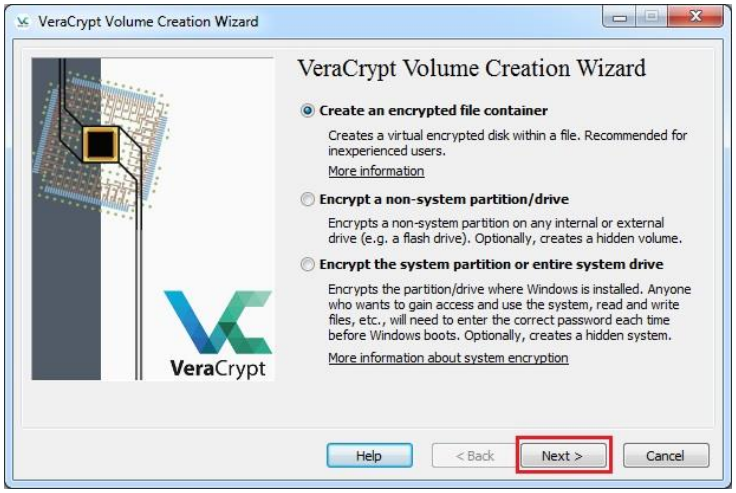


Figura 12 - Selezione del volume in VeraCrypt

3. Scegliere se creare un volume VeraCrypt standard (**Standard VeraCrypt**) o nascosto (**Hidden VeraCrypt volume**);
4. Scegliere dove creare il volume di VeraCrypt cliccando su **Select File** (apparirà una finestra di selezione di file; la finestra della creazione guidata del volume di VeraCrypt rimarrà aperta sullo sfondo);

5. Selezionare il percorso desiderato (dove si desidera creare il contenitore), digitare in **File name** il nome del file contenitore desiderato e cliccare su **Save** (sparirà la finestra di selezione di file), in questo esempio *My Volume* in *F:\Data*;

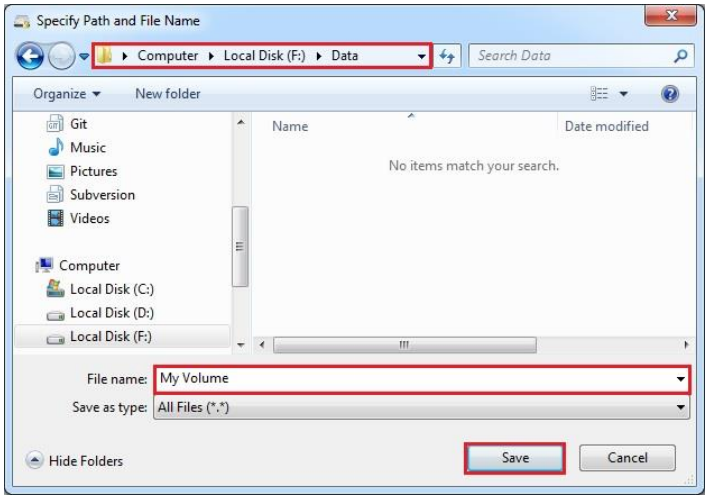


Figura 13 - Creazione del volume in VeraCrypt

Quando viene creato un contenitore di file, VeraCrypt non effettua alcuna operazione di cifratura ad alcun file esistente. Se si seleziona un file esistente in questo passaggio, tale file verrà sovrascritto e sostituito dal volume appena creato, perdendo il file precedente. In seguito sarà possibile cifrare i file esistenti spostandoli sul volume VeraCrypt creato.

