# IBM Client Security Software - Guida alla distribuzione
# Versione 5.4.0

*Aggiornata: 18 novembre 2004*

**Quarta edizione (ottobre 2004)**

# Prefazione

E' necessario che i responsabili IT comprendano e pianifichino i numerosi fattori relativi alla distribuzione dell'IBM Client Security Software. Questa guida non intende illustrare il modo in cui utilizzare Embedded Security Subsystem Chip o Client Security Software, ma il modo in cui distribuire il software su elaboratori che dispongono di Embedded Security Chip all'interno di un'azienda.

## A chi è rivolto questo manuale

Questo manuale è rivolto ai responsabili IT o ai responsabili della distribuzione di IBM Client Security Software versione 5.4 (CSS) sugli elaboratori dell'azienda. Questo manuale fornisce le informazioni richieste per l'installazione di IBM Client Security Software su uno o più elaboratori. Consultare il manuale *IBM Client Security Software versione 5.4 - Guida per l'utente e del responsabile* come prerequisito prima di leggere questo manuale. La IBM fornisce il manuale *IBM Client Security Software versione 5.4 - Guida per l'utente e del responsabile* e le guide delle applicazioni da consultare per informazioni sull'utilizzo dell'applicazione.

## Pubblicazioni del prodotto

I seguenti documenti sono disponibili nella libreria di Client Security Software versione 5.4:

- *Client Security Software versione 5.4 - Guida per l'utente e del responsabile*,

  Questo manuale contiene informazioni sulla configurazione e l'utilizzo delle funzioni di Client Security Software e sull'esecuzione di attività con Client Security Software, come ad esempio la protezione del collegamento UVM, la configurazione dello screen saver di Client Security, la creazione di un certificato digitale e l'utilizzo di User Configuration Utility.
- *Client Security Software Versione 5.4 - Guida all'installazione*,

  Contiene le informazioni sull'installazione di Client Security Software su PC di rete IBM contenenti IBM embedded security chip.

## Ulteriori informazioni

E' possibile ottenere ulteriori informazioni e aggiornamenti per la protezione dei prodotti, se disponibili, visitando il sito web IBM all'indirizzo http://www.pc.ibm.com/us/security/index.html.

# Indice

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

La distribuzione centrale di IBM Client Security Software versione 5.4.0 viene effettuata mediante il modo di configurazione avanzata della procedura guidata alla configurazione di IBM Client Security Software. IBM Client Security Software versione 5.4 non supporta i security chip di prima generazione (non TCPA). Pertanto, è necessario utilizzare Client Security Software versione 5.3.

Esistono vari modi per distribuire IBM Client Security Software (CSS), che utilizza l'hardware IBM Embedded Security Subsystem (ESS) 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 costituito essenzialmente da due parti, come illustrato nella Figura 1:

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

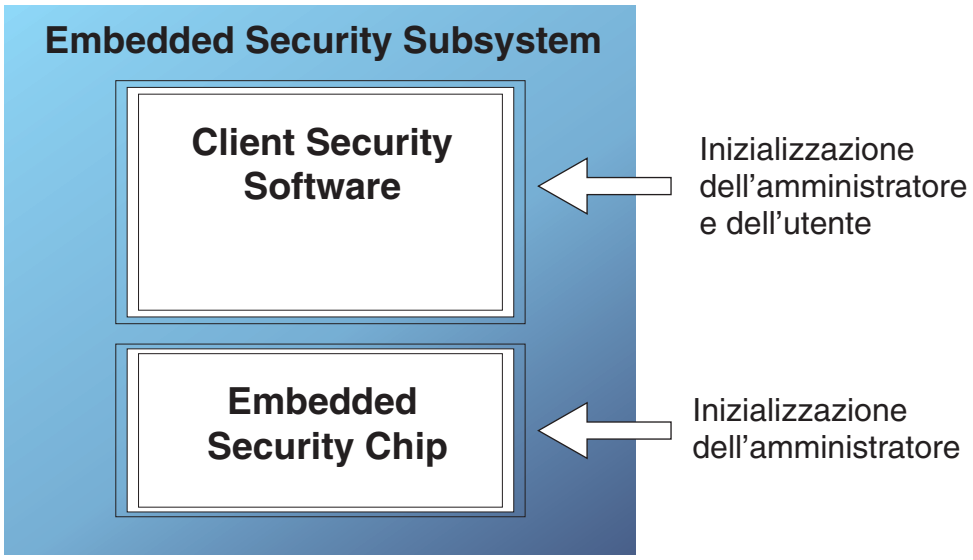


*Figura 1. Componenti di IBM Client Security System*

## Requisiti e specifiche per la distribuzione

Se si pianifica di installare IBM Client Security Software su elaboratori che dispongono di Embedded Security chip, organizzare lo spazio di memorizzazione sul server, i tempi di installazione e i requisiti.

