CRYPTSETUP “RAPIDO”

La presente guida non vuole essere completa, si tratta solo della somma degli appunti utilizzati per creare e gestire una zona cifrata ove salvare i documenti.
La distribuzione di riferimento e' slackware 12.0 (la prima, l'unica). Il tool usato e' cryptsetup, gia' correttamente installato e funzionante. L'hardware di test si compone di un portatile asus f5vl e di una chiavetta usb kingston dalla capacita' di 2 GB . Il sistma riconosce tale chiave usb come /dev/sdc. Occorre adattare tali parametri alla propria realta'.
Per iniziare leggiamo la pagina man di cryptsetup

    man cryptsetup

e qui vediamo che esiste uno standard chiamato LUKS, acronimo di Linux Unified Key Setup . Utilizzeremo questo standard.
Ecco una rapida panoramica dei comandi possibili:

cryptsetup luksFormat <device> [<key file>]

    formatta una partizione e la predispone all'utilizzo tramite cifratura. <key file> contiene la chiave. Se <key file> viene omesso ecco che il sistema chiede una password. Tale password deve essere utilizzata per l'accesso e la gestione della zona cifrata.

cryptsetup luksOpen <device> <name>

    accede ad una zona cifrata, previa richiesta dalla password utilizzata all'atto della creazione. Specificando l'opzione --key-file ed indicando il file contenente la chiave, ecco che non viene chiesta la password ed in sua sostituzione viene utilizzata la chiave indicata. La zone cifrata e' accessibile nella posizione /dev/mapper/nome_scelto. Non e' ancora possibile accedere ai dati. Occorre prima fare il mount della zona cifrata. Gli esempi spiegano nel dettaglio questo passaggio.

cryptsetup luksClose <name>

indica al sistema la nostra intenzione di non utilizzare piu' la zona cifrata identificata da <nome> , e la rende non piu' disponibile per l'accesso.

cryptsetup luksAddKey <device> [<new key file>]

indica al sistema la nostra volonta' di aggiungere un'ulteriore chiave per l'acecsso alla zona cifrata <device>. Se l'opzione <new key file> non viene indicata, ecco che il sistema intende che vogliamo utilizzare una password in sostituzione del file chiave. Per impostare una chiave aggiuntiva occorre conoscere almeno una chiave valida gia' dichiarata. Viene chiesta espressamente.

cryptsetup luksDelKey <device> <key slot number>

indica al sistema che intendiamo rimuovere una delle password utili per l'accesso alla zona cifrata. Occorre specificare il device ed almeno un'altra password valida.

cryptsetup luksUUID <device>

mostra le informazioni UUID del device indicato. Non accetta alcuna opzione.

cryptsetup isLuks <device>

analizza la zona indicata e controlla se si tratta di una zona cifrata. In caso affermativo ecco che nulla viene riportato a video. Qualora la zona indicata non sia una zona cifrata, ecco che viene notificato.

cryptsetup luksDump <device>

esegue un'analisi approfondita della zona indicata e riporta a video le informazioni ottenute.

Vediamo ora un esempio pratico di come utilizzare cryptsetup, ed ottenere una zona accessibile solo previa fornitura di password. E' il caso tipico di un computer portatile, ove una partizione viene resa cifrata. In caso di furto, risulta impossibile accedere ai dati salvati nella zona cifrata. Noi invece useremo una chiavetta usb da

2 Gb di marca kigston. Il sistema riconosce tale chiavetta come /dev/sdc .
Creiamo quindi la partizione /dev/sdc1 utilizzando cfdisk oppure fdisk. Come “tipo fs” indichamo linux, e salviamo le modifiche.
Ora predisponiamo /dev/sdc1 a ricevere dei dati criptati

```
cryptsetup luksFormat /dev/sdc1
```

Il sistema ci chiede conferma , e dobbiamo rispondere con “ YES “ scritto obbligatoriamente in maiuscolo. Ci viene poi chesta una password che dobbiamo digitare due volte per conferma. Smarrita questa password non vi e' alcuna maniera di recuperare i dati cifrati. Occorre essere attenti.
Adesso “apriamo” la zona cifrata che ancora non e' pronta per accogliere i dati.

```
cryptsetup luksOpen /dev/sdc1 daticifrati
```

Il sistema ci chiede la password specificata prima. Ora la zona cifarta e' disponibile nella posizione /dev/mapper/daticifrati. In sostituzione di “daticifrati” possiamo indicare un nome qualunque. Quello che indicheremo sara' presente nella posizione /dev/mapper/ e sara' qui che opereremo per accedere ai dati cifrati. Ora occorre costruire un file system sulla zona cifrata. Io prediligo reiserfs.

```
mkfs.reiserfs /dev/mapper/daticifrati
```

