(19) CONFEDERAZIONE SVIZZERA
ISTITUTO FEDERALE DELLA PROPRIETÀ INTELLETTUALE

(11) CH 706 584 B1

(51) Int. Cl.: G06F 3/08 (2006.01)
G06F 21/00 (2013.01)
H04L 9/32 (2006.01)

Brevetto d'invenzione rilasciato per la Svizzera ed il Liechtenstein
Trattato sui brevetti, del 22 dicembre 1978, fra la Svizzera ed il Liechtenstein

(12) FASCICOLO DEL BREVETTO

(21) Numero della domanda: 00753/12

(22) Data di deposito: 01.06.2012

(43) Domanda pubblicata: 13.12.2013

(24) Brevetto rilasciato: 15.06.2017

(45) Fascicolo del brevetto pubblicato: 15.06.2017

(73) Titolare/Titolari:
Quantec SA, Corso San Gottardo 86
6830 Chiasso (CH)

(72) Inventore/Inventori:
Pierluigi Pentimalli, 6830 Chiasso (CH)

(74) Mandatario:
Fiammenghi-Fiammenghi, Via San Gottardo 15
6900 Lugano (CH)

(54) Dispositivo portatile di back up/restore.

(57) Dispositivo (100) portatile di back-up/restore associabile ad un dispositivo esterno (90) per criptare/decriptare e/o comprimere/decomprimere dati;

detto dispositivo (100) di back-up/restore comprendendo:

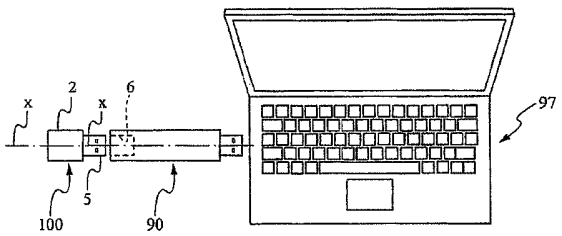
un involucro esterno;

almeno una CPU comprendente almeno un microcontrollore ed almeno un motore crittografico;

almeno un chip di autenticazione crittografico per associare in modo univoco un detto dispositivo di back-up/restore con un dispositivo esterno per criptare/decriptare e/o comprimere/decomprimere dati;

almeno una memoria di tipo flash;

almeno una prima porta (5) di ingresso/uscita atta ad essere interfacciata con il dispositivo esterno per criptare/decriptare e/o comprimere/decomprimere dati.



Descrizione

Campo dell'invenzione

[0001] La presente invenzione concerne il campo della crittografia e/o compressione di dati ed in particolare un dispositivo di back-up/restore associabile ad un dispositivo portatile per criptare/decriptare e/o comprimere/decomprimere dati e informazioni di qualsiasi tipo e genere.

Tecnica nota

[0002] Nel campo della criptazione dei dati sono presenti sul mercato sia soluzioni software che hardware.

[0003] Le soluzioni software generalmente prevedono che l'utilizzatore effettui mediamente minimo due operazioni distinte, se non di più, con sistemi tra loro diversi per poter garantire lo scambio di informazioni in sicurezza.

[0004] Prendendo ad esempio il caso in cui un utente debba inviare contenuti riservati a terzi a lui noti e, quindi, intenda crittografare tali dati ed informazioni (caso estendibile anche alla compressione), l'utente dovrà, in sequenza:

- Crittografare le informazioni che intende inviare;
- Memorizzare tale informazioni crittografate sul proprio sistema (computer, PC etc.);
- Inviarle tramite un altro sistema al/ai destinatario/i (e-mail, web transfer tramite sistemi di terzi, Skype, MSN, sistemi peer-to-peer, spedizione fisica di un dispositivo di memorizzazione di massa, ad es. CD Rom, «chiavetta» USB, Hard Disk USB etc.).

[0005] A questo punto chi riceve i dati crittografati deve fare esattamente il contrario e la procedura dipende chiaramente dal sistema software utilizzato per crittografare nonché dal metodo utilizzato per inviare le informazioni crittografate.

[0006] La Richiedente ha inoltre notato che il sistema software soffre di un grande limite comune alla totalità dei sistemi presenti sul mercato: la chiave di crittografia con cui sono state, appunto, crittografate le informazioni «viaggia» insieme alle informazioni crittografate stesse.

[0007] Spesso, tra l'altro, tali soluzioni software sono open-source e, quindi, anche se la chiave viene «offuscata» nel file stesso tramite appositi algoritmi, è abbastanza semplice, con poche ore di lavoro, recuperarla.

[0008] La Richiedente ha inoltre osservato che anche semmai tale chiave di crittografia non «viaggiasse» insieme ai dati ed alle informazioni crittografate, la soluzione software è facilmente esposta a tentativi di memory dumping, snooping, spoofing e intercettazione in genere della chiave stessa. Ciò è possibile tramite appositi programmi come trojan e malware in genere, keylogger, etc. che creano una «backdoor» sul computer dell'utente andando ad intercettare sia quanto digitato con la tastiera o con il «click» del mouse, nonché addirittura effettuando tramite la tecnica del «memory dumping» l'analisi delle chiavi crittografiche e delle informazioni critiche degli algoritmi di crittografia direttamente in memoria del computer, ovvero direttamente nello spazio di esecuzione della soluzione software stessa.

[0009] Visto quanto sopra, la Richiedente si è resa conto che le soluzioni software note sono pertanto intrinsecamente insicure e richiedono inoltre una certa capacità ad operare con il computer.

[0010] Sul mercato esistono inoltre alcune soluzioni hardware.

[0011] Generalmente tali soluzioni consistono, nella stragrande maggioranza dei casi, in dispositivi USB (del tutto simili ad una «chiavetta» USB) dotati al proprio interno, di una memoria di massa locale (come, appunto, le normali «chiavette» USB di Storage) e di chip crittografici. Tali soluzioni consentono, sostanzialmente, di inserire il dispositivo in un computer (esclusivamente tramite l'interfaccia USB) e di poter scrivere e leggere dati e file su e dalla memoria di Storage integrata in maniera sicura: i dati vengono crittografati e decrittografati in tempo reale.

[0012] La Richiedente ha comunque osservato che tali dispositivi non sono provvisti di una soluzione di interfacciamento supplementare, di tipo fisico, verso ulteriori dispositivi esterni utilizzabili per proteggere le chiavi crittografiche e/o i dati dell'utente presenti all'interno del dispositivo hardware stesso.

[0013] Inoltre come per la soluzione software nel caso in cui un utente debba inviare contenuti riservati a terzi a lui noti deve inviare comunque la «chiavetta USB» contenete i dati crittografati fornendo la chiave di accesso alla chiavetta medesima tramite un altro sistema riproponendo le problematiche sopraesposte.

[0014] La Richiedente ha quindi riscontrato l'esigenza di fornire un dispositivo per criptare/decriptare e/o comprimere/decomprimere dati che sia strutturalmente semplice, sicuro e che consenta di risolvere i problemi sopraesposti delle soluzioni note.

[0015] La Richiedente ha notato che nel caso di perdita di un dispositivo hardware portatile per criptare/decriptare e/o comprimere/decomprimere dati del tipo sopra descritto è impossibile, per le limitazioni dei dispositivi presenti sul mercato, dialogare con dispositivi esterni già opportunamente autenticati atti ad eseguire un back-up (archiviazione) sicuro ed un successivo restore (ripristino) delle chiavi crittografiche e/o dei dati stessi dell'utente.

[0016] In altri termini, non esiste sul mercato una soluzione hardware, ovvero un dispositivo in grado di criptare/decriptare e/o comprimere/decomprimere dati e informazioni in genere che sia in grado non solo di svolgere queste operazioni

mantenendo le chiavi crittografiche e/o anche i dati al suo interno, ma che renda anche possibile il recupero sicuro e certo di tali chiavi crittografiche e/o dei dati stessi in maniera semplice, affidabile tramite un ulteriore dispositivo esterno, sempre di tipo hardware, di back-up e restore.

[0017] La Richiedente si è quindi posta il problema di trovare un dispositivo hardware che nel caso di perdita di un dispositivo quale quello sopra descritto oggetto della domanda di brevetto CH 212/12, a nome della stessa richiedente consenta di ripristinare, ovvero inizializzare un nuovo dispositivo recuperando e condividendo tutte le chiavi ed i segreti e, dove previsto anche i dati, atti a consentire l'accesso ai dati precedentemente crittografati e/o compressi.

Sommario dell'invenzione

[0018] Pertanto, in un suo primo aspetto l'invenzione riguarda un dispositivo di back-up/restore di un dispositivo esterno per criptare/decriptare e/o comprimere/decomprimere dati associabile a detto dispositivo di back-up/restore;
detto dispositivo di back-up/restore comprendendo:
un involucro esterno;
almeno una CPU comprendente almeno un microcontrollore ed almeno un motore crittografico;
almeno un chip di autenticazione crittografico per associare in modo univoco il detto dispositivo di back-up/restore con un dispositivo esterno per criptare/decriptare e/o comprimere/decomprimere dati;
almeno una memoria di tipo flash;
almeno una prima porta di ingresso/uscita atta ad essere interfacciata con il dispositivo esterno per criptare/decriptare e/o comprimere/decomprimere dati.

[0019] Nel contesto della presente invenzione con il termine chip viene indicato un circuito elettronico ad alta integrazione.

[0020] Inoltre con il termine back-up viene indicata l'operazione di salvataggio dati dal dispositivo esterno per criptare/decriptare e/o comprimere/decomprimere dati verso il dispositivo di back-up/restore stesso.

[0021] Con l'espressione restore viene indicata l'operazione di recupero (restore) dei dati salvati attraverso un'operazione di back-up. In altri termini quando, in seguito ad errori umani, guasti hardware o perdita del dispositivo esterno per criptare/decriptare e/o comprimere/decomprimere dati, i dati presenti sul tale supporto non sono più accessibili, il recupero (restore) dei dati salvati attraverso un operazione di back-up permette di ricostruire la situazione iniziale su di un nuovo dispositivo esterno per criptare/decriptare e/o comprimere/decomprimere dati.

[0022] La presente invenzione, nel suddetto aspetto, può presentare almeno una delle caratteristiche preferite che qui di seguito sono descritte.

[0023] Vantaggiosamente, la porta di ingresso/uscita dati comprende delle connessioni atte a comunicare dati con dispositivi esterni per criptare/decriptare e/o comprimere/decomprimere dati secondo uno standard internazionale di comunicazione scelto tra Ethernet, USB, FireWire, ThunderBolt, Bluetooth, Wi-Fi, UWB, ZigBee, ANT, WirelessHART, SATA, PATA, EIDE, RS232, RS485, CAN, Lin, Profibus.

[0024] Convenientemente, la porta di ingresso/uscita dati comprende una connessione maschio atta ad interfacciarsi con una connessione femmina di un dispositivo esterno per criptare/decriptare e/o comprimere/decomprimere dati.

[0025] Nel contesto della presente invenzione per connessione maschio viene inteso un organo di connessione atto ad entrare almeno parzialmente in un recesso che rappresenta un organo di connessione femmina.

[0026] Nel contesto della presente invenzione per connessione femmina viene inteso un organo di connessione atto ad accogliere almeno parzialmente un organo di connessione maschio.

[0027] Convenientemente, la prima porta di ingresso/uscita dati comprende una connessione maschio USB.

[0028] Convenientemente, la CPU comprende al suo interno una memoria di tipo flash.

[0029] Secondo un altro aspetto la presente invenzione concerne un processo di back-up/restore dati tra un dispositivo esterno per criptare/decriptare e/o comprimere/decomprimere dati ed un dispositivo di back-up/restore come precedentemente descritto. Il processo comprendendo le fasi di:

- connettere un connettore maschio di una porta di ingresso/uscita dati del dispositivo di back-up/restore con un connettore femmina di una porta di ingresso/uscita dati del dispositivo per criptare/decriptare e/o comprimere/decomprimere dati; detto dispositivo per criptare/decriptare e/o comprimere/decomprimere dati essendo a sua volta collegato ad un computer o un notebook o un desktop, o un server o una workstation, o un tablet, o uno smartphone, tramite ulteriori connessioni disponibili del dispositivo esterno per criptare/decriptare e/o comprimere/decomprimere dati; detto dispositivo per esterno per criptare/decriptare e/o comprimere/decomprimere dati comprendendo almeno un database comprendente un archivio delle chiavi crittografiche, dei dati dell'utente e, in aggiunta ove previsto, anche dei dati e delle informazioni stesse;
- verifica dello stato di configurazione del dispositivo di back-up/restore e del dispositivo per criptare/decriptare e/o comprimere/decomprimere dati;
- verifica dello stato di associazione del dispositivo di back-up/restore e del dispositivo per criptare/decriptare e/o comprimere/decomprimere dati.

[0030] Nel contesto della presente invenzione per funzione crittografica di hash viene intesa una funzione crittografica che trasforma dei dati di lunghezza arbitraria (un messaggio) in una stringa di dimensione fissa chiamata valore di hash, impronta del messaggio o somma di controllo.

[0031] Inoltre con l'espressione «nonce» viene indicato un numero, generalmente casuale o pseudo-casuale, che ha un utilizzo unico. Nonce è infatti la contrazione delle parole inglesi «number used once», che significano appunto «numero usato solo una volta».

[0032] Per vettore di inizializzazione (IV),viene invece indicato un blocco di bit di lunghezza predefinita che viene utilizzato per inizializzare lo stato di un cifrario a flusso, oppure di un cifrario a blocchi quando questi opera in una modalità tale da trasformarsi in un cifrario a flusso, in modo che a chiavi identiche il keystream risultante sia differente.

[0033] Nel contesto della presente invenzione per «associazione tra dispositivo di back-up/restore e dispositivo per criptare/decriptare e/o comprimere/decomprimere dati» viene intesa un'associazione univoca. In altri termini una associazione matematicamente univoca, vale a dire che è sempre e solo così. Non è possibile che un dispositivo di back-up/restore sia associato a più dispositivi per criptare/decriptare e/o comprimere/decomprimere dati e viceversa. L'associazione univoca avviene tramite la generazione di dati crittografici e combinatori derivati a partire dai numeri di serie dei due dispositivi a loro volta univoci perché scritti in maniera non modificabile a livello hardware nel chip di autenticazione crittografica, nonché a partire dalla password personale dell'utente e da altri dati e funzioni private e protette. Questo insieme di dati, generato durante la fase di inizializzazione ed associazione, consente ai due dispositivi di poter operare correttamente, in maniera sicura ed univoca, quando sono fisicamente tra loro connessi, oppure individualmente quando utilizzati in abbinamento alla password personale dell'utente. In nessun caso, individualmente, il singolo dispositivo detiene l'insieme dei dati necessari per poter accedere al data base interno, alle chiavi crittografiche dell'utente ed agli eventuali dati ed informazioni aggiuntive internamente memorizzate.

[0034] Vantaggiosamente il processo comprende una fase di autenticazione reciproca del dispositivo di back-up/restore e del dispositivo per criptare/decriptare e/o comprimere/decomprimere dati.

[0035] Preferibilmente la fase di autenticazione del dispositivo di back-up/restore e del dispositivo per criptare/decriptare e/o comprimere/decomprimere dati comprende:
creazione di un primo vettore di inizializzazione $(CKvector\ 1)_{CT}$ in funzione di un segreto (csk) inserito dal costruttore del dispositivo per criptare/decriptare e/o comprimere/decomprimere dati e di un primo numero radonmico $(CH1)_{CT}$, da parte del motore di crittografia del detto dispositivo per criptare/decriptare e/o comprimere/decomprimere dati;

- invio del primo vettore di inizializzazione $(CKvector\ 1)_{CT}$ e del primo numero radonmico $(CH1)_{CT}$ al detto dispositivo di back-up/restore;
- calcolo del primo vettore di inizializzazione $(CKvector\ 1)_{T}$ da parte del motore crittografia detto dispositivo di back-up/restore;
- confronto del primo vettore di inizializzazione $(CKvector\ 1)_{CT}$ inviato dal dispositivo per criptare/decriptare e/o comprimere/decomprimere dati con il primo vettore di inizializzazione $(CKvector\ 1)_{T}$ calcolato da parte del motore crittografia del detto dispositivo di back-up/restore;
- generazione di un secondo numero randomico $(CH2)_{T}$
- calcolo della chiave di sessione (K_{sess}) da parte del motore di crittografia del dispositivo (100) di back-up/restore;
- creazione da parte del motore di crittografia del detto dispositivo (100) di back-up/restore di un secondo vettore di inizializzazione $(CKvector\ 2)_{T}$ in funzione di un segreto (csk) inserito dal costruttore del detto dispositivo di back-up/restore e del secondo numero randomico $(CH2)_{T}$;
- invio del secondo vettore di inizializzazione $(CKvector\ 2)_{T}$ e del detto secondo numero randomico $(CH2)_{T}$ al detto dispositivo (90) per criptare/decriptare e/o comprimere/decomprimere dati;
- calcolo della chiave di sessione (K_{sess}) da parte del motore di crittografia del dispositivo (90) per criptare/decriptare e/o comprimere/decomprimere dati;
- calcolo del secondo vettore di inizializzazione $(CKvector\ 2)_{CT}$ da parte del motore crittografia del detto dispositivo per criptare/decriptare e/o comprimere/decomprimere dati;
- confronto del secondo vettore di inizializzazione $(CKvector\ 2)_{T}$ inviato dal dispositivo di back-up/restore con il secondo vettore di inizializzazione $(CKvector\ 2)_{CT}$ calcolato da parte del motore crittografia del detto dispositivo per criptare/decriptare e/o comprimere/decomprimere dati,
- attivazione della cifratura del canale di comunicazione da parte del dispositivo per criptare/decriptare e/o comprimere/decomprimere dati utilizzando un algoritmo di crittografia presente nel proprio motore crittografico e la relativa chiave di sessione (K_{sess}) precedentemente derivata;
- attivazione della cifratura del canale di comunicazione da parte del dispositivo di back-up/restore utilizzando un algoritmo di crittografia presente nel proprio motore crittografico e la relativa chiave di sessione (K_{sess}) derivata precedentemente;
- invio da parte del dispositivo per criptare/decriptare e/o comprimere/decomprimere al dispositivo di back-up/restore di un comando di connessione noto sul canale crittografato precedentemente instaurato ed attivato;
- ricezione di tale comando sul canale crittografato da parte del dispositivo (100) di back-up/restore e verifica della sua consistenza dopo una fase di decrittografia;

– invio di un comando di risposta noto da parte del dispositivo (100) di back-up/restore al dispositivo per criptare/decriptare e/o comprimere/decomprimere dati sul medesimo canale crittografato già instaurato ed attivo;
– verifica, da parte del dispositivo per criptare/decriptare e/o comprimere/decomprimere dati della consistenza del comando di risposta ricevuto da parte del dispositivo di back-up/restore dopo la relativa decrittografia.

[0036] Preferibilmente il processo comprende le fasi di:

– richiesta dello stato di associazione al detto dispositivo di back-up/restore;
– richiesta dello stato di associazione al detto dispositivo per criptare/decriptare e/o comprimere/decomprimere dati.

[0037] Vantaggiosamente, se ne il dispositivo di back-up/restore, ne dispositivo per criptare/decriptare e/o comprimere/decomprimere dati sono associati ed il dispositivo di back-up/restore non è mai stato configurato comprende le fasi di:

– configurazione iniziale del dispositivo di back-up/restore;
– invio richiesta di associazione tra dispositivo di back-up/restore e dispositivo esterno per criptare/decriptare e/o comprimere/decomprimere dati;
– generazione e scambio di chiavi crittografiche e di dati di accesso secondo predeterminate funzioni in entrambi i suddetti dispositivi;
– invio da dispositivo di back-up/restore di conferma di associazione completata al dispositivo esterno per criptare/decriptare e/o comprimere/decomprimere dati e/o viceversa.

