ITALIAN PATENT OFFICE

Document No.

102010901816512A1

Publication Date

20110905

Applicant

ELSAG DATAMAT SPA

Title

DISPOSITIVO ELETTRONICO PORTATILE INTERFACCIABILE AD UN CALCOLATORE

Front page automatically generated by WIPO

DESCRIZIONE

del brevetto per invenzione industriale dal titolo:

"DISPOSITIVO ELETTRONICO PORTATILE INTERFACCIABILE AD UN CALCOLATORE"

di ELSAG DATAMAT SPA

di nazionalità italiana

con sede: VIA GIACOMO PUCCINI, 2

GENOVA (GE)

Inventore: GIGANTESCO Aldo

* * *

La presente invenzione è relativa ad un dispositivo elettronico portatile, ed in particolare ad un dispositivo elettronico portatile interfacciabile ad un calcolatore.

Come è noto, le attuali esigenze di mobilità impongono l'utilizzo di apparecchi informatici mobili (computer portatili, palmari, ecc.), i quali possono essere portati dagli utenti, in maniera tale per cui gli utenti stessi dispongono, in qualsiasi punto in cui essi si trovino, dei suddetti apparecchi informatici mobili. In tal modo, agli utenti è fornita la possibilità di svolgere attività lavorative e non, anche quando essi si trovano lontano da aree prestabilite quali, ad esempio, postazioni lavorative, internet point, ecc.

Data la sempre crescente esigenza di condividere informazioni, e quindi di comunicare con calcolatori posti

Simone BONGIOVANNI
(Iscrizione Albo nr. 615/BM)

anche a grande distanza rispetto all'utente, tipicamente gli apparecchi informatici mobili sono provvisti di opportuni sistemi di ricetrasmissione, al fine consentire la connessione con il "mondo esterno", ovvero, in termini più tecnici, la connessione ad una o più reti di calcolatori, quale ad esempio la cosiddetta rete Internet. In generale, tali sistemi di ricetrasmissione consentono di collegare gli apparecchi informatici mobili ad una generica rete di calcolatori, indifferentemente in modo cablato o wireless. In entrambi i casi, i collegamenti avvengono nel rispetto di opportuni protocolli di comunicazione, i quali, come è noto, possono essere relativi ad uno o più livelli ("layer") della pila ("stack") di livelli descritta nel modello Organizzazione Internazionale per la Standardizzazione - Interconnessione di Sistemi Aperti ("International Organization for Standardization - Open Systems Interconnection", ISO-OSI), per citare l'esempio di standardizzazione più noto. Senza entrare in ulteriori dettagli, e ancora con riferimento allo standard ISO-OSI, il collegamento tra due generici dispositivi informatici (calcolatori, apparecchi informatici mobili, ecc.) prevede tipicamente il coinvolgimento di più livelli della summenzionata pila di livelli, ciascuno associato ad un rispettivo protocollo di comunicazione. In pratica, e con particolare riferimento al caso degli apparecchi

informatici mobili, l'implementazione di ciascuno dei protocolli utili a collegare due generici dispositivi informatici è demandata in tutto o in parte ai summenzionati sistemi di ricetrasmissione, eventualmente in cooperazione con ulteriori sottosistemi presenti all'interno degli apparecchi informatici mobili. Indipendentemente da tali dettagli, nel caso in cui si voglia collegare in modo cablato un generico apparecchio informatico mobile al mondo esterno, è sufficiente collegare l'apparecchio informatico mobile ad una cosiddetta "presa di rete", mediante un opportuno cavo di rete; alternativamente, nel caso in cui si voglia stabilire un collegamento di tipo wireless, tipicamente il sistema di ricetrasmissione dell'apparecchio informatico mobile è in grado di trasmettere e ricevere segnali elettromagnetici con cosiddetti punti di accesso ("access point"), i quali trovano oggi una sempre più capillare diffusione, e svolgono una funzione analoga a quella delle prese di rete.

Gli apparecchi informatici mobili oggi disponibili consentono dunque una grande flessibilità di utilizzo, tuttavia presentano un'elevata complessità circuitale, in quanto necessitano, tra l'altro, di primi componenti quali, ad esempio, rispettive memorie RAM, cioè memorie ad accesso casuale in lettura/scrittura e di tipo volatile, e rispettive memorie ROM, cioè memorie non volatili in cui

possono essere memorizzati rispettivi sistemi operativi. Tali primi componenti hanno subito e subiscono nel tempo una continua riduzione dei rispettivi ingombri, pesi e consumi. Inoltre, gli apparecchi informatici mobili necessitano di secondi componenti quali, ad esempio, tastiere, mouse e schermi di visualizzazione ("display"), al fine di consentire agli utenti di interagire con gli apparecchi informatici mobili stessi, oltre che con il mondo esterno. A differenza dei summenzionati primi componenti, tali secondi componenti non possono essere miniaturizzati eccessivamente senza comprometterne ergonomia e comodità di impiego.

Oltre ai summenzionati apparecchi informatici mobili, sono oggi disponibili memorie di massa portatili e non volatili, il cui esempio forse più noto è rappresentato dalle cosiddette chiavette "Universal Serial Bus" (USB), anche note come penne USB o "pendrive". Trattasi in particolare di memorie portatili collegabili a calcolatori da tavolo ("desktop"), oppure ad apparecchi informatici mobili, mediante il cosiddetto protocollo USB. In maggior dettaglio, le chiavette USB oggi più diffuse sono formate da memorie di tipo "flash", cioè memorie non volatili appartenenti alla classe delle memorie a sola lettura programmabili e cancellabili elettricamente ("Electrically Erasable and Programmable Read Only Memory", EEPROM), in

cui le operazioni di scrittura, cancellazione e riscrittura sono appunto svolte per via elettrica. Tali chiavette USB dispongono di rispettivi connettori USB, perciò, dal momento che ormai la quasi totalità dei calcolatori da tavolo e degli apparecchi informatici mobili dispone di connettori conformi allo standard USB (e complementari ai connettori che solitamente equipaggiano le chiavette USB), è possibile collegare le chiavette USB ai calcolatori da tavolo ed agli apparecchi informatici mobili, e comandare operazioni di lettura, di scrittura, cancellazione e riscrittura di informazioni su tali chiavette USB mediante i calcolatori da tavolo e/o gli apparecchi informatici mobili.

Ulteriori esempi di memorie di massa portatili e non volatili, alle quali per semplicità ci si riferisce in seguito come alle schede di memoria, sono rappresentati dalle cosiddette "Memory stick", "MicroSD", "Smart Media", ecc.

Operativamente, le schede di memoria sono circuitalmente semplici ed economiche, e consentono di memorizzare informazioni in modo flessibile. Tuttavia, al fine di memorizzare informazioni o modificare informazioni già memorizzate, le schede di memoria necessitano di essere accoppiate elettricamente a calcolatori, siano essi calcolatori da tavolo oppure apparecchi informatici mobili,

al fine di utilizzarne uno o più componenti, quali ad esempio le tastiere e gli schermi di visualizzazione. Infatti, dato un calcolatore a cui è connessa una data scheda di memoria, se provvisto degli opportuni "driver" relativi alla data scheda di memoria, il sistema operativo del dato calcolatore monta la data scheda di memoria come una qualsiasi periferica connessa al dato calcolatore; successivamente, è quindi possibile visualizzare e/o modificare le informazioni presenti nella data scheda di memoria. A titolo di precisazione, per driver si intende un insieme di istruzioni software, sovente scritte in un linguaggio di basso livello (ad esempio, assembly), che consente ad un sistema operativo di controllare un corrispondente dispositivo hardware.

In pratica, le schede di memoria consentono agli utenti di portare con sé tutte le informazioni necessarie (ivi compresi sistemi operativi) su un supporto dalle dimensioni molto ridotte, comodo da trasportare. Nel momento in cui si manifesta l'esigenza di accedere a tali informazioni, è sufficiente collegare le scheda di memoria a un calcolatore da tavolo, ovvero a un apparecchio informatico mobile, ai quali in seguito ci si riferisce genericamente come a un calcolatore ospite. Tuttavia, molto spesso capita che il possessore della scheda di memoria, cioè colui che fisicamente dispone della scheda di memoria,

sia differente dal proprietario del calcolatore ospite, e che pertanto le informazioni presenti nel calcolatore ospite e nella scheda di memoria debbano essere reciprocamente inaccessibili, rispettivamente, al possessore della scheda di memoria ed al proprietario del calcolatore ospite. Tuttavia, nel momento in cui si accede al calcolatore ospite, ed una volta connessa la scheda di memoria, chi effettivamente utilizza il calcolatore ospite può accedere, in generale, non solo alle informazioni contenute nella scheda di memoria, bensì anche alle informazioni contenute nel calcolatore ospite, ed in particolare in un eventuale disco rigido ("hard-disk") del calcolatore ospite.