6. Nella finestra della creazione guidata del volume di VeraCrypt cliccare su **Next**;

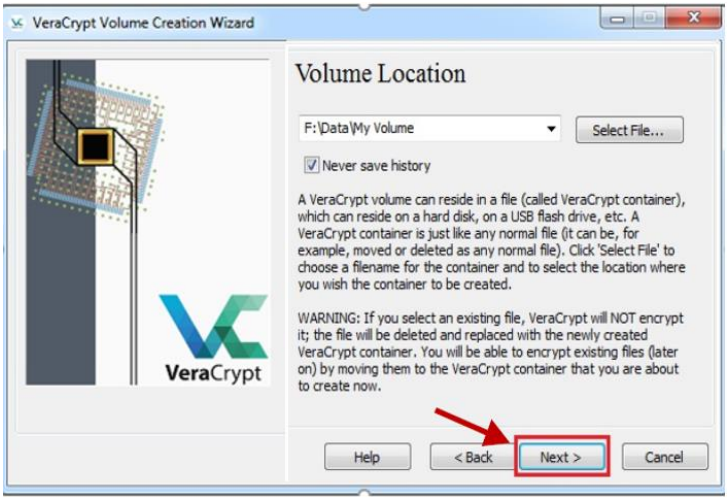


Figura 14 - Creazione del volume su VeraCrypt

7. Scegliere un algoritmo di cifratura e di hash per il volume e cliccare su **Next**;

Figura 15 - Opzioni di cifratura su VeraCrypt

8. Specificare la dimensione del contenitore VeraCrypt e cliccare su **Next** (es. 250 megabyte);

9. Scegliere una password per il volume, digitarla in **Password** e successivamente in **Confirm**, quindi cliccare su **Next**;

10. Muovere il mouse il più casualmente possibile all'interno della finestra della creazione guidata (almeno finché l'indicatore di casualità diventa verde), quindi cliccare su **Format**;

Si consiglia di muovere il mouse per almeno 30 secondi.

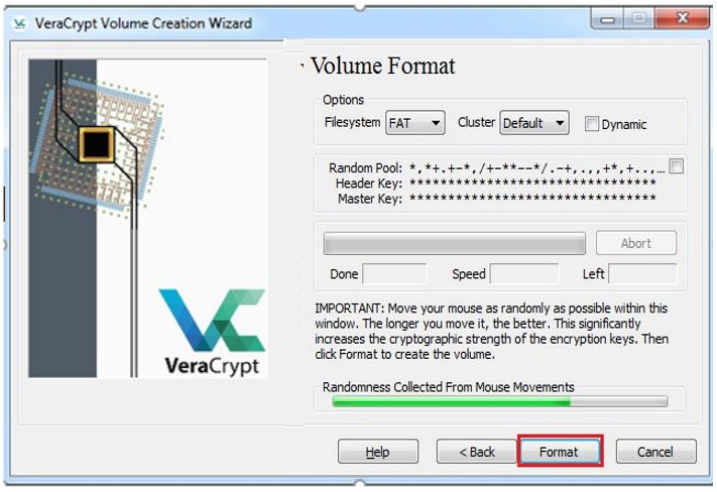


Figura 16 - Creazione del volume in VeraCrypt

11. Attendere la creazione del volume (il processo potrebbe richiedere molto tempo, a seconda delle dimensioni del volume), al termine verrà visualizzata la finestra di dialogo di seguito riportata, quindi cliccare su **OK**;

In questo passaggio VeraCrypt crea un file chiamato *My Volume* nella cartella *F:\Data* (come specificato al punto 5). Tale file sarà un contenitore VeraCrypt:

12. Una volta creato il volume VeraCrypt cliccare su **Exit** per chiudere la finestra della procedura guidata.

5.4.2 Mount di un volume VeraCrypt

1. Avviare VeraCrypt e selezionare l'unità dall'elenco sulla quale montare il contenitore VeraCrypt e cliccare su **Select File**, cercare il file contenitore e selezionarlo, quindi cliccare su **Open;**