Il sistema ci chiede la solita conferma e crea il fle system. Non rimane che decidere il punto di mount, ed eseguire il mount stesso.

```
mkdir /mnt/daticifrati

mount -t reiserfs /dev/mapper/daticifrati  /mnt/daticifrati
```

Ora e' effettivamente disponibile la zona cifrata, tramite il mount point /mnt/daticifrati. Il passaggio successivo consiste nel fare in modo che all'accensione dell'elaboratore la zona cifrata venga rilevata e resa disponibile. Ci viene in aiuto in file /etc/crypttab , non presente nell'installazione di default di slackware. Si tratta del solito file di testo piano tipico delle configurazioni di linux. Ogni linea rappresenta una direttiva, ed il simbolo cancelletto # introduce un commento. Nel nostro caso specifico la sintassi esatta e' la seguente:

daticifrati /dev/sdc1

E' sufficiente questo per fare in modo che all'avvio il sistema riconosca la zona cifrata e chieda la relativa password di sblocco. Se vogliamo anche effettuare il mount point automatico allora occorre utilizzare il file /etf/fstab, secondo la sintassi tipica. Nel nostro caso la direttiva corretta e' la seguente:

/dev/mapper/daticifrati /mnt/daticifrati reiserfs defaults 0 0

Alcuni esempi di utlizzo del tool crypttab, sempre riferito a /dev/sdc1 e con distribuzione slackware 12.0 :

cryptsetup luksOpen /dev/sdc1 dati

Aprimo la zona cifrata /dev/sdc1 , e dopo aver fornito la password possiamo accedere alla zona tramite /dev/mapper/dati [un file system reiserfs e' gia' presente].

cryptsetup luksAddKey /dev/sdc1

Il sistema ci chiede la password di accesso, e successivamente possiamo immettere una seconda password, ripetendola due volte per conferma. Ambedue le password hanno la medesima importanza e possiamo utilizzarle nella medesima maniera.

cryptsetup luksDelKey /dev/sdc1 password

Eliminiamo la password “password” . Il sistema ci chiede un'altra password valida. Attenzione a non eliminare tutte le password di accesso, poiche' cosi' facendo non esiste alcun sistema per leggere le informazioni cifrate.

cryptsetup luksDump /dev/sdc1

chiediamo al sistema di fornirci per esteso le informazioni sulla zona cifrata /dev/sdc1 . Ecco un output ipotetico:

LUKS header information for /dev/sdc1

Version: 1

```
Cipher name:    aes
Cipher mode:    cbc-essiv:sha256
Hash spec:      sha1
Payload offset: 1032
MK bits:        128
MK digest:      a4 b6 96 34 f2 9d 6f 21 8e e9 3f f4 69 8e e5 e8 46 51 3e e0
MK salt:        81 46 44 8b 32 10 6b 48 ac d2 a6 aa 44 d8 68 d6
                c3 0c f5 5d 1a 5f 00 56 bc 62 2c 48 2d 01 a8 0f
MK iterations:  10
UUID:           259c3c6f-2706-4835-a070-4285fdecb36e

Key Slot 0: ENABLED
        Iterations:             115649
        Salt:                   0e bb bb bb d5 3b dd 96 d2 17 5b ac ef 0e c2 52
                                97 ba 85 68 8d 22 0b 4f 24 11 ad c9 45 1f 51 97
        Key material offset:    8
        AF stripes:             4000
Key Slot 1: ENABLED
        Iterations:             114977
        Salt:                   e6 6d 95 1a fe 45 c4 e0 db 6b 08 49 7e b8 52 6e
                                33 0d 7d 79 98 96 e6 7d ec 84 d2 65 78 5c 1c 0a
        Key material offset:    136
        AF stripes:             4000
Key Slot 2: ENABLED
        Iterations:             115648
        Salt:                   34 17 e8 1f 84 8c 23 ec 64 b8 3d 04 d8 7a 32 b5
                                f0 7d ba 03 0f 04 0e 23 78 c2 b0 e9 f0 9d 6a 01
        Key material offset:    264
        AF stripes:             4000
Key Slot 3: DISABLED
Key Slot 4: DISABLED
Key Slot 5: DISABLED
Key Slot 6: DISABLED
Key Slot 7: DISABLED
```

autore: Veronese Claudio, claudiovero@claudiove.com