IBM Client Security Software
Versione 5.30 - Guida per la distribuzione

Terza edizione (Luglio 2004)

Prefazione

E' necessario che i responsabili IT comprendano e pianifichino i numerosi fattori relativi alla distribuzione dell'IBM Client Security Software. Questo manuale non intende spiegare il modo in cui utilizzare ESS (Embedded Security Subsystem). Chip o Client Security Software; è piuttosto una guida sulle modalità di distribuzione del software a computer dotati di Embedded Security Chip attraverso un impresa.

A chi è rivolto questo manuale

Questo manuale è rivolto ai responsabili IT o ai responsabili della distribuzione dell' IBM CSS (Client Security Software) versione 5.3 su computer nell'organizzazione. Questo manuale fornisce le informazioni richieste per l'installazione dell'IBM Client Security Software su uno o più computer. IBM fornisce una Guida per l'utente, una Guida per i responsabili di Client Security Software e guide alle applicazioni per Client Security Software, che è possibile consultare per le informazioni sull'utilizzo dell'applicazione stessa.

Pubblicazioni del prodotto

I seguenti documenti sono disponibili nella libreria di Client Security Software Versione 5.3:

- *Client Security Software Versione 5.3 - Guida per il responsabile* ,

  Fornisce le informazioni sull'impostazione e l'utilizzo delle funzioni di sicurezza fornite con Client Security Software.
- *Client Security Software Versione 5.3 - Guida per l'utente*,

  Contiene le informazioni sull'esecuzione delle attività di Client Security Software, come l'utilizzo della protezione per il collegamento UVM, l'impostazione dello screen saver di Client Security, la creazione di un certificato digitale e l'utilizzo di User Configuration Utility.
- *Client Security Software Versione 5.3 - Guida per l'installazione*,

  Contiene le informazioni sull'installazione di Client Security Software sui computer della rete IBM che contengono i chip dell'IBM Embedded Security.
- *Utilizzo di Client Security Software Versione 5.3 con Tivoli Access Manager*,

  Contiene informazioni di supporto sull'impostazione del programma Client Security Software da utilizzare con Tivoli Access Manager.

Ulteriori informazioni

E' possibile ottenere ulteriori informazioni e aggiornamenti del prodotto di sicurezza, se disponibili, dall'indirizzo http://www-132.ibm.com/content/search/security.html sul sito web dell'IBM.

Indice

Prefazione iii
A chi è rivolto questo manuale iii
Pubblicazioni del prodotto iii
Ulteriori informazioni iii

Capitolo 1. Considerazioni prima della distribuzione di IBM Client Security Software 1
Requisiti e specifiche per la distribuzione 1

Capitolo 2. ESC (Embedded Security Chip)- Istruzioni 3
Gerarchia di scambio-chiavi 5
Utilizzo scambio delle chiavi 6

Capitolo 3. Considerazioni sull'archiviazione chiave 7
Perché disporre di una coppia di chiavi del responsabile 10

Capitolo 4. IBM Client Security Software 21
Iscrizione utenti e gestione iscrizioni 21
Richiesta di un passphrase 22
Impostazione di un passphrase 22
Utilizzo di un passphrase. 23
Inizializzazione TPM 26
Prestazioni ottimali 27
Inizializzazione utente 28
Inizializzazione personale 29
Scenari di distribuzione 30
Installazione ed inizializzazione 35

Capitolo 5. Installazione del componente Client Security su un server Tivoli Access Manager 43
Prerequisiti 43
Scaricamento e installazione del componente Client Security 43
Aggiunta del componente Client Security sul server di Tivoli Access Manager 44
Stabilire una connessione protetta tra il client IBM e il server di Tivoli Access Manager 45
Configurazione dei client IBM 46
Prerequisiti 46
Configurazione delle informazioni di impostazione di Tivoli Access Manager 46
Impostazione ed uso della funzione di cache locale 47
Abilitazione di Access Manager per controllare gli oggetti del client IBM 48
Prospetti per la risoluzione dei problemi. 49
Informazioni sulla risoluzione dei problemi relativi al certificato digitale 49
Informazioni sulla risoluzione dei problemi di Tivoli Access Manager 50
Informazioni sulla risoluzione dei problemi relativi a Lotus Notes 50
Informazioni sulla risoluzione dei problemi relativi alla cifratura 51

Capitolo 6. Installazione driver di periferica hardware di terza parte complementari all'IBM Client Security Software 53

Capitolo 7. Distribuzione in remoto di file di politica della sicurezza nuovi o revisionati 55

Appendice. Informazioni particolari . . 57
Siti web diversi dall'IBM 58
Marchi 58

Capitolo 1. Considerazioni prima della distribuzione di IBM Client Security Software

Esistono varie modalità per distribuire IBM CSS (Client Security Software), che utilizza l'hardware IBM ESS (Embedded Security Subsystem) integrato nei PC IBM. Questo documento sarà di supporto per determinare la modalità di distribuzione di ESS nel proprio ambiente. E' importante guardare al modo i cui la società distribuisce i computer dalla creazione dell'immagine al modo in cui il PC viene dato ad un utente finale. Questo processo influenzerà molto il modo in cui la società distribuirà ESS. IBM ESS è composto essenzialmente di due parti come mostrato in Figura 1:

1. CSS (Client Security Software)
2. ESC (Embedded Security Chip)

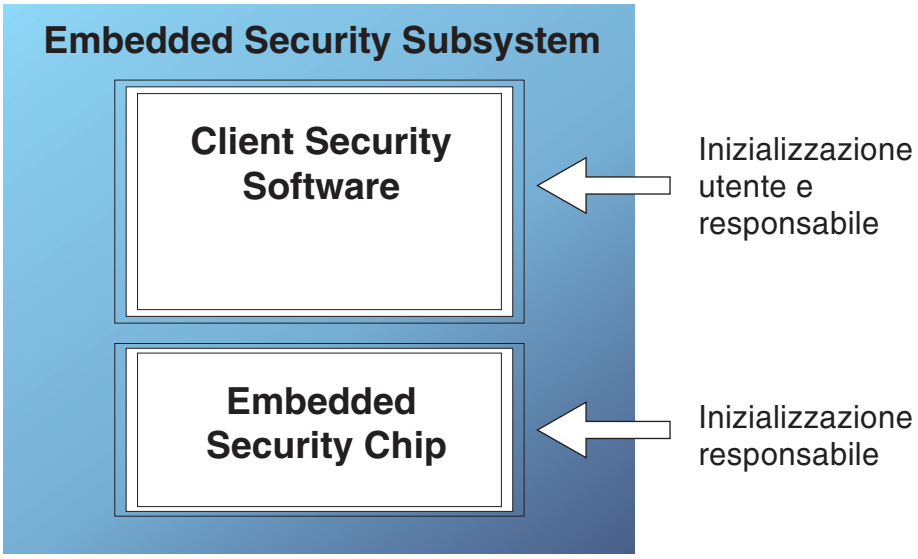

Figura 1. ComponentiIBM Client Security System

Requisiti e specifiche per la distribuzione

Se si pianifica di installare IBM Client Security Software su computer equipaggiati con il chip di Embedded Security, organizzare il piano sulla memoria server seguente e scaricare i requisiti ed i tempi d'installazione:

1. PCIBM con ESC (Embedded Security Chip)
2. Requisiti memoria server per codice installabile: approssimativamente 12 MB
3. Requisito di memorizzazione media server per utente per i dati archivio chiave: 200 KB per utente per memorizzazione archivio

Capitolo 2. ESC (Embedded Security Chip)- Istruzioni

L'ESC IBM è rappresentato graficamente in Figura 2. I componenti maggiori sono tre:

1. La password del responsabile
2. La chiave pubblica hardware
3. La chiave privata hardware

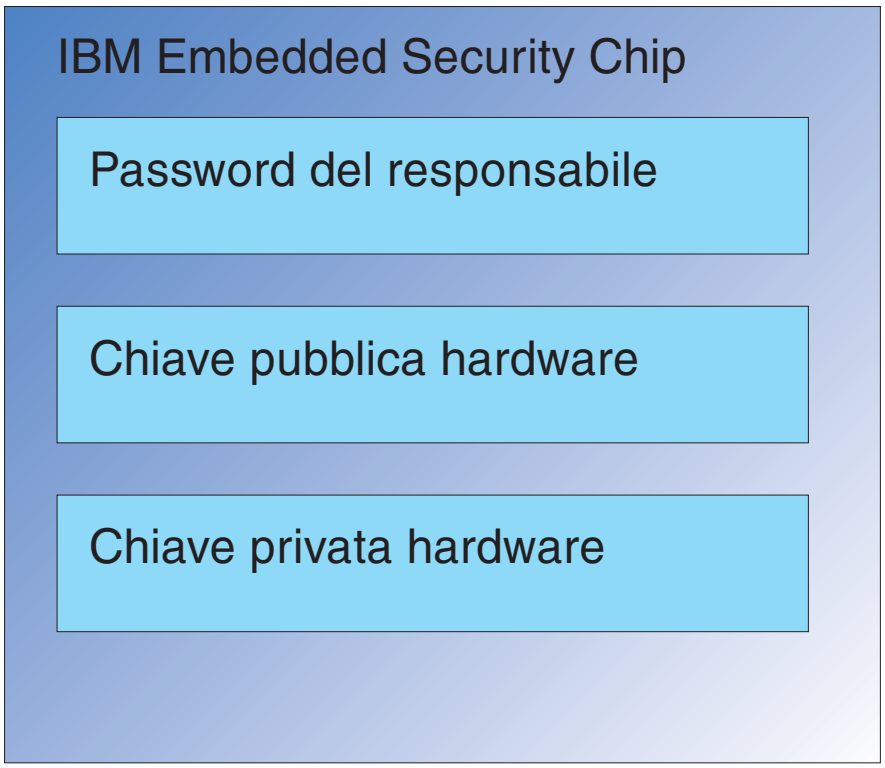

Figura 2. Dati contenuti nell'ESC (Embedded Security Chip)IBM

Le chiavi hardware pubblica e privata sono univoche su tutti i computer. Non è possibile estrarre dal chip la chiave privata hardware. E' possibile creare coppie di chiavi nuove nei modi seguenti:

- Mediante la procedura guidata all'installazione di Client Security Software
- Mediante il programma Administrator Utility
- Mediante gli script

E' bene notare che non è possibile estrarre le chiavi hardware dal chip.

Il responsabile utilizza la password del responsabile per accedere alle seguenti funzioni, che includono:

- Aggiunta utenti
- Impostazione politica di sicurezza
- Impostazione politica passphrase
- Iscrizione smartcard

- Iscrizione periferiche biometriche

Ad esempio, potrebbe essere necessario che un responsabile consenta ad un utente supplementare di trarre vantaggio dalle funzioni dell'ESC (Embedded Security Chip). La password del responsabile viene impostata al momento dell'installazione di Client Security Software. I dettagli riguardo le modalità di impostazione delle password del responsabile verranno esposti più avanti in questo documento.

Importante: Sviluppare una strategia per conservare le password del responsabile, da stabilire al momento della prima configurazione di ESS. E' possibile che ogni computer che disponga di un ESC (Embedded Security Chip) utilizzi la stessa password del responsabile se deciso dal responsabile IT o dal responsabile della sicurezza. In alternativa, è possibile assegnare ad ogni reparto o edificio diverse password del responsabile.

Gli altri componenti dell'ESCIBM sono la chiave pubblica hardware e la chiave privata hardware. Questa coppia di chiavi RSA viene generata al momento della configurazione di Client Security Software.

Ciascun computer disporrà di una chiave pubblica ed una chiave privata hardware univoche. La capacità di numerazione casuale di IBM Embedded Security Chip assicura che ogni coppia di chiavi hardware sia statisticamente univoca.

Figura 3 a pagina 5 descrive due componenti supplementari di IBM Embedded Security Chip. La comprensione di questi due componenti è critica per la gestione effettiva dell'infrastruttura di IBM Embedded Security Subsystem. Figura 3 a pagina 5 mostra sia le chiavi pubblica e privata del responsabile che quelle pubblica e privata dell'utente. Segue un riepilogo delle chiavi pubbliche e private.

- Le chiavi pubblica e privata vengono considerate una ″coppia di chiavi.″
- Le chiavi pubblica e privata sono collegate matematicamente in modo che:
  - I dati cifrati con la chiave pubblica possano essere decifrati solo con la chiave privata.
  - I dati cifrati con la chiave privata possano essere decifrati solo con la chiave pubblica.
  - La conoscenza della chiave privata non consente di derivare quella pubblica.
  - La conoscenza della chiave pubblica non consente di derivare quella privata.
  - La chiave pubblica generalmente è resa disponibile a tutti.
- La chiave privata deve essere assolutamente protetta.
- Le chiavi pubblica e privata sono la base per la PKI (public key infrastructure).

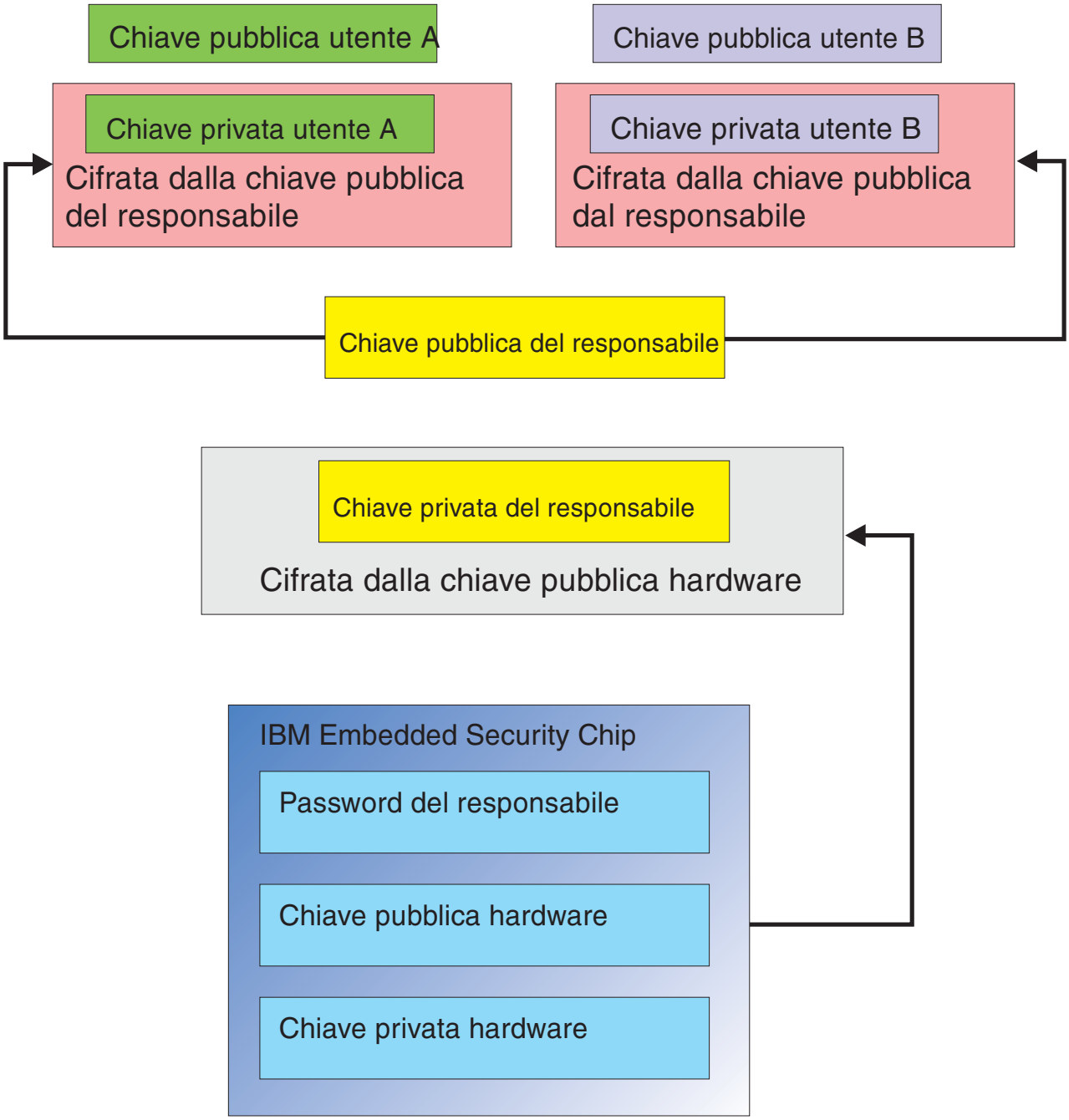

Figura 3. Vari livelli di cifratura forniscono un alto livello di sicurezza

Gerarchia di scambio-chiavi

Parte dell'architettura ESSIBM è composta da una gerarchia di "scambio-chiavi". Informazioni dettagliate sul suo funzionamento verranno fornite nel manuale *Guida per il responsabile*; tuttavia, segue qui un'introduzione sulle modalità di applicazione alla configurazione, alla distribuzione ed alla gestione generali. Nella Figura 3, è possibile visualizzare le chiavi hardware pubblica e privata. Come precedentemente menzionato queste chiavi vengono create dal Client Security Software e sono statisticamente univoche su ciascun client. Sopra l'IBM Embedded

Security Chip è possibile visualizzare la coppia di chiavi pubblica e privata del responsabile. La coppia di chiavi del responsabile può essere univoca per ciascun computer o può essere la stessa per tutti i client o sottoinsiemi di client. I vantaggi e gli svantaggi verranno discussi in un secondo momento. Le chiavi pubbliche e private del responsabile hanno le funzioni seguenti:

- Proteggere le chiavi pubblica e privata dell'utente
- Consentire l'archiviazione ed il recupero delle credenziali dell'utente
- Consentire il roaming delle credenziali dell'utente, descritto nel manuale *Guida per il responsabile*

Utilizzo scambio delle chiavi

Nelle sezioni seguenti si tratterà degli utenti nell'ambiente IBM ESS. Le informazioni dettagliate relative al modo in cui impostare IBM Client Security Software e ESS per accogliere tali utenti verranno fornite in quelle sezioni. In questo caso si desidera solo specificare che ogni utente dispone di una chiave pubblica e di una privata. La chiave utente privata viene cifrata con la chiave pubblica del responsabile. In Figura 3 a pagina 5, è possibile verificare che la chiave privata del responsabile viene cifrata con la chiave pubblica hardware. Perché si cifrano queste chiavi private.

Il motivo risale alla gerarchia precedentemente menzionata. Per lo spazio di memorizzazione limitato nell'IBM Embedded Security Chip, il chip è in grado di contenere solo un limitato numero di chiavi alla volta. Le chiavi hardware pubblica e privata solo le sole chiavi che restano memorizzate in questo scenario. Per consentire la memorizzazione di più chiavi e più utenti, IBM ESS implementa una gerarchia basata sullo scambio di chiavi. Ogni volta che viene richiesta una chiave viene ″scambiata″ nell'IBM Embedded Security Chip. Scambiando le chiavi private cifrate nel chip, è possibile decifrare ed utilizzare la chiave privata solo nell'ambiente protetto del chip.

La chiave privata del responsabile viene cifrata con la chiave hardware pubblica. La chiave privata hardware, disponibile solo nel chip, viene utilizzata per decifrare la chiave privata del responsabile. Una volta decifrata la chiave privata del responsabile nel chip, è possibile passare una chiave utente privata (cifrata con la chiave pubblica del responsabile) nel chip dal disco fisso e decifrarla con la chiave privata del responsabile. In Figura 3 a pagina 5, si può constatare che è possibile disporre di più chiavi utente private cifrate con la chiave pubblica del responsabile. Ciò consente di impostare il numero di utenti necessario su un computer con IBM ESS.

Capitolo 3. Considerazioni sull'archiviazione chiave

Le Password e le chiavi operano in sincronia, insieme alle altre funzioni opzionali di autenticazione per verificare l'identità degli utenti del sistema.