[0038] Alternativamente, se il dispositivo di back-up/restore non è associato, ma il dispositivo per criptare/decriptare comprimere/decomprimere dati è già stato precedentemente configurato ed associato ad un precedente dispositivo di back-up/restore il processo si sviluppa secondo le fasi di:

– richiesta all'utente, di inserire un codice identificativo utente predeterminato;
– generazione e scambio di chiavi crittografiche e di dati di accesso secondo predeterminate funzioni in entrambi i suddetti dispositivi;
– se il codice identificativo è inserito validamente, avviene un invio di una richiesta di associazione tra dispositivo di back-up/restore e dispositivo per criptare/decriptare e/o comprimere/decomprimere dati;
– invio da parte dal dispositivo di back-up/restore di conferma di associazione completata al dispositivo esterno per criptare/decriptare e/o comprimere/decomprimere dati;
– invio della propria versione di back-up $(V)_{CT}$ dei dati crittografici e dei dati in genere memorizzati nel proprio database del dispositivo per criptare/decriptare e/o comprimere/decomprimere dati al dispositivo di back-up/restore;
– aggiornamento della versione di back-up $(V)_T$ del dispositivo di back-up/restore in funzione della versione di back-up $(V)_{CT}$ ricevuta dal dispositivo per criptare/decriptare e/o comprimere/decomprimere dati.

[0039] Ancora alternativamente, se il dispositivo di back-up/restore è stato precedentemente associato ad un dispositivo per comprimere/decomprimere dati, ma il dispositivo per comprimere/decomprimere dati non è mai stato configurato ed associato ad un dispositivo di back-up/restore comprende le fasi di:

– richiesta all'utente, di inserire un codice identificativo utente predeterminato;
– generazione e scambio di chiavi crittografiche e di dati di accesso secondo predeterminate funzioni in entrambi i suddetti dispositivi;
– se il codice identificativo è validamente inserito, avviene un invio richiesta di associazione tra dispositivo di back-up/restore e dispositivo esterno per criptare/decriptare e/o comprimere/decomprimere dati;
– invio da parte dal dispositivo di back-up/restore di conferma di associazione completata al dispositivo esterno per criptare/decriptare e/o comprimere/decomprimere dati.
– invio della propria versione di back-up $(V)_T$ dei dati crittografici e dei dati in genere memorizzati nel proprio database del dispositivo di back-up/restore al dispositivo per criptare/decriptare e/o comprimere/decomprimere dati;
– aggiornamento della versione di back-up $(V)_{CT}$ del dispositivo per criptare/decriptare e/o comprimere/decomprimere dati in funzione della versione di back-up $(V)_T$ ricevuta dal dispositivo di back-up/restore.

[0040] Ancora alternativamente, rispetto alle precedenti ipotesi, se il dispositivo di back-up/restore ed il dispositivo per criptare/decriptare e/o comprimere/decomprimere dati sono associati ed il dispositivo di back-up/restore è già stato precedentemente configurato comprende le fasi di:

– richiesta all'utente, di inserire un codice identificativo utente predeterminato;
– verifica delle chiavi crittografiche e dei dati di accesso secondo predeterminate funzioni presenti in entrambi i suddetti dispositivi;
– se il codice identificativo è validamente inserito avviene un invio richiesta di verifica della versione di back-up $(V)_T$ del dispositivo di back-up/restore da parte del dispositivo per criptare/decriptare e/o comprimere/decomprimere dati;
– viene confrontata la versione di back-up $(V)_T$ del detto dispositivo di back-up/restore con la versione di back-up $(V)_{CT}$ del dispositivo per criptare/decriptare e/o comprimere/decomprimere dati;

se la versione del dispositivo per criptare/decriptare e/o comprimere/decomprimere dati è successiva a quella del dispositivo (100) di back-up/restore, il dispositivo per criptare/decriptare e/o comprimere/decomprimere dati invia la propria versione di back-up $(V)_{CT}$ memorizzati nel proprio database al dispositivo di back-up/restore.
Vantaggiosamente, la versione di back-up $(V)_T$ comprende:
delle chiavi crittografiche;

dei dati utente;
dati ed informazioni crittografate.

[0041] Preferibilmente, la versione di back-up $(V)_{CT}$ del detto dispositivo per criptare/decriptare e/o comprimere/decomprimere dati comprende:
delle chiavi crittografiche;
dei dati utente;
dati ed informazioni crittografate.

[0042] Secondo un altro aspetto la presente invenzione concerne un processo di back-up/restore dati tra un dispositivo esterno per criptare/decriptare e/o comprimere/decomprimere dati ed un dispositivo di back-up/restore come precedentemente descritto. Il processo comprendendo le fasi di:

- connettere un connettore maschio di una porta di ingresso/uscita dati del dispositivo di back-up/restore con un connettore femmina di una porta di ingresso/uscita dati del dispositivo per criptare/decriptare e/o comprimere/decomprimere dati; detto dispositivo per criptare/decriptare e/o comprimere/decomprimere dati essendo a sua volta collegato ad un computer o un notebook o un desktop, o un server o una workstation, o un tablet, o uno smartphone, tramite ulteriori connessioni disponibili del dispositivo esterno per criptare/decriptare e/o comprimere/decomprimere dati; detto dispositivo per esterno per criptare/decriptare e/o comprimere/decomprimere dati comprendendo almeno un database comprendente un archivio delle chiavi crittografiche, dei dati dell'utente e, in aggiunta ove previsto, anche dei dati e delle informazioni stesse;
- verifica dello stato di configurazione del dispositivo di back-up/restore e del dispositivo per criptare/decriptare e/o comprimere/decomprimere dati;
- verifica dello stato di associazione del dispositivo di back-up/restore e del dispositivo per criptare/decriptare e/o comprimere/decomprimere dati;
  se il dispositivo di back-up/restore e il dispositivo (90) per criptare/decriptare e/o comprimere/decomprimere dati sono associati viene confrontata la versione di back-up $(V)_T$ del detto dispositivo (100) di back-up/restore con la versione di back-up $(V)_{CT}$ del dispositivo (90) per criptare/decriptare e/o comprimere/decomprimere dati;
  se la versione del back-up $(V)_{CT}$ presente nel dispositivo per criptare/decriptare e/o comprimere/decomprimere dati è successiva a quella del dispositivo (100) di back-up/restore il dispositivo per criptare/decriptare e/o comprimere/decomprimere dati invia la propria versione dei dati crittografici e dei dati in genere memorizzati nel proprio database al dispositivo di back-up/restore;
- il dispositivo per criptare/decriptare e/o comprimere/decomprimere dati invia all'utente un messaggio per scollegare il dispositivo di back-up/restore dai dispositivo per criptare/decriptare e/o comprimere/decomprimere dati.

Breve descrizione dei disegni

[0043] Ulteriori caratteristiche e vantaggi dell'invenzione appariranno maggiormente dalla descrizione dettagliata di alcune forme di esecuzione preferite, ma non esclusive di un dispositivo portatile per criptare/decriptare e/o comprimere/decomprimere dati secondo la presente invenzione.

[0044] Tale descrizione verrà esposta qui di seguito con riferimento agli uniti disegni, forniti a scopo solo indicativo e, pertanto non limitativo, nei quali:

la fig. 1	è una vista schematica di un dispositivo di back-up/restore secondo la presente invenzione portatile atto ad essere associato con un dispositivo portatile per criptare/decriptare e/o comprimere/decomprimere dati secondo la presente invenzione;
la fig. 2	è uno schema a blocchi di una forma realizzativa di configurazione hardware di un dispositivo portatile di back-up/restore secondo la presente invenzione;
la fig. 3	è uno schema a blocchi di una funzione del dispositivo portatile di back-up/restore secondo la presente invenzione;
la fig. 4	è uno schema a blocchi di una funzione del dispositivo portatile di back-up/restore secondo la presente invenzione.

Descrizione dettagliata di forme realizzative dell'invenzione

[0045] Con riferimento alle fig. 1–4, un dispositivo portatile per eseguire il back-up/restore di un dispositivo per criptare/decriptare e/o comprimere/decomprimere dati secondo la presente invenzione, viene identificato con il riferimento numerico 100.

[0046] Il dispositivo 100, nella forma di realizzazione mostrata in fig. 1, presenta un involucro esterno 2, almeno una CPU 3, almeno un chip crittografico di autenticazione 4 ed almeno una prima porta 5 di ingresso/uscita dati atta ad essere interfacciata con un dispositivo di dispositivi esterni.

[0047] L'involucro esterno preferibilmente si estende lungo una direzione principale in modo da individuare una direzione di estensione X–X. Nella forma di realizzazione schematicamente mostrata in fig. 1, la prima porta 5 si trova all'estremità dell'involucro 2 lungo la direzione di estensione.

[0048] Preferibilmente, per rendere il dispositivo 100 facilmente portatile, l'involucro 2, di forma sostanzialmente di parallelepipedo, presenta un'estensione longitudinale L con $L \leq 10$ cm, ancor più preferibilmente con $L \leq 5$ cm.

[0049] Sempre rendere il dispositivo 100 facilmente portatile, lo stesso presenta complessivamente un peso compreso tra 0,01 e 0,5 kg.

[0050] L'involucro 2 contiene al suo interno almeno la CPU 3 ed almeno il chip crittografico 4 di supporto di autenticazione, più dettagliatamente descritti nel seguito.

[0051] La CPU 3 comprende almeno un microcontrollore ed almeno un motore crittografico. Secondo una forma di realizzazione, il microcontrollore è un microcontrollore a 16 o 32 bit dotato di motore di crittografia hardware integrato al suo interno, memoria flash integrata ed adeguata capacità di calcolo atta a svolgere in maniera sicura, veloce ed affidabile le operazioni di back-up/restore fin qui descritte.

[0052] Il chip crittografico 4 di supporto di autenticazione crittografica grazie alle specifiche caratteristiche consente di associare univocamente il dispositivo 100 di back-up/restore con un dispositivo 90 per criptare/decriptare e/o comprimere/decomprimere dati. Ciò grazie alla propria capacità di memorizzare al proprio interno dati crittografici in maniera protetta dall'accesso esterno ivi inclusi tentativi di manomissione e di ispezione magneto-elettrica, nonché grazie alla propria capacità di eseguire, sempre internamente ed in maniera protetta, funzioni crittografiche di hash in maniera hardware a partire anche dai segreti ivi presenti. Inoltre, sempre grazie a tali peculiari caratteristiche, consente di individuare univocamente ciascun singolo dispositivo grazie ad un numero di serie definito a livello hardware, universalmente univoco, non ripetibile e non modificabile.

[0053] Il dispositivo 100 secondo la presente invenzione permette quindi di eseguire in modo sicuro ed hardware la funzione di back-up/restore di un dispositivo 90 per criptare/decriptare e/o comprimere/decomprimere dati, quale quello oggetto della domanda di brevetto qui incluso come riferimento per le caratteristiche descrittive del dispositivo 90 per criptare/decriptare e/o comprimere/decomprimere dati.

[0054] Durante il normale funzionamento o alla semplice accensione del dispositivo 90 per criptare/decriptare e/o comprimere/decomprimere dati, connesso a sua volta con dispositivo esterno 97, quale un PC, la CPU del dispositivo 90 per criptare/decriptare e/o comprimere/decomprimere dati verifica costantemente l'eventuale inserimento in una sua seconda porta di ingresso/uscita dati di una connessione di un dispositivo 100 portatile di back-up/restore quale quello oggetto della presente invenzione.

[0055] In dettaglio, la CPU del dispositivo 90 per criptare/decriptare e/o comprimere/decomprimere dati verifica l'inserimento di una connessione di tipo maschio, quale ad esempio una connessione 7 USB maschio, in una sua connessione di tipo femmina USB.

[0056] A questo punto, dopo aver riconosciuto il tipo di dispositivo che ha inserito la connessione maschio 7 e il produttore dello stesso attraverso la richiesta di due parametri identificativi, VID e PID, avviene una verifica dello stato di configurazione del dispositivo di back-up/restore 100 e del dispositivo 90 per criptare/decriptare e/o comprimere/decomprimere dati 90.

[0057] Contestualmente alla suddetta verifica avviene una verifica dello stato di associazione del dispositivo 100 di back-up/restore e del dispositivo 90 per criptare/decriptare e/o comprimere/decomprimere dati.

[0058] Contestualmente alle due verifiche suddette avviene la creazione di un canale di comunicazione criptato per lo scambio dati tra il detto dispositivo di back-up/restore 100 ed il dispositivo per criptare criptare/decriptare e/o comprimere/decomprimere dati 90.

[0059] Durante al verifica dello stato di associazione del dispositivo 100 di back-up/restore e del dispositivo 90 per criptare/decriptare e/o comprimere/decomprimere dati entrambi i dispositivi si scambiano i propri dati ed informazioni crittografiche e combinatorie a disposizione. Tali dati ed informazioni, ove presenti, sono stati generati e scambiati in precedenza durante la fase di inizializzazione e associazione univoca tra i due dispositivi.

[0060] Se i dati scambiati tra i due dispositivi sono tra loro coerenti avviene l'invio della richiesta di verifica della versione delle chiavi crittografiche, dati utente e dati in genere contenuti nel dispositivo di back-up/restore da parte del dispositivo per criptare/decriptare e/o comprimere/decomprimere dati.

[0061] In funzione della versione dei dati presenti nel dispositivo di back-up/restore rispetto a quelli presenti nel dispositivo 90 per criptare/decriptare e/o comprimere/decomprimere dati, è possibile effettuare un nuovo back-up dei dati presenti in quest'ultimo nel primo dispositivo 100 di back-up/restore (se i dati presenti nel dispositivo 90 per criptare/decriptare e/o comprimere/decomprimere sono più recenti) altrimenti viene rilevato un tentativo di manomissione del sistema in quanto non è possibile che un dispositivo per criptare/decriptare e/o comprimere/decomprimere già associato con un dispositivo di back-up/restore disponga di una versione dei dati da archiviare su tale ultimo dispositivo più vecchia. Se la versione dei dati da archiviare è la medesima in entrambi i dispositivi, non succede nulla.

[0062] Finita la fase precedente, il dispositivo 90 per criptare criptare/decriptare e/o comprimere/decomprimere dati invia all'utente un messaggio per scollegare il dispositivo 100 di back-up/restore da detto dispositivo 90 per criptare criptare/ decriptare e/o comprimere/decomprimere dati.

[0063] Ogni volta che un dispositivo 100 di back-up/restore secondo la presente invenzione, viene collegato con un dispositivo 90 per criptare criptare/decriptare e/o comprimere/decomprimere dati avviene una fase di autenticazione reciproca e verifica della genuinità.

[0064] Autenticandosi reciprocamente i due dispositivi escludono la possibilità di attacchi del tipo «men in the middle» (che in questo casa sarebbe un utente illecito che intercetta pacchetti in transito dal dispositivo 100 di back-up/restore al dispositivo del dispositivo per criptare/decriptare e/o comprimere/decomprimere dati 90 o viceversa.

[0065] In fig. 3 è mostrata uno schema a blocchi della fase di autenticazione reciproca e di verifica della genuinità del dispositivo di back-up/restore 100 e del dispositivo per criptare/decriptare e/o comprimere/decomprimere dati 90.

[0066] In dettaglio, viene creato un numero randomico (CH1) mediante il chip di crittografia del detto dispositivo 90 per criptare/decriptare e/o comprimere/decomprimere dati.

[0067] Nel contesto della presente invenzione per numero randomico viene inteso un numero casuale.

[0068] Successivamente, tramite il chip crittografico viene creata una chiave preliminare (K_{prelim}) attraverso una prima funzione di hash in funzione del numero randomico $(CH1)_{CT}$ ad alta entropia e di un segreto (csk) inserito dal costruttore del dispositivo 90 per criptare/decriptare e/o comprimere/decomprimere dati.

[0069] Viene, quindi creato un primo vettore di inizializzazione $(CKvector\ 1)_{CT}$ attraverso una funzione matematica segreta in funzione del numero randomico $(CH1)_{CT}$ e della chiave preliminare.

[0070] Viene, quindi, inviato il primo vettore di inizializzazione (CKvector 1) e il numero randomico $(CH1)_{CT}$ al detto dispositivo 100 di back-up/restore.

[0071] Viene creato da parte del motore crittografico del dispositivo 100 di back-up/restore una chiava preliminare (K_{prelim}) attraverso detta prima funzione di hash, privata e protetta, in funzione del numero randomico $(CH1)_{CT}$ e di detto segreto (csk) inserito dal costruttore del dispositivo 100 di back-up/restore.

[0072] Si precisa che affinché le funzioni suddette siano in corso, significa che il costruttore del dispositivo 100 di back-up/restore è lo stesso del dispositivo 90 per criptare/decriptare e/o comprimere/decomprimere dati è quindi del tutto identico nel contesto della presente invenzione riferirsi al primo o al secondo in merito all'inserimento di segreti all'interno dei dispositivi, rispettivamente di back-up/restore 100 o del dispositivo 90 per criptare/decriptare e/o comprimere/decomprimere dati.

[0073] Il processo continua con la creazione da parte del motore crittografico del dispositivo 100 di back-up/restore della prima chiave $(CKvector\ 1)_T$ attraverso la seconda funzione matematica segreta in funzione del numero randomico $(CH1)_{CT}$ e della chiave preliminare (K_{prelim}).

[0074] Viene quindi confrontato, il primo vettore di inizializzazione $(CKvector\ 1)_T$ generato dal dispositivo 100 di back-up/ restore con il primo vettore di inizializzazione $(CKvector\ 1\ )_{CT}$ inviato dal dispositivo 90 per criptare/decriptare e/o comprimere/decomprimere dati.

[0075] A questo punto, il chip di crittografia del dispositivo 100 di back-up/restore genera un secondo numero randomico $(CH2)_T$, ad elevata entropia.

[0076] Il motore di crittografia del dispositivo 100 di back-up/restore genera, quindi, un Nonce attraverso la seconda funzione matematica segreta in funzione del primo e del secondo numero randomico (CH1; CH2).

[0077] Il chip di crittografia del dispositivo 100 di back-up/restore genera, quindi, una chiave crittografica di sessione K_{sess} attraverso la prima funzione di hash in funzione del Nonce e del segreto (csk) inserito dal costruttore del dispositivo 100 di back-up/restore.

[0078] Conseguentemente, il motore di crittografia del dispositivo 100 di back-up/restore genera un secondo vettore di inizializzazione (CKvector 2) attraverso detta seconda funzione matematica segreta in funzione del Nonce e della chiave di sessione (K_{sess}).

[0079] Viene quindi inviato un secondo vettore di inizializzazione (CKvector 2) e il numero randomico (CH2) dal dispositivo 100 di back-up/restore al detto dispositivo 90 per criptare/decriptare e/o comprimere/decomprimere dati.

[0080] A questo punto, il motore di crittografia del dispositivo 90 per criptare/decriptare e/o comprimere/decomprimere dati crea un Nonce attraverso detta seconda funzione matematica segreta in funzione del primo e del secondo numero randomico (CH1;CH2).

[0081] Quindi, il chip di autenticazione crittografica del dispositivo 90 per criptare/decriptare e/o comprimere/decomprimere dati crea una chiave di sessione (K_{sess}) attraverso la prima funzione di hash in funzione del Nonce e del segreto (csk) inserito dal costruttore del dispositivo 90 per criptare/decriptare e/o comprimere/decomprimere dati.

[0082] A questo punto, il motore di crittografia del dispositivo 90 per criptare/decriptare e/o comprimere/decomprimere dati calcola un secondo vettore di inizializzazione $(CKvector\ 2)_{CT}$ applicando la seconda funzione matematica segreta in funzione del Nonce condiviso precedentemente calcolato e della chiave di sessione (K_{sess}).

[0083] Viene quindi confrontato, il secondo vettore di inizializzazione $(CKvector\ 2)_{CT}$ calcolato dal dispositivo 90 per criptare/decriptare e/o comprimere/decomprimere dati con il secondo vettore di inizializzazione $(CKvector\ 2)_{T}$ inviato dal dispositivo 100 di back-up/restore.

[0084] Avviene quindi l'attivazione della cifratura del canale attraverso la chiave di sessione (K_{sess}). In altri termini il dispositivo 90 per criptare/decriptare e/o comprimere/decomprimere dati ed il dispositivo 100 di back-up/restore codificano tutti i dati successivi in transito in entrambe le direzioni come segue:

- attivazione della cifratura del canale di comunicazione da parte del dispositivo 90 per criptare/decriptare e/o comprimere/decomprimere dati utilizzando un algoritmo di crittografia presente nel proprio motore crittografico e la relativa chiave di sessione (K_{sess}) derivata lungo il procedimento sopra descritto;
- attivazione della cifratura del canale di comunicazione da parte del dispositivo 100 di back-up/restore utilizzando un algoritmo di crittografia presente nel proprio motore crittografico e la relativa chiave di sessione (K_{sess}) derivata lungo il procedimento sopra descritto;
- invio da parte del dispositivo 90 per criptare/decriptare e/o comprimere/decomprimere dati al dispositivo 100 di back-up/restore di un comando di connessione noto sul canale crittografato precedentemente instaurato ed attivato;
- ricezione di tale comando su canale crittografato da parte del dispositivo di back-up/restore e verifica della sua consistenza dopo l'opportuna decrittografia;
- invio di un comando di risposta noto da parte del dispositivo 100 di back-up/restore al dispositivo 90 per criptare/decriptare e/o comprimere/decomprimere sempre sul medesimo canale crittografato già instaurato ed attivo.
- verifica, da parte del dispositivo 100 di back-up/restore al dispositivo 90 per criptare/decriptare e/o comprimere/decomprimere della consistenza del comando di risposta ricevuto da parte del dispositivo 100 di back-up/restore dopo la relativa decrittografia.
- se entrambe le verifiche hanno successo il canale crittografato è valido ed è attivo per tutte le successive comunicazioni tra i due detti dispositivi ovvero sia quello 100 di back-up/restore e sia quello 90 per criptare/decriptare e/o comprimere/decomprime.

[0085] Tornado alla schema a blocchi mostrato in fig. 4, si vede come la fase di verifica dello stato di associazione del dispositivo 100 di back-up/restore e del dispositivo 90 per criptare/decriptare e/o comprimere/decomprimere dati comprende le fasi di:

- richiesta dello stato di associazione al detto dispositivo 100 di back-up/restore;
- richiesta dello stato di associazione al dispositivo 90 per criptare/decriptare e/o comprimere/decomprimere dati.

[0086] Con riferimento alla fig. 3 e 4, si evidenzia che il dispositivo 90 per criptare/decriptare e/o comprimere decomprimere dati è stato indicato con la lettera CT, tale lettera contraddistingue quindi come pedice anche tutte le funzioni ed i parametri dello schema ad esso relativi, mentre il dispositivo 100 di back-up/restore è stato indicato con la lettera T tale lettere contraddistingue quindi come pedice anche tutte le funzioni ed i parametri dello schema relativi a tale dispositivo.

[0087] Il processo si sviluppa secondo quattro percorsi alternativi in funzione della risposta in merito allo stato di associazione dei due dispositivi.

[0088] Se nè il dispositivo 100 back-up/restore, nè dispositivo 90 per criptare/decriptare e/o comprimere/decomprimere dati sono associati ed il dispositivo di back-up/restore non è mai stato configurato.

[0089] Il processo si sviluppa secondo le seguenti fasi:

- configurazione iniziale del dispositivo 100 di back-up/restore;
- invio richiesta di associazione tra dispositivo 100 di back-up/restore e dispositivo 90 esterno per criptare/decriptare e/o comprimere/decomprimere dati;
- generazione e scambio di chiavi crittografiche e di dati di accesso univoci secondo funzioni private e protette in entrambi i dispositivi rispettivamente 90 e 100.
- invio da parte dal dispositivo 100 di back-up/restore di conferma di associazione completata al dispositivo esterno per criptare/decriptare e/o comprimere/decomprimere dati.

[0090] Alternativamente se il dispositivo 100 di back-up/restore non è associato, ma il dispositivo 90 per comprimere/decomprimere dati è già stato precedentemente configurato ed associato ad un altro dispositivo 100 di back/up restore siamo nel caso di dispositivo 100 di back-up/restore vergine, ad esempio nel caso che un dispositivo di back-up/restore che era precedentemente associato al dispositivo 90 per criptare/decriptare e/o comprimere/decomprimere dati sia andato perso. In tal caso, il processo si sviluppa secondo le seguenti fasi:

- richiesta all'utente, di inserire un codice identificativo utente predeterminato, vale a dire una password che lui solo conosce e aveva provveduto precedentemente ad inserire ed associare al dispositivo 90 per criptare/decriptare e/o comprimere/decomprimere dati;

- generazione e scambio delle chiavi crittografiche e dei dati di accesso secondo funzioni private e protette presenti nel dispositivo per il back-up/restore derivando parte dei dati di accesso stessi tramite le richiamate funzioni private e protette partendo anche dalla password dell'utente;
- verifica delle chiavi crittografiche e dei dati di accesso presenti nel dispositivo 90 per criptare/decriptare e/o comprimere/decomprimere dati;
- se il codice identificativo è inserito validamente, ovvero se i dati di accesso derivati tramite le opportune funzioni private e protette risultano essere coerenti con quanto presente nel dispositivo 90 per criptare/decriptare e/o comprimere/decomprimere dati, avviene un invio di una richiesta di associazione tra il dispositivo 90 per criptare/decriptare e/o comprimere/decomprimere dati ed il dispositivo 100 di back-up/restore;
- generazione nel dispositivo di back-up/restore dei dati crittografici e di accesso necessari per confermare l'associazione univoca con il dispositivo per criptare/decriptare e/o comprimere/decomprimere dati;
- invio da parte dal dispositivo di back-up/restore di conferma di associazione completata al dispositivo esterno per criptare/decriptare e/o comprimere/decomprimere dati;
- invio della propria versione di back-up $(V)_{CT}$ dei dati crittografici e dei dati in genere memorizzati nel proprio database del dispositivo (90) per criptare/decriptare e/o comprimere/decomprimere dati al dispositivo (100) di back-up/restore;
- aggiornamento della versione di back-up $(V)_{T}$ del dispositivo (100) di back-up/restore in funzione della versione di back-up $(V)_{CT}$ ricevuta dal dispositivo (90) per criptare/decriptare e/o comprimere/decomprimere dati.

[0091] Secondo un'altra alternativa, se il dispositivo di back-up/restore è stato precedentemente associato ad un dispositivo 90 per criptare/decriptare e/o comprimere/decomprimere dati, ma il dispositivo 90 per criptare/decriptare e/o comprimere/decomprimere dati non è mai stato configurato ed associato ad un dispositivo 100 di back-up/restore siamo nel caso di dispositivo 90 per criptare/decriptare e/o comprimere/decomprimere dati vergine, è questo il caso in cui un precedente dispositivo 90 per criptare/decriptare e/o comprimere/decomprimere dati associato al dispositivo 100 di back-up/restore è andato perduto.

[0092] In questo caso il processo si sviluppa secondo le seguenti fasi:
Richiesta all'utente, di inserire un codice identificativo utente predeterminato vale a dire una password che lui solo conosce e aveva provveduto precedentemente ad inserire ed associare al dispositivo 100 di back-up/restore;

- generazione e scambio delle chiavi crittografiche e dei dati di accesso secondo funzioni private e protette presenti nel dispositivo per il back-up/restore derivando parte dei dati di accesso stessi tramite le richiamate funzioni private e protette partendo anche dalla password dell'utente;
- verifica delle chiavi crittografiche e dei dati di accesso presenti nel dispositivo 100 di back-up/restore;
- se il codice identificativo è inserito validamente, ovvero se i dati di accesso derivati tramite le opportune funzioni private e protette risultano essere coerenti con quanto presente nel dispositivo 100 di back-up/restore avviene un invio di una richiesta di associazione tra il dispositivo 90 per criptare/decriptare e/o comprimere/decomprimere dati ed il dispositivo 100 di back-up/restore;
- generazione nel dispositivo per criptare/decriptare e/o comprimere/decomprimere dati dei dati crittografici e di accesso necessari per confermare l'associazione univoca con il dispositivo di back-up/restore;
- invio da parte dal dispositivo per criptare/decriptare e/o comprimere/decomprimere dati di conferma di associazione completata al dispositivo esterno di back-up/restore;
- invio della propria versione di back-up $(V)_{T}$ dei dati crittografici e dei dati in genere memorizzati nel proprio database del (100) di back-up/restore al dispositivo (90) per criptare/decriptare e/o comprimere/decomprimere dati al dispositivo;
- aggiornamento della versione di back-up $(V)_{CT}$ del dispositivo (90) per criptare/decriptare e/o comprimere/decomprimere dati in funzione della versione di back-up $(V)_{T}$ ricevuta dal dispositivo (100) di back-up/restore.

[0093] Infine ancora alternativamente, se il dispositivo 100 back-up/restore ed il dispositivo 90 per criptare/decriptare e/o comprimere/decomprimere dati sono già stati associati ed il dispositivo di back-up/restore è già stato precedentemente configurato, siamo nella condizione normale di riutilizzo dei dispositivi ed il processo si sviluppa secondo le seguenti fasi:

- verifica delle chiavi crittografiche e dei dati di accesso secondo funzioni private e protette presenti in entrambi i dispositivi;
- se lo scambio dei dati di accesso è coerente, ovvero entrambi i dispositivi tramite le funzioni private e protette verificano che sono effettivamente tra loro correttamente associati, avviene un invio richiesta di verifica della versione delle chiavi crittografiche, dati utente e dati in genere contenuti nel dispositivo di back-up/restore da parte del dispositivo per criptare/decriptare e/o comprimere/decomprimere dati;
- in funzione della versione dei dati presenti nel dispositivo di back-up/restore rispetto a quelli presenti nel dispositivo 90 per criptare/decriptare e/o comprimere/decomprimere dati, è possibile effettuare un nuovo back-up dei dati presenti in quest'ultimo nel primo dispositivo 100 di back-up/restore (se i dati presenti nel dispositivo 90 per criptare/decriptare e/o comprimere/decomprimere sono più recenti) altrimenti viene rilevato un tentativo di manomissione del sistema in quanto non è possibile che un dispositivo per criptare/decriptare e/o comprimere/decomprimere già associato con un dispositivo di back-up/restore disponga di una versione dei dati da archiviare su tale ultimo dispositivo più vecchia. Se la versione dei dati è identica, non accade nulla.

[0094] In altri termini se le funzioni private e protette verificano che i dati di accesso crittografici sono corretti e coerenti tra i due dispositivi, avviene un invio richiesta di verifica della versione di back-up $(V)_T$ del dispositivo (100) di back-up/restore da parte del dispositivo (90) per criptare/decriptare e/o comprimere/decomprimere dati.

[0095] Viene quindi confrontata la versione di back-up $(V)_T$ del detto dispositivo (100) di back-up/restore con la versione di back-up $(V)_{CT}$ del dispositivo (90) per criptare/decriptare e/o comprimere/decomprimere dati.

[0096] Se la versione del dispositivo 90 per criptare/decriptare e/o comprimere/decomprimere dati è successiva a quella del dispositivo 100 di back-up/restore, il dispositivo 90 per criptare/decriptare e/o comprimere/decomprimere dati invia la propria versione di back-up $(V)_{CT}$ memorizzati nel proprio database al dispositivo (100) di back-up/restore.

[0097] La presente invenzione è stata descritta con riferimento ad alcune forme realizzative. Diverse modifiche possono essere apportate alle forme realizzative descritte nel dettaglio, rimanendo comunque nell'ambito di protezione dell'invenzione, definito dalle rivendicazioni seguenti.

Rivendicazioni

1. Dispositivo (100) portatile di back-up/restore associabile ad un dispositivo esterno (90), detto dispositivo esterno (90) essendo configurato per criptare/decriptare e/o comprimere/decomprimere dati;
   detto dispositivo (100) di back-up/restore comprendendo:
   un involucro esterno;
   almeno una CPU comprendente almeno un microcontrollore ed almeno un motore crittografico;
   almeno un chip di autenticazione crittografico per associare in modo univoco un detto dispositivo di back-up/restore con un dispositivo esterno configurato per criptare/decriptare e/o comprimere/decomprimere dati;
   almeno una memoria di tipo flash;
   almeno una prima porta (5) di ingresso/uscita atta ad essere interfacciata con il dispositivo esterno per criptare/decriptare e/o comprimere/decomprimere dati.
2. Dispositivo (100) portatile di back-up/restore secondo la rivendicazione 1, caratterizzato dal fatto che la detta prima porta (5) di ingresso/uscita dati comprende delle connessioni atte a comunicare dati con dispositivi esterni secondo uno standard internazionale di comunicazione.
3. Dispositivo (100) portatile di back-up/restore secondo la rivendicazione 1 o 2, caratterizzato dal fatto che la detta prima porta (5) di ingresso/uscita dati comprende una connessione maschio (7) atta ad interfacciali con una connessione femmina di un primo dispositivo esterno (90) per criptare/decriptare e/o comprimere/decomprimere dati.
4. Dispositivo (100) portatile di back-up/restore secondo una qualsiasi delle rivendicazioni da 1 a 3, caratterizzato dal fatto che la detta prima porta (5) di ingresso/uscita dati comprende una connessione maschio (8) USB.
5. Dispositivo (100) portatile di back-up/restore secondo una qualsiasi delle rivendicazioni da 1 a 4, caratterizzato dal fatto che la detta CPU comprende al suo interno almeno una memoria di tipo flash.
6. Processo di back-up/restore dati tra un dispositivo esterno (90) per criptare/decriptare e/o comprimere/decomprimere dati ed un dispositivo (100) di back-up/restore secondo una qualsiasi delle precedenti rivendicazioni da 1 a 5, Il processo comprendendo le fasi di:
   – connettere un connettore maschio di una porta di ingresso/uscita dati del dispositivo (100) di back-up/restore con un connettore femmina di una porta di ingresso/uscita dati del dispositivo (90) per criptare/decriptare e/o comprimere/decomprimere dati; detto dispositivo (90) per criptare/decriptare e/o comprimere/decomprimere dati essendo a sua volta collegato ad un computer o un notebook o un desktop, o un server o una workstation, o un tablet, o uno smartphone, tramite ulteriori connessioni disponibili del dispositivo esterno (90) per criptare/decriptare e/o comprimere/decomprimere dati; detto dispositivo esterno (90) per criptare/decriptare e/o comprimere/decomprimere dati comprendendo almeno un database comprendente una versione di back-up;
   – verifica dello stato di configurazione del dispositivo 100 di back-up/restore e del dispositivo (90) per criptare/decriptare e/o comprimere/decomprimere dati;
   – verifica dello stato di associazione del dispositivo (100) di back-up/restore e del dispositivo per criptare/decriptare e/o comprimere/decomprimere dati;
   ed in cui la fase di autenticazione del dispositivo (100) di back-up/restore e del dispositivo (90) per criptare/decriptare e/o comprimere/decomprimere dati comprende:
   creazione di un primo vettore di inizializzazione $(CKvector\ 1)_{CT}$ in funzione di un segreto (csk) inserito dal costruttore del dispositivo (90) per criptare/decriptare e/o comprimere/decomprimere dati e di un primo numero randomico $(CH1)_{CT}$, da parte del motore di crittografia del detto dispositivo (90) per criptare/decriptare e/o comprimere/decomprimere dati;
   – invio del primo vettore di inizializzazione $(CKvector\ 1)_{CT}$ e del primo numero randomico $(CH1)_{CT}$ al detto dispositivo di back-up/restore;
   – calcolo del primo vettore di inizializzazione $(CKvector\ 1)_T$ da parte del motore crittografia detto dispositivo (100) di back-up/restore;

– confronto del primo vettore di inizializzazione (CKvector 1)$_{CT}$ inviato dal dispositivo (90) per criptare/decriptare e/o comprimere/decomprimere dati con il primo vettore di inizializzazione (CKvector 1)$_{T}$ calcolato da parte del motore crittografia del detto dispositivo (100) di back-up/restore;
– generazione di un secondo numero randomico (CH2)$_{T}$
– calcolo della chiave di sessione (K_{sess}) da parte del motore di crittografia del dispositivo (100) di back-up/restore;
– creazione da parte del motore di crittografia del detto dispositivo (100) di back-up/restore di un secondo vettore di inizializzazione (CKvector 2)$_{T}$ in funzione di un segreto (csk) inserito dal costruttore del detto dispositivo di back-up/restore;
– invio del secondo vettore di inizializzazione (CKvector 2)$_{T}$ e del detto secondo numero randomico (CH2)$_{T}$ al detto dispositivo (90) per criptare/decriptare e/o comprimere/decomprimere dati;
– calcolo della chiave di sessione (K_{sess}) da parte del motore di crittografia del dispositivo (90) per criptare/decriptare e/o comprimere/decomprimere dati;
– calcolo del secondo vettore di inizializzazione (CKvector 2)$_{CT}$ da parte del motore crittografia del detto dispositivo per criptare/decriptare e/o comprimere/decomprimere dati;
– confronto del secondo vettore di inizializzazione (CKvector 2)$_{T}$ inviato dal dispositivo di back-up/restore con il secondo vettore di inizializzazione (CKvector 2)$_{CT}$ calcolato da parte del motore crittografia del detto dispositivo per criptare/decriptare e/o comprimere/decomprimere dati;
– attivazione della cifratura del canale di comunicazione da parte del dispositivo (90) per criptare/decriptare e/o comprimere/decomprimere utilizzando un algoritmo di crittografia presente nel proprio motore crittografico e la relativa chiave di sessione (K_{sess}) precedentemente derivata;
– attivazione della cifratura del canale di comunicazione da parte del dispositivo (100) di back-up/restore utilizzando un algoritmo di crittografia presente nel proprio motore crittografico e la relativa chiave di sessione (K_{sess}) derivata precedentemente;
– invio da parte del dispositivo (90) per criptare/decriptare e/o comprimere/decomprimere al dispositivo di back-up/restore di un comando di connessione noto sul canale crittografato precedentemente instaurato ed attivato;
– ricezione di tale comando sul canale crittografato da parte del dispositivo (100) di back-up/restore e verifica della sua consistenza dopo una fase di decrittografia;
– invio di un comando di risposta noto da parte del dispositivo (100) di back-up/restore al dispositivo (90) per criptare/decriptare e/o comprimere/decomprimere dati sul medesimo canale crittografato già instaurato ed attivo;
– verifica, da parte del dispositivo (90) per criptare/decriptare e/o comprimere/decomprimere della consistenza del comando di risposta ricevuto da parte del dispositivo (100) di back-up/restore dopo una fase di decrittografia ed in cui dettoprocesso comprende una fase di autenticazione reciproca del dispositivo (100) di back-up/restore e del dispositivo (90) per criptare/decriptare e/o comprimere/decomprimere dati.

7. Processo secondo la rivendicazione 6 caratterizzato dal fatto che la fase di verifica dello stato di associazione del dispositivo di back-up/restore e del dispositivo per criptare/decriptare e/o comprimere/decomprimere dati comprende le fasi di:
– richiesta dello stato di associazione al detto dispositivo (100) di back-up/restore;
– richiesta dello stato di associazione al detto dispositivo (90) per criptare/decriptare e/o comprimere/decomprimere dati.

8. Processo secondo la rivendicazione 6 o 7 caratterizzato dal fatto che se nè il dispositivo (100) di back-up/restore, nè dispositivo per criptare/decriptare e/o comprimere/decomprimere dati sono associati ed il dispositivo (100) di back-up/restore non è mai stato configurato comprende le fasi di:
– configurazione iniziale del dispositivo (100) di back-up/restore;
– invio richiesta di associazione tra dispositivo (100) di back-up/restore e il dispositivo esterno (90) per criptare/decriptare e/o comprimere/decomprimere dati;
– generazione e scambio di chiavi crittografiche e di dati di accesso secondo predeterminate funzioni in entrambi i suddetti dispositivi;
– invio da dispositivo (100) di back-up/restore di conferma di associazione completata al dispositivo esterno (90) per criptare/decriptare e/o comprimere/decomprimere dati e/o viceversa.

9. Processo secondo la rivendicazione 6 o 7, caratterizzato dal fatto che se il dispositivo (100) di back-up/restore non è associato, ma il dispositivo (90) per criptare/decriptare comprimere/decomprimere dati è già stato precedentemente configurato ed associato ad un precedente dispositivo (100) di back-up/restore comprende le fasi di:
– richiesta all'utente, di inserire un codice identificativo utente predeterminato;
– verifica del codice identificativo, comprendente una verifica della coerenza del codice inserito con i dati di accesso derivati tramite le opportune funzioni da quanto presente nel dispositivo 90 per criptare/decriptare e/o comprimere/decomprimere dati;
– se il codice identificativo è inserito validamente, avviene un invio di una richiesta di associazione tra dispositivo di back-up/restore e dispositivo per criptare/decriptare e/o comprimere/decomprimere dati;
– invio da parte dal dispositivo (100) di back-up/restore di conferma di associazione completata al dispositivo esterno (90) per criptare/decriptare e/o comprimere/decomprimere dati;

– invio della propria versione di back-up $(V)_{CT}$ dei dati crittografici e dei dati in genere memorizzati nel proprio database del dispositivo (90) per criptare/decriptare e/o comprimere/decomprimere dati al dispositivo (100) di back-up/restore;
– aggiornamento della versione di back-up $(V)_T$ del dispositivo (100) di back-up/restore in funzione della versione di back-up $(V)_{CT}$ ricevuta dal dispositivo (90) per criptare/decriptare e/o comprimere/decomprimere dati.

10. Processo secondo la rivendicazione 7 o 8, caratterizzato dal fatto che se il dispositivo di back-up/restore è stato precedentemente associato ad un dispositivo per comprimere/decomprimere dati, ma il dispositivo per comprimere/decomprimere dati non è mai stato configurato ed associato ad un dispositivo di back/up restore comprende le fasi di:
– richiesta all'utente, di inserire un codice identificativo utente predeterminato;
– verifica del codice identificativo, comprendente una verifica della coerenza del codice inserito con i dati di accesso derivati tramite le opportune funzioni da quanto presente nel dispositivo 100 di back-up/restore;
– se il codice identificativo è validamente inserito, avviene un invio richiesta di associazione tra dispositivo (100) di back-up/restore e il dispositivo (90) esterno per criptare/decriptare e/o comprimere/decomprimere dati;
– invio da parte dal dispositivo (90) esterno per criptare/decriptare e/o comprimere/decomprimere dati di conferma di associazione completata al dispositivo (100) di back-up/restore;
– invio della propria versione di back-up $(V)_T$ dei dati crittografici e dei dati in genere memorizzati nel proprio database del dispositivo (100) di back-up/restore al dispositivo (90) per criptare/decriptare e/o comprimere/decomprimere dati;
– aggiornamento della versione di back-up $(V)_{CT}$ del dispositivo (90) per criptare/decriptare e/o comprimere/decomprimere dati in funzione della versione di back-up $(V)_T$ ricevuta dal dispositivo (100) di back-up/restore.

11. Processo secondo la rivendicazione 7 caratterizzato dal fatto che se il dispositivo (100) di back-up/restore ed il dispositivo (90) per criptare/decriptare e/o comprimere/decomprimere dati sono associati ed il dispositivo (100) di back-up/restore è già stato precedentemente configurato comprende le fasi di:
– verifica delle chiavi crittografiche e dei dati di accesso secondo predeterminate funzioni presenti in entrambi i suddetti dispositivi;
– verifica della corretta mutua associazione tra i due dispositivi tramite predeterminate funzioni presenti in entrambi i dispositivi partendo dai dati di accesso precedentemente scambiati;
– se la verifica ha esito positivo avviene un invio richiesta di verifica della versione di back-up $(V)_T$ del dispositivo (100) di back-up/restore da parte del dispositivo (90) per criptare/decriptare e/o comprimere/decomprimere dati;
– viene confrontata la versione di back-up $(V)_T$ del detto dispositivo (100) di back-up/restore con la versione di back-up $(V)_{CT}$ del dispositivo (90) per criptare/decriptare e/o comprimere/decomprimere dati;
– se la versione del dispositivo (90) per criptare/decriptare e/o comprimere/decomprimere dati è successiva a quella del dispositivo (100) di back-up/restore, il dispositivo (90) per criptare/decriptare e/o comprimere/decomprimere dati invia la propria versione di back-up $(V)_{CT}$ memorizzati nel proprio database al dispositivo (100) di back-up/restore.

12. Processo secondo una qualsiasi delle precedenti rivendicazioni da 6 a 11, caratterizzato dal fatto che la versione di back-up $(V)_T$ comprende:
delle chiavi crittografiche;
dei dati utente;
dati ed informazioni crittografati.

13. Processo secondo una qualsiasi delle precedenti rivendicazioni da 6 a 12 caratterizzato dal fatto che la versione di back-up (V)CT del detto dispositivo (90) per criptare/decriptare e/o comprimere/decomprimere dati comprende:
delle chiavi crittografiche;
dei dati utente;
dati ed informazioni crittografati.

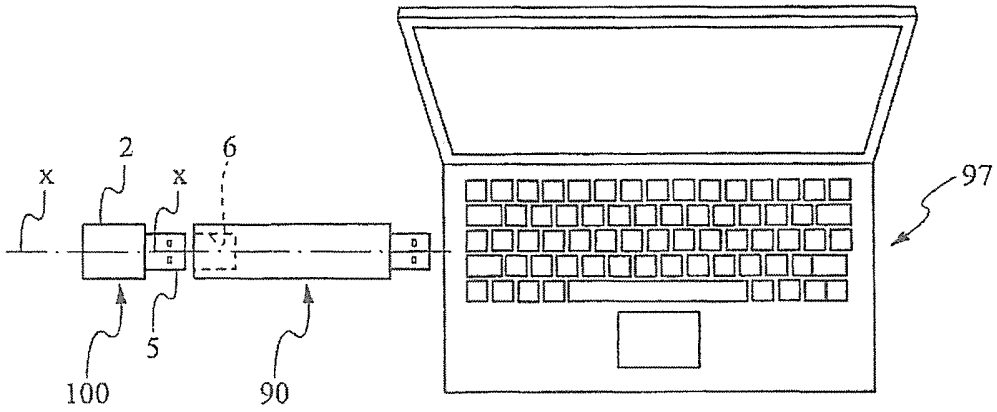


Fig. 1

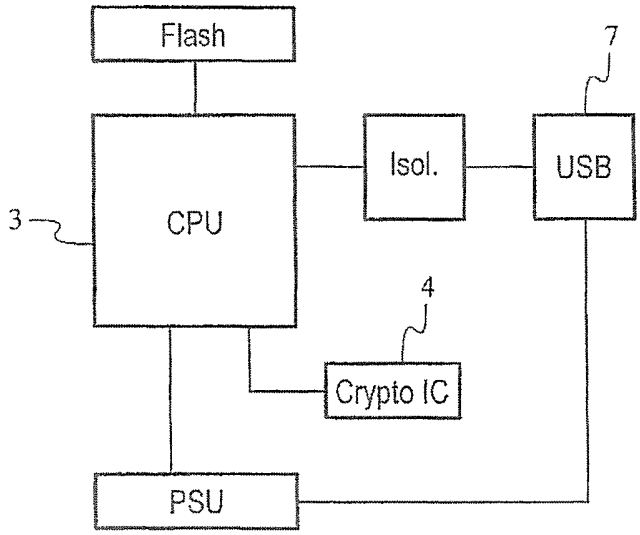


Fig. 2

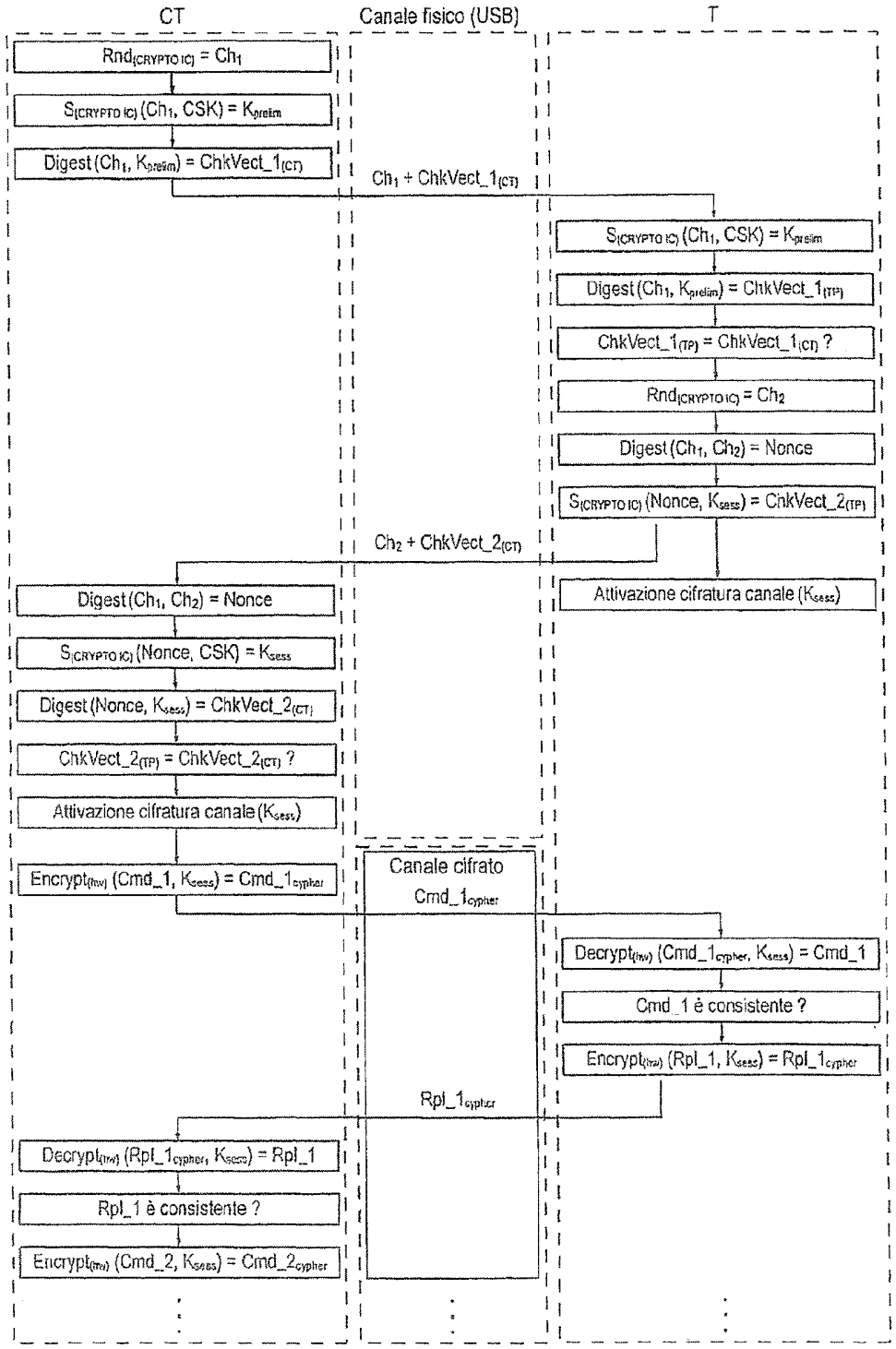

CT
Canale fisico (USB)
T
Rnd(CRYPTO IC) = Ch1
S(CRYPTO IC) (Ch1, CSK) = Kprelim
Digest (Ch1, Kprelim) = ChkVect_1(CT)
Ch1 + ChkVect_1(CT)
S(CRYPTO IC) (Ch1, CSK) = Kprelim
Digest (Ch1, Kprelim) = ChkVect_1(TP)
ChkVect_1(TP) = ChkVect_1(CT) ?
Rnd(CRYPTO IC) = Ch2
Digest (Ch1, Ch2) = Nonce
S(CRYPTO IC) (Nonce, Ksess) = ChkVect_2(TP)
Ch2 + ChkVect_2(CT)
Digest (Ch1, Ch2) = Nonce
Attivazione cifratura canale (Ksess)
S(CRYPTO IC) (Nonce, CSK) = Ksess
Digest (Nonce, Ksess) = ChkVect_2(CT)
ChkVect_2(TP) = ChkVect_2(CT) ?
Attivazione cifratura canale (Ksess)
Canale cifrato
Encrypt(inv) (Cmd_1, Ksess) = Cmd_1cypher
Cmd_1cypher
Decrypt(inv) (Cmd_1cypher, Ksess) = Cmd_1
Cmd_1 è consistente ?
Encrypt(inv) (Rpl_1, Ksess) = Rpl_1cypher
Rpl_1cypher
Decrypt(inv) (Rpl_1cypher, Ksess) = Rpl_1
Rpl_1 è consistente ?
Encrypt(inv) (Cmd_2, Ksess) = Cmd_2cypher

Fig. 3

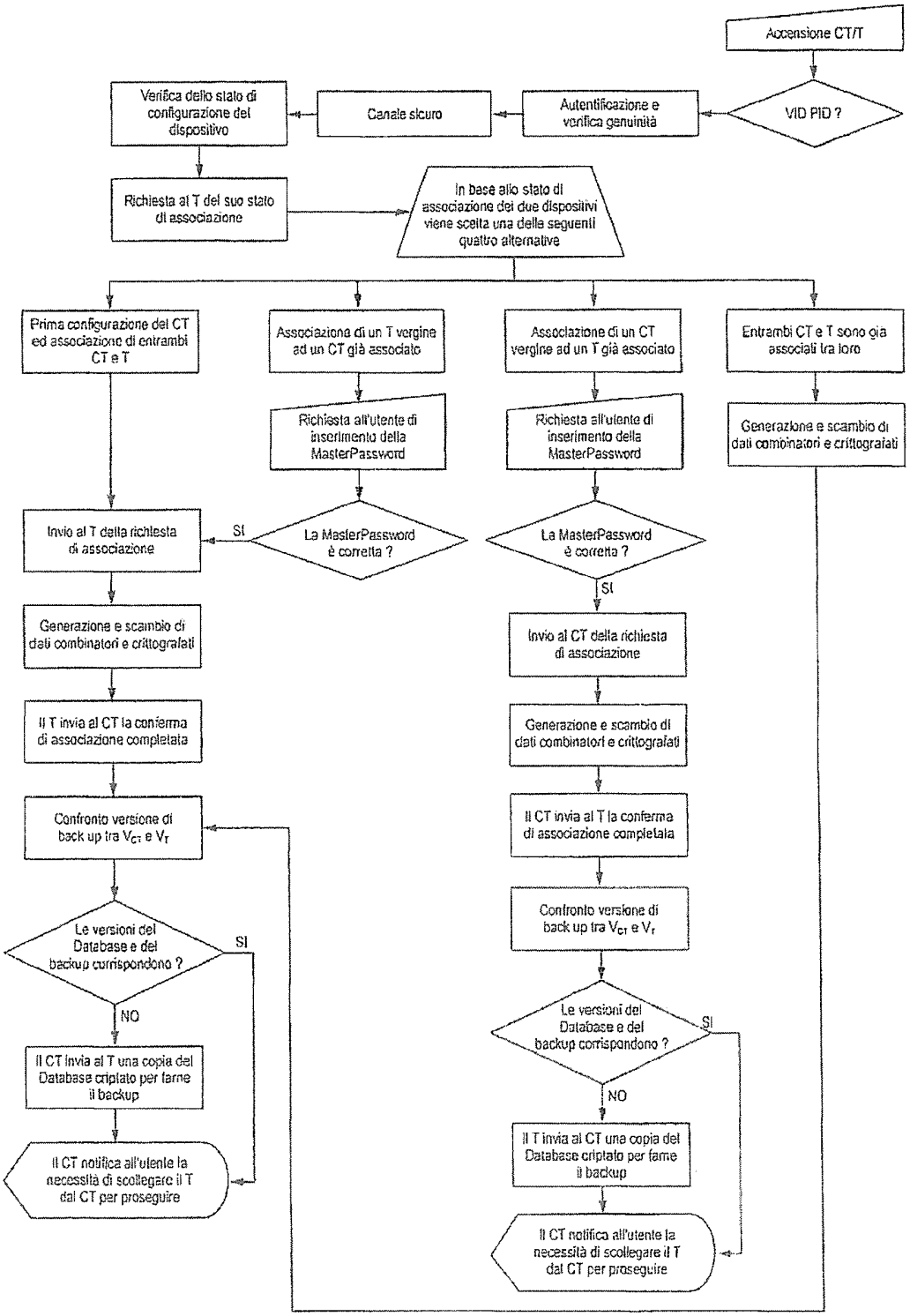

Accensione CT/T
VID PID ?
Autentificazione e verifica genuinità
Canale sicuro
Verifica dello stato di configurazione del dispositivo
Richiesta al T del suo stato di associazione
In base allo stato di associazione dei due dispositivi viene scelta una della seguenti quattro alternative
Prima configurazione del CT ed associazione di entrambi CT e T
Associazione di un T vergine ad un CT già associato
Associazione di un CT vergine ad un T già associato
Entrambi CT e T sono già associati tra loro
Richiesta all'utente di inserimento della MasterPassword
Richiesta all'utente di inserimento della MasterPassword
Generazione e scambio di dati combinatori e crittografati
Invio al T della richiesta di associazione
SI
La MasterPassword è corretta ?
La MasterPassword è corretta ?
SI
Generazione e scambio di dati combinatori e crittografati
Il T invia al CT la conferma di associazione completata
Invio al CT della richiesta di associazione
Generazione e scambio di dati combinatori e crittografati
Il CT invia al T la conferma di associazione completata
Confronto versione di back up tra V_{CT} e V_T
Confronto versione di back up tra V_{CT} e V_T
Le versioni del Database e del backup corrispondono ?
SI
NO
Le versioni del Database e del backup corrispondono ?
SI
NO
Il CT invia al T una copia del Database criptato per farne il backup
Il T invia al CT una copia del Database criptato per farne il backup
Il CT notifica all'utente la necessità di scollegare il T dal CT per proseguire
Il CT notifica all'utente la necessità di scollegare il T dal CT per proseguire

Fig. 4