A titolo esemplificativo, è frequente una situazione in cui il proprietario del calcolatore ospite autorizza il possessore della scheda di memoria ad utilizzare il proprio calcolatore. In tal modo, il possessore della scheda di memoria può accedere ai dati presenti nell'hard-disk del calcolatore ospite, sia in lettura che in scrittura, e può dunque alterarne i dati contenuti; inoltre, egli stesso si espone al rischio che il calcolatore ospite (ed in particolare i programmi ivi contenuti) sia di per sé non sicuro, e dunque si espone al rischio che informazioni presenti nella scheda di memoria siano danneggiate. E' altresì possibile che, in seguito all'utilizzo descritto,

informazioni riservate presenti nella scheda di memoria restino memorizzate all'interno del calcolatore ospite anche dopo che la scheda di memoria è stata scollegata dal calcolatore ospite, e diventino dunque accessibili a successivi utenti del calcolatore ospite, oltre che al proprietario del calcolatore ospite.

Scopo della presente invenzione è fornire un dispositivo elettronico portatile che risolva almeno in parte gli inconvenienti dell'arte nota.

Secondo l'invenzione, viene fornito un dispositivo elettronico portatile come definito, rispettivamente, nella rivendicazione 1.

Per una migliore comprensione dell'invenzione, ne vengono ora descritte forme di realizzazione, a puro titolo di esempio non limitativo e con riferimento ai disegni allegati, nei quali:

- la figura 1 mostra uno schema a blocchi di una forma di realizzazione di un dispositivo elettronico portatile secondo la presente invenzione; e

- la figura 2 mostra uno schema a blocchi di una differente forma di realizzazione del presente dispositivo elettronico portatile.

Come mostrato in figura 1, il presente dispositivo elettronico portatile 1 comprende un involucro esterno 2, al cui interno sono contenuti, per quanto concerne la

Simone BONGIOVANNI
(Iscrizione Albo nr. 615/BM)

componentistica elettronica: un'unità di elaborazione interna 4; una memoria volatile, ad esempio formata da una memoria RAM ed alla quale ci si riferisce in seguito come alla memoria volatile interna 6; una memoria non volatile, ad esempio di tipo flash ed alla quale ci si riferisce in seguito come alla memoria non volatile interna 8; un modulo per una piattaforma fidata ("Trusted Platform Module", TPM), cui nel seguito ci si riferisce come al modulo TPM 9; almeno un primo connettore interno 10a, il quale nella forma di realizzazione illustrata è di tipo USB, ed una rispettiva prima unità di controllo interna 10b, collegata al primo connettore interno 10a in modo da formare una prima porta interna 10; almeno un primo connettore esterno 14a, il quale nella forma di realizzazione illustrata è di tipo USB, ed una rispettiva prima unità di controllo esterna 14b, collegata al primo connettore esterno 14a in modo da formare una prima porta esterna 14.

Il dispositivo elettronico portatile 1 comprende inoltre almeno un indicatore luminoso 17, mediante il quale l'unità di elaborazione interna 4 può notificare al possessore del dispositivo elettronico mobile 1 informazioni quali, ad esempio, stati di funzionamento del dispositivo elettronico portatile 1. Come descritto a titolo esemplificativo in seguito, tali stati di funzionamento possono comprendere uno stato di accensione,

Simone BONGIOVANNI
(Iscrizione Albo nr. 615/BM)

uno stato di richiesta di autenticazione, uno stato di errore e uno stato di trasmissione. Il dispositivo elettronico portatile 1 comprende inoltre un dispositivo di riconoscimento di impronta 18, il quale è in grado di rilevare, in modo di per sé noto, un'impronta digitale.

Il dispositivo elettronico portatile 1 comprende poi almeno un bus di collegamento 20, il quale collega elettricamente i componenti elettronici del dispositivo elettronico portatile 1, e quindi l'unità di elaborazione interna 4, la memoria volatile interna 6, la memoria non volatile interna 8, il modulo TPM 9, la prima unità di controllo interna 10b, la prima unità di controllo esterna 14b e il dispositivo di riconoscimento di impronta 18.

In maggior dettaglio, all'interno della memoria non volatile interna 8 sono memorizzati, oltre ad eventuali dati utente, un primo ed un secondo sistema operativo, ai quali ci si riferisce in seguito, rispettivamente, come al sistema operativo interno OS1 ed al sistema operativo esterno OS2. Inoltre, nella memoria non volatile interna 8 sono memorizzati driver (descritti in seguito) ed eventuali parametri di funzionamento del sistema operativo interno OS1 e del sistema operativo esterno OS2, quali ad esempio rispettivi elenchi di utenti accreditati e di rispettivi dispositivi di comunicazione interfacciabili con i sistemi operativi OS1, OS2 stessi.

Simone BONGIOVANNI
(Iscrizione Albo nr. 615/BM)

In particolare, la memoria non volatile interna 8 può comprendere una prima ed una seconda porzione, indicate rispettivamente con 8a e 8b.

In dettaglio, la prima porzione 8a può essere impiegata per memorizzare i dati utente, una pluralità di driver esterni, il sistema operativo esterno OS2, eventuali parametri di funzionamento relativi al sistema operativo esterno OS2, ed inoltre eventuali applicazioni eseguibili dal sistema operativo esterno OS2.

La seconda porzione 8b può invece essere utilizzata per memorizzare una pluralità di driver interni, il sistema operativo interno OS1, eventuali parametri di funzionamento relativi al sistema operativo interno OS1, ed inoltre eventuali applicazioni eseguibili dal sistema operativo interno OS1. Inoltre, nella seconda porzione 8b possono essere memorizzati dati di configurazione del dispositivo elettronico portatile 1, quali ad esempio abilitazioni all'uso della prima porta interna 10 o della prima porta esterna 14, oppure prime credenziali (ad esempio una rispettiva coppia formata da un username e da una password) da utilizzare quando si trasmette attraverso una corrispondente porta, come descritto in seguito.

Sia il sistema operativo interno OS1 che sistema operativo esterno OS2 sono tipo certificato, ad esempio secondo il programma noto come "Common Criteria", il quale

comprende una serie di standard riconosciuti a livello internazionale (standard ISO 15408) che definiscono uno schema di valutazione delle caratteristiche di sicurezza di un prodotto informatico. In altre parole, sia il sistema operativo interno OS1 che sistema operativo esterno OS2 possono presentare funzioni di sicurezza (ad esempio, obbligo di inserire una password per poter utilizzare il sistema operativo) che non possono essere aggirate per via elettronica da malintenzionati. Inoltre, come precedentemente accennato, sia il primo che il secondo sistema operativo OS1, OS2 possono eseguire un rispettivo numero di applicazioni (ad esempio, "browser internet", "text editor", ecc.).

In dettaglio, il sistema operativo interno OS1 è tale per cui, quando caricato nella memoria volatile interna 6 ed eseguito dall'unità di elaborazione interna 4, esso consente di controllare il dispositivo elettronico portatile 1, nonché di interfacciare il dispositivo elettronico portatile 1 con ulteriori dispositivi elettronici o calcolatori ad esso connessi, come descritto in dettaglio in seguito. Pertanto, il sistema operativo interno OS1 è configurato per caricare nella memoria volatile interna 6 i summenzionati driver interni, che permettono al sistema operativo interno OS1 stesso di controllare i componenti elettronici del dispositivo

elettronico portatile 1, ed in particolare la prima unità di controllo interna 10b e la prima unità di controllo esterna 14b. Pertanto, il dispositivo elettronico portatile 1 è in grado di comunicare con altri dispositivi elettronici attraverso la prima porta interna 10 e la prima porta esterna 14, come descritto in maggior dettaglio in seguito. Inoltre, il sistema operativo interno OS1 è in grado di controllare, mediante un apposito driver interno, il dispositivo di riconoscimento di impronta 18, nonché di eseguire eventuali applicazioni (contenute nella porzione 8b), e quindi di caricare programmi nella memoria volatile interna 6.

Per quanto concerne, invece, il sistema operativo esterno OS2, esso è configurato in modo da poter disporre, come descritto in dettaglio in seguito, dei soli driver esterni, memorizzati nella porzione 8a della memoria non volatile interna 8. In particolare, i driver esterni sono relativi solamente a componenti elettronici quali schermi e relative schede video, tastiere, mouse e dispositivi interni di controllo quali, ad esempio, processori, temporizzatori ("clock"), memorie volatili, dispositivi di accesso diretto a memoria ("direct memory access", DMA), controllori di interruzione ("interrupt controller"), nonché porte di collegamento del tipo della prima porta 10 (ad esempio, nella forma di realizzazione mostrata in

Simone BONGIOVANNI
(Iscrizione Albo nr. 615/BM)

figura 1, porte USB). In particolare, nella porzione 8a della memoria non volatile 8 non sono presenti driver relativi a dischi rigidi, lettori CD o dischi flessibili ("floppy disk"), né driver relativi a porte di comunicazione differenti dalla prima porta interna 10; in altre parole nella porzione 8a non sono presenti driver relativi a supporti di memorizzazione di tipo non volatile. Inoltre, il sistema operativo esterno OS2 è configurato per cancellare qualsiasi dato sia stato scritto in una qualsiasi memoria volatile di un generico calcolatore in cui il sistema operativo esterno OS2 stesso sia stato caricato, ogni qual volta si verifica una tra le seguenti condizioni di cancellazione: i) termine di una sessione (logout) durante l'esecuzione del sistema operativo esterno OS2 stesso, ii) spegnimento del generico calcolatore e iii) scollegamento del dispositivo elettronico mobile 1 dal generico calcolatore.

Per quanto concerne, invece, il modulo TPM 9, esso contiene quanto necessario per implementare una tecnica di crittografia asimmetrica (anche nota come crittografia/cifratura a chiave pubblica), e quindi una o più chiavi private relative a rispettivi uno o più utenti abilitati; ciascuna di tali chiavi private corrisponde (in modo di per sé noto) ad una rispettiva chiave pubblica, la quale è associata a un certificato digitale relativo al

rispettivo utente abilitato. Nel modulo TPM 9 possono inoltre essere memorizzate una o più impronte digitali (o, più precisamente, dati caratteristici relativi alle medesime) dei summenzionati utenti abilitati, il cui uso verrà chiarito in seguito. A titolo esemplificativo la memorizzazione di tali una o più impronte digitali può essere effettuata al primo utilizzo in assoluto del dispositivo elettronico portatile 1, oppure mediante una procedura di impostazione (eventualmente ripetibile) eseguita dal sistema operativo interno OS1.

Come mostrato ancora in figura 1, il dispositivo elettronico portatile 1 può essere collegato ad un calcolatore ospite 22, il quale può essere formato da un calcolatore da tavolo, da un calcolatore mobile, da un tablet-PC o da un qualsiasi apparecchio informatico, purché provvisto, oltre che di un rispettivo processore 23, di uno schermo 24, di una tastiera 26 e di un primo connettore di aggancio 28a adatto ad essere meccanicamente ed elettricamente accoppiato al primo connettore interno 10a, e collegato in modo di per sé noto ad una prima unità di controllo di aggancio 28b in maniera da formare una prima porta di aggancio 28. Ad esempio, nel caso in cui, come illustrato in figura 1, la prima porta interna 10 sia di tipo USB, anche la prima porta di aggancio 28 è di tipo USB. Sempre a titolo esemplificativo, ed in modo di per sé

Simone BONGIOVANNI
(Iscrizione Albo nr. 615/BM)

noto, in tale caso è inoltre possibile che la prima porta di aggancio 28 sia una porta USB di tipo master, e che la prima porta interna 10 sia una porta USB di tipo slave; in tal modo, il dispositivo elettronico portatile 1 può essere alimentato dal calcolatore ospite 22.

Tipicamente, oltre ad opportuni bus di collegamento (non mostrati), il calcolatore ospite 22 comprende inoltre almeno un disco rigido 29 ("hard-disk") di tipo non volatile, e una rispettiva memoria volatile, alla quale ci si riferisce in seguito come alla memoria volatile esterna 30. Inoltre, il calcolatore ospite 22 comprende generalmente una memoria non volatile dedicata (non mostrata), al cui interno è contenuto il cosiddetto "Basic Input-Output System" (BIOS), cioè una porzione di codice responsabile dell'esecuzione delle operazioni comprese tra l'accensione del calcolatore ospite 22 ed il caricamento di almeno un sistema operativo nella memoria volatile esterna 30. Queste fasi sono generalmente note, nel loro complesso, come "boot" o "bootstrap", e tipicamente si concludono con il caricamento nella memoria volatile esterna 30 di un sistema operativo residente (solitamente memorizzato nel disco rigido 29 oppure in una rispettiva memoria non volatile dedicata), e nella successiva esecuzione di tale sistema operativo residente da parte del processore 23.

In modo di per sé noto, è possibile impostare il BIOS

Simone BONGIOVANNI
(Iscrizione Albo nr. 615/BM)

del calcolatore ospite 22 in modo che il bootstrap avvenga attraverso la prima porta di aggancio 28, e che avvenga in maniera tale da caricare nella memoria volatile esterna 30 il sistema operativo esterno OS2 contenuto nella memoria non volatile interna 8 del dispositivo elettronico portatile 1, dunque un sistema operativo certificato.

In pratica, come precedentemente accennato, il sistema operativo esterno OS2 è configurato in maniera tale per cui, quando eseguito dal processore 23, non può caricare nella memoria volatile esterna 30 alcun altro driver al di fuori dei driver esterni, memorizzati nella prima porzione 8a della memoria non volatile interna 8. Inoltre, come detto in precedenza, il sistema operativo esterno OS2 è configurato per cancellare, ogni qual volta si verifica una delle summenzionate condizioni di spegnimento i-iii), qualsiasi dato sia stato scritto nella memoria volatile esterna 30 (oppure in eventuali ulteriori memorie volatili del calcolatore ospite 22).

In tal modo, il possessore del dispositivo elettronico portatile 1, previa verifica (descritta in seguito) del fatto che egli sia effettivamente uno dei summenzionati utenti abilitati, può disporre delle risorse hardware del calcolatore ospite 22, senza però poter accedere ai dati ivi contenuti, in particolare i dati contenuti nel disco rigido 29. Tuttavia, mediante la tastiera 26 e lo schermo

Simone BONGIOVANNI
(Iscrizione Albo nr. 615/BM)

24, il summenzionato possessore può modificare/visualizzare i dati utente presenti nella prima porzione 8a della memoria non volatile 8 del dispositivo elettronico portatile 1, la quale è vista dal sistema operativo esterno OS2 come una generica unità di supporto di memorizzazione, quando la prima porta interna 10 e la prima porta di aggancio 28 sono tra loro connesse.

In dettaglio, quando eseguito, il sistema operativo interno OS1 ed il sistema operativo esterno OS2 cooperano in modo che il sistema operativo esterno OS2 veda la prima porzione 8a della memoria non volatile interna 8 come risorsa accessibile al sistema operativo esterno OS2 stesso, cioè come una comune chiavetta di memoria di tipo USB. Inoltre, il sistema operativo interno OS1 ed il sistema operativo esterno OS2 cooperano in modo che la seconda porzione 8b della memoria non volatile interna 8 non sia accessibile al sistema operativo esterno OS2, e dunque calcolatore ospite 22. Ad esempio, è possibile che il sistema operativo interno OS1 notifichi al sistema operativo esterno OS la presenza della sola prima porzione 8a della memoria non volatile interna 8.

In pratica, la prima porzione 8a della memoria non volatile interna 8 funge sia da prima chiavetta di memoria di tipo USB in cui è memorizzato il sistema operativo esterno OS2, sia da seconda chiavetta di memoria di tipo

Simone BONGIOVANNI
(Iscrizione Albo nr. 615/BM)

USB in cui sono memorizzati i dati utente, accessibili al sistema operativo esterno OS2 quando eseguito dal calcolatore ospite 22. In particolare, il sistema operativo esterno OS2 può identificare le summenzionate prima e seconda chiavetta di memoria di tipo USB come una singola unità logica, oppure come due o più unità logiche distinte.

Nel caso in cui il sistema operativo esterno OS2 sia configurato per identificare le summenzionate prima e seconda chiavetta di memoria di tipo USB come due unità logiche distinte, esso è inoltre configurato in modo che l'unità logica in cui è memorizzato il sistema operativo esterno OS2 stesso non sia modificabile da chi utilizza il calcolatore ospite 22, cioè sia montata in modalità di sola lettura ("mounted read only"). Inoltre, in tale caso il sistema operativo esterno OS2 è configurato in modo che l'unità logica in cui sono memorizzati i dati utente risulti accessibile a chi utilizza il calcolatore ospite 22, cioè sia montata in modalità di lettura e scrittura ("mounted read and write").

Sulle base di quanto descritto, ne consegue che l'utilizzo del calcolatore ospite 22 da parte del summenzionato possessore risulta trasparente rispetto al calcolatore ospite 22 stesso. Inoltre, è possibile garantire che il summenzionato possessore del dispositivo elettronico portatile 1 sia effettivamente un utente

abilitato ad usare tale dispositivo elettronico portatile 1, e che quindi l'accesso ai dati utente presenti nella memoria non volatile interna 8 sia effettuato da parte di un utente abilitato.

In dettaglio, come precedentemente accennato, nel modulo TPM 9 è memorizzata almeno un'impronta digitale (o i parametri caratteristici di un'impronta digitale) di almeno un utente abilitato. Inoltre, dopo che il dispositivo elettronico portatile 1 viene collegato al calcolatore ospite 22, e dunque viene alimentato, il sistema operativo interno OS1 viene caricato nella memoria volatile interna 6 ed eseguito dall'unità di elaborazione interna 4. Successivamente, il sistema operativo interno OS1, che durante la fase di caricamento del sistema operativo interno OS1 comanda l'indicatore luminoso 17 in modo da notificare lo stato di accensione, notifica al possessore del dispositivo elettronico portatile 1 che il dispositivo elettronico portatile 1 si trova nello stato di richiesta di autenticazione, sempre mediante l'indicatore luminoso 17.

In seguito alla segnalazione dello stato di richiesta di autenticazione, il possessore del dispositivo elettronico portatile 1 può interagire in modo di per sé noto con il dispositivo di riconoscimento di impronta 18, in modo che esso acquisisca un'impronta digitale relativa

Simone BONGIOVANNI
(Iscrizione Albo nr. 615/BM)

al possessore del dispositivo elettronico portatile 1.

Successivamente, il modulo TPM 9, l'unità di elaborazione interna 4 e il dispositivo di riconoscimento di impronta 18 cooperano per verificare che l'impronta digitale acquisita dal dispositivo di riconoscimento di impronta 18 e relativa al possessore del dispositivo elettronico portatile 1 sia uguale ad almeno una delle impronte digitali memorizzate nel modulo TPM 9.

Qualora vi sia coincidenza tra l'impronta digitale acquisita e almeno una impronta digitale memorizzata, significa che il possessore del dispositivo elettronico portatile è effettivamente uno dei summenzionati utenti abilitati. Pertanto, il sistema operativo interno OS1, eventualmente mediante un'opportuna applicazione, trasmette al calcolatore ospite 22 il sistema operativo esterno OS2, attraverso la prima porta interna 10, consentendo dunque il completamento del "bootstrap" nel calcolatore ospite 22.

Viceversa, il sistema operativo interno OS1 comanda l'indicatore luminoso 17 in modo da notificare lo stato di errore. Inoltre, il sistema operativo interno OS1 controlla la prima unità di controllo interna 10b in modo che, conformemente al protocollo USB, la prima porta 10 risulti in stato di attesa, perciò il "bootstrap" non può essere completato, e quindi il sistema operativo esterno OS2 non viene caricato nel calcolatore ospite 22. Alternativamente,

Simone BONGIOVANNI
(Iscrizione Albo nr. 615/BM)

il sistema operativo interno OS1 trasmette effettivamente il sistema operativo esterno OS2, ma in maniera tale per cui, a bootstrap ultimato, il sistema operativo esterno OS2 resti in attesa dell'inserimento di una password. In altre parole, nel caso in cui non sia acquisita alcuna impronta digitale, oppure l'impronta digitale acquisita non coincida con alcune delle impronte digitali memorizzate, il calcolatore ospite 22 risulta inutilizzabile, e quindi anche i dati utente presenti nella memoria non volatile interna 8 risultano inaccessibili. Invece, nel caso in cui il possessore del dispositivo elettronico portatile 1 sia effettivamente un utente abilitato, egli può impiegare il calcolatore ospite 22 per modificare/visualizzare i dati utente eventualmente presenti nella prima porzione 8a della memoria non volatile interna 8, come precedentemente descritto.

Nel seguito ci si riferisce all'utente autorizzato per indicare l'utente abilitato la cui impronta digitale memorizzata coincide con l'impronta digitale acquisita. Nel caso in cui le operazioni precedentemente descritte si concludano positivamente, il possessore del dispositivo elettronico portatile 1 è in effetti l'utente autorizzato; pertanto, per motivi di brevità e di semplicità, nel seguito ci si riferisce all'utente autorizzato per indicare il possessore del dispositivo elettronico portatile 1.

Nuovamente con riferimento al dispositivo elettronico portatile 1, il sistema operativo interno OS1 coopera con il sistema operativo esterno OS2 in maniera tale per cui il sistema operativo esterno OS2 rilevi almeno una porta di comunicazione virtuale, attraverso la quale chi utilizza il calcolatore ospite 22 può comunicare con il mondo esterno, ad esempio con un gateway aziendale. In pratica, il dispositivo elettronico portatile 1 consente di stabilire almeno un primo canale di comunicazione tra il calcolatore ospite 22 ed il mondo esterno.

In dettaglio, attraverso la prima porta esterna 14, è possibile collegare il dispositivo elettronico portatile 1 ad una scheda di comunicazione 40 di tipo noto, ad esempio formata da una scheda Wi-fi, GSM/GPRS/HSDPA o similari. Come mostrato a titolo esemplificativo in figura 1, la prima porta esterna 14 può essere una porta USB di tipo master, e la scheda di comunicazione 40 può comprendere un circuito integrato 42 e una porta di scheda 44 accoppiabile meccanicamente ed elettricamente alla prima porta esterna 14, nonché elettricamente collegata al circuito integrato 42. Ad esempio, la porta di scheda 44 può essere formata da una porta USB di tipo slave. Inoltre, la scheda di comunicazione 40 può comprendere un apparato di comunicazione wireless 46, anch'esso collegato al circuito integrato 42.

Simone BONGIOVANNI
(Iscrizione Albo nr. 615/BM)

In pratica, nel caso in cui l'utente autorizzato voglia trasmettere al mondo esterno dei dati, ai quali ci si riferisce in seguito come alle informazioni utente (ad esempio, un sottoinsieme dei dati utente), il sistema operativo esterno OS2 può eseguire una prima applicazione e comunicare con una seconda applicazione eseguita dal sistema operativo interno OS1. Ad esempio, tale comunicazione può avvenire, in modo di per sé noto, mediante impiego di un primo indirizzo IP univocamente assegnato al dispositivo elettronico portatile 1 e noto agli utenti abilitati, in maniera tale per cui l'utente autorizzato può impostare tale primo indirizzo IP nella prima applicazione, la quale può essere analoga ad una comune applicazione di tipo "web browser", la seconda applicazione potendo invece essere del tipo "web server".

In dettaglio, la seconda applicazione notifica alla prima applicazione la presenza di uno o più canali di comunicazione, rilevati dal sistema operativo interno OS1 come descritto in seguito.

A tal proposito, si anticipa che, come mostrato in figura 2, il dispositivo elettronico portatile 1 può disporre, oltre che della prima porta esterna 14, di almeno una seconda porta esterna 50, formata da un secondo connettore esterno 50a e da una rispettiva seconda unità di controllo esterna 50b collegata al secondo connettore

esterno 50a ed al bus di collegamento 20. In particolare, nella forma di realizzazione mostrata a titolo esemplificativo in figura 2, la seconda porta esterna 50 è formata da una porta di tipo "Registered Jack 45" (RJ45), e dunque la seconda unità di controllo esterna 50b è una scheda di rete cablata; inoltre, la seconda porta esterna 50 è in grado di accoppiarsi in modo cablato ad un dispositivo di rete quale, ad esempio, un router, uno switch o un hub. Nel seguito della presente descrizione si assume per semplicità che, salvo laddove diversamente specificato, la prima e la seconda porta esterna 14, 50 siano appunto di tipo, rispettivamente, USB e RJ45. Inoltre ci si riferisce alle porte di collegamento esterno per indicare in generale la prima porta esterna 14, la seconda porta esterna 50 (se presente) ed eventuali ulteriori porte che hanno la funzione di consentire il collegamento del dispositivo elettronico portatile 1 con dispositivi elettronici ulteriori rispetto al calcolatore ospite 22.

Per rilevare i summenzionati uno o più canali di comunicazione, prima di eseguire la summenzionata seconda applicazione (ad esempio, non appena il dispositivo elettronico portatile 1 viene alimentato, oppure dopo l'inizio dell'esecuzione della prima applicazione), il sistema operativo interno OS1 seleziona ciascuna porta di collegamento esterno e verifica se è presente un

corrispondente canale di comunicazione, cioè verifica se la porta di collegamento selezionata è effettivamente collegata ad un rispettivo dispositivo di rete. Inoltre, il sistema operativo interno OS1 determina le caratteristiche di ciascun canale di comunicazione (canale Wi-fi, canale cablato, ecc.) ed associa ciascun canale di comunicazione alla rispettiva porta di collegamento esterno.

Ad esempio, relativamente alla prima porta esterna 14, il sistema operativo interno OS1 verifica se essa è effettivamente collegata alla scheda di comunicazione 40. Inoltre, assumendo che la scheda di comunicazione 40 sia di tipo Wi-fi, il sistema operativo OS1 rileva la presenza di un canale di comunicazione di tipo Wi-fi e associa tale canale di comunicazione di tipo Wi-fi alla prima porta esterna 14. Analogamente, nel caso della seconda porta esterna 50 (se presente), il sistema operativo interno OS1 verifica se essa è effettivamente collegata a un router o a un dispositivo analogo, nel qual caso rileva la presenza di un canale di comunicazione di tipo cablato, associato alla seconda porta esterna 50.

La seconda applicazione notifica quindi alla prima applicazione la presenza dei canali di comunicazione rilevati dal sistema operativo interno OS1. La prima applicazione è quindi in grado di visualizzare sullo schermo 24 i canali di comunicazione rilevati.

Mediante cooperazione tra la prima e la seconda applicazione, l'utente autorizzato può quindi selezionare un canale di comunicazione tra i canali di comunicazione rilevati dal sistema operativo interno OS1. Dal punto di vista del sistema operativo interno OS1, la selezione da parte dell'utente autorizzato di uno dei canali di comunicazione rilevati implica la selezione della porta di collegamento esterno associata al canale di comunicazione selezionato, alla quale ci si riferisce in seguito come alla porta esterna selezionata. Eventualmente, più canali di comunicazione possono essere selezionati dall'utente autorizzato, sebbene nel seguito si faccia riferimento per semplicità al caso in cui l'utente autorizzato possa selezionare un solo canale di comunicazione.

Ai fini pratici, la porta esterna selezionata rappresenta, per il sistema operativo esterno OS2, la summenzionata porta di comunicazione virtuale. Tale porta di comunicazione virtuale consente al calcolatore ospite 22 di comunicare, attraverso il dispositivo elettronico portatile 1, con il mondo esterno, ad esempio con un calcolatore destinazione 54 collegato al dispositivo elettronico portatile 1 mediante interposizione di una generica rete di collegamento 56. In particolare, la rete di collegamento 56 può essere collegata alla scheda di comunicazione 40, e dunque alla prima porta esterna 14,

come mostrato a titolo esemplificativo in figura 2; in particolare, in tale caso la rete di collegamento 56 è collegata in modo wireless all'apparato di comunicazione wireless 46 della scheda di comunicazione 40. Considerazioni analoghe possono tuttavia essere fatte qualora la rete di collegamento 56 si connetta al dispositivo elettronico portatile 1 attraverso la seconda porta esterna 50.

In maggior dettaglio, mediante cooperazione tra la prima e la seconda applicazione, l'utente autorizzato può inoltre comunicare al sistema operativo interno OS1 eventuali parametri tecnici e/o di accesso utili a configurare la porta esterna selezionata. Tali parametri tecnici e/o di accesso possono comprendere seconde credenziali (ad esempio un'ulteriore coppia di username e password), nel caso in cui il canale di comunicazione selezionato sia di tipo wireless, oppure, nel caso in cui il canale di comunicazione selezionato sia di tipo cablato, un secondo indirizzo IP dinamico o statico (ad esempio, relativo alla seconda porta esterna 50), nonché gli indirizzi IP di un rispettivo gateway e di un rispettivo sistema di nomi di dominio ("Domain Name System", DNS).

In particolare, per quanto concerne le seconde credenziali, le quali possono essere differenti dalle summenzionate prime credenziali, è possibile che esse siano

richieste all'utente autorizzato, ad esempio per consentire l'accesso del dispositivo elettronico portatile 1 alla rete di comunicazione 56 attraverso la porta esterna selezionata; ad esempio, tali seconde credenziali possono essere richieste per consentire il collegamento della scheda di comunicazione 40 con un gateway pubblico (non mostrato) della rete di comunicazione 56. In tal caso, come precedentemente accennato, mediante cooperazione tra la prima e la seconda applicazione, l'utente autorizzato può comunicare tali seconde credenziali al sistema operativo interno OS1, ad esempio al momento della selezione della porta di comunicazione. Tali seconde credenziali possono essere temporaneamente memorizzate nella memoria volatile esterna 30 del calcolatore ospite 22 e/o nella prima porzione 8a della memoria non volatile interna 8 del dispositivo elettronico portatile 1.

Successivamente, il sistema operativo interno OS1 imposta/trasmette tali eventuali parametri tecnici e/o di accesso comunicati dall'utente autorizzato, configurando la porta esterna selezionata, in maniera tale per cui la porta esterna selezionata è pronta per trasmettere.

In seguito, la prima applicazione trasmette alla seconda applicazione le summenzionate informazioni utente, le quali possono essere memorizzate nella memoria volatile esterna 30 del calcolatore ospite 22 e/o nella prima

Simone BONGIOVANNI
(Iscrizione Albo nr. 615/BM)

porzione 8a della memoria non volatile interna 8 del dispositivo elettronico portatile 1. In modo di per sé noto e pertanto non descritto, ulteriori applicazioni possono essere coinvolte durante le operazioni di determinazione/trasmissione delle informazioni utente.

Successivamente, il sistema operativo interno OS1, tipicamente mediante esecuzione di una terza applicazione, si fa carico di trasmettere le informazioni utente alla porta esterna selezionata, eventualmente previa operazione di crittografia, da cui sono poi trasmesse verso il mondo esterno.

Indipendentemente dal tipo di canale di comunicazione selezionato dall'utente autorizzato, e quindi dal tipo di porta esterna selezionata, il sistema operativo interno OS1 del dispositivo elettronico portatile 1 provvede a fornire, se richiesto dal calcolatore destinazione 54, le prime credenziali relative all'utente autorizzato e memorizzate nella seconda porzione 8b, nonché ad instaurare una cosiddetta rete privata virtuale ("virtual private network", VPN) di tipo sicuro (ad esempio, una rete VPN cosiddetta IPsec) con il calcolatore destinazione 54, utilizzando (per autenticarsi) in modo di per sé noto la chiave privata dell'utente autorizzato contenuta nel modulo TPM 9 e la corrispondente chiave pubblica, la quale per definizione è appunto pubblica.

Ad esempio, per instaurare la rete VPN, il sistema operativo OS1 può generare in modo pseudocasuale una chiave di sessione, cifrarla con la chiave pubblica che corrisponde al calcolatore destinazione 54 ed inviare al calcolatore destinazione 54 l'esito della cifratura. Successive trasmissioni tra il dispositivo elettronico portatile 1 ed il calcolatore destinazione 54 vengono quindi cifrate sulla base della chiave di sessione. Il sistema operativo interno OS1 può comunque implementare tecniche di crittografia differenti da quanto descritto.

In pratica, la sicurezza delle comunicazioni presenta caratteristiche di possibilità di identificazione, autenticazione, confidenzialità (grazie alla VPN) ed integrità dei dati, quest'ultima caratteristica essendo ottenibile mediante impiego, ad esempio, di codici di controllo di errore. Per quanto concerne invece l'identificazione, essa è relativa alla possibilità di identificare l'utente autorizzato da parte del calcolatore destinazione 54. A tal fine, il dispositivo elettronico portatile 1 può ad esempio criptare le informazioni utente con la chiave privata dell'utente autorizzato, ed inviarle al calcolatore destinazione 54 insieme a dati relativi all'utente autorizzato (ad esempio, nome e cognome), in maniera tale per cui il calcolatore destinazione 54, previo ottenimento (ad esempio, da una autorità di certificazione)

della corrispondente chiave pubblica relativa all'utente autorizzato, possa decifrare le informazioni ricevute, impiegando la chiave pubblica ottenuta, e verificando quindi l'identità dell'utente autorizzato. L'autenticazione deriva invece dalla possibilità di implementare regole di accesso, ad esempio nel calcolatore destinazione 54, sulla base dell'identificazione.

Infine, qualora non sia disponibile alcun canale di comunicazione, è possibile collegare la prima porta esterna 14, ad una scheda di memoria (non mostrata) nella quale l'utente autorizzato può memorizzare le informazioni utente, ad esempio comandando il sistema operativo esterno OS2 in modo che controlli il sistema operativo interno OS1 in maniera tale per cui il sistema operativo interno OS1 memorizzi, eventualmente in modo cifrato, le informazioni utente nella scheda di memoria collegata. Ad esempio, la cifratura può avvenire sulla base di una chiave pubblica corrispondente ad un utilizzatore, il quale sarà il solo a poter accedere alle informazioni utente così cifrate.

Sulla base di quanto descritto, si desume che le comunicazioni tra l'utente autorizzato ed il mondo esterno sono effettuate unicamente attraverso le comunicazioni tra il dispositivo elettronico portatile 1 ed il mondo esterno, le quali sono gestite interamente dal sistema operativo interno OS1. Questo comporta che le prime credenziali

memorizzate nella porzione 8b della memoria non volatile interna 8, gli algoritmi di crittografia ed eventuali codici di sicurezza (ad esempio, la summenzionata chiave di sessione) rimangano all'interno del dispositivo elettronico portatile 1, siano elaborati dal sistema operativo interno OS1 e non siamo mai trasmessi al calcolatore ospite 22.

Per quanto concerne, invece, lo scambio di dati tra il calcolatore ospite 22 ed il dispositivo elettronico portatile 1, vi è cooperazione tra il sistema operativo interno OS1 ed il sistema operativo esterno OS2. A tal proposito, si noti che, come mostrato a titolo esemplificativo in figura 2, il dispositivo elettronico portatile 1 può comprendere una seconda porta interna 60 formata da un secondo connettore interno 60a e da una seconda unità di controllo interno 60b. In particolare, la seconda unità di controllo interno 60b è collegata al secondo connettore interno 60a ed al bus di collegamento 20. In dettaglio, nella forma di realizzazione mostrata in figura 2, la seconda porta interna 60 è di tipo RJ45. In tal modo, assumendo che il calcolatore ospite 22 disponga di una seconda porta di aggancio 62 compatibile con la seconda porta interna 60 (e collegata ai rimanenti componenti del calcolatore ospite 22 in modo di per sé noto), è possibile stabilire un ulteriore collegamento tra il dispositivo elettronico portatile 1 ed il calcolatore

ospite 22. A tal fine, nella porzione 8a della memoria non volatile 8 è presente almeno un driver relativo a porte di comunicazione del tipo della seconda porta interna 60.

Operativamente, e con riferimento ancora alla forma di realizzazione mostrata in figura 2, è dunque possibile alimentare il dispositivo elettronico portatile 1 mediante il collegamento presente tra la prima porta interna 10 e la prima porta di aggancio 28, utilizzando invece il collegamento presente tra la seconda porta interna 60 e la seconda porta di aggancio 62 per scambiare dati tra il calcolatore ospite 22 ed il dispositivo elettronico portatile 1.

Sono comunque possibili altre forme di realizzazione in cui, ad esempio, anche la seconda porta esterna 50 è di tipo USB, in maniera tale per cui può essere collegata ad una scheda di comunicazione addizionale (non mostrata) differente dalla scheda di comunicazione 40 ed utilizzabile dall'utente autorizzato per effettuare connessioni con il mondo esterno. E' inoltre possibile realizzare il dispositivo elettronico portatile 1 in modo che integri al proprio interno anche le funzioni radio tradizionalmente assolte dalla scheda di comunicazione 40 (o similari).

I vantaggi che il presente dispositivo elettronico portatile consente di ottenere emergono chiaramente dalla discussione precedente. In particolare, il presente il

presente dispositivo elettronico portatile consente di disporre in ogni momento di dati, senza gli ingombri ed i pesi tipici dei calcolatori portatili (soprattutto per quanto concerne lo schermo e la tastiera), grazie alla possibilità di avvalersi in modo sicuro di componenti hardware di calcolatori messi a disposizione da terzi. In particolare, l'utilizzo di tali calcolatori messi a disposizione da terzi avviene senza lasciare traccia alcuna di tale utilizzo all'interno dei calcolatori medesimi, e senza pericolo per i dati contenuti nel dispositivo elettronico portatile.

Ancora, il presente dispositivo elettronico mobile consente di comunicare in modo sicuro con un eventuale calcolatore esterno, quale ad esempio un "gateway" aziendale, senza che il calcolatore ospite debba generare in modo pseudocasuale un codice da utilizzare per la criptatura, ed evitando dunque il rischio che tale codice generato in modo pseudocasuale resti in qualche modo memorizzato all'interno del calcolatore ospite e sia recuperato da qualche altro utente del calcolatore ospite.

Risulta infine evidente che al dispositivo elettronico portatile descritto possono essere apportate modifiche e varianti, senza uscire dall'ambito della presente invenzione.

Ad esempio, il dispositivo elettronico mobile 1 può

comprendere, oltre alla memoria non volatile interna 8, almeno una memoria non volatile addizionale, nel qual caso è possibile memorizzare il sistema operativo interno OS1 e il sistema operativo esterno OS2 rispettivamente all'interno della memoria non volatile interna 8 e della memoria non volatile addizionale (o viceversa), evitando di partizionare la memoria non volatile interna 8, come è invece opportuno fare nel caso in cui vi sia la sola memoria non volatile interna 8. La stessa memoria non volatile interna 8 può essere di tipo differente da quanto descritto. Ancora, per quanto concerne i driver esterni, è possibile memorizzare ulteriori driver rispetto a quanto descritto, quali ad esempio driver di stampanti, sebbene ciò possa comportare una riduzione della sicurezza complessiva. E' altresì possibile che alcune delle operazioni descritte siano effettuate da applicazioni eseguite dal sistema operativo interno OS1 o dal sistema operativo esterno OS2, invece che dal sistema operativo interno OS1 e dal sistema operativo esterno OS2 stessi, oppure che siano in tutto o in parte demandate a componenti del dispositivo elettronico portatile 1 (ad esempio, il modulo TPM 9).

Inoltre, insieme oppure in alternativa al modulo TPM 9, è possibile che sia presente un lettore di smart-card, con funzioni equivalenti. In tal caso, i driver interni

comprendono driver relativi al lettore di smart-card. Similmente, il dispositivo elettronico portatile 1 può essere provvisto di un lettore di etichetta di identificazione a radiofrequenza ("radio frequency identification tag", RFID), in maniera tale da poter interagire con dispositivi RFID e implementare funzioni di verifica di prossimità.

Ancora, in caso di forma di realizzazione provvista della seconda porta interna 60 di tipo RJ45, e nel caso in cui il BIOS del calcolatore ospite 22 lo consenta, è possibile effettuare il bootstrap del calcolatore ospite 22 attraverso tale seconda porta interna 60.

E' altresì possibile che il dispositivo mobile portatile 1 disponga di ulteriori porte rispetto a quanto descritto e mostrato, e che le summenzionate prima porta interna 10, prima porta esterna 14, seconda porta esterna 50 e seconda porta interna 60 siano di tipo differente rispetto a quanto descritto e mostrato.

Analogamente, è possibile che ci siano indicatori luminosi addizionali rispetto all'indicatore luminoso 17, e/o che il dispositivo elettronico portatile 1 disponga di dispositivi di segnalazione di tipo differente, quali ad esempio un proprio schermo di visualizzazione (non mostrato), oppure dispositivi di segnalazione acustica.

Per quanto concerne, invece, il dispositivo di

riconoscimento di impronta 18, esso può essere sostituito da un dispositivo di riconoscimento biometrico, cioè un dispositivo capace di rilevare dati relativi a caratteristiche biologiche (ad esempio, una retina) del possessore del dispositivo elettronico mobile 1. In tal caso, nel modulo TPM 9 sono quindi memorizzati dati biometrici relativi a tali caratteristiche biologiche.

Il dispositivo elettronico portatile 1 può inoltre essere equipaggiato in maniera tale da poter essere alimentato da un alimentatore esterno, così da poter operare anche in assenza di collegamento con il calcolatore ospite; inoltre il dispositivo elettronico portatile 1 può comprendere una rispettiva batteria (non mostrata).

Si noti inoltre che il presente dispositivo elettronico portatile 1 può essere collegato anche ad un calcolatore ospite privo di supporti di memorizzazione di tipo non volatile. Ad esempio, il calcolatore ospite può essere privo di disco rigido, nel qual caso non vi è comunque pericolo che l'utente autorizzato acceda ad informazioni riservate al proprietario del calcolatore ospite. In pratica, anche nel caso in cui il calcolatore ospite risulti privo del proprio sistema operativo residente, il presente dispositivo elettronico portatile 1 ne consente un opportuno utilizzo.

Infine, si noti che tra il calcolatore destinazione 54

e la rete di collegamento 56 può essere interposto un gateway (non mostrato), quale ad esempio un gateway aziendale, nel qual caso può essere tale gateway aziendale a richiedere al dispositivo elettronico portatile 1 le prime credenziali relative all'utente autorizzato e memorizzate nella seconda porzione 8b. Inoltre, in tale caso, il dispositivo elettronico portatile 1 può instaurare la rete privata virtuale con tale gateway aziendale, in modo analogo a quanto precedentemente descritto relativamente al calcolatore destinazione 54.

Simone BONGIOVANNI
(Iscrizione Albo nr. 615/BM)

RIVENDICAZIONI

1. Dispositivo elettronico portatile comprendente:

- primi mezzi di memorizzazione (8) di tipo non volatile, in cui sono memorizzati un primo ed un secondo sistema operativo (OS1,OS2);

- secondi mezzi di memorizzazione (6) di tipo volatile;

- una prima unità di elaborazione (4) collegata a detti primi e secondi mezzi di memorizzazione (8,6) e configurata per eseguire detto primo sistema operativo (OS1), detto primo sistema operativo (OS1) essendo configurato per controllare detto dispositivo elettronico portatile;

- una prima porta interna (10) collegata a detti primi mezzi di memorizzazione (8) e configurata per essere collegata ad una prima porta di connessione (28) di un primo sistema informatico (22) provvisto di una memoria di sistema (30) di tipo volatile, di una seconda unità di elaborazione (23) e di un supporto di memorizzazione (29) di tipo non volatile;

caratterizzato dal fatto che detto secondo sistema operativo (OS2) è configurato in maniera tale per cui, quando, previo collegamento di detta prima porta interna (10) con detta prima porta di connessione (28), viene caricato in detta memoria di sistema (30) ed eseguito da

Simone BONGIOVANNI
(Iscrizione Albo nr. 615/BM)

detta seconda unità di elaborazione (23), previene l'accesso da parte di un utente del primo sistema informatico (22) a detto supporto di memorizzazione (29).

2. Dispositivo secondo la rivendicazione 1, in cui detti primi mezzi di memorizzazione (8) contengono una prima pluralità di driver, detto secondo sistema operativo (OS2) essendo configurato per prevenire, quando eseguito da detta seconda unità di elaborazione (23), il caricamento in detta memoria di sistema (30) di driver differenti da detta prima pluralità di driver.

3. Dispositivo secondo la rivendicazione 2, in cui detta prima pluralità di driver non comprende driver relativi a dischi rigidi, dischi flessibili e lettori CD.

4. Dispositivo secondo una qualsiasi delle rivendicazioni precedenti, in cui detto secondo sistema operativo (OS2) è configurato in maniera tale da cancellare detta memoria di sistema (30) in caso di:

- scollegamento di detta prima porta interna (10) da detta prima porta di connessione (28); o

- termine di una sessione ("logout") durante l'esecuzione di detto secondo sistema operativo (OS2).

5. Dispositivo secondo una qualsiasi delle rivendicazioni precedenti, in cui detti primi mezzi di memorizzazione (8) comprendono una prima ed una seconda porzione di memoria (8a,8b), detto primo sistema operativo

Simone BONGIOVANNI
(Iscrizione Albo nr. 615/BM)

(OS1) essendo memorizzato in detta seconda porzione di memoria (8b), detto secondo sistema operativo (OS2) essendo memorizzato in detta prima porzione di memoria (8a).

6. Dispositivo secondo la rivendicazione 5, in cui detti primo e secondo sistema operativo (OS1,OS2) sono configurati per cooperare, quando eseguiti rispettivamente da dette prima e seconda unità di elaborazione (4,23), in maniera tale per cui detta prima porzione di memoria (8a) sia accessibile a detto secondo sistema operativo (OS2).

7. Dispositivo secondo la rivendicazione 6, in cui detti primo e secondo sistema operativo (OS1,OS2) sono configurati per cooperare, quando eseguiti rispettivamente da dette prima e seconda unità di elaborazione (4,23), in maniera tale per cui detta seconda porzione di memoria (8b) sia inaccessibile a detto secondo sistema operativo (OS2).

8. Dispositivo secondo una qualsiasi delle rivendicazioni precedenti, comprendente inoltre un modulo di sicurezza (9,18) in cui è memorizzato almeno un primo dato biometrico relativo a un utente abilitato, detto dispositivo comprendendo inoltre un sistema di riconoscimento biometrico (4,9,18) configurato per acquisire un secondo dato biometrico e confrontare detto secondo dato biometrico con detto primo dato biometrico.

9. Dispositivo secondo la rivendicazione 8, in cui detto sistema di riconoscimento biometrico (4,9,18)

comprende un'unità di riconoscimento di impronta digitale (18).

10. Dispositivo secondo la rivendicazione 8 o 9, in cui detto primo sistema operativo (OS1) è configurato per cooperare con detto sistema di riconoscimento biometrico (4,9,18) e, qualora detti primo e secondo dato biometrico siano differenti, eseguire almeno una tra le operazioni di:

- impostare detta prima porta interna (10) in uno stato di attesa, durante detto stato di attesa la prima porta interna (10) essendo inaccessibile al primo sistema informatico (22);

- modificare detto secondo sistema operativo (OS2) memorizzato in detti primi mezzi di memorizzazione (8) in maniera tale per cui detto secondo sistema operativo (OS2), quando caricato in detta memoria di sistema (30) attraverso detta prima porta interna (10) ed eseguito da detta seconda unità di elaborazione (23), richiede un'operazione di autenticazione.

11. Dispositivo secondo una qualsiasi delle rivendicazioni da 8 a 10, comprendente inoltre una prima porta esterna (14) configurata per essere collegata ad un secondo sistema informatico (54) definendo un canale di comunicazione, detti primo e secondo sistema operativo (OS1,OS2) essendo inoltre configurati per cooperare, quando eseguiti rispettivamente da dette prima e seconda unità di elaborazione (4,23), per selezionare e trasmettere primi dati attraverso detto canale di comunicazione, detti

primi dati essendo memorizzati alternativamente in detti primi mezzi di memorizzazione (8) o in detta memoria di sistema (30).

12. Dispositivo secondo la rivendicazione 11, in cui detto primo sistema operativo (OS1) è inoltre configurato per instaurare una rete privata virtuale con detto secondo sistema informatico (54), ed effettuare la trasmissione di detti primi dati attraverso detta rete privata virtuale.

13. Dispositivo secondo la rivendicazione 12, in cui in detto modulo di sicurezza (9,18) è inoltre memorizzata almeno una chiave crittografica relativa a detto utente abilitato, detto primo sistema operativo (OS1) essendo inoltre configurato per instaurare detta rete privata virtuale sulla base di detta chiave crittografica, e per prevenire l'accesso a detto modulo di sicurezza (9,18) da parte di detto secondo sistema operativo (OS2) quando detto secondo sistema operativo (OS2) è eseguito da detta seconda unità di elaborazione (23).

14. Dispositivo secondo una qualsiasi delle rivendicazioni da 11 a 13, in cui detto canale di comunicazione è almeno in parte di tipo wireless.

15. Dispositivo secondo una qualsiasi delle rivendicazioni da 8 a 14, in cui detto modulo di sicurezza comprende un modulo per una piattaforma fidata (9).

p.i.: ELSAG DATAMAT SPA

Simone BONGIOVANNI

Simone BONGIOVANNI
(Iscrizione Albo nr. 615/BM)

CLAIMS

1. A hand-held electronic device comprising:

- first non-volatile storing means (8), wherein a first and a second operating system (OS1, OS2) are stored;

- second volatile storing means (6);

- a first processing unit (4) connected to said first and second storing means (8, 6) and configured to run said first operating system (OS1), said first operating system (OS1) being configured to control said hand-held electronic device;

- a first internal port (10) connected to said first storing means (8) and configured to be connected to a first connection port (28) of a first computer system (22) provided with a volatile system memory (30), a second processing unit (23) and a non-volatile storing support (29);

characterised in that said second operating system (OS2) is configured so that, when loaded in said system memory (30) and run by said second processing unit (23) after said first internal port (10) has been connected to said first connection port (28), it prevents access by a user of the first computer system (22) to said storing support (29).

2. The device according to claim 1, wherein said first storing means (8) contain a first plurality of drivers,

Lorenzo NANNUCCI
(Iscrizione Albo nr. 1214/B)

said second operating system (OS2) being configured to prevent, when run by said second processing unit (23), the loading in said system memory (30) of drivers other than said first plurality of drivers.

3. The device according to claim 2, wherein said first plurality of drivers does not comprise drivers related to hard disks, floppy disks and CD players.

4. The device according to any of the preceding claims, wherein said second operating system (OS2) is configured so as to erase said system memory (30) in case of:

- disconnection of said first internal port (10) from said first connection port (28); or

- logout when said second operating system is running (OS2).

5. The device according to any of the preceding claims, wherein said first storing means (8) comprise a first and a second memory portion (8a, 8b), said first operating system (OS1) being stored in said second memory portion (8b), said second operating system (OS2) being stored in said first memory portion (8a).

6. The device according to claim 5, wherein said first and second operating systems (OS1, OS2) are configured to cooperate, when run respectively by said first and second

Lorenzo NANNUCCI
(Iscrizione Albo nr. 1214/B)

processing units (4, 23), so that said first memory portion (8a) is accessible to said second operating system (OS2).

7. The device according to claim 6, wherein said first and second operating systems (OS1, OS2) are configured to cooperate, when run respectively on said first and second processing units (4, 23), so that said second memory portion (8a) is non-accessible to said second operating system (OS2).

8. The device according to any of the preceding claims, further comprising a safety module (9, 18) in which at least a first biometric datum relating to an enabled user is stored, said device further comprising a biometric recognition system (4, 9, 18) configured to acquire a second biometric datum and compare said second biometric datum with said first biometric datum.

9. The device according to claim 8, wherein said biometric recognition system (4, 9, 18) comprises a fingerprint recognition unit (18).

10. The device according to claim 8 or 9, wherein said first operating system (OS1) is configured to cooperate with said biometric recognition system (4, 9, 18) and, when said first and second biometric data are different, carry out at least one of the operations of:

- setting said first internal port (10) in a standby condition, during said standby condition the first internal

Lorenzo NANNUCCI
(Iscrizione Albo nr. 1214/B)

port (10) being non-accessible to the first computer system (22);

- modifying said second operating system (OS2) stored in said first storing means (8) so that said second operating system (OS2) requires an authentication operation when loaded in said system memory (30) through said first internal port (10) and run by said second processing unit (23).

11. The device according to any of claims 8 to 10, further comprising a first external port (14) configured to be connected to a second computer system (54) defining a communication channel, said first and second operating systems (OS1,OS2) also being configured to cooperate, when run respectively by said first and second processing units (4, 23), to select and transmit first data through said communication channel, said first data being stored alternatively in said first storing means (8) or said system memory (30).

12. The device according to claim 11, wherein said first operating system (OS1) is also configured to establish a virtual private network with said second computer system (54), and perform the transmission of said first data through said virtual private network.

13. The device according to claim 12, wherein at least one cryptographic key relating to said enabled user is also stored in said safety module (9, 18), said first operating system (OS1) also

Lorenzo NANNUCCI
(Iscrizione Albo nr. 1214/B)

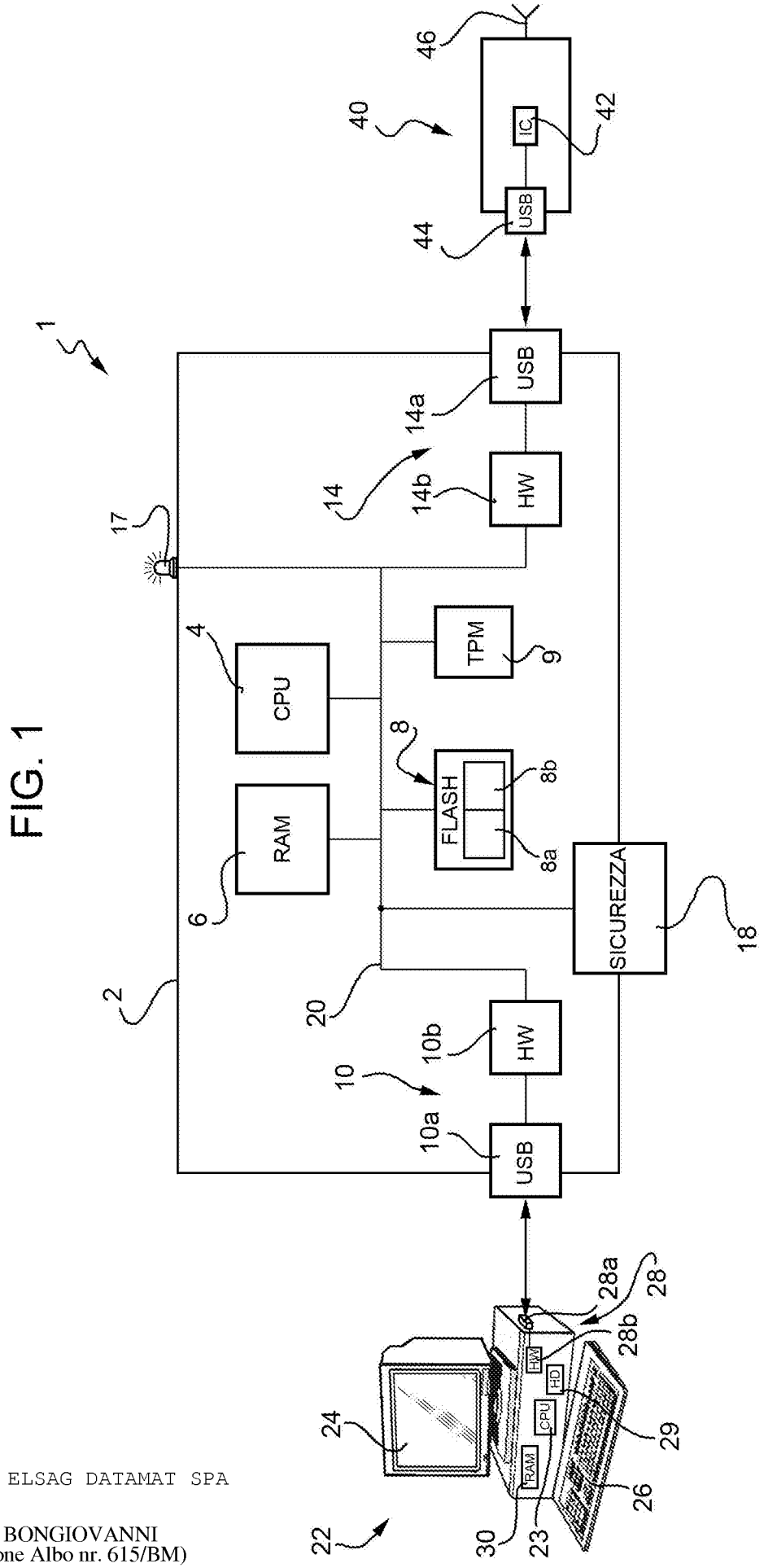
being configured to establish said virtual private network on the basis of said cryptographic key, and to prevent access to said safety module (9,18) by said second operating system (OS2) when said second operating system (OS2) is run by said second processing unit (23).

14. The device according to any of claims 11 to 13, wherein said communication channel is at least partially of the wireless type.

15. The device according to any of claims 8 to 14, wherein said safety module comprises a module for a trusted platform (9).

Lorenzo NANNUCCI
(Iscrizione Albo nr. 1214/B)

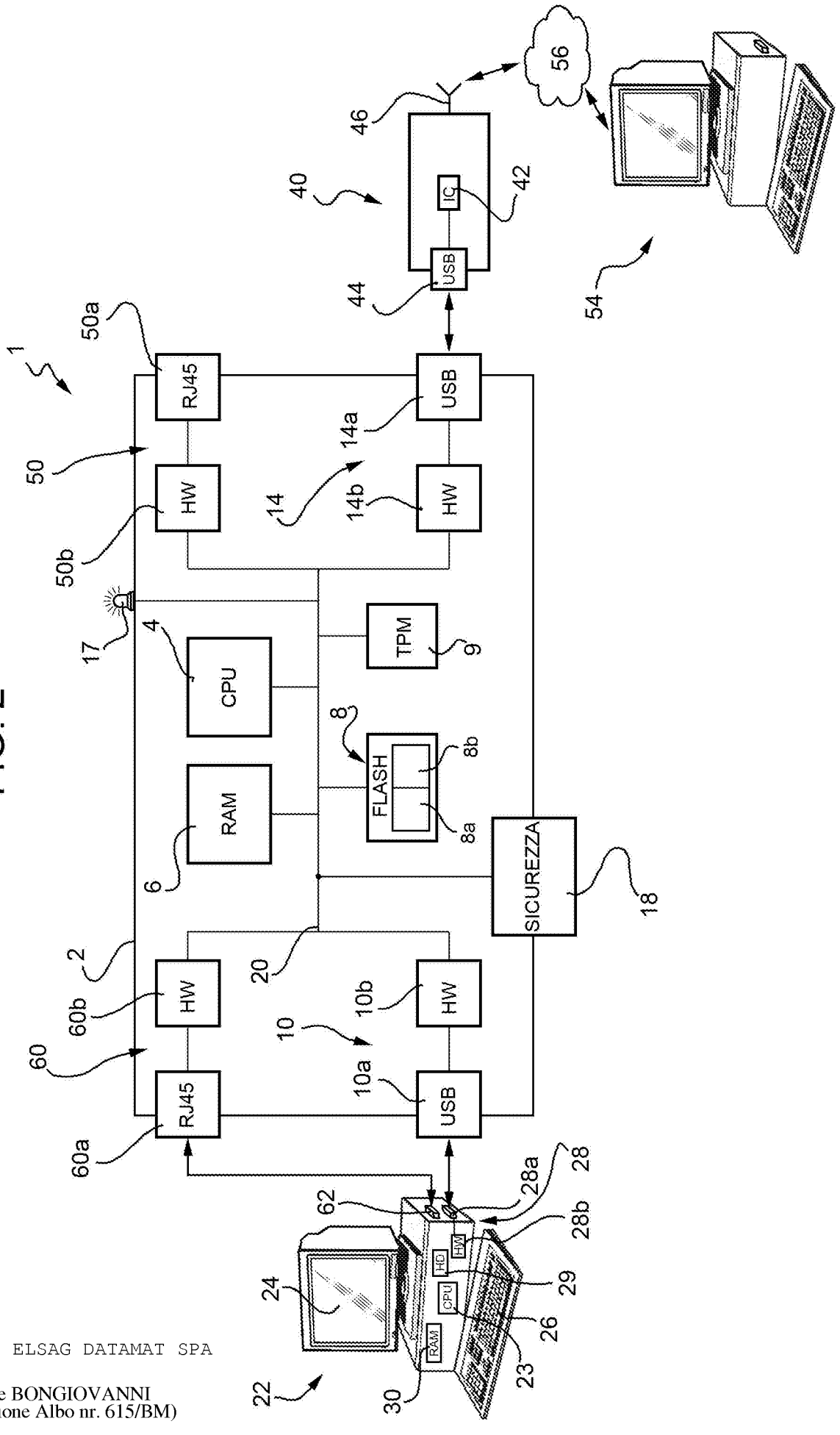
FIG. 1



p.i.: ELSAG DATAMAT SPA

Simone BONGIOVANNI
(Iscrizione Albo nr. 615/BM)

FIG. 2



p.i.: ELSAG DATAMAT SPA

Simone BONGIOVANNI
(Iscrizione Albo nr. 615/BM)