Figura 4 mostra il modo in cuiIBM Embedded Security Subsystem e Client Security Software funzionano insieme. Windows richiede all'Utente A di collegarsi e l'utente A si collega. IBM CSS (Client Security System) determina l'utente corrente tramite le informazioni fornite dal sistema operativo. La chiave privata del responsabile, cifrata con la chiave hardware pubblica, viene caricata nel chip di Embedded Security.

Figura 4. La chiave privata del responsabile, cifrata dalla chiave hardware pubblica, viene caricata nel chip di Embedded Security.

Figura 5 mostra che la chiave hardware privata (disponibile solo nel chip) viene utilizzata per decifrare la chiave privata del responsabile. Adesso la chiave privata del responsabile è disponibile per essere utilizzata nel chip.

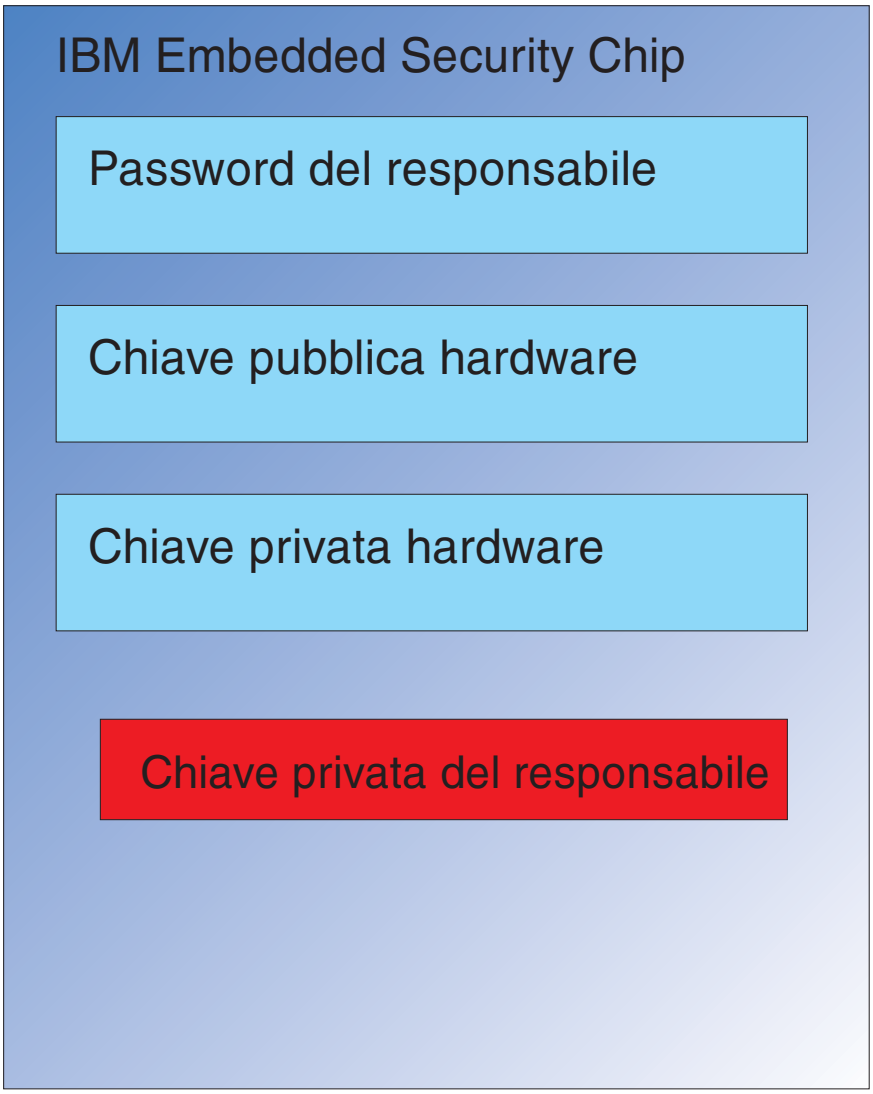

Figura 5. La chiave privata del responsabile è disponibile per essere utilizzata nel chip di sicurezza.

mostra che poiché l'Utente A è collegato al computer, la chiave privata relativa (cifrata con la chiave pubblica del responsabile) viene passata nel chip come visualizzato in Figura 6 a pagina 9.

Figura 6. La chiave privata dell'Utente A' cifrata dalla chiave pubblica del responsabile, viene passata nel chip di sicurezza.

La chiave privata del responsabile viene utilizzata per decifrare la chiave privata dell'Utente A. Adesso la chiave privata del responsabile è pronta per essere utilizzata come mostrato in Figura 7 a pagina 10.

Figura 7. La chiave privata dell'Utente A' è pronta per essere utilizzata.

Esistono varie altre chiavi che è possibile cifrare con la chiave pubblica dell'Utente A. ad esempio una chiave privata utilizzata per la firma delle e-mail. Quando l'Utente A invia una e-mail firmata la chiave privata utilizzata per la firma (cifrata con la chiave pubblica dell'Utente A) deve essere passata nel chip. La chiave privata dell'Utente A (già presente nel chip) decifrerà la chiave privata per la firma dell'Utente A. Adesso la chiave privata per la firma dell'Utente A è disponibile nel chip per eseguire l'operazione desiderata, in questo caso la creazione di una firma digitale (cifrando un hash). E' bene notare che è possibile utilizzare lo stesso processo per spostare le chiavi all'interno ed all'esterno del chip quando l'Utente B si collega al computer.

Perché disporre di una coppia di chiavi del responsabile

La ragione principale di disporre di una coppia di chiavi del responsabile è quella di archiviare e ripristinare le capacità. La coppia di chiavi del responsabile serve come livello di astrazione tra il chip e le credenziali dell'utente. Le informazioni sulla chiave privata specifiche dell'utente sono cifrate con la chiave pubblica del responsabile come mostrato in Figura 8 a pagina 11.

Importante: sviluppare una strategia per conservare le coppie di chiavi del responsabile. E' possibile che ogni computer che disponga di un ESC (Embedded Security Chip) utilizzi la stessa coppia di chiavi del responsabile, se deciso dal responsabile IT o dal responsabile della sicurezza. In alternativa, è possibile assegnare ad ogni reparto o edificio diverse coppie di chiavi del responsabile.

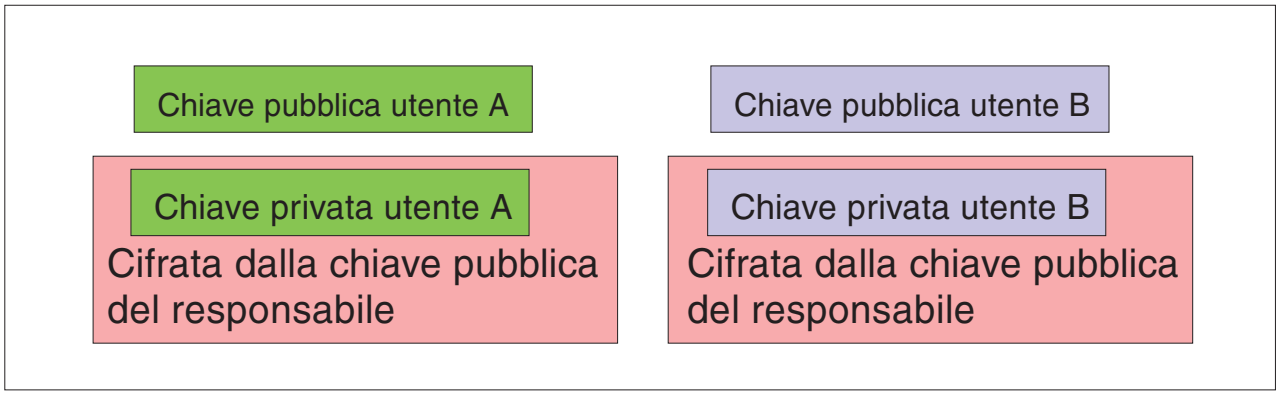

Figura 8. Le informazioni sulla chiave privata specifica dell'utente vengono cifrate con la chiave pubblica del responsabile.

Un altro motivo per disporre di una coppia di chiavi del responsabile è quello di poter firmare il file di politica della sicurezza del client, in modo da evitare che chiunque, tranne il responsabile, possa modificare la politica di sicurezza. Per ottenere un alto grado di sicurezza per i file di politica della sicurezza del client, è possibile suddividere la chiave privata del responsabile tra cinque persone al massimo. In tal caso, è necessario che le cinque persone che condividono parte della chiave privata, siano tute presenti per firmare e cifrare i file, come il file di politica della sicurezza del client. Ciò evita che sia una sola persona a svolgere le funzioni di responsabile. Per informazioni sulla suddivisione della chiave privata del responsabile consultare l'impostazione Keysplit=1 in Tabella 4 a pagina 37.

Durante l'inizializzazione dell'IBM Client Security Software, è possibile che le coppie di chiavi vengano create o dal software o che vengano importate da un file esterno. Se si desidera utilizzare una copia di chiavi del responsabile comune, si specificherà l'ubicazione dei file necessari durante l'installazione del client.

Una copia di backup di queste informazioni specifiche dell'utente viene eseguita (scritta) in un'ubicazione d'archivio definita del responsabile come mostrato in Figura 8. E' possibile che l'ubicazione d'archivio sia qualsiasi tipo di supporto fisicamente o logicamente collegato al client. La sezione sull'installazione dell'IBM Client Security System tratterà le prestazioni ottimali per tale ubicazione di archivio.

Le chiavi privata e pubblica del responsabile non sono archiviate. I dati utente nell'ubicazione di archivio viene cifrata con la chiave pubblica del responsabile. Disporre dei dati dell'archivio utente di per sé non apporta alcun vantaggio se non si dispone della chiave privata del responsabile per sbloccare i dati. Si fa spesso riferimento alle chiavi pubblica e privata del responsabile nella documentazione dell'IBM Client Security Software come alla ″Coppia di chiavi di archivio.″ E' bene notare che la chiave privata di archivio non viene cifrata. E' necessario porre una particolare attenzione nella memorizzazione e nella protezione della coppia di chiavi di archivio.

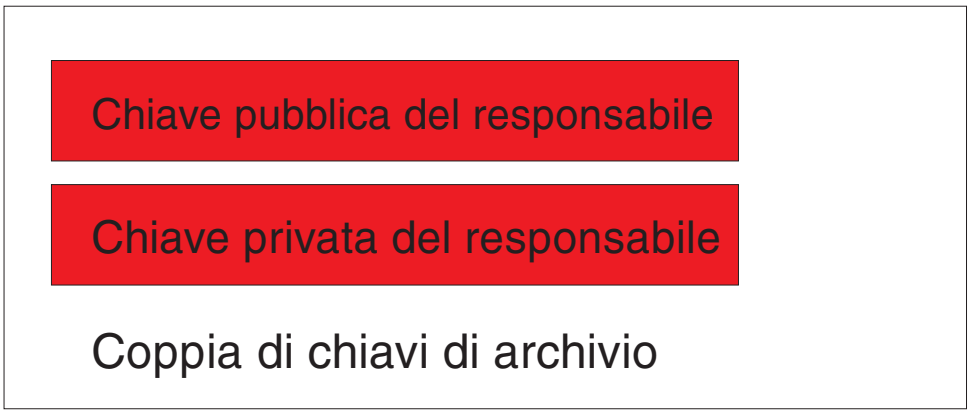

Figura 9. Le chiavi pubblica e privata del responsabile formano la coppia di chiavi di archivio.

Come precedentemente menzionato, una delle funzioni più importanti delle chiavi pubblica e privata del responsabile è quella di eseguire il back up ed il ripristino del contenuto del disco. Questa capacità è mostrata in 10 fino a15. I passaggi sono i seguenti:

1. Il Client A, per alcuni motivi, non è utilizzabile dall'Utente A. In questo esempio, si supporrà che il computer, Client A, è stato colpito da un fulmine come mostrato in Figura 10 a pagina 13.

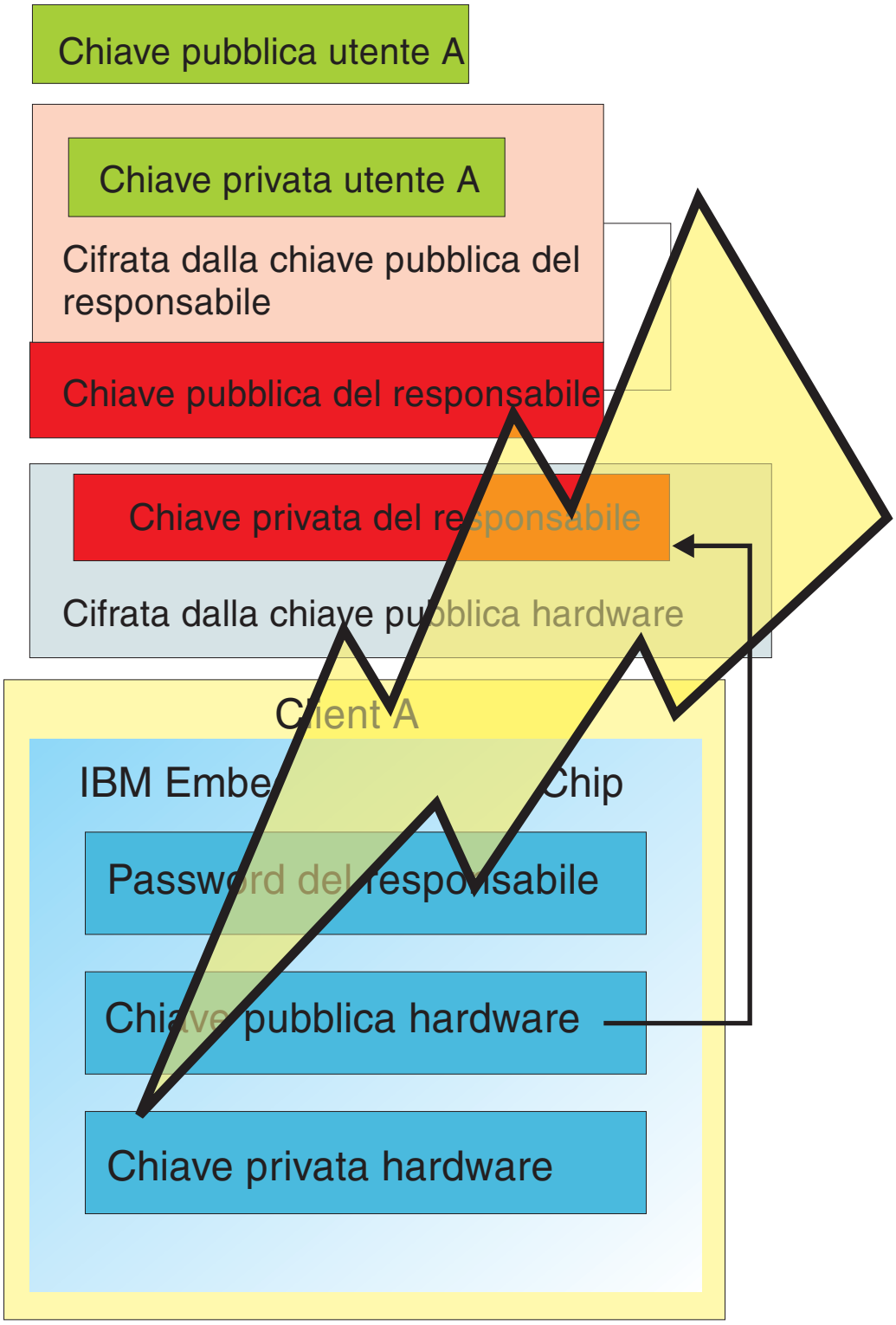

Figura 10. Il computer dell'Utente A' viene colpito da un fulmine e reso quindi inutilizzabile.

2. L'Utente A ne utilizza un computer IBM nuovo e più potente, denominato Client B come mostrato in Figura 11 a pagina 14. Il Client B è diverso dal Client A: le chiavi hardware pubblica e privata sono diverse da quelle del Client A. Questa differenza viene visualizzata dalle chiavi di colore grigio nel Client B e

da quelle di colore verde nel Client A. Tuttavia, è bene notare che la password del responsabile è la stessa per entrambi i client.

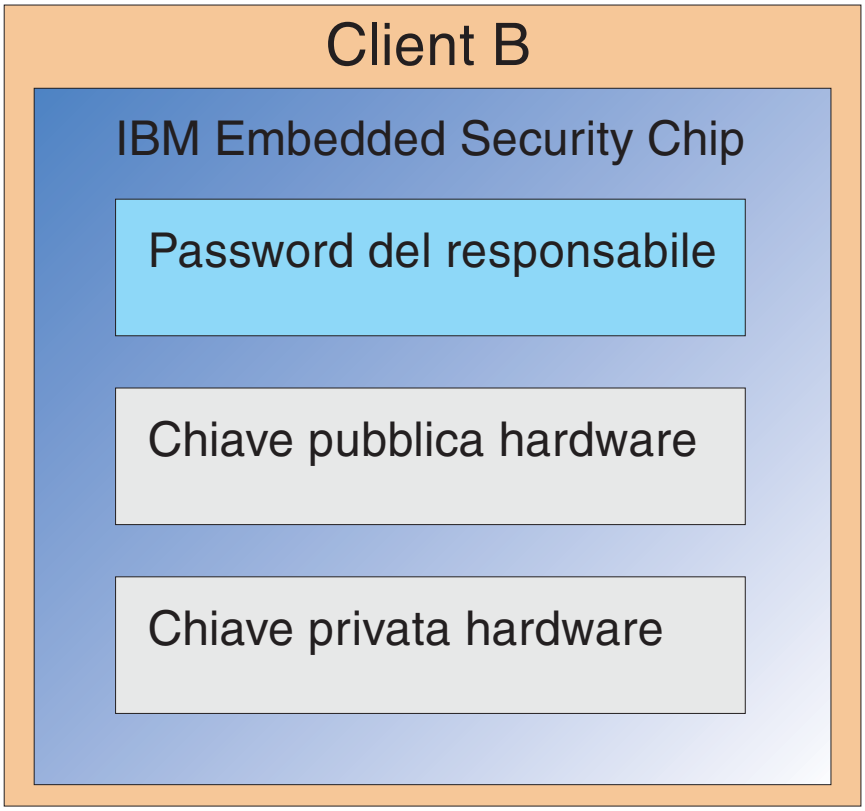

Figura 11. L'Utente A riceve un computer nuovo, Client B, con un nuovo chip di Embedded Security.

3. E' adesso necessario che il Client B disponga delle stesse credenziali utente presenti sul Client A. Queste informazioni sono state archiviate dal Client A. Consultando Figura 8 a pagina 11, sarà possibile ricordare che le chiavi utente sono cifrate con la chiave pubblica del responsabile e memorizzate nell'ubicazione di archivio. Per rendere le credenziali utente disponibili sul Client B, sarà necessario trasferire le chiavi pubblica e privata su questa macchina. La Figura 12 mostra il Client B che richiama le chiavi pubblica e privata del responsabile per recuperare i dati utente dall'ubicazione di archivio.

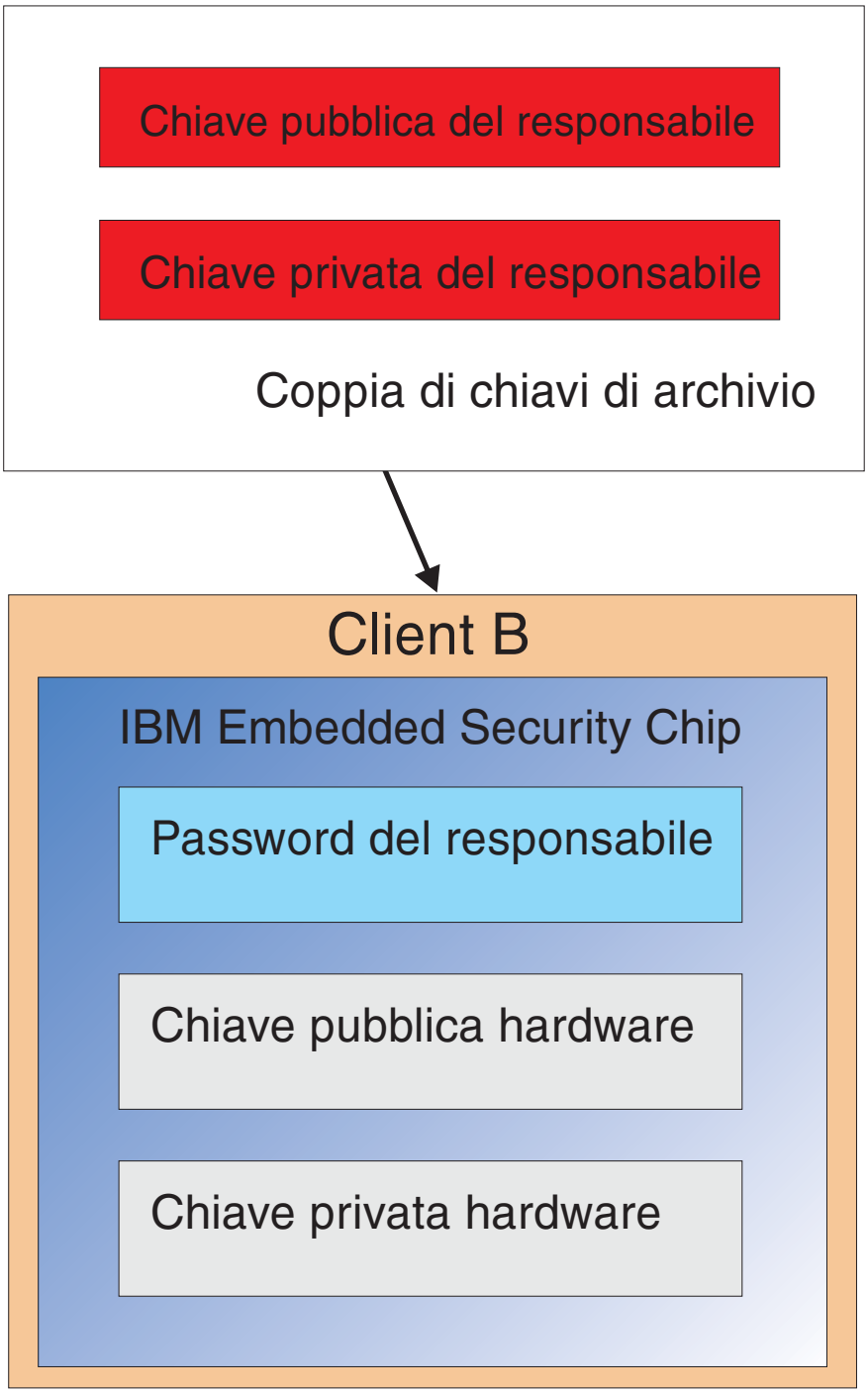

Figura 12. Il Client B richiama le chiavi pubblica e privata del responsabile dall'ubicazione di archivio.

4. Figura 13 a pagina 16 mostra la chiave privata del responsabile che viene cifrata con la chiave hardware pubblica del Client B.

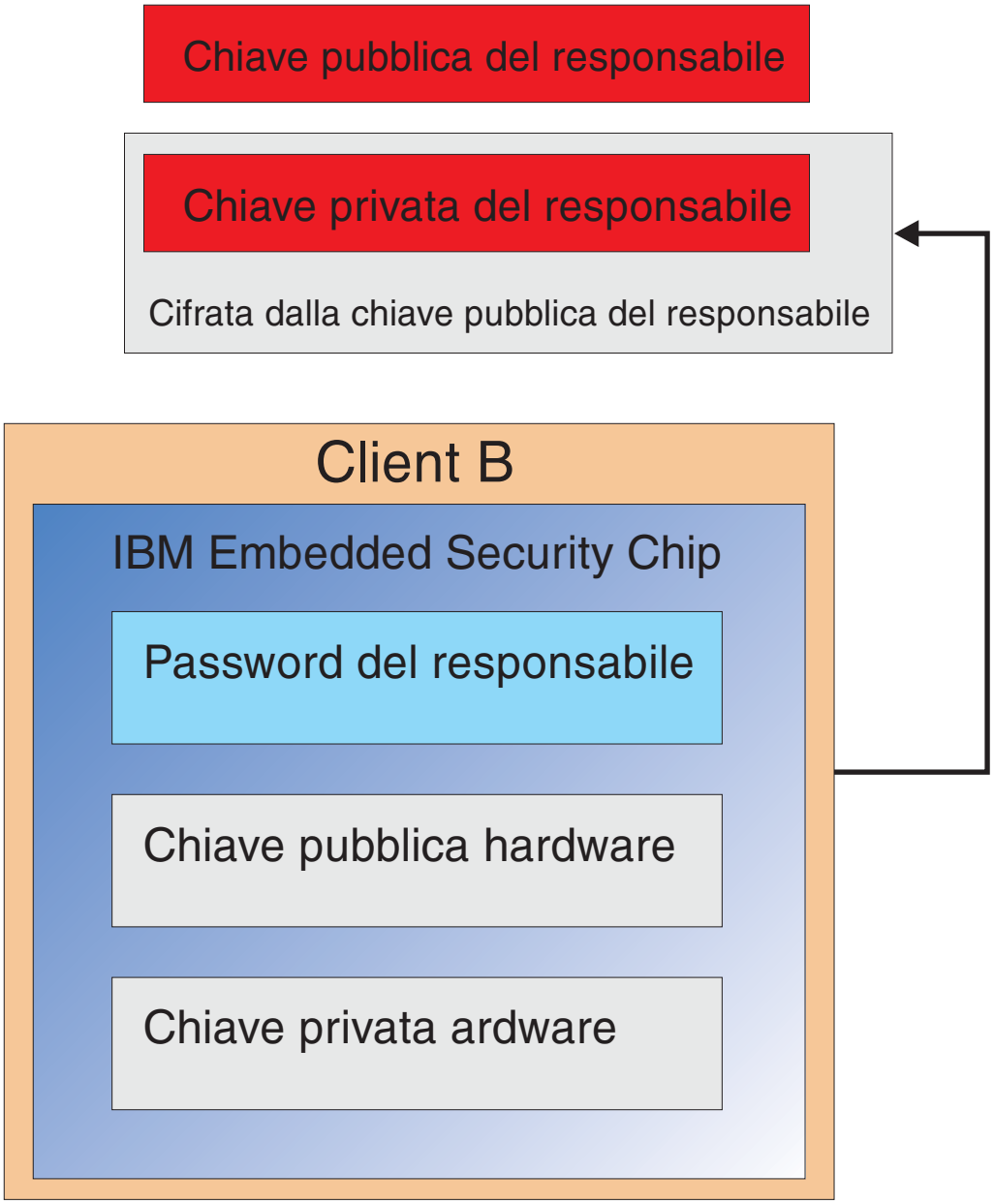

Figura 13. La chiave privata del responsabile viene cifrata con la chiave hardware del Client B.

Una volta cifrata la chiave privata del responsabile con la chiave hardware pubblica, è possibile scaricare le credenziali utente A sul Client B come mostrato in Figura 14 a pagina 17.

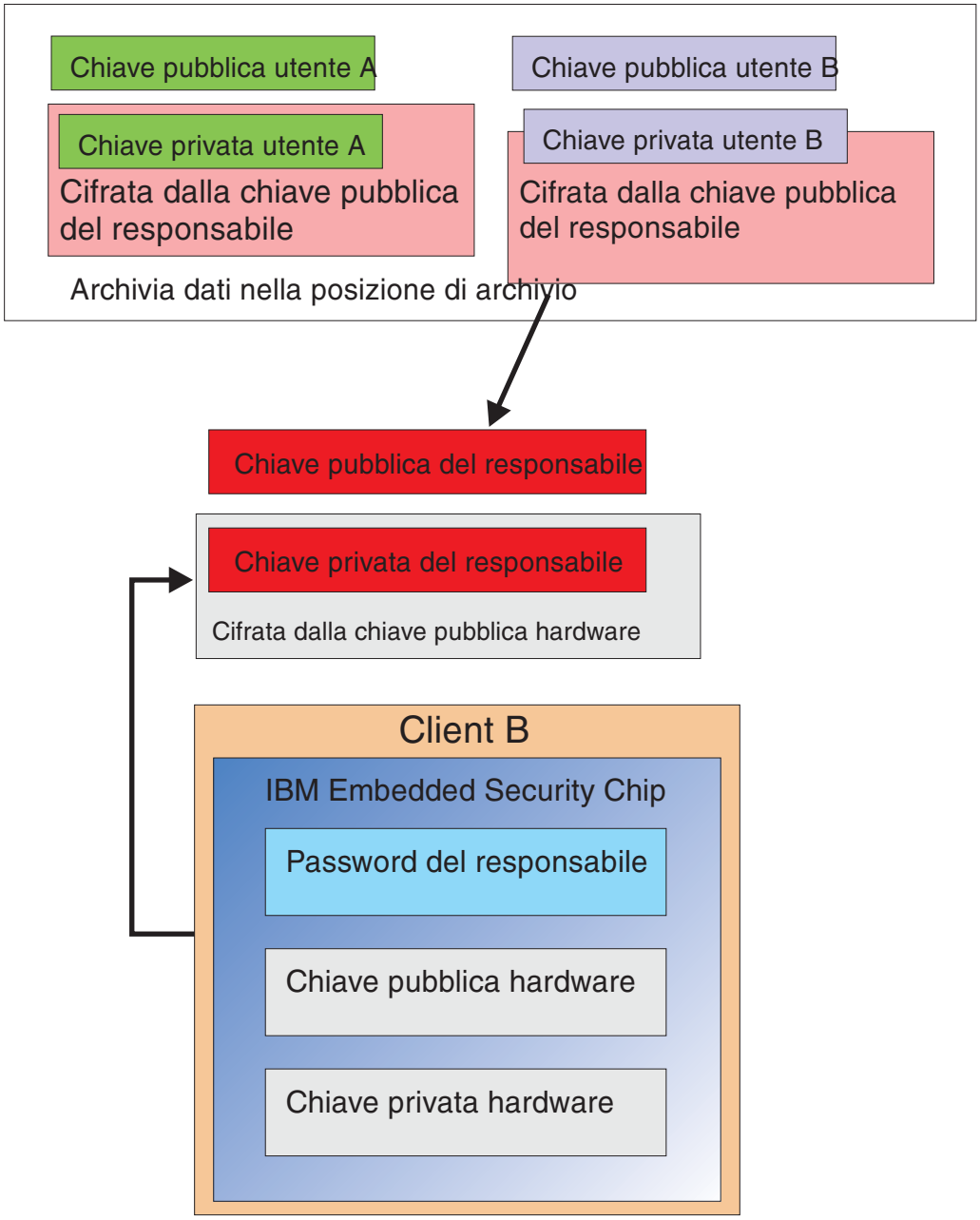

Figura 14. E' possibile caricare le credenziali dell'Utente A sul Client B dopo la cifratura della chiave privata del responsabile.

Figura 15 a pagina 18 mostra l'Utente A completamente ripristinato sul Client B. E' bene notare che a chiave privata dell'Utente A è stata cifrata con la chiave pubblica del responsabile sul server di archivio. La chiave pubblica del responsabile è una chiave RSA a 2048-bit ed è virtualmente impossibile violarla. Ciò significa che non è necessario proteggere l'ubicazione di archivio o disporre un accurato controllo degli accessi. Fino a che la coppia di chiavi di archivio (le chiavi privata e pubblica del responsabile) e più specificamente la chiave privata del responsabile, restano sicure, l'ubicazione delle credenziali utente può essere essenzialmente dovunque.

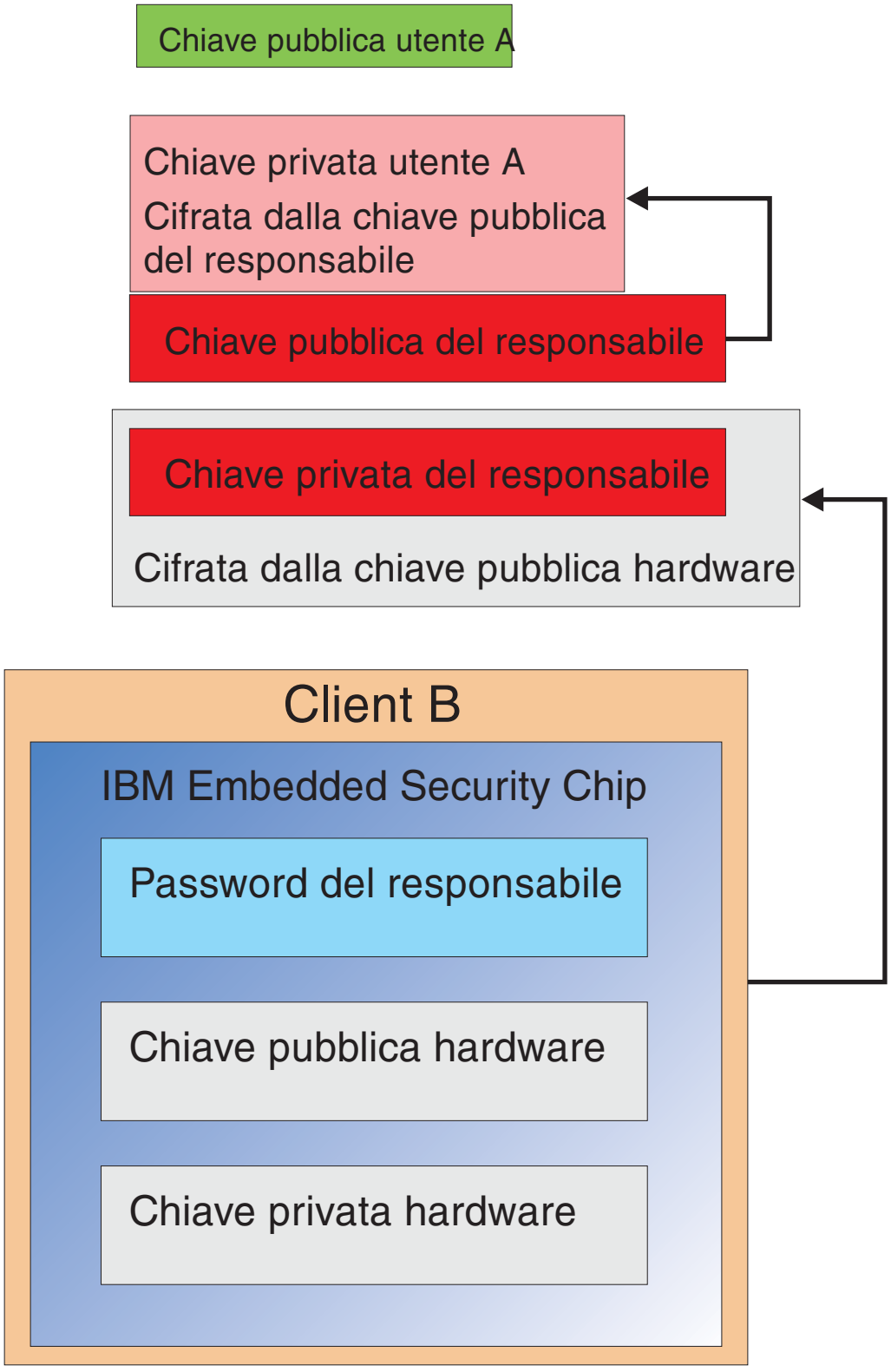

Figura 15. L'Utente A è completamente ripristinato sul B.

I dettagli sulle modalità d'impostazione della password del responsabile, dove si trovano le ubicazioni di archivio, ecc.. verranno trattati molto accuratamente nella sezione sull'installazione software. La Figura 16 mostra una panoramica dei componenti presenti in un ambiente ESS. Il punto fondamentale è che ogni client è

univoco dalla prospettiva delle chiavi hardware pubblica e privata, ma dispone di una chiave pubblica e privata del responsabile comune. I Client dispongono di un'ubicazione di archivio comune ma tale ubicazione può essere utilizzata per un segmento o un gruppo di utenti.

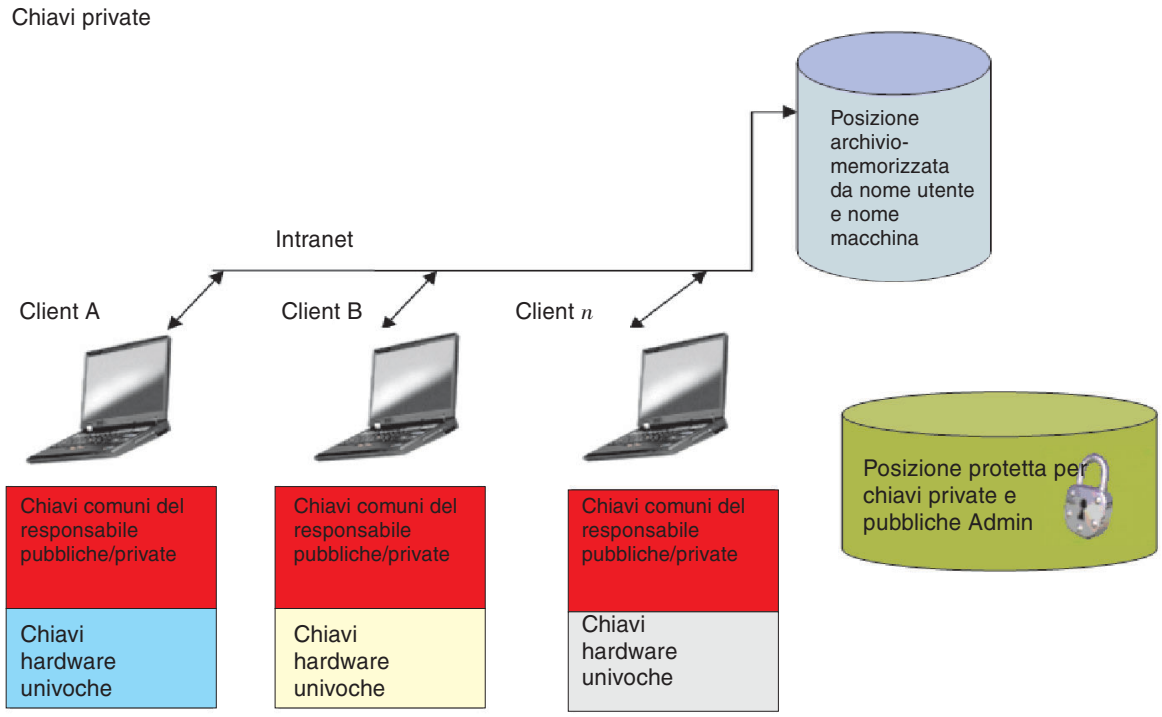

Figura 16. Componenti principali dell'IBM Client Security System.

Si consideri l'esempio seguente. Il dipartimento delle risorse umane ha un'ubicazione di archivio separata rispetto al dipartimento di ingegneria. L'archiviazione viene eseguita sulla base di un nome utente e un nome computer. IBM Client Security Software archivierà gli utenti di un sistema nell'ubicazione di archivio definita in base al nome utente ed al nome del computer come precedentemente mostrato per l'Utente A e l'Utente B. Notare inoltre che l'ubicazione protetta per le chiavi privata e pubblica del responsabile.

Nota: E' necessario che ogni nome computer e nome utente archiviati nella stessa ubicazione siano univoci. Un nome computer o un nome utente duplicati sovrascriveranno quelli precedentemente archiviati.

Capitolo 4. IBM Client Security Software

The IBM Client Security Software è il collegamento tra le applicazioni e il chip IBM Embedded Security, oltre all'interfaccia per iscrivere gli utenti, impostare la politica ed eseguire le funzioni di gestione di base. IBM Client Security System è composto essenzialmente dai seguenti componenti:

- Administrator Utility
- User Configuration Utility
- Administrator Console
- Procedura guidata per l'installazione
- UVM (User Verification Manager)
- CSP (Cryptographic Service Provider)
- Modulo PKCS#11

IBM Client Security System consente di eseguire alcune funzioni chiave:

- Registrare gli utenti
- Impostare la politica
- Impostare la politica passphrase
- Reimpostare le passphrase dimenticate
- Ripristinare le credenziali dell'utente

Ad esempio, se l'Utente A si collega al sistema operativo, IBM Client Security System basa tute le decisioni sul presupposto che l'Utente A sia collegato. (**Nota:** la politica di sicurezza è basata sulla macchina e non sull'utente; tale politica si applica a tutti gli utenti di un singolo computer.) Se l'Utente A tenta di utilizzare IBM Embedded Security Subsystem, IBM Client Security System rafforzerà le politiche di sicurezza impostate per l'Utente A su quel computer, quali il passphrase o l'autenticazione delle impronte digitali. Se la persona collegata come Utente A non è in grado di fornire il passphrase o le impronte digitali corrette per l'autenticazione, IBM ESS impedirà all'utente l'esecuzione dell'azione richiesta.

Iscrizione utenti e gestione iscrizioni

Gli utenti IBM ESS sono semplicemente utenti Windows iscritti nell'ambiente IBM ESS. Gli utenti possono iscriversi in diversi modi, che verranno descritti in seguito dettagliatamente. Iscrizione utenti. La comprensione di questo processo chiarirà il funzionamento di IBM ESS e le corrette modalità di gestione all'interno del proprio ambiente.

Client Security software utilizza l'UVM (User Verification Manager) per gestire passphrase ed altri elementi che consentono l'autenticazione degli utenti del sistema. Il software UVM abilita le seguenti funzioni:

- Protezione della politica del client UVM
- Protezione collegamento del sistema UVM
- Protezione screen saver sicurezza client UVM

Ogni utente all'interno dell'ambiente IBM ESS dispone di almeno un oggetto di personalizzazione associato utilizzato per l'autenticazione. Il requisito minimo è un passphrase. Ciascun utente nel componente UVM dell'ambiente ESS (dalla

prospettiva dell'utente, UVM gestisce l'autenticazione e rafforza la politica della sicurezza) deve disporre di un passphrase che deve essere inserita come minimo una volta per ogni avvio del computer. Le sezioni seguenti illustreranno il perché viene utilizzato un passphrase, il modo di impostarne uno e come utilizzarlo.

Richiesta di un passphrase

Inserire semplicemente, un passphrase viene richiesto per motivi di sicurezza. Disporre di un elemento hardware quale IBM Embedded Security Subsystem offre grandi vantaggi perché fornisce un'ubicazione sicura ed autonoma per le credenziali dell'utente su cui operare. Tuttavia, la protezione fornita da un chip hardware è di poca utilità se l'autenticazione richiesta per accedere al chip è debole. Ad esempio, si consideri di disporre di un chip hardware che esegua le funzioni di sicurezza. Tuttavia, l'autenticazione richiesta per richiamare un'azione dal chip è una sola cifra. Ciò consentirebbe ad un potenziale malintenzionato la possibilità di indovinare una sola cifra numerica (da 0 a 9) per richiamare le azioni con le credenziali. L'autenticazione ad una sola cifra indebolisce la sicurezza del chip cosicché questi fornisce un minimo o nessun vantaggio aggiunto ad una soluzione basata su software. Se non si dispone di una forte autenticazione insieme alla protezione hardware, non è possibile ottenere sicurezza. Il passphrase richiesto da IBM ESS viene utilizzato per autenticare un utente prima che venga intrapresa qualsiasi azione con le credenziali dell'utente nell'hardware. Il passphrase UVM può essere richiamato solo tramite la coppia di chiavi del responsabile, quindi non può essere recuperato da un sistema in modo illegale.

Impostazione di un passphrase

Ogni utente seleziona un passphrase per proteggere le proprie credenziali. In Capitolo 2, "ESC (Embedded Security Chip)- Istruzioni", a pagina 3, si è visto che una chiave privata utente viene cifrata con la chiave pubblica del responsabile. Anche la chiave privata utente dispone di un passphrase associato. Tale passphrase viene utilizzato per autenticare l'utente con le proprie credenziali. Figura 17 mostra il passphrase più il componente della chiave privata cifrato con la chiave pubblica del responsabile.

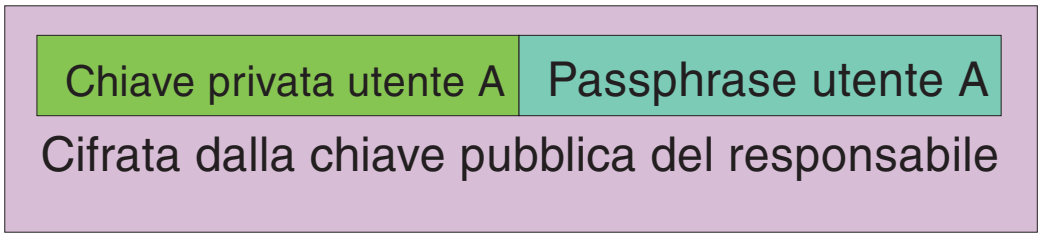

Figura 17. E' necessario che l'Utente A fornisca il passphrase per eseguire qualsiasi funzione che richieda la chiave privata dell'Utente A'.

Il passphrase illustrato in Figura 17 viene selezionato dall'utente in base alla politica esistente, cioè, in base alle regole che controllano la creazione della password come il numero di caratteri ed il numero di giorni per cui è valida la password. Il passphrase viene creato quando un utente viene iscritto nell'UVM. Le modalità in cui ciò accade quando si esce da IBM Client Security Software verranno illustrate in un secondo momento.

La chiave privata dell'Utente A viene cifrata con la chiave pubblica del responsabile, perché la decifrazione della chiave privata richiede la chiave privata del responsabile. Perciò, se viene dimenticata il passphrase dell'Utente A, il responsabile può reimpostare un nuovo passphrase.

Utilizzo di un passphrase

Figura 18 con Figura 20 a pagina 25, mostra il modo in cui il passphrase dell'utente viene elaborata sul chip. E' sempre necessario utilizzare un passphrase all'inizio ed almeno una volta per sessione. E' sempre richiesto un passphrase. E' possibile scegliere di aggiungere ulteriori periferiche di autenticazione, ma nessuna di esse è in grado di sostituire il requisito passphrase utente iniziale. Brevemente, la biometrica o altri dati di autenticazione vengono cifrati con la chiave pubblica dell'utente. E' richiesto l'accesso alla chiave privata per decifrare questi dati di sicurezza aggiuntivi.

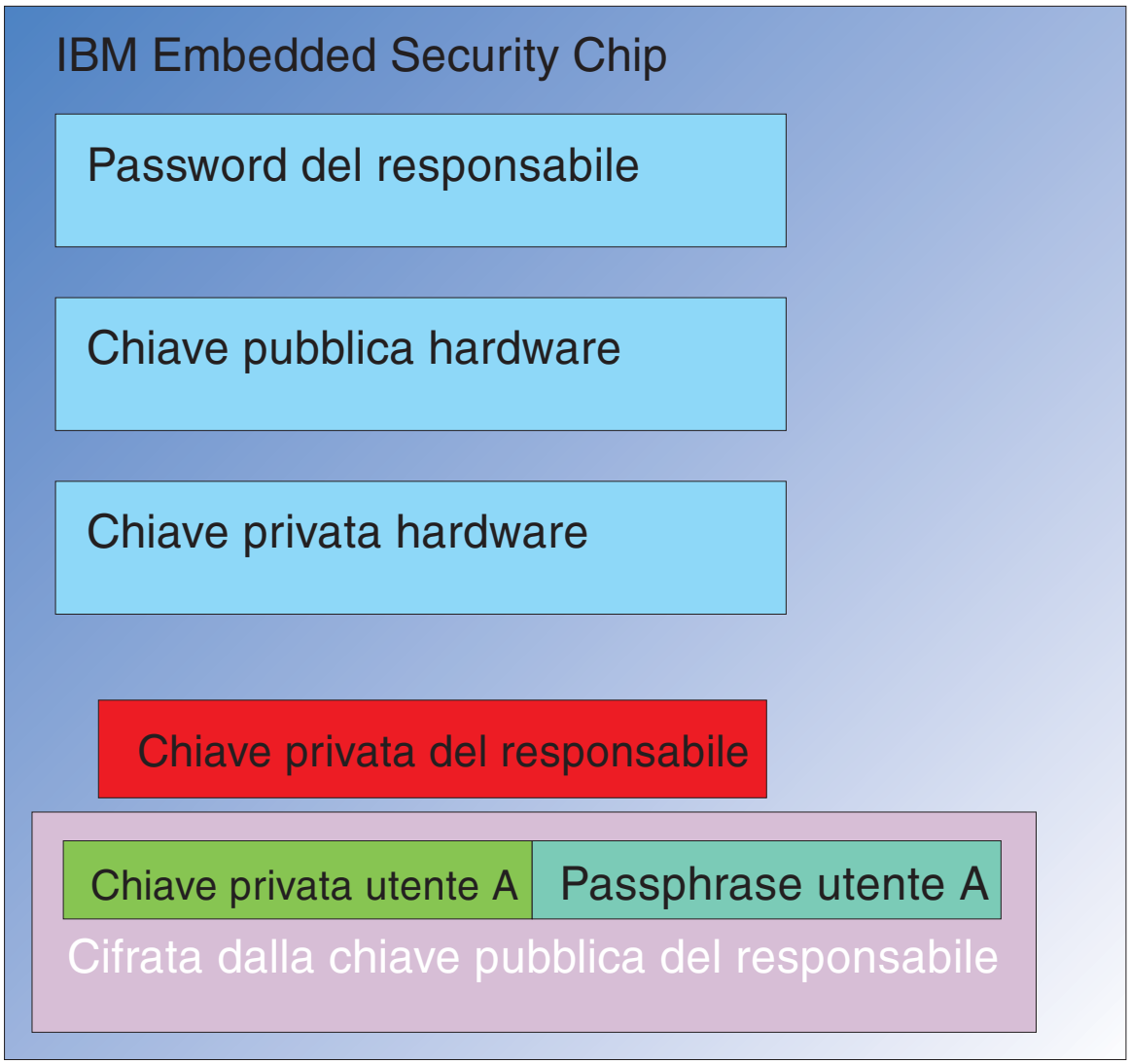

Figura 18. La chiave privata del responsabile viene decifrata nel chip.

Perciò, viene richiesto di fornire il passphrase almeno una volta per sessione per decifrare i dati aggiuntivi. Le credenziali che costituiscono la chiave privata e il passphrase dell'Utente A cifrate con la chiave pubblica del responsabile vengono inserite nell'IBM Embedded Security Chip. La chiave privata del responsabile è già decifrata nel chip, come precedentemente descritto. Le credenziali vengono passate come descritto in Figura 19 a pagina 24.

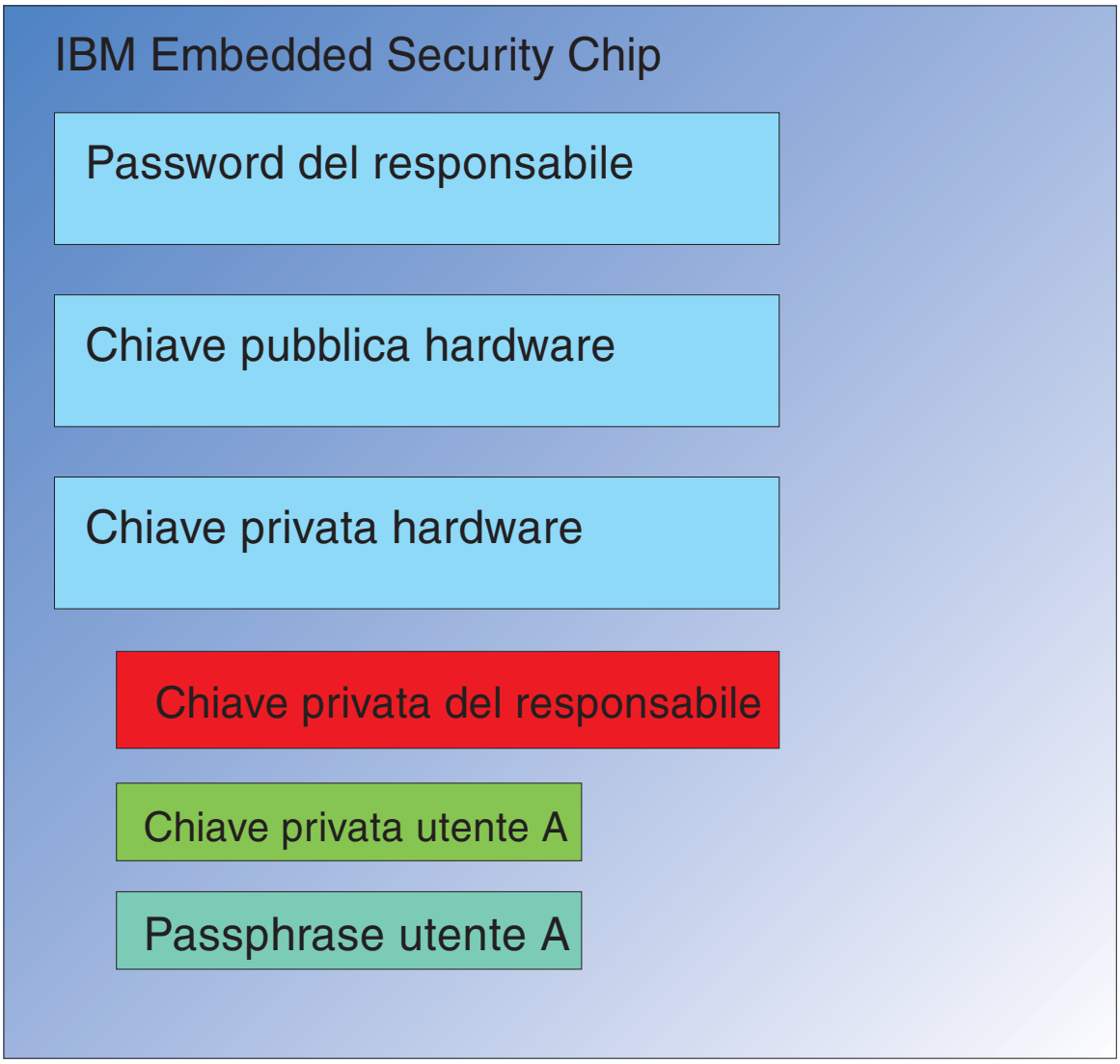

Figura 19. La chiave privata e il passphrase dell'Utente A sono disponibili nel chip.

Le credenziali vengono decifrate, rendendo disponibili nel chip sia la chiave privata che il passphrase dell'Utente A. Quando l'utente correntemente collegato, identificato dall'IBM Client Security System come Utente A, tenta di utilizzare le credenziali dell'Utente A , verrà visualizzata una finestra di dialogo come mostrato in Figura 20 a pagina 25.

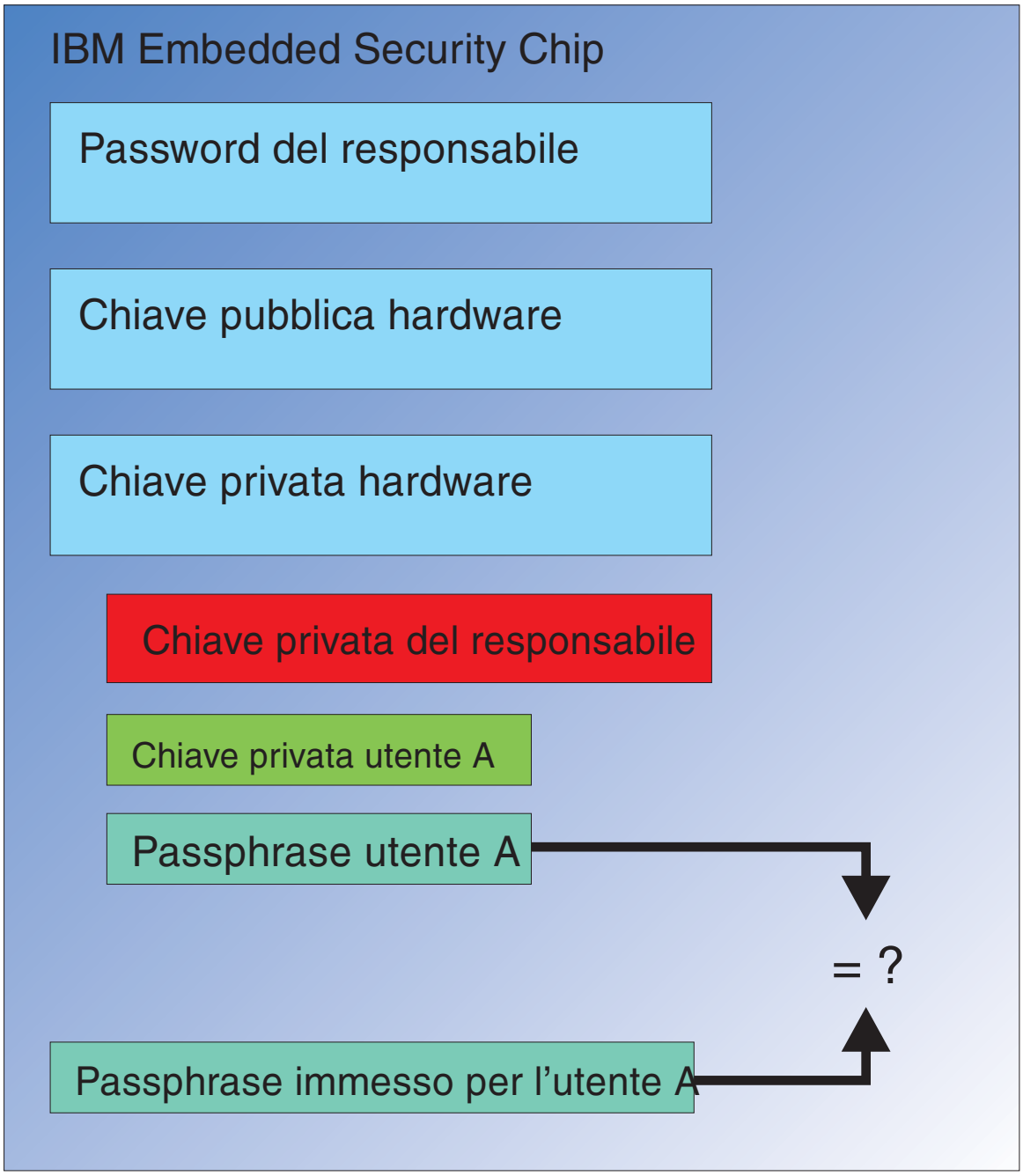

Figura 20. Quando l'Utente A tenta di utilizzare le credenziali dell'Utente A viene visualizzata una finestra di dialogo passphrase.

Il passphrase immesso viene passato al chip e paragonato al valore passphrase decifrato. Se i valori corrispondono, le credenziali dell'Utente A possono essere utilizzate per varie funzioni come le firme digitali o per decifrare la posta elettronica. E' bene notare che il confronto tra i valori passphrase viene eseguito nell'ambiente di sicurezza del chip. Il chip ha la capacità di rilevare i tentativi ripetuti di accesso non riuscito. E' bene inoltre notare che un passphrase registrato di un Utente A non viene mai esposta al di fuori del chip. Gli utenti vengono iscritti come parte dell'installazione dell'IBM Client Security Software. Una parte di

questo processo d'iscrizione è la creazione del passphrase dell'utente. Verrà illustrato dettagliatamente il modo in cui impostare questo passphrase e rafforzarne le regole.

Figura 1 a pagina 1 mostrati IBM Embedded Security Chip e IBM Client Security System. Figura 1 a pagina 1illustra inoltre l'inizializzazione dell'utente e della società. L'inizializzazione della società viene associata all'ESS (Embedded Security Subsystem) e l'inizializzazione dell'utente all'IBM Client Security Software. Le sezioni precedenti hanno descritto l'inizializzazione intrapresa per consentire una migliore comprensione del concetto generale. Le sezioni seguenti illustreranno in modo più dettagliato il processo di inizializzazione.

Inizializzazione TPM

L'inizializzazione TPM è essenzialmente il processo di aggiunta delle chiavi pubblica e privata hardware e della password del responsabile. Questo processo utilizza una macchina generica come spedita dall'IBM e la rende univoca. La tabella seguente illustrerà i metodi per l'inizializzazione delle chiavi pubblica e privata e delle password del responsabile.

Tabella 1. Metodi d'inizializzazione hardware

Azione	Creazione in BIOS	Creazione manuale del responsabile nel software CSS	Creazione in uno script
Creazione chiave hardware pubblica/privata	No	Sì	Sì
Creazione password del responsabile	Su alcuni client compatibili TCPA, sì. Verificare la voce BIOS.	Sì	Sì

Tabella 1 dimostra che le chiavi hardware pubblica e privata non vengono create automaticamente al momento dell'installazione del software. E' necessario che la creazione della chiave hardware pubblica e privata venga iniziata manualmente nel software o per script. E' possibile creare la password del responsabile in BIOS,l'applicazione IBM Client Security Software o per script. Il chip controlla i valori impostati per le chiavi hardware pubblica e privata; è impossibile impostare i valori. La capacità di numerazione casuale nel chip viene utilizzata per produrre coppie di chiavi pubbliche e private statisticamente a caso. Impostare la password del responsabile.

La password del responsabile tuttavia, è diversa perché è necessario che questo valore venga impostato del responsabile stesso. E' necessario affrontare alcune questioni riguardanti la password del responsabile:

- Cosa impostare come password del responsabile.
- Se si dispone di più di una password per i vari gruppi. In questo caso, come determinare in modo logico l'appartenenza di ciascuna password al computer relativo.
- Quale responsabile avrà accesso alla password. Se si dispone di più di una password per gruppi di utenti separati, come abbinarli.
- Se gli utenti finali a gestione autonoma hanno accesso alla password del responsabile.

Per rendere valida una decisione relativa alle questioni su riportate, è importate comprendere cosa consente l'utilizzo della password del responsabile:

- Consente l'accesso ai programmi di utilità del responsabile
- Consente di aggiungere/rimuovere utenti
- Consente di definire l'applicazione/funzione IBM Client Security Software da utilizzare

Le sezioni successive illustreranno il collegamento tra il file della politica e la chiave privata del responsabile. E' bene per ora notare che la chiave privata del responsabile viene richiesta per modificare la politica. Tabella 2 riepiloga quanto consentito dalla password del responsabile e/o dalla chiave privata del responsabile.

Tabella 2. Password e chiave privata basate sulle azioni del responsabile

Azione	**La password del responsabile**	**Chiave privata del responsabile**
Consente l'accesso a Admin Utility	Sì	No
Aggiunta/Rimozione/Ripristino utenti	Sì	No
Definizione delle applicazioni/funzioni CSS che è possibile utilizzare	Sì	No
Definizione/Modifica politica	Sì	Sì
Creazione file per reimpostare il passphrase utenti'	Sì	Sì

L'inizializzazione TPM fa inoltre riferimento alle chiavi pubblica e privata del responsabile. Dalla tabella su riportata è possibile visualizzare le capacità associate a queste chiavi. Alcune considerazioni per impostare le chiavi pubblica e privata del responsabile. E' possibile che questa coppia di chiavi sia univoca per ciascun computer o può essere la stessa per tutte le macchine. Quando IBM Client Security Software viene inizializzato il responsabile ha la possibilità di scegliere di utilizzare una coppia di chiavi esistente o di crearne una nuova per il client. Nuovamente, il modello di utilizzo determinerà cosa è meglio per l'iniziativa.

Prestazioni ottimali

Le grandi imprese possono utilizzare una chiave univoca per ogni macchina o una chiave univoca per ciascun reparto. Ad esempio, impostare una password del responsabile e/o una chiave privata del responsabile per tutti i computer utilizzati nel reparto risorse umane, un'altra per il reparto di ingegneria, ecc. E' anche possibile diversificare su una base fisica, come per edificio o ubicazione. Essere in grado di determinare la chiave privata del responsabile da utilizzare quando si crea un file di reimpostazione passphrase dovrebbe essere un processo semplice basato su chi sta richiedendo la reimpostazione. Come indicato in Tabella 1 a pagina 26 e Tabella 3 a pagina 30, è necessario inoltre che venga eseguita l'inizializzazione utente e società o hardware.

Impostazione politica di sicurezza prima della distribuzione di CSS

I requisiti di autenticazione e sicurezza derivano dalle varie parti interessate nell'organizzazione. Sebbene le singole persone con l'accesso del responsabile possano modificare la politica e inserire le modifiche nei computer dei client (consultare Capitolo 7, "Distribuzione in remoto di file di politica della sicurezza

nuovi o revisionati", a pagina 55), la configurazione delle impostazioni della politica prima della distribuzione fornisce migliori risultati. Per informazioni ulteriori sull'impostazione della politica, fare riferimento a "Funzionamento della politica UVM" nel manuale *Guida per il responsabile di Client Security Software'*.

Preparazione passphrase dimenticati o cattivo funzionamento periferiche di autenticazione

Inevitabilmente capita che gli utenti dimentichino un passphrase ed esiste la possibilità che le periferiche di autenticazione, come le periferiche biometriche d'impronta digitale o SmartCard, non funzionino correttamente.

Passphrase dimenticato: Il passphrase utente' non è memorizzato sul disco fisso del client o nel chip di sicurezza inserito in un modulo leggibile. E' conservata nella mente dell'utente 'ed in un'altra ubicazione: l'archivio protetto dalla coppia di chiavi del responsabile. Il responsabile potrà decifrare le informazioni dell'utente ' contenute nell'archivio, utilizzando la chiave privata. Sarà quindi in grado di fornire il passphrase decifrato all'utente.

Quando l'utente modifica il passphrase, le nuove informazioni vengono archiviate nell'ubicazione dell'archivio specificata.

In caso di cattivo funzionamento di una periferica di autenticazione, è possibile configurare IBM Client Security Software per visualizzare il pulsante **Fare clic qui per andare avanti**. Fare clic sul pulsante di bypass consente solamente all'utente di immettere con successo il passphrase. A questo punto l'utente potrà operare con sicurezza.

Per configurare CSS in modo che mostri il pulsante di bypass, seguire queste indicazioni:

1. Nel file CSEC.INI (ubicato nella directory root) localizzare la voce `AllowBypass= 0`. Il valore predefinito `0` imposta CSS in modo che nasconda il pulsante di bypass.
2. Impostare il valore `AllowBypass` su 1. Il pulsante di bypass verrà visualizzato quando la finestra del CSS consentirà all'utente di fornire l'autenticazione in aggiunta al passphrase.
3. Salvare il file CSEC.INI.

Nota:

1. Per archiviare queste informazioni, è essenziale che l'ubicazione dell'archivio venga specificata nel file CSEC.INI`kal=c:\jgk\archive`. Inoltre, se c:\jgk\archive è un'unità di rete, è necessario che tale unità venga mappata sul computer client per poter archiviare il passphrase.
2. Se non viene specificata un'ubicazione per l'archivio e l'ubicazione non è mappata sul computer client, non sarà possibile recuperare i passphrase.

Inizializzazione utente

IBM ESS consente a vari utenti di eseguire transazioni indipendenti e sicure su un computer singolo. E' necessario che tali utenti dispongano di un passphrase a loro associata e dispongano inoltre di altri elementi di autenticazione quali impronte digitali e/o smartcard. Si tratta di una *Autorizzazione a più fattori* . L'inizializzazione utente è un passo critico nella configurazione dei computer client per l'utilizzo di IBM ESS. E' bene notare che l'inizializzazione utente è un processo a due parti:

1. Registrazione
2. Personalizzazione

Registrazione

La registrazione è la semplice aggiunta di un utente a, o la registrazione di un utente con IBM Client Security System. In Figura 21, è possibile visualizzare il componente UVM (User Verification Manger) di IBM Client Security Software. UVM controlla le credenziali di ciascun utente oltre ad applicare la politica. Un file di politica, come quello rappresentato in Figura 21, contiene i requisiti di

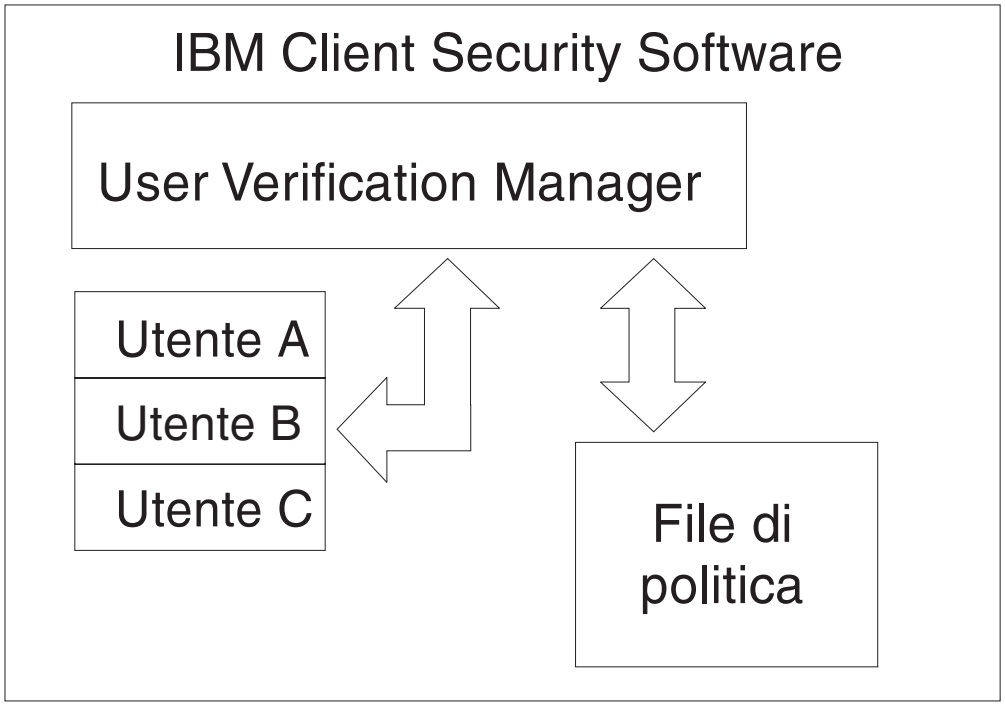

Figura 21. UVM (User Verification Manager) controlla le credenziali di ciascun utente' ed applica le politiche di sicurezza.

autenticazione per ciascun utente gestito dall'UVM. E' bene notare che gli utenti UVM sono semplici utenti Windows (locali o di dominio). UVM gestisce le credenziali in base a chi è collegato al momento al computer ed al sistema operativo. Ad esempio, se l'Utente A si collega in Windows ed è anche parte di UVM, UVM applicherà la politica nel momento in cui l'Utente A tenterà di eseguire operazioni che richiedono le credenziali. In un altro esempio, l'Utente A si collega al computer. Quindi va in Microsoft Outlook ed invia una e-mail con firma digitale. La chiave privata utilizzata per inviare la e-mail con firma digitale viene protetta nell'IBM Embedded Security Subsystem. Prima che UVM consenta di eseguire l'operazione, applicherà la politica nel modo definito nel file di politica. In questo esempio, il requisito è che un passphrase deve essere autenticato prima di eseguire l'operazione. UVM richiederà all'utente il passphrase e se la verifica ha successo l'operazione della chiave privata verrà eseguita nel chip.

Inizializzazione personale

L'inizializzazione personale è la semplice impostazione di un passphrase UVM singola. Le parti distinte del processo possono essere eseguite da persone diverse. Il passphrase UVM singola dovrebbe essere conosciuta solo dall'interessato. Tuttavia, se ogni individuo non esegue il processo di inizializzazione tale persona potrebbe aver necessità di eseguire un passaggio ulteriore. E' possibile anche configurare l'UVM in modo da forzare l'utente a modificare il passphrase la prima volta che si collega.

Ad esempio, l'Utente A viene inizializzato dal responsabile IT. Il responsabile IT seleziona l'Utente A da un elenco di utenti Windows (da un dominio, ad esempio). UVM richiede che il passphrase UVM venga associato all'Utente A. Il responsabile IT inserisce un ″valore predefinito″ di ″IT Admin Passphrase.″ Per assicurare protezione al sistema, dopo che l'Utente ha ricevuto il sistema è necessario che personalizzi il passphrase in modo che nessuno possa eseguire transazioni sicure utilizzando il passphrase predefinito.

Tabella 3. Metodi d'inizializzazione utente

Metodo	**Processo di comando**	**Requisiti processo**
Manuale	E' possibile che il responsabile personalizzi manualmente CSS per l'utente tramite il programma di utilità del responsabile	E' necessario che il responsabile sia presenta in ogni computer per l'impostazione.
File di configurazione responsabile	E' possibile che il responsabile crei un file di configurazione, che contenga una versione cifrata della password del responsabile. Tale file viene inviato all'utente, che può iscriversi singolarmente senza l'intervento o la presenza del responsabile	L'utente completa il processo di inizializzazione.
*.ini	Il responsabile crea uno script che esegua il file .ini e inserisca una password predefinita o personalizzata.	Presenza facoltativa dell'utente o del responsabile.

Scenari di distribuzione

Sono in distribuzione 1,000 client a 1,000 utenti finali. Le seguenti situazioni descrivono approcci diversi alla distribuzione:

- Si conoscono esattamente la macchina e l'utente finale a cui è distribuita. Ad esempio, la macchina 1 va a Bob, quindi si registra Bob sulla macchina 1. E' necessario che Bob personalizzi il computer quando lo riceve (impostando il proprio passphrase). Bob riceve il computer, avvia IBM Client Security Software e quindi imposta il passphrase.
- Non si conoscono né la macchina né l'utente a cui verrà distribuita. Il client 1 viene spedito all'utente finale X.

Questi due fattori variabili rendono diversa la distribuzione di IBM ESS rispetto ad un'applicazione tipica. Tuttavia, esistono varie opzioni di distribuzione che forniscono flessibilità alla distribuzione dell'IBM ESS.

Un tipico diagramma di flusso di distribuzione PC in una società potrebbe essere il seguente:

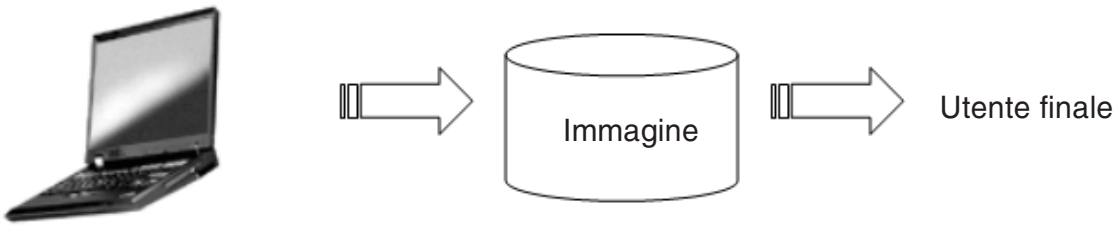

Figura 22. Diagramma di flusso distribuzione PC tipico

Sei scenari di distribuzione

Esistono sei metodi di distribuzione per l'IBM Client Security Software:

1. **Componente aggiunto**—Il codice IBM Client Security Software non fa è parte dell'immagine del disco. Viene installato, inizializzato e personalizzato dopo la distribuzione dei computers.
2. **Componente immagine**—Il codice IBM Client Security Software è parte dell'immagine, ma non non è installato. Non sono state avviate né la personalizzazione della società né quella dell'utente. (Consultare Figura 23 a pagina 32.)
3. **Installazione semplice**—IBM Client Security Software è installato ed è stato personalizzato per la società o per l'utente finale. (Consultare Figura 24 a pagina 33.)
4. **Personalizzazione parziale**—IBM Client Security Software è installato e si è verificata la personalizzazione della società, ma non si è verificata la personalizzazione dell'utente finale. (Consultare Figura 24 a pagina 33.)
5. **Personalizzazione temporanea**—IBM Client Security Software è installato e sono state impostate si ala personalizzazione della società che quella dell'utente. Sarà necessario che l'utente reimposti il passphrase utente e, se richiesto, fornisca altre informazioni sull'autenticazione come le impronte digitali o l'associazione smartcard. (Consultare Figura 25 a pagina 34.)
6. **Personalizzazione completa**—IBM Client Security Software è installato e sono state impostate sia la personalizzazione della società che quella dell'utente. Il responsabile imposta il passphrase utente. Se viene richiesta una scansione delle impronte digitali o un'altra autenticazione, è necessario che l'utente fornisca tale personalizzazione. (Consultare Figura 25 a pagina 34.)

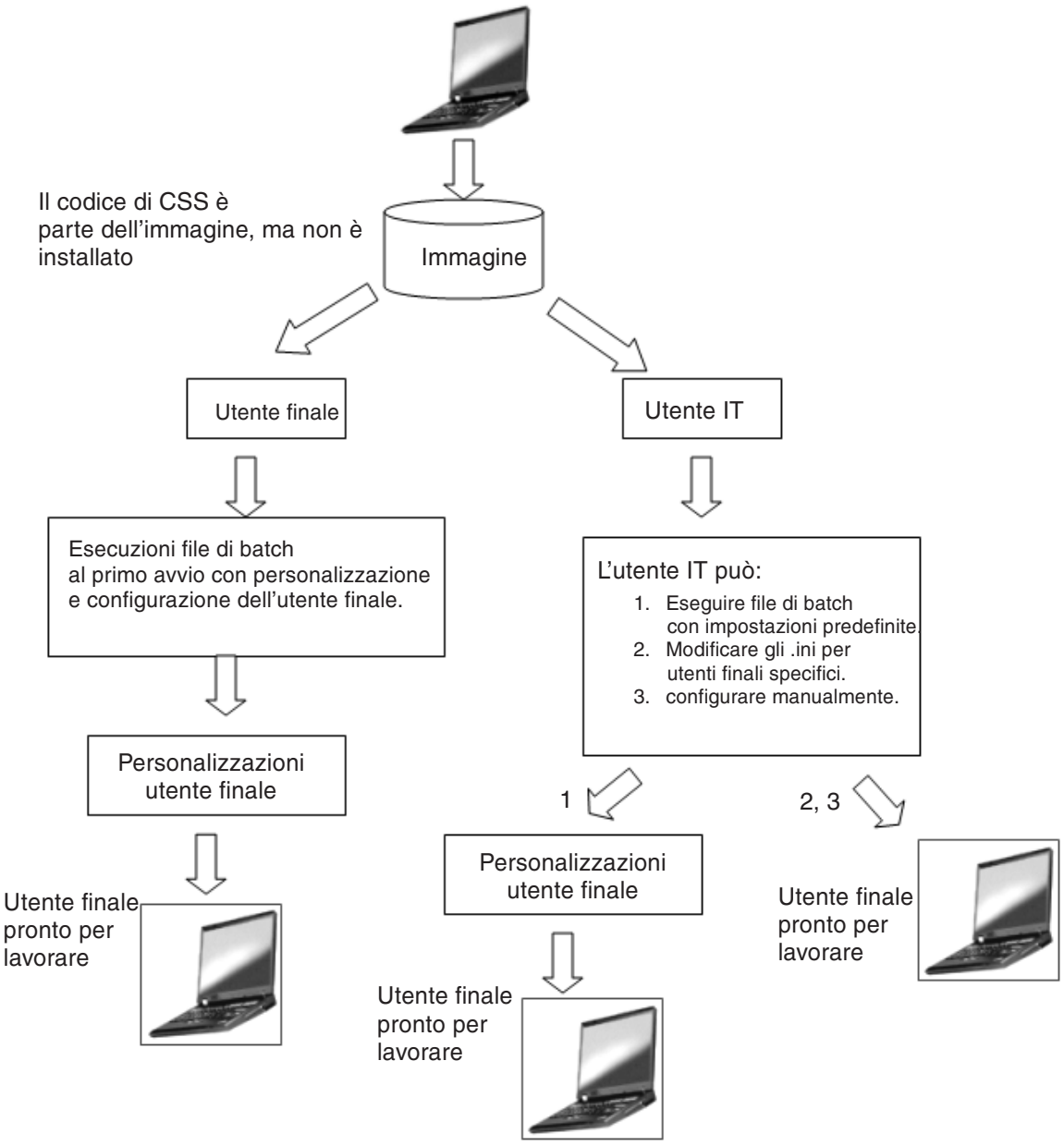

Figura 23. Il codice dell'IBM Client Security Software è parte dell'immagine, ma non è installato.

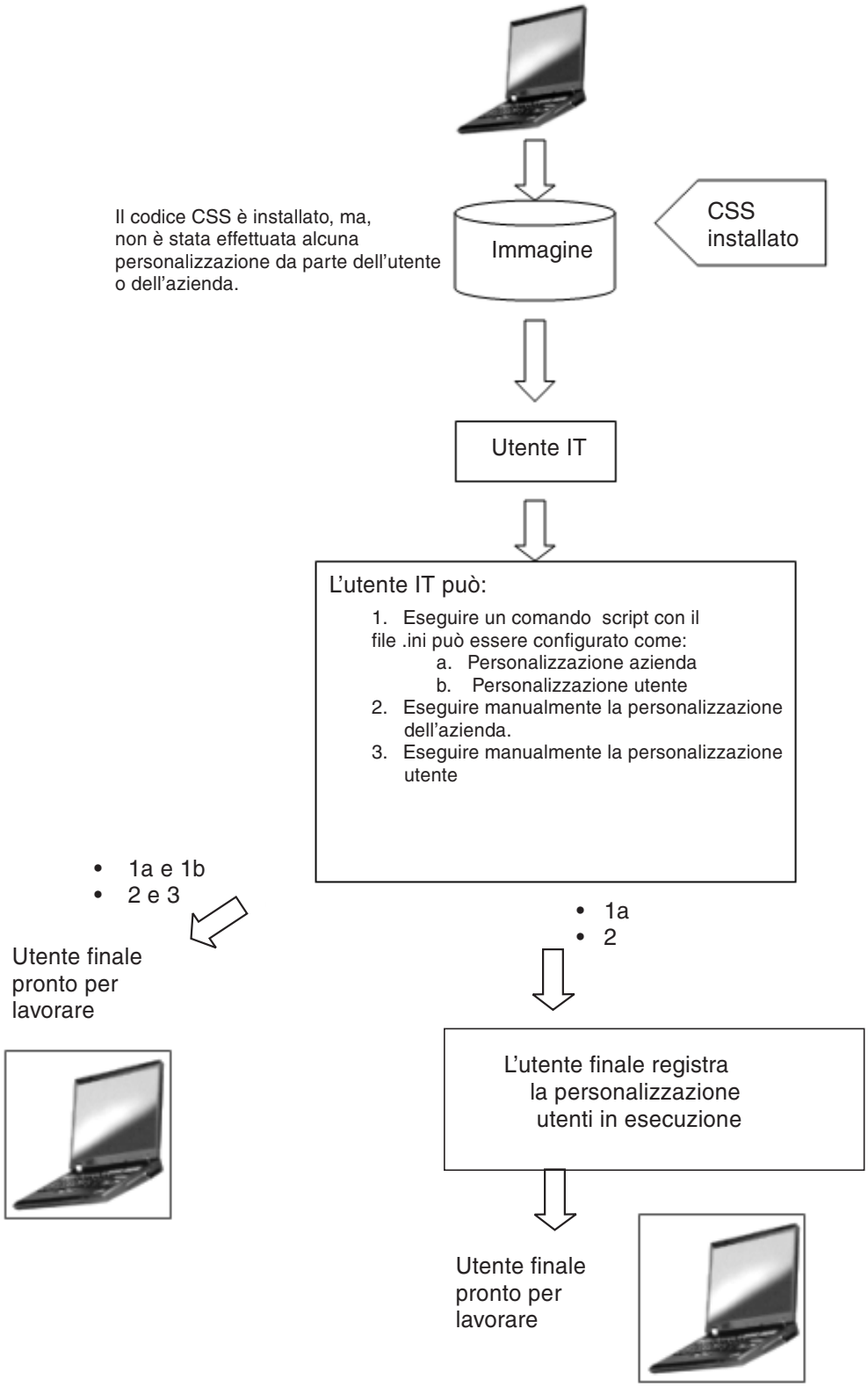

Figura 24. Il codice dell'IBM Client Security Software è installato ma non si è verificata né la personalizzazione della società né quella dell'utente.

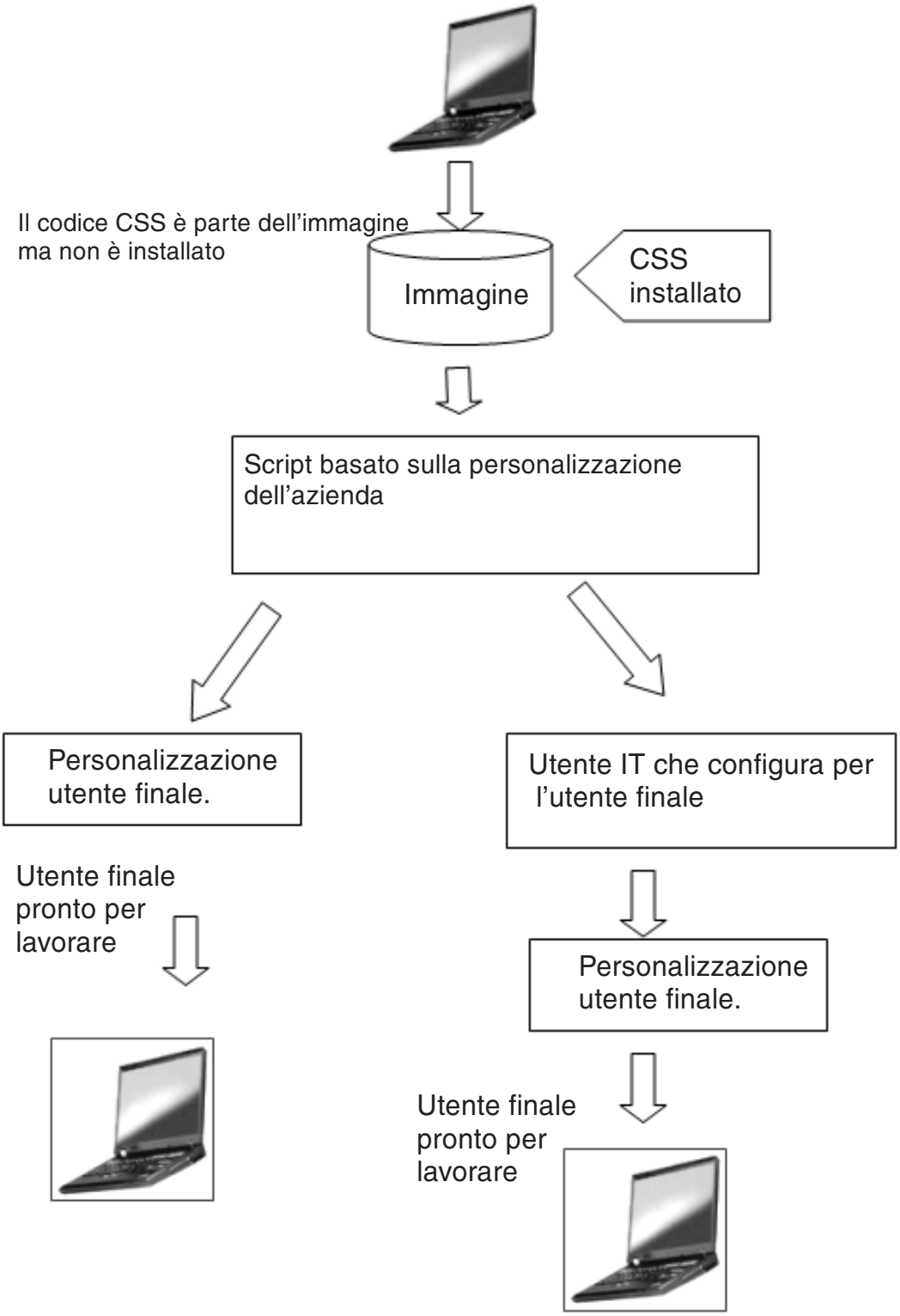

Figura 25. IBM Client Security Software è installato e sono state impostate sia la personalizzazione della società che quella dell'utente.

Nello scenario 1, IBM Client Security Software viene distribuito dopo che l'immagine del disco è stata messa sul computer. L'IBM Client Security Software è installato e configurato e l'Embedded Security Chip verrà configurato dopo l'installazione dell'immagine del disco.

Gli scenari da 2 a 6 rappresentano varie opzioni di distribuzione e configurazione software e di configurazione chip. A seconda delle necessità e del proprio ambiente, è possibile selezionare lo scenario ed il metodo d'installazione che meglio incontrano i propri requisiti. Consultare ″Installazione e inizializzazione″ per ulteriori informazioni relativi ai metodi d'installazione.

Installazione ed inizializzazione

E' possibile dividere in due processi l'installazione dell'IBM Client Security Software: installazione ed inizializzazione. Il processo d'installazione è simile all'installazione software tipica. E' possibile realizzare questa installazione con due metodi:

1. Client Security Software viene aggiunto ai computer distribuiti. (Consultare lo scenario 1 a pagina 31.)
2. Client Security Software è parte dell'immagine base. (Consultare gli scenari 2 a pagina 31 fino allo scenario6 a pagina 31.)

Installazione

Nel metodo 1 IBM Client Security Software viene aggiunto ad un'immagine aggiunta a sua volta ad ogni computer da programmi come IBM ImageUltra Builder.

Nel metodo 2, IBM Client Security Software viene aggiunto ad un PC di utente finale dopo la distribuzione del computer con l'immagine base. E' possibile eseguire il metodo 2 in due modi:

1. **Diretto dall'utente**—L'utente avvia e completa l'installazione facendo clic sulle finestre di dialogo e fornendo tutti gli input utente richiesti.
2. **Installazione silenziosa**—E' possibile avviare il processo d'installazione in remoto e e completarlo senza coinvolgimento dell'utente.

Inizializzazione

Esistono due modalità d'inizializzazione:

1. Inizializzazione di massa
2. Inizializzazione singola

Nell'opzione dell'inizializzazione di massa, è necessario utilizzare un file CSS.ini. Tale file fornisce i parametri per le opzioni come l'iscrizione di tutti gli utenti ad un sistema e i passphrase relativi impostati. Nell'inizializzazione singola, è possibile fornire all'utente finale un file che consenta iscrizioni autonome e password definite dall'utente.

Aggiunta dell'IBM Client Security Software a computer distribuiti con il chip di protezione

E' possibile che il responsabile distribuisca IBM Client Security Software solo (su immagine base) (senza personalizzazione o configurazione) e quindi configuri i client. In alternativa, è possibile che il responsabile distribuisca in generale IBM Client Security Software e quindi la configurazione di massa venga eseguita automaticamente. In entrambi i casi, eseguire prima l'installazione e poi la configurazione del software.

Installazione IBM Client Security Software: Per aggiungere IBM Client Security Software all'immagine base, è necessario includere i seguenti componenti:

1. Driver: LPC (per sistemi TCPA) e SMBus

   Nota:

   a. Sebbene SMBus disponga di un codice per l'installazione automatica, questo driver non è stato ancora firmato da Microsoft e quindi, è necessario che qualcuno sia presente durante l'installazione. Questa limitazione è in via di rimozione nel processo.

   b. Se si sta creando un'immagine sponsor Sysprep per la distribuzione, sarà necessario che l'installazione di questo driver sia presente solo durante la creazione dell'immagine sponsor.

   c. se si sta utilizzando IBM ImageUltra Builder, è necessario preparare una Portable Sysprep Image. E' necessario che SMBus sia parte dell'immagine base. Se non si desidera che tutti i computer abbiano SMBus come parte dell'immagine base, sarà necessario creare due immagini base.

2. CodiceIBM Client Security Software
3. Password del responsabile e coppia di chiavi private definita
4. Installare gli applet IBM Client Security Software (E' necessario installare File and Folder Encryption e Password Manager, se richiesto nel file di politica. Consultare il manuale *IBM Client Security - Guida per l'installazione'* per l'installazione silenziosa di questi applets)

Dopo aver aggiunto al sistema sponsor i tre componenti sopra elencati, E' necessario inizializzare l'hardware (il chip di protezione) di ESS (Embedded Security Subsystem). Per cominciare un'installazione di massa, completare la seguente procedura:

1. Creare il file CSEC.INI. (E' possibile creare il file CSEC.INI, utilizzando la procedura guidata di sicurezza client: CSECWIZ.EXE nella directory Security. Dopo aver completato la procedura, selezionare la casella di controllo accanto a **Salvare le impostazioni, ma non configurare il sottosistema. (Le impostazioni verranno salvate in C:\CSEC.INI)**.
2. Estrarre il contenuto del pacchetto d'installazione dell'IBM Client Security Software (csecxxxxx_00xx.exe) con Winzip utilizzando i nomi cartelle.
3. Modificare le voci szIniPath e szDir, richieste per una configurazione di massa, nel file SETUP.ISS. Verrà richiesto il parametro szIniPath per la configurazione di massa. (Consultare il file SETUP.ISS completo sottostante.)
4. Copiare i file sul sistema di destinazione.
5. Creare l'istruzione della riga comandi \setup -s. Eseguire l'istruzione della riga comandi dal desktop di un utente che dispone dei diritti di responsabile. Il gruppo dei programmi Startup o il tasto Esegui si trovano in una buona posizione per eseguire tale operazione.
6. Rimuovere l'istruzione della riga comandi al successivo avvio.

L'intero contenuto del file setup.iss viene elencato di seguito insieme ad alcune descrizioni:

```
[InstallShield Silent] Version=v6.00.000 File=Response File szIniPath=d:\csec.ini
```

(Il parametro precedente rappresenta il nome e l'ubicazione del file .ini, richiesto per una configurazione di massa. Se l'ubicazione del file .ini è su un'unità di rete, è necessario che sia mappata. Se si sta eseguendo un'installazione silenziosa che non è parte di una configurazione di massa, rimuovere questa voce. se si desidera installare solo IBM Client

Security Software, eliminare szIniPath=d:\csec.ini dalla riga di codice precedente. Se si desidera eseguire un'installazione ed una configurazione, lasciare il comando in posizione e verificare il percorso.)

```
[FileTransfer] OverwrittenReadOnly=NoToAll [{7BD2CFF6-B037-47D6-A76BD941EE13AD96}-
DlgOrder] Dlg0={7BD2CFF6-B037-47D6-A76B-D941EE13AD96}-
SdLicense-0 Count=4 Dlg1={7BD2CFF6-B037-47D6-A76B-D941EE13AD96}-
SdAskDestPath-0 Dlg2={7BD2CFF6-B037-47D6-A76B-D941EE13AD96}-
SdSelectFolder-0 Dlg3={7BD2CFF6-B037-47D6-A76B-D941EE13AD96}-
SdFinishReboot-0 [{7BD2CFF6-B037-47D6-A76B-D941EE13AD96}-SdLicense-0]
Result=1 [{7BD2CFF6-B037-47D6-A76B-D941EE13AD96}-SdAskDestPath-0]
szDir=C:\Program Files\IBM\Security
```

(Il parametro precedente è la directory utilizzata per installare Client Security. E' necessario che sia una directory locale del computer.)

```
Result=1
[{7BD2CFF6-B037-47D6-A76B-D941EE13AD96}-SdSelectFolder-0]
szFolder=IBM Client Security Software
```

(Il parametro precedente rappresenta il gruppo di programmi di Client Security.)

```
Result=1 [Application] Name=Client Security Version=5.00.002f
Company=IBM Lang=0009 [{7BD2CFF6-B037-47D6-A76B-D941EE13AD96}-
SdFinishReboot-0] Result=6 BootOption=3
```

Configurazione: Il seguente file è fondamentale per l'avvio di una configurazione di massa. Il file può essere definito in qualsiasi modo, ammesso che abbia un'estensione .ini. L'elenco seguente illustra le impostazioni e le spiegazione per l'impostazione del file .ini che è necessario creare. Prima di aprire e revisionare il file CSEC.INI, è necessario prima decifrarlo, utilizzando CONSOLE.EXE nella cartella Security.

Il comando seguente esegue il file .ini dalla riga comandi quando la configurazione di massa non viene eseguita insieme ad un'installazione di massa:

```
<CSS installation folder>\acamucli /ccf:c:\csec.ini
```

Tabella 4. Impostazioni di configurazione di Client Security System

[CSSSetup]	Intestazione della sezione per l'installazione CSS.
suppw=bootup	Password del Responsabile/supervisore BIOS. Lasciare lo spazio vuoto se non richiesto.
hwpw=11111111	Password hardware CSS. E' necessario che sia costituita da otto caratteri. Viene sempre richiesta. E' necessario che sia corretta se la password hardware è stata già impostata.
newkp=1	1 per creare una nuova coppia di chiavi del responsabile 0 per utilizzare una coppia di chiavi del responsabile.
keysplit=1	Quando newkp è 1, determina il numero dei componenti delle chiavi private. **Nota:** se la coppia di chiavi esistente utilizza più parti della chiave privata, è necessario che tutte le parti siano memorizzate nella stessa directory.
kpl=c:\jgk	Posizione della coppia di chiavi del responsabile quando newkp è 1, se si tratta di un'unità di rete mappata.
kal=c:\jgk\archive	Posizione della chiave di archivio dell'utente, se si tratta di un'unità di rete, è necessario che sia mappata.
pub=c:\jk\admin.key	Posizione della chiave pubblica del responsabile quando si utilizza una relativa coppia di chiavi esistente, se si tratta di un'unità di rete, è necessario che sia mappata.

Tabella 4. Impostazioni di configurazione di Client Security System (Continua)

pri=c:\jk\private1.key	Posizione della chiave privata del responsabile quando si utilizza una relativa coppia di chiavi esistente, se si tratta di un'unità di rete, è necessario che sia mappata.
wiz=0	Determina se il file è stato generato dalla procedura guidata all'installazione di CSS. Non è necessaria alcuna operazione aggiuntiva. Se si include nel file, il valore deve essere uguale a 0.
clean=0	1 per eliminare il file .ini in seguito all'inizializzazione, 0 per lasciare il file .ini in seguito all'inizializzazione.
enableroaming=1	1 per abilitare il roaming per il client, 0 per disabilitare il roaming per il client.
username= [promptcurrent]	[promptcurrent] per richiedere all'utente corrente la password di registrazione del sistema. [current] quando la password di registrazione del sistema per l'utente corrente viene fornita dalla voce sysregpwd e l'utente corrente è stato autorizzato per registrare il sistema con il server di roaming. [<account utente specifico>] se l'utente designato è stato autorizzato a registrare il sistema con il server di roaming e se la password di registrazione del sistema di tale utente viene fornita dalla voce sysregpwd. Non utilizzare questa voce se il valore di abilitazione del roaming è 0 o non è presente.
sysregpwd=12345678	Password di registrazione del sistema. Impostare questo valore alla password corretta per abilitare il sistema alla registrazione con il server di roaming. Non utilizzare questa voce se il valore relativo al nome utente è impostato su [promptcurrent], o se non è presente.
[UVMEnrollment]	Intestazione della sezione per la registrazione dell'utente.
enrollall=0	1 per registrare tutti gli account utente locale in UVM, 0 per registrare account utente specifici in UVM.
defaultuvmpw=top	Quando enrollall è 1, esso indica il passphrase UVM per tutti gli utenti.
defaultwinpw=down	Quando enrollall è 1, indica la password Windows registrata con UVM per tutti gli utenti.
defaultppchange=0	Quando enrollall è 1, stabilisce la politica di modifica passphrase UVM per tutti gli utenti. 1 per richiedere all'utente di modificare il passphrase UVM al collegamento successivo, 0 per non richiedere all'utente di modificare il passphrase UVM al successivo collegamento.
defaultppexppolicy=1	Quando enrollall è 1, stabilisce la politica di scadenza del passphrase UVM per tutti gli utenti. 0 per indicare che il passphrase UVM scade 1 per indicare che il passphrase UVM non scade
defaultppexpdays=0	Quando enrollall è 1, stabilisce la data di scadenza del passphrase UVM per tutti gli utenti. Quando ppexppolicy è impostato su 0, immettere questo valore per stabilire la data di scadenza del passphrase UVM.
enrollusers=*x*, dove x è il numero totale di utenti che verranno iscritti sul computer.	il valore in questa istruzione specifica il numero totale di utenti che verranno iscritti. Quando enrollall è 0, esso indica il numero degli utenti registrati in UVM.

Tabella 4. Impostazioni di configurazione di Client Security System (Continua)

user1=jknox	Fornire le informazioni per ciascun utente da iscrivere iniziando dall'utente 1. (Non esiste un utente 0.) E' necessario che i nomi utenti siano i nomi account. Per reperire il nome account corrente in XP, procedere nel modo seguente 1. Avviare Gestione computer (Gestione periferiche). 2. Espandere il nodo Utenti e gruppi locali. 3. Aprire la cartella Utenti. Gli elementi elencati nella colonna Nome sono i nomi account.
user1uvmpw=chrome	Specificare il passphrase UVM dell'utente 1 UVM.
user1winpw=spinning	Specificare il passphrase Windows dell'utente 1 da registrare con UVM.
user1domain=0	Specificare se l'account dell'utente 1 è locale o sul dominio. 0 per indicare che si tratta di un account locale, 1 per indicare che questo è presente sul dominio.
user1ppchange=0	Specificare se all'utente 1 verrà richiesto di modificare il passphrase UVM al successivo collegamento. 1 per richiedere all'utente di modificare il passphrase UVM al collegamento successivo, 0 per non richiedere all'utente di modificare il passphrase UVM al successivo collegamento.
user1ppexppolicy=1	Specificare se il passphrase UVM dell'utente 1 scade. 0 per indicare che il passphrase UVM scade. 1 per indicare che il passphrase UVM non scade.
user1ppexpdays=0	Se user1ppexppolicy=0, impostare questo valore per indicare la data di scadenza dal passphrase UVM.
Fornire per ogni utente una serie completa di impostazioni di configurazione nell'ordine specificato nella parte ombreggiata della tabella. Fornire tutti i parametri di un utente e quindi quelli del successivo. Se per esempio enrollusers fosse impostato su 2, si aggiungerebbe il gruppo seguente di impostazioni di configurazione.	
user2=chrome	
user2uvmpw=left	
user2winpw=right	
user2domain=0	
user2ppchange=1	
user2ppexppolicy=0	
user2ppexpdays=90	
[UVMAppConfig]	Intestazione della sezione per l'installazione del modulo e l'installazione di applicazioni, compatibili con UVM.
uvmlogon=0	1 per utilizzare la protezione del collegamento UVM, 0 per utilizzare il collegamento Windows.
entrust=0	1 per utilizzare UVM per l'autenticazione entrust, 0 per utilizzare l'autenticazione entrust.
notes=1	1 per utilizzare la protezione UVM per Lotus Notes, 0 per utilizzare la protezione della password di Notes.
netscape=0	1 per firmare e cifrare e-mail con il modulo IBM PKCS#11, 0 per non firmare e cifrare e-mail con il modulo IBM PKCS#11.

Tabella 4. Impostazioni di configurazione di Client Security System (Continua)

passman=0	1 per utilizzare Password Manager, 0 per non utilizzare Password Manager
folderprotect=0	1 per utilizzare File and Folder Encryption, 0 per non utilizzare File and Folder Encryption.

Nota:

1. Se qualsiasi file o percorso si trovano su un'unità di rete, è necessario che l'unità venga associata ad una lettera.
2. Il file INI consente di aggiungere nuovi utenti dopo la configurazione del sottosistema, il che è utile per l'iscrizione utenti. Eseguire un file INI come descritto in precedenza, ma non includere i valori ″pub=″ e ″pri=″. Il codice prevedrà solo l'iscrizione utenti e non inizializzerà nuovamente il sottosistema.
3. E' necessario che il file CSEC.ini venga cifrato perché il software carichi i contenuto. E' necessario che venga cifrato tramite CONSOLE.EXE nella directory Security. E' anche possibile ce venga utilizzato il comando seguente per cifrare un file INI tramite script. (Le virgolette sono necessarie per i nomi percorso lunghi): `CSS installation folder>\console.exe /q /ini:` *`percorso completo per un file ini decifrato`*
4. Mentre IBM Client Security Software viene potenziato e aggiornato, i parametri *.ini potrebbero cambiare.

IBM Client Security Software consente di eseguire i file CSEC.INI una seconda volta senza influenzare l'installazione corrente di CSS (Client Security Software). E' possibile eseguire questo file una seconda volta per iscrivere utenti aggiuntivi, ad esempio.

Tabella 5. Impostazioni di configurazione Client Security System alla seconda esecuzione

[CSSSetup]	Intestazione della sezione per l'installazione CSS.
suppw=	Password del Responsabile/supervisore BIOS. Lasciare lo spazio vuoto se non richiesto.
hwpw=11111111	Password hardware CSS. E' necessario che sia costituita da otto caratteri. Viene sempre richiesta. E' necessario che sia corretta se la password hardware è stata già impostata.
newkp=0	Immettere 0 per utilizzare una coppia di chiavi del responsabile esistente.
keysplit=1	Quando newkp è 1, determina il numero dei componenti delle chiavi private. **Nota:** se la coppia di chiavi esistente utilizza più parti della chiave privata, è necessario che tutte le parti siano memorizzate nella stessa directory.
pub=	Lasciare in bianco
pri=	Lasciare in bianco
kal=c:\archive	Posizione della chiave di archivio dell'utente, se si tratta di un'unità di rete, è necessario che sia mappata.
wiz=0	Determina se il file è stato generato dalla procedura guidata all'installazione di CSS. Non è necessaria alcuna operazione aggiuntiva. Se si include nel file, il valore deve essere uguale a 0.
clean=0	Immettere 0 per lasciare il file .ini dopo l'inizializzazione.
enableroaming=0	Immettere 0 per disabilitare il roaming per il client.

Tabella 5. Impostazioni di configurazione Client Security System alla seconda esecuzione (Continua)

[UVMEnrollment]	Intestazione della sezione per la registrazione dell'utente.
enrollall=0	1 per registrare tutti gli account utente locale in UVM, 0 per registrare account utente specifici in UVM.
enrollusers=1	il valore in questa istruzione specifica il numero totale di utenti che verranno iscritti.
user1=*eddy*	Questo è il nome del nuovo utente che sta per essere iscritto.
user1uvmpw=pass1word	Specificare il passphrase UVM dell'utente 1 UVM.
user1winpw=	Specificare il passphrase Windows dell'utente 1 da registrare con UVM.
user1domain=0	Specificare se l'account dell'utente 1 è locale o sul dominio. 0 per indicare che si tratta di un account locale, 1 per indicare che questo è presente sul dominio.
user1ppchange=0	Specificare se all'utente 1 verrà richiesto di modificare il passphrase UVM al successivo collegamento. 1 per richiedere all'utente di modificare il passphrase UVM al collegamento successivo, 0 per non richiedere all'utente di modificare il passphrase UVM al successivo collegamento.
user1ppexppolicy=1	Specificare se il passphrase UVM dell'utente 1 scade. 0 per indicare che il passphrase UVM scade. 1 per indicare che il passphrase UVM non scade.
user1ppexpdays=0	Se user1ppexppolicy=0, impostare questo valore per indicare la data di scadenza dal passphrase UVM.

Capitolo 5. Installazione del componente Client Security su un server Tivoli Access Manager

L'autenticazione degli utenti finali a livello di client è un problema di politica di sicurezza di rilevante importanza. Il programma Client Security Software fornisce l'interfaccia richiesta per gestire la politica di protezione di un client IBM. Questa interfaccia appartiene al software di autenticazione UVM (User Verification Manager), che è il componente principale del programma Client Security Software.

La politica di sicurezza UVM per un client IBM può essere gestita in due modi:

- Localmente, utilizzando un editor di politica che risieda sul client IBM
- In tutta l'azienda, utilizzando Tivoli Access Manager

Prima di poter utilizzare Client Security con Tivoli Access Manager, è necessario installare il componente Client Security di Tivoli Access Manager. E' possibile scaricare questo componente dal sito web IBM all'indirizzo http://www.pc.ibm.com/us/security/index.html.

Prerequisiti

Prima di poter stabilire una connessione protetta tra il client IBM e il server Tivoli Access Manager, è necessario installare i seguenti componenti sul client IBM:

- IBM Global Security Toolkit
- IBM SecureWay Directory Client
- Ambiente di esecuzione di Tivoli Access Manager

Per informazioni dettagliate sull'installazione e l'uso di Tivoli Access Manager, consultare la documentazione fornita sul sito Web http://www.tivoli.com/products/index/secureway_policy_dir/index.htm.

Scaricamento e installazione del componente Client Security

Il componente Client Security è disponibile gratuitamente sul sito Web IBM.

Per scaricare e installare il componente Client Security sul server Tivoli Access Manager e sul client IBM, completare la seguente procedura:

1. Utilizzando le informazioni sul sito Web, verificare che il chip IBM Embedded Security sia presente sul sistema e che il numero del modello corrisponda a quello fornito nella tabella per i requisiti del sistema; quindi, fare clic su **Continua**.
2. Selezionare il pallino che corrisponde al Tipo di macchina e fare clic su **Continua**.
3. Creare un ID utente, effettuare la registrazione presso la IBM compilando il modulo in linea e consultare l'Accordo di licenza; quindi, fare clic su **Accetto la licenza**.

   Verrà visualizzata la pagina per lo scaricamento del programma Client Security in modo automatico.
4. Seguire la procedura presente nella pagina di scaricamento per installare tutti i driver di periferica necessari, i file README, il software, i documenti di riferimento ed i programmi di utilità aggiuntivi.

5. Installare il programma Client Security Software completando la seguente procedura:
   a. Dal desktop di Windows fare clic su **Start > Esegui**.
   b. Nel campo Esegui, immettere `d:\directory\csec53.exe`, dove d:\directory\ è la lettera corrispondente all'unità seguita dalla directory in cui è ubicato il file.
   c. Fare clic su **OK**.

      Viene visualizzata la finestra Benvenuti nella procedura guidata InstallShield per IBM Client Security Software.
   d. Fare clic su **Avanti**.

      La creazione guidata estrae i file ed installa il software. Una volta completata l'installazione, verrà fornita l'opzione per riavviare l'elaboratore in questo momento oppure successivamente.
   e. Selezionare il pallino appropriato e fare clic su **OK**.
6. Una volta riavviato il computer dal desktop di Windows, fare clic su **Start > Esegui**.
7. Nel campo Esegui, immettere `d:\directory\TAMCSS.exe`, dove d:\directory\ indica la lettera identificativa dell'unità e la directory in cui viene situato il file oppure fare clic su **Sfoglia** per individuare il file.
8. Fare clic su **OK**.
9. Specificare una cartella di destinazione e fare clic su **Decomprimi**.

   La creazione guidata estrae i file nella cartella specificata. Un messaggio indica che i file vengono decompressi in modo corretto.
10. Fare clic su **OK**.

Aggiunta del componente Client Security sul server di Tivoli Access Manager

Il programma pdadmin è uno strumento di riga comandi che un responsabile può utilizzare per eseguire le attività di gestione di Tivoli Access Manager. L'esecuzione di più comandi consente a un responsabile di utilizzare un file che contenga più comandi pdadmin per eseguire un'attività completa o una serie di attività. La comunicazione tra il programma pdadmin e Management Server (pdmgrd) viene protetta su SSL. Il programma di utilità pdadmin viene installato come parte del pacchetto Tivoli Access Manager Runtime Environment (PDRTE).

Il programma di utilità pdadmin accetta un argomento di nome file che identifica l'ubicazione di un tale file, ad esempio:

```
MSDOS>pdadmin [-a <admin-user >][-p <password >]<file-pathname >
```

Il comando di seguito riportato è un esempio per creare lo spazio oggetti delle Soluzioni IBM, le azioni di Client Security e le singole voci ACL sul server di Tivoli Access Manager:

```
MSDOS>pdadmin -a sec_master -p password C:\TAM_Add_ClientSecurity.txt
```

Fare riferimento al manuale relativo alla guida per il responsabile di *Tivoli Access Manager Base* per ulteriori informazioni sul programma pdadmin e sulla sintassi dei comandi.

Stabilire una connessione protetta tra il client IBM e il server di Tivoli Access Manager

Il client IBM deve stabilire la sua identità autenticata all'interno del dominio protetto di Tivoli Access Manager per richiedere l'autorizzazione dal servizio delle autorizzazioni di Tivoli Access Manager.

E' necessario creare un'identità univoca per l'applicazione nel dominio protetto di Tivoli Access Manager. Affinché l'identità autenticata esegue i controlli di autenticazione, l'applicazione deve essere membro del gruppo remote-acl-users. Quando l'applicazione tenta di collegarsi ad uno dei servizi di dominio protetto, è prima necessario collegarsi al dominio protetto.

Il programma di utilità svrsslcfg consente alle applicazioni IBM Client Security di comunicare con i server di gestione e autorizzazione di Tivoli Access Manager.

Il programma di utilità svrsslcfg consente alle applicazioni IBM Client Security di comunicare con i server di gestione e autorizzazione di Tivoli Access Manager.

Il programma di utilità svrsslcfg consente di effettuare le seguenti attività:

- Crea un'identità utente per l'applicazione. Ad esempio, DemoUser/HOSTNAME
- Crea un file di chiavi SSL per quell'utente. Ad esempio, DemoUser.kdb e DemoUser.sth
- Aggiunge l'utente al gruppo remote-acl-users

E' necessario inserire i seguenti parametri:

- **-f file_cfg** nome e percorso del file di configurazione, utilizzare TAMCSS.conf
- **-d dir_kdb** la directory che deve contenere i file di database key ring per il server.
- **-n nome_server** il nome utente reale Windows nomeutente/UVM dell'utente IBM Client inserito.
- **-P pwd_admin**la password di responsabile di Tivoli Access Manager.
- **-s tipo_server** specificarlo come remoto.
- **-S pwd_server**la password per l'utente appena creato. Questo parametro è obbligatorio.
- **-r num_porta** impostare il numero di porta di ascolto per il client IBM. Si tratta del parametro specificato nella porta server SSL della variabile PDRE (Tivoli Access Manager Runtime) per il server di gestione PD.
- **-e pwd_life** Impostare la scadenza della password in numero di giorni.

Per stabilire una connessione protetta tra il client IBM e il server di Tivoli Access Manager, seguire questa procedura:

1. Creare una directory e spostare il file TAMCSS.conf sulla nuova directory.

   Ad esempio, `MSDOS> mkdir C:\TAMCSS MSDOS> move C:\TAMCSS.conf C:\TAMCSS\`
2. Eseguire svrsslcfg per creare l'utente.

   MSDOS> svrsslcfg -config -f C:\TAMCSS\TAMCSS.conf -d C:\TAMCSS\ -n <server_name> - s remote -S <server_pwd> -P <admin_pwd> -e 365 -r 199

   Nota: Sostituire <nome_server> con il nome utente UVM ed il nome host del client IBM.Ad esempio: –n DemoUser/MyHostName. Il nome host del client IBM può essere rilevato immettendo "hostname" al prompt di MSDOS. Il

programma svrsslcfg crea una voce valida nel server di Tivoli Access Manager e fornisce il file di chiavi SSL univoco per le comunicazioni cifrate.

3. Eseguire svrsslcfg per aggiungere l'ubicazione di ivacld al file TAMCSS.conf.

   L'impostazione predefinita prevede che il server di autorizzazione PD sia in ascolto sulla porta 7136. Ciò può essere verificato rilevando il parametro tcp_req_port nella stanza ivacld del file ivacld.conf sul server di Tivoli Access Manager. E' importante riportare correttamente il nome host ivacld. Utilizzare il comando di elenco del server pdadmin per ottenere queste informazioni. I server sono denominati: <nome_server>-<nome_host>. Quello che segue è un esempio di esecuzione dell'elenco del server pdadmin:

```
MSDOS> pdadmin server list   ivacld-MyHost.ibm.com
```

Il comando che segue viene poi utilizzato per aggiungere una voce di replica per il server ivacld sopra riportato. Si presume che ivacld sia in ascolto sulla porta predefinita 7136.

```
svrsslcfg -add_replica  -f <config file path> -h <host_name>
MSDOS>svrsslcfg -add_replica  -f C:\TAMCSS\TAMCSS.conf -h MyHost.ibm.com
```

Configurazione dei client IBM

Prima di utilizzare Tivoli Access Manager per controllare gli oggetti di autenticazioni per i client IBM, è necessario configurare ciascun client utilizzando Administrator Utility, un componente che viene fornito con Client Security Software. Questa sezione contiene i prerequisiti e le istruzioni per la configurazione dei client IBM.

Prerequisiti

Assicurarsi che il seguente software sia installato sul client IBM nel seguente ordine:

1. **Sistema operativo Microsoft Windows.** E' possibile utilizzare Tivoli Access Manager per controllare i requisiti di autenticazione per i client IBM su cui è in esecuzione Windows XP, Windows 2000 o Windows NT Workstation 4.0.
2. **Client Security Software versione 3.0 o successiva.** Una volta installato il software ed abilitato IBM embedded Security Chip, è possibile utilizzare il programma Client Security Administrator Utility per impostare l'autenticazione utente e per modificare la politica di sicurezza UVM. Per le istruzioni estese sull'installazione e l'uso di Client Security Software, consultare la *Guida all'installazione di Client Security Software* e la *Guida per il responsabile di Client Security Software*.

Configurazione delle informazioni di impostazione di Tivoli Access Manager

Una volta installato Tivoli Access Manager sul client locale, è possibile configurare le informazioni sull'installazione di Access Manager mediante il programma Administrator Utility, un componente software fornito da Client Security Software. Le informazioni di impostazione di Access Manager comprendono:

- La selezione del percorso completo del file di configurazione
- La selezione dell'intervallo di aggiornamento cache locale

Per configurare le informazioni di impostazione di Tivoli Access Manager sul client IBM, completare la seguente procedura:

1. Fare clic su **Start > Impostazioni > Pannello di controllo > IBM Embedded Security Subsystem**.
2. Inserire la password per il responsabile e fare clic su **OK**.

   Dopo aver immesso la password, viene visualizzata la finestra principale del programma Administrator Utility.
3. Fare clic sul pulsante **Configura politica e supporto dell'applicazione**.

   Viene visualizzato il pannello Configurazione della politica e applicazione UVM.
4. Selezionare la casella **Sostituisci il collegamento Windows standard con il collegamento protetto di UVM**.
5. Fare clic sul pulsante **Politica dell'applicazione**.
6. Nell'area Informazioni di impostazione di Tivoli Access Manager, selezionare il percorso completo del file di configurazione TAMCSS.conf. Ad esempio, `C:\TAMCSS\TAMCSS.conf`

   E' necessario che Tivoli Access Manager sia installato sul client per questa area disponibile.
7. Fare clic sul pulsante **Modifica politica**.

   Viene visualizzato il pannello Inserisci password del responsabile.
8. Inserire la password per il responsabile nel campo fornito e fare clic su **OK**.

   Viene visualizzata la finestra Politica UVM IBM.
9. Selezionare le azioni che si desidera che Tivoli Access Manager controlli dal menu a discesa Azioni.
10. Selezionare la casella Access Manager controlla l'oggetto selezionato in modo da rendere visibile un segno di spunta nella casella.
11. Fare clic sul pulsante **Applica**.

    Le modifiche vengono applicate al successivo aggiornamento della cache. Se si desidera che le modifiche siano applicate adesso, fare clic sul pulsante **aggiorna cache locale**.

Impostazione ed uso della funzione di cache locale

Una volta selezionato il file di configurazione di Tivoli Access Manager, è possibile impostare l'intervallo di aggiornamento della cache locale. Una replica locale delle informazioni sulla politica di sicurezza nel modo in cui viene gestito da Tivoli Access Manager viene conservata sul client IBM. E' possibile pianificare un aggiornamento automatico della cache locale con frequenze di mesi (0-12) o giorni (0-30).

Per impostare o aggiornare la cache locale, completare la seguente procedura:

1. Fare clic su **Start > Impostazioni > Pannello di controllo > IBM Embedded Security Subsystem**.
2. Immettere la password del responsabile, quindi fare clic su **OK**.

   Viene visualizzata la finestra Administrator Utility. Per informazioni complete sull'uso di Administrator Utility, consultare la *guida alla gestione di Client Security Software*.
3. In Administrator Utility, fare clic sul pulsante **Configura politica e supporto dell'applicazione**, quindi fare clic su **Politica dell'applicazione**.

   Viene visualizzata la finestra Modifica configurazione della politica di Client Security.
4. Effettuare una delle seguenti operazioni:
   - Per aggiornare la cache locale, fare clic su **Aggiorna cache locale**.

- Per impostare la frequenza di aggiornamento, inserire il numero dei mesi (0-12) e dei giorni (0-30) nei campi forniti e fare clic su **Aggiorna cache locale**. La cache locale e data di scadenza del file della cache locale vengono aggiornate in modo da indicare il successivo aggiornamento automatico.

Abilitazione di Access Manager per controllare gli oggetti del client IBM

La politica UVM viene controllata tramite un file globale della politica. Il file della politica globale, chiamato file di politica UVM, contiene i requisiti di autenticazione per le azioni che vengono eseguite sul sistema client IBM, come la registrazione di sistema, l'aggiornamento dello screen saver o la firma dei messaggi di e-mail.

Prima di attivare Tivoli Access Manager in modo da controllare gli oggetti di autenticazione per un client IBM, utilizzare l'editor della politica UVM per modificare il file della politica UVM. L'editor della politica UVM fa parte di Administrator Utility.

Importante: l'attivazione di Tivoli Access Manager per il controllo di un oggetto fornisce il controllo dell'object space di Tivoli Access Manager. In tal caso, è necessario installare di nuovo Client Security Software per ristabilire il controllo locale su quell'oggetto.

Modifica di una politica UVM locale

Prima di tentare di modificare la politica UVM per il client locale, verificare che almeno un utente sia stato registrato in UVM. Diversamente, un messaggio di errore viene visualizzato quando Policy Editor tenta di aprire il file della politica locale.

Modificare una politica locale UVM ed utilizzarla solo sul client per il quale è stata modificata. Se Client Security è installato nella propria posizione predefinita, la politica locale UVM viene memorizzata come \Program Files\IBM\Security\UVM_Policy\globalpolicy.gvm. Solo un utente che è stato aggiunto a UVM può utilizzare l'editor della politica UVM.

Nota: quando si imposta la politica UVM per richiedere l'impronta digitale per un oggetto di autenticazione (quali il collegamento al sistema operativo), ciascun utente, che viene aggiunto a UVM, per utilizzare quell'oggetto deve registrare le proprie impronte digitali.

Per avviare l'editor della politica UVM, completare la seguente procedura di Administrator Utility:

1. Fare clic sul pulsante **Configura politica e supporto dell'applicazione**, quindi fare clic sul pulsante **Politica dell'applicazione**.

   Viene visualizzata la finestra Modifica configurazione della politica di Client Security.
2. Fare clic sul pulsante **Modifica politica**.

   Viene visualizzato il pannello Inserisci password del responsabile.
3. Inserire la password per il responsabile nel campo fornito e fare clic su **OK**.

   Viene visualizzata la finestra Politica UVM IBM.
4. Nel separatore Selezione dell'oggetto, fare clic su **Azione** o **Tipo di oggetto** e selezionare l'oggetto per il quale si desidera assegnare in requisiti di autenticazione.

Gli esempi di azioni valide comprendono il collegamento al sistema, lo sblocco del sistema e la decifra e-mail; un esempio di tipo oggetto è Acquire Digital Certificate.

5. Per ciascun oggetto selezionato, scegliere **Tivoli Access Manager controlla l'oggetto selezionato** per attivare Tivoli Access Manager per quell'oggetto.

   Importante: l'attivazione di Tivoli Access Manager per il controllo di un oggetto fornisce il controllo dell'object space di Tivoli Access Manager. In tal caso, è necessario installare di nuovo Client Security Software per ristabilire il controllo locale su quell'oggetto.

   Nota: durante la modifica della politica UVM, è possibile visualizzare le informazioni di riepilogo della politica facendo clic su **Riepilogo della politica**.
6. Fare clic su **Applica** per salvare le modifiche apportate.
7. Fare clic su **OK** per uscire.

Modifica e utilizzo della politica UVM per i client remoti

Per utilizzare la politica UVM per più client IBM, modificare e salvare la politica UVM per un client remoto e, quindi, copiare il file della politica UVM su altri client IBM. Se si installa Client Security nella relativa posizione predefinita, il file della politica UVM sarà memorizzato come \Program Files\IBM\Security\UVM_Policy\remote\globalpolicy.gvm.

Copiare i seguenti file su altri client remoti IBM che utilizzano questa politica UVM:

- \IBM\Security\UVM_Policy\remote\globalpolicy.gvm
- \IBM\Security\UVM_Policy\remote\globalpolicy.gvm.sig

Se è stato installato Client Security Software nella propria posizione predefinita, la directory principale per i percorsi precedenti è \Program Files. Copiare entrambi i file nel percorso di directory \IBM\Security\UVM_Policy\ sui client remoti.

Prospetti per la risoluzione dei problemi

Le seguenti informazioni sulla risoluzione dei problemi possono essere utili se si rilevano problemi quando si installa il programma Client Security Software.

Informazioni sulla risoluzione dei problemi relativi al certificato digitale

Le seguenti informazioni sulla risoluzione dei problemi possono essere utili quando si utilizza un certificato digitale.

Problema	**Possibile soluzione**
La finestra del passphrase UVM o la finestra di autenticazione delle impronte digitali viene visualizzata più volte durante una richiesta del certificato digitale.	**Azione**
La politica di sicurezza UVM indica che un utente fornisce il passphrase UVM o le impronte digitali prima di poter acquistato un certificato digitale. Se l'utente tenta di acquistare un certificato, la finestra di autenticazione richiede che la scansione delle impronte digitali o il passphrase UVM viene visualizzata più di una volta.	Inserire il passphrase UVM oppure eseguire la scansione delle impronte digitali ogni volta in cui viene visualizzata la finestra di autenticazione.

Problema	Possibile soluzione
Viene visualizzato un messaggio di errore VBScript o JavaScript	**Azione**
Se si richiede un certificato digitale, è possibile che sia un messaggio di errore relativo a VBScript o JavaScript.	Riavviare il computer e reperire di nuovo il certificato.

Informazioni sulla risoluzione dei problemi di Tivoli Access Manager

Le seguenti informazioni sulla risoluzione dei problemi potrebbero essere utili se si verificano problemi durante l'utilizzo di Tivoli Access Manager con Client Security Software.

Problema	Possibile soluzione
Le impostazioni sulla politica locali non corrispondono a quelle sul server	**Azione**
Tivoli Access Manager consente alcune configurazioni non supportate da UVM. Di conseguenza, i requisiti sulla politica locali possono ignorare le impostazioni del responsabile durante la configurazione del server PD.	Si tratta di un limite conosciuto.
Le impostazioni di Tivoli Access Manager non sono accessibili.	**Azione**
Le impostazioni di Tivoli Access e della cache locale non sono accessibili dalla pagina relativa in Administrator Utility.	Installare Tivoli Access runtime Environment. Se Runtime Environment non è installato sul client IBM, le impostazioni di Tivoli Access sulla pagina relativa non saranno disponibili.
Il controllo utente è valido sia per l'utente che per il gruppo	**Azione**
Quando viene configurato il server di Tivoli Access, se si definisce l'utente di un gruppo, il controllo utente è valido sia per l'utente che per il gruppo.	Non è richiesta alcuna azione.

Informazioni sulla risoluzione dei problemi relativi a Lotus Notes

Le seguenti informazioni sulla risoluzione dei problemi possono essere utili quando si utilizza Lotus Notes con il programma Client Security Software.

Problema	Possibile soluzione
Dopo l'abilitazione della protezione UVM per Lotus Notes, Notes non è in grado di terminare l'installazione	**Azione**
Lotus Notes non è in grado di terminare l'installazione dopo che viene abilitata la protezione UVM utilizzando il programma Administrator Utility.	Si tratta di un limite conosciuto. E' necessario che Lotus Notes sia configurato e sia in esecuzione prima che sia abilitato il supporto Lotus Notes nel programma Administrator Utility.

Problema	Possibile soluzione
Un messaggio di errore viene visualizzato quando si tenta di modificare la password di Notes	**Azione**
E' possibile che la modifica della password di Notes durante l'utilizzo del programma Client Security Software visualizzi un messaggio di errore.	Riprovare la modifica della password. Se non funziona, riavviare il client.
Un messaggio di errore viene visualizzato in seguito ad una creazione casuale di una password	**Azione**
E' possibile che un messaggio di errore sia visualizzato quando si procede nel modo seguente: • Utilizzare lo strumento Configurazione di Lotus Notes per impostare la protezione UVM per un ID Notes • Visualizzare Notes ed utilizzare la funzione fornita da Notes per modificare la password per il file ID Notes • Chiudere Notes immediatamente dopo la modifica della password	Fare clic su **OK** per chiudere il messaggio di errore. Non è richiesta ulteriore azione. Diversamente dal messaggio di errore, la password è stata modificata. La nuova password è una password creata in modo casuale dal programma Client Security Software. Il file ID Notes viene cifrato con la password creata in modo casuale e l'utente non necessita di un nuovo file ID utente. Se l'utente modifica di nuovo la password, UVM crea una nuova password casuale per ID Notes.

Informazioni sulla risoluzione dei problemi relativi alla cifratura

le seguenti informazioni sulla risoluzione dei problemi possono risultare utili se si conoscono i problemi quando si cifrano i file utilizzando il programma Client Security Software 3.0 o successive.

Problema	Possibile soluzione
I file cifrati precedentemente non saranno decifrati	**Azione**
I file cifrati con le versioni precedenti del programma Client Security Software non sono cifrati in seguito all'aggiornamento del programma Client Security Software 3.0 o successive.	Si tratta di un limite conosciuto. E' necessario decifrare tutti i file che sono stati cifrati, utilizzando versioni precedenti del programma Client Security Software, *prima* di installare il programma Client Security Software 3.0. Il programma Client Security Software 3.0 non può decifrare i file che sono stati cifrati utilizzando le versioni precedenti del programma Client Security Software a causa delle modifiche contenute nell'implementazione di cifra del file.

Capitolo 6. Installazione driver di periferica hardware di terza parte complementari all'IBM Client Security Software

Con Client Security e le soluzioni di terza parte, è possibile proteggere l'intera infrastruttura integrando le offerte aggiuntive, consentendo di adattare il livello di protezione dell'ambiente di elaborazione.

IBM Embedded Security Subsystem è stato testato in modo da ottemperare alle offerte hardware di autenticazione di sicurezza selezionate da tali organizzazioni:

- Targus per lettori d'impronte
- Gemplus per soluzioni smart card
- Ensure Technologies per proximity badge

Visitare il sito Web con i collegamenti a queste organizzazioni per conoscere meglio le offerte di ogni organizzazione': http://www.pc.ibm.com/us/security/index.html

Come per i componenti che sono parte delle immagini del disco, l'ordine d'installazione è molto importante. Se si prevede di distribuire le periferiche di autenticazione sopra elencate,i driver associati ed altro software, è necessario installare primaIBM Client Security Software. I driver ed il software per queste periferiche non verranno installati correttamente, se CSS non verrà messo sul disco fisso prima dei file del driver di periferica.

Per informazioni specifiche ed aggiornate sull'installazione del software e dei driver che abilitano l'hardware di autenticazione, fare riferimento alla documentazione fornita con le periferiche.

Capitolo 7. Distribuzione in remoto di file di politica della sicurezza nuovi o revisionati

Se si stanno aggiornando le politiche di sicurezza o creando politiche diverse per computer diversi, il responsabile IT con l'autorità di firma può revisionare e distribuire i file di politica. Modificare il file di politica, utilizzando ACAMUCLI.EXE. E' inoltre possibile modificare la politica facendo due volte clic sull'icona dell'IBM Security Subsystem sul Pannello di controllo.)

Firmare il file di politica secondo le istruzioni visualizzate dopo aver fatto clic su Applica. (**Nota:** se la chiave privata del responsabile è stata suddivisa, è necessario che vengano inseriti tutti i componenti per firmare il file di politica.) I file modificati sono GLOBALPOLICY.GVM e GLOBPOLICY.GVM.SIG. Distribuire questi file agli utenti appropriati, accertandosi che vengano salvati nella cartella Security\UVM_Policy.

E' possibile aggiornare le politiche di passphrase in remoto dopo la distribuzione. L'aggiornamento del file di politica di passphrase consente di cambiare i requisiti passphrase quando (o se) l'utente modifica successivamente il passphrase. Il responsabile può stabilire un periodo di tempo, dopo il quale l'utente è obbligato a modificare il passphrase. Questo periodo di tempo viene definito durante l'iscrizione o la registrazione dell'utente. Un esempio: il responsabile iscrive un utente, Jane e la politica iniziale specifica che l'utente Jane deve disporre di una password ad otto caratteri che scadrà ogni 30 giorni. Il responsabile può aggiornare il file di politica e richiedere che la volta successiva che Jane cambia il passphrase, sarà necessario che questa sia composta di 12 caratteri. Il responsabile può inoltre cambiare il periodo di scadenza. Ad esempio, invece di ogni 30 giorni il responsabile può richiedere che Jane cambi le passphrase ogni 15 giorni. Cosa avviene nello scenario seguente. E' il decimo giorno di "vita" del passphrase con scadenza a 30 giorni. Un nuovo file di politica viene inviato al computer client che specifica che è necessario che il passphrase venga cambiata ogni 15 giorni. Quando scadrà il passphrase in 5 giorni o in 20? Il passphrase scadrà in 20 giorni come specificato dalla politica originale. la politica di scadenza passphrase diviene effettiva al momento dell'impostazione delil passphrase. La politica di modifica a 15 giorni di scadenza inizierà quando Jane cambierà il passphrase dopo i 20 giorni

Se si desidera modificare le caratteristiche richieste del passphrase, seguire le istruzioni sopra descritte. Quindi distribuire i file seguenti dalla cartella SECURITY\UVM_POLICY: UVM_PP_POLICY.DAT and UVM_PP_POLICY.DAT.SIG.

Appendice. Informazioni particolari

I riferimenti contenuti in questa pubblicazione relativi a prodotti o serviziIBM non implicano che l'IBM intenda renderli disponibili in tutti i paesi in cui opera. Consultare il rappresentante IBM locale per le informazioni relative ai prodotti ed ai servizi disponibili al momento nel proprio paese. Qualsiasi riferimento a prodotti,programmi o servizi IBM, non implica che possano essere utilizzati solo tali prodotti programmi o servizi IBM. In sostituzione a quelli forniti dall'IBM possono essere utilizzati prodotti, programmi o servizi funzionalmente equivalenti che non comportino violazione dei diritti di proprietà intellettuale dell'IBM. Tuttavia, è responsabilità dell'utente' valutare e verificare la possibilità di utilizzare altri programmi e/o prodotti non forniti dall'IBM.

IBM può avere brevetti o domande di brevetto in corso relativi a quanto trattato nel presente documento. La fornitura di questa pubblicazione non implica la concessione di alcuna licenza su di essi. Coloro che desiderassero ricevere informazioni relative alle licenze, potranno rivolgersi per iscritto a:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

L'INTERNATIONAL BUSINESS MACHINES CORPORATION FORNISCE QUESTA PUBBLICAZIONE "NELLO STATO IN CUI SI TROVA" SENZA ALCUNA GARANZIA ESPLICITA O IMPLICITA, IVI INCLUSE EVENTUALI GARANZIE DI COMMERCIABILITA' ED IDONEITA' AD UNO SCOPO PARTICOLARE. Alcuni stati non consentono la rinuncia a garanzie esplicite o implicite in determinate transazioni; quindi la presente dichiarazione potrebbe non essere a voi applicabile.

Questa pubblicazione potrebbe contenere imprecisioni tecniche o errori tipografici. Le informazioni incluse in questo documento vengono modificate periodicamente; tali modifiche verranno integrate nelle nuove edizioni della pubblicazione. L'IBM si riserva il diritto di apportare miglioramenti e/o modifiche al prodotto e/o al programma descritto nel manuale in qualsiasi momento e senza preavviso.

I prodotti descritti in questo documento non sono intesi per essere utilizzati in implantologia o per altri dispositivi di supporto alla vita dove un cattivo funzionamento possa apportare danni o la morte. Le informazioni contenute in questo documento non riguardano o modificano le specifiche o le garanzie dei prodotti dell'IBM. Niente in questo documento potrÓ essere considerato una licenza esplicita o implicita o un'indennitÓ per le violazioni di diritti di proprietÓ intellettuale diIBM o terze parti. Tutte le informazioni contenute in questo documento sono state ottenute in ambienti specifici e sono presentate come illustrazioni. Il risultato ottenuto in altri ambienti operativi può variare.

L'IBM si riserva di utilizzare e distribuire le informazioni fornite dagli utenti a propria discrezione senza incorrere in alcun obbligo legale.

Siti web diversi dall'IBM

Tutti i riferimenti a siti web non appartenenti all'IBM, contenuti in questa pubblicazione, sono forniti per consultazione; per essi, l'IBM, non fornisce alcuna garanzia. Imateriali disponibili in questi siti Web non fanno parte di questo prodotto IBM e l'utilizzo di questi è a discrezione dell'utente.

Marchi

I seguenti termini sono marchi della International Business Machines Corporation.
IBM
ThinkPad
ThinkCentre
Tivoli

Microsoft, Windows e Windows NT sono marchi della Microsoft Corporation negli Stati Uniti e/o negli altri paesi.

I nomi di altre società, prodotti e servizi potrebbero essere marchi di altre società.