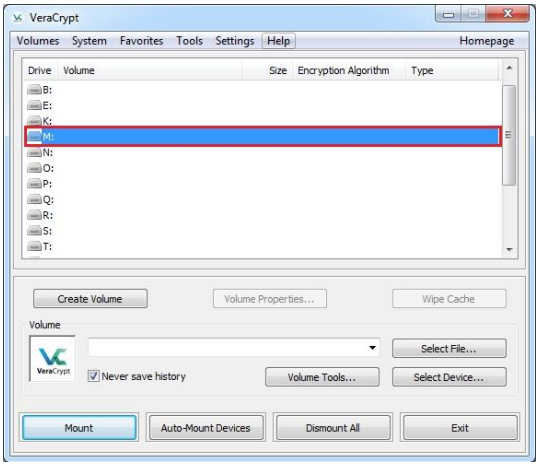


Figura 17 - Mount del volume in VeraCrypt

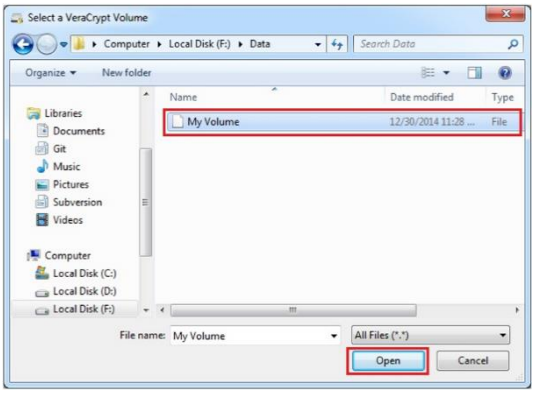


Figura 18 - Selezione del volume in VeraCrypt

2. Nella finestra principale di VeraCrypt cliccare su **Mount;**

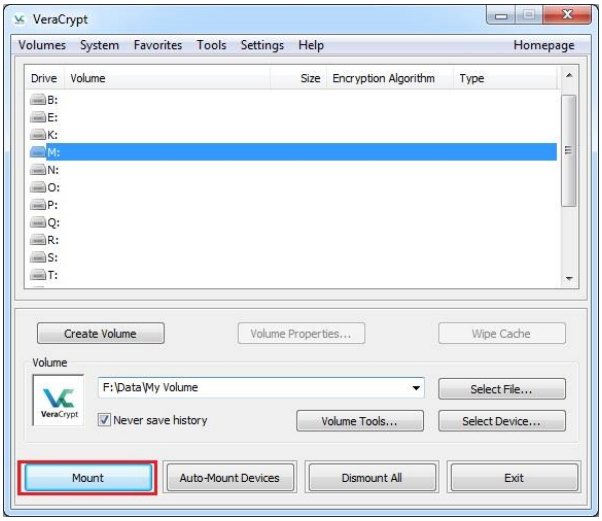


Figura 19 - Drive del volume in VeraCrypt

3. Inserire la password nell'apposito campo, selezionare l'algoritmo PRF (Pseudo-Random Function) che è stato usato durante la creazione del volume, è possibile usare l'*autodetection*, ma il processo di montaggio richiederà più tempo, il default è HMAC-SHA512

4. creazione del volume

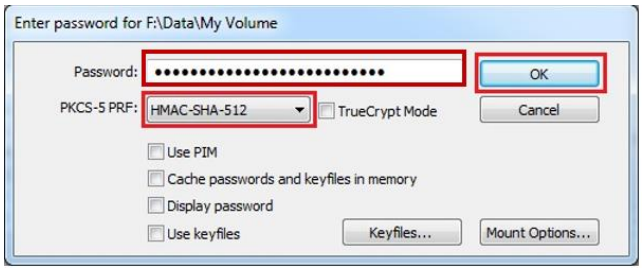


Figura 20 - Password del volume in VeraCrypt

5. Il contenitore è stato montato con successo come disco virtuale *M*;

Nel disco virtuale si possono salvare (copiare, spostare, ecc.) file che vengono cifrati nel momento in cui sono scritti.

5.4.3 Dismount di un volume VeraCrypt

1. Avviare VeraCrypt, selezionare il volume che si vuole rendere inaccessibile e cliccare su **Dismount**:

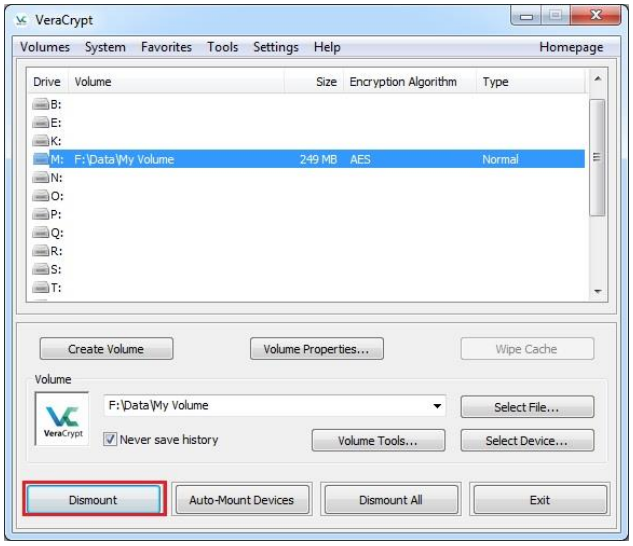


Figura 21 - Dismount del volume in VeraCrypt

Il *dismount* di un volume avviene automaticamente al momento del riavvio o dello spegnimento del computer.

7. Gpg4win (Keopatra)

Gpg4win è una collezione di software Open Source pensati per la crittografia dei file su sistemi operativi Windows.

6.1 Installare e cifrare file con Gpg4win (Kleopatra)

È possibile scaricarlo all'indirizzo https://gpg4win.org/thanks-for-download.html. Una volta eseguita l'installazione, sarà possibile utilizzare lo strumento "Kleopatra".

Una volta avviato il programma, per cifrare un file fare click sul tasto "firma/cifra…" in alto a sinistra:

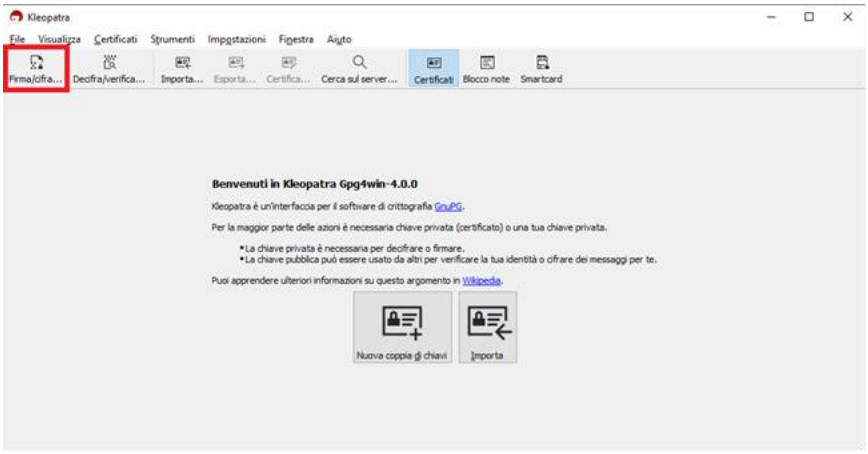


Figura 22 - Cifrare un file in Windows con Kleopatra

E selezionare il file da cifrare (in questo esempio viene illustrato un file Excel, ma è possibile cifrare qualunque file, comprese le cartelle .zip):

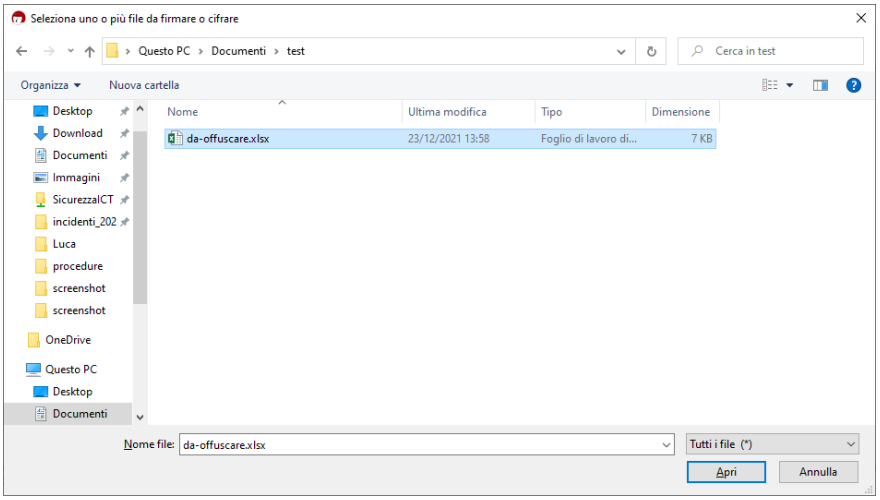


Figura 23 - Selezionare file da cifrare con Kleopatra

Successivamente compare una finestra di riepilogo come quella seguente:

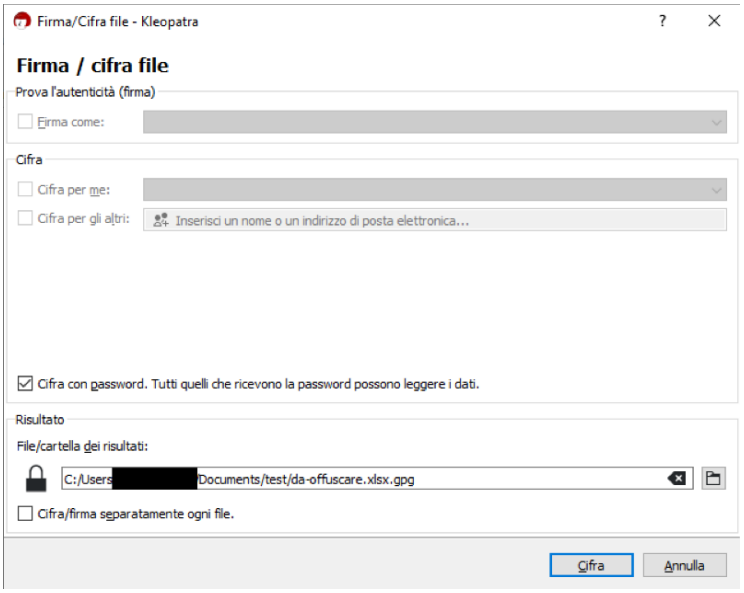


Figura 24 - Salvare file da cifrare in Kleopatra

Fare click su "Cifra" e inserire la password nel campo passphrase quando compare la relativa finestra (si faccia riferimento alle linee guida presenti all'indirizzo https://work.unimi.it/servizi/servizi_tec/59030.htm per indicazioni sui requisiti sulle creazioni delle password):

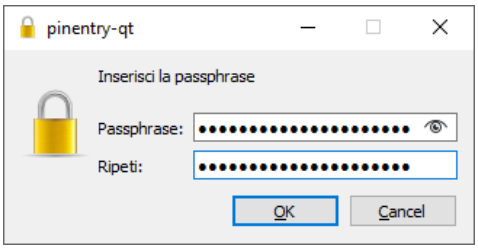


Figura 25 - Inserimento passphrase in Kleopatra

Se la passphrase inserita risulta "debole", il software ne darà un avviso e si raccomanda di sceglierne una più forte.
Un'ultima finestra comunicherà l'avvenuta cifratura del file. Fare click su Fine.
Il file cifrato avrà come estensione standard il formato .gpg appeso in fondo al nome del file.

6.2 Decifrare file con Gpg4win (Kleopatra)

Per decifrare un file in formato gpg su Windows sarà sufficiente aprirlo con Kleopatra, facendo doppio click sullo stesso o premendo il tasto "Decifra/verifica…". A questo punto sarà sufficiente inserire la password nell'apposito campo e dare indicazione di salvataggio al programma. In ogni caso, una volta selezionato il file si aprirà la seguente finestra in cui verrà richiesto di inserire la password:

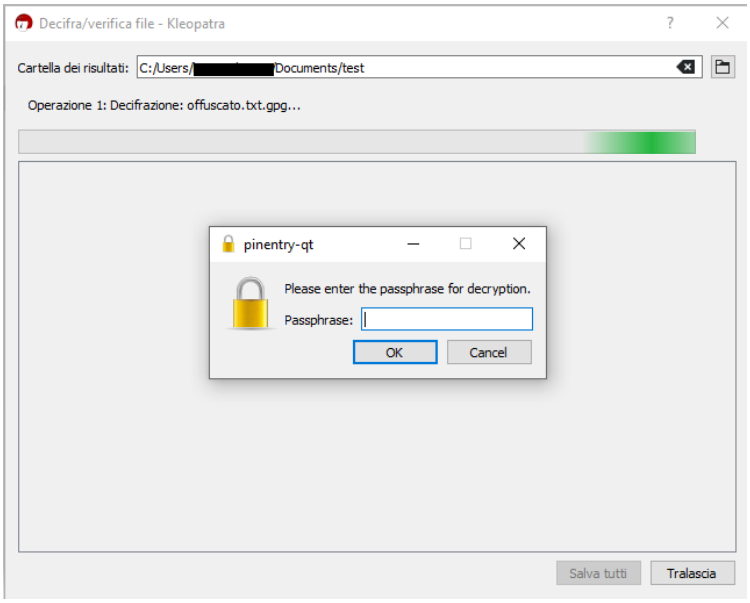


Figura 26 - Decifrare file con Kleopatra

6.3 Considerazioni finali e di sicurezza di Gpg4win (Kleopatra)

Se viene aperto un file che è stato cifrato sul proprio computer da Kleopatra, è possibile che il software non chieda il reinserimento della password. Non si tratta di un errore, ma di una funzionalità del software che è in grado di riconoscere quali file ha cifrato ed è in grado di decifrarli senza chiedere il reinserimento della password.

La condivisone della password scelta in momento di cifratura col destinatario deve avvenire attraverso un canale di comunicazione sicuro, che sia telefonico o verbale, avendo cura che l'informazione non venga ascoltata da terzi. È assolutamente da evitare lo scambio di password via mail.

8. Azure Information Protection

Azure Information Protection è una soluzione cloud Microsoft che consente agli utenti di proteggere i documenti mediante l'applicazione di etichette al contenuto.

Per ulteriori informazioni su Azure Information Protection è possibile consultare le Linee Guida di Ateneo dedicate: *Azure Information Protection: le etichette*.