1. PC IBM PC con 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. Installazione di Client Security Software

Questo capitolo illustra due modi diversi per installare Client Security Software, ovvero l'installazione standard e l'installazione amministrativa.

## Installazione standard

Il file z046zis2018usaa.exe è un pacchetto di installazione estraibile automaticamente che estrae i file di origine di installazione avviandola. Questo file accetta una serie di parametri della riga comandi, descritti di seguito. Le opzioni della riga comandi che richiedono un parametro devono essere specificate senza alcuno spazio tra l'opzione ed il relativo parametro. Ad esempio, `z046zis2018usaa.exe /s /v"/qn REBOOT="R""` è valido, mentre `Setup.exe /s /v "/qn REBOOT="R""` non lo è (**"/qn REBOOT="R""** è un parametro dell'opzione **/v**. I doppi apici che racchiudono il parametro dell'opzione sono richiesti solo se il parametro contiene degli spazi.

Il comportamento predefinito dell'installazione quando viene eseguito Setup.exe senza alcun parametro, che esegue l'installazione con un'interfaccia utente, è di richiedere un riavvio alla fine dell'installazione. Il comportamento predefinito quando si esegue l'installazione senza interfaccia utente è di riavviare alla fine dell'installazione. Tuttavia, il riavvio può essere differito con la proprietà REBOOT, come illustrato in precedenza e nella sezione degli esempi.

**/a** Questo parametro consente al file eseguibile di eseguire un'installazione amministrativa. Un'installazione amministrativa copia i file di dati in una directory specificata dall'utente, ma non crea collegamenti, registra i server COM o crea un log di disinstallazione.

**/x** Questo parametro consente al file eseguibile di disinstallare un prodotto installato in precedenza.

**/s Silent mode**
Questo parametro consente al file eseguibile di eseguire un'installazione non presidiata.

**/v** Il parametro **/v** viene utilizzato per passare commutazioni della riga comandi e valori di proprietà pubbliche attraverso Msiexec.exe.

**/w** Questo parametro forza il file eseguibile ad attendere prima di uscire fino a quando l'installazione non viene completata. Se si utilizza questo parametro in un file di batch, è probabile che si desideri inserire prima dell'argomento della riga comandi del file eseguibile il parametro `start /WAIT`. Di seguito viene riportato un esempio del formato corretto di questo utilizzo:

```
start /WAIT z046zis2018usaa.exe /w
```

## Installazione amministrativa

Il programma di utilità Microsoft Windows Installer consente di eseguire un'installazione amministrativa di un'applicazione o prodotto in rete per l'utilizzo da parte di un gruppo di lavoro o per scopi di personalizzazione. Per il pacchetto di installazione di Client Security Software, l'installazione amministrativa estrae il pacchetto dei file di origine di installazione in una posizione specificata. Per eseguire un'installazione amministrativa, è necessario che il pacchetto di installazione sia eseguito dalla riga comandi utilizzando il parametro **/a**:

```
z046zis2018usaa.exe /a
```

E' possibile indicare una nuova posizione che può comprendere un'unità diversa da C:, come ad esempio altri dischi fissi locali, unità di rete mappate e così via. Inoltre, è possibile creare nuove directory durante questo passo.

Se l'installazione amministrativa viene eseguita in modo non presidiato, è possibile impostare la proprietà pubblica TARGETDIR dalla riga comandi per specificare la posizione di estrazione:

```
Setup.exe /s /v"/qn TARGETDIR=F:\IBMCSS"
```

o

```
msiexec.exe /i "IBM Client Security Software.msi" /qn TARGERDIR=F:\IBMCSS
```

Per eseguire l'installazione da un'origine non estratta dopo l'esecuzione delle personalizzazioni, richiamare msiexec.exe dalla riga comandi. La sezione "Parametri della riga comandi" descrive i parametri della riga comandi disponibili che possono essere utilizzati con msiexec.exe, oltre ad un esempio del modo di utilizzo. Inoltre, è possibile impostare direttamente le proprietà pubbliche richiamando dalla riga comandi msiexec.

## Parametri della riga comandi

**/i** *pacchetto* **o** *prodotto*
: Utilizzare questa sintassi per installare il prodotto:

```
msiexec /i "C:\WindowsFfolder\Profiles\UserName\Personal\MySetups\Othello\Trial
Version\Release\DiskImages\Disk1\productOthello Beta.msi"
```

Il codice del prodotto fa riferimento alla GUID che viene generata automaticamente nella proprietà del codice del prodotto della vista del progetto del prodotto stesso.

**Nota:** L'esempio precedente è stato diviso in due righe solo per motivi di impaginazione. Immettere il comando in una sola riga.

**/a** *pacchetto*
: Il parametro **/a** consente agli utenti con privilegi da responsabile di installare un prodotto in rete.

**/x** *pacchetto* **o** *codice prodotto*
: Questo parametro disinstalla un prodotto.

**/L [i | w | e | a | r | u | c | m | p | v | +]** *logfile*
: Questo parametro specifica il percorso del file di log. I flag di seguito riportati indicano le informazioni da registrare nel file di log:

- **i**
  Registra i messaggi di stato
- **w**
  Registra i messaggi di avviso non irreversibili
- **e**
  Registra qualunque messaggio di errore
- **a**
  Registra l'inizio delle sequenze di azione
- **r**
  Registra record di azioni specifiche

- **u**
  Registra le richieste utente
- **c**
  Registra i parametri dell'interfaccia utente
- **m**
  Registra i messaggi di memoria esaurita
- **p**
  Registra le impostazioni del terminale
- **v**
  Registra le impostazioni di output dettagliato
- **+**
  Viene apposto ad un file esistente
- *****
  E' un carattere globale che consente di registrare tutte le informazioni escluso l'impostazione di output dettagliato.

**/? o /h**
Entrambi i comandi visualizzano le informazioni sul copyright di Windows Installer

**TRANSFORMS**
Utilizzare il parametro della riga comandi TRANSFORMS per specificare le eventuali trasformazioni da applicare al pacchetto di base. La riga comandi che richiama la trasformazione potrebbe essere visualizzata nel modo seguente:

```
msiexec /i "C:\WindowsFolder\Profiles\UserName\Personal\MySetups\Project Name\
Trial Version\My Release-1\DiskImages\Disk1\ProductName.msi"
TRANSFORMS="New Transform 1.mst"
```

Poiché è possibile separare più trasformazioni con punto e virgola, si consiglia di non utilizzare il punto e virgola nel nome della trasformazione, in quanto il programma di utilità Windows Installer non interpreta correttamente il comando.

**Nota:** L'esempio precedente è stato diviso in tre righe solo per motivi di impaginazione. Immettere il comando in una sola riga.

**Proprietà**
E' possibile impostare o modificare tutte le proprietà pubbliche dalla riga comandi. Le proprietà pubbliche sono distinte dalle proprietà private, dal momento che sono scritte in lettere maiuscole. Ad esempio, COMPANYNAME è una proprietà pubblica.

Per impostare una proprietà dalla riga comandi, utilizzare la seguente sintassi: `PROPERTY=VALUE`. Per modificare il valore di *COMPANYNAME*, immettere:

```
msiexec /i "C:\WindowsFolder\Profiles\UserName\Personal\MySetups\Nome progetto\
Trial Version\My Release-1\DiskImages\Disk1\ProductName.msi"
COMPANYNAME="InstallShield"
```

**Nota:** L'esempio precedente è stato diviso in tre righe solo per motivi di impaginazione. Immettere il comando in una sola riga.

## Proprietà pubbliche personalizzate di Client Security Software

Il pacchetto di installazione di Client Security Software contiene una serie di proprietà pubbliche da impostare dalla riga comandi quando viene eseguita l'installazione. Le proprietà pubbliche personalizzate disponibili sono:

**INSTALLPWM**
Viene utilizzato per controllare se Password Manager viene installato durante l'installazione iniziale. Impostato su 1 per installare Password Manager, impostato su 0 per non installare Password Manager. Il valore predefinito è 1.

**CFGFILE**
Questa proprietà può essere utilizzata durante un'installazione non presidiata per specificare la posizione di un file di configurazione. Il file di configurazione può contenere il valore di password per security chip. Ciò consente di completare l'installazione senza interazione dell'utente anche se già esiste una password sul chip. Ad esempio:

```
CFGFILE=C:\csec.ini
```

## Funzioni di installazione di Client Security Software

La funzione di installazione con un solo clic di Client Security Software dispone di due funzioni principali, *Security* (IBM Client Security Software) e *PWManager* (IBM Password Manager). Per impostazione predefinita, sono installate entrambe le funzioni, tuttavia sono disponibile varie opzioni per eseguire l'installazione, in modo che verrà installata solo la funzione Security (viene richiesta la funzione Security, quella PWManager non è richiesta). Se l'utente esegue l'installazione con un'interfaccia utente e IBM Password Manager versione 1.3 o precedente non è già installato, quindi viene visualizzato un pannello che consente di scegliere se installare solo IBM Client Security Software o anche IBM Client Security Software e IBM Password Manager. Se l'utente esegue un'installazione senza interfaccia utente (non presidiata), è possibile controllare se Password Manager viene installato utilizzando la proprietà INSTALLPWM (impostato su 0 per non installare Password Manager). Se l'utente sceglie di installare IBM Client Security solo durante l'installazione iniziale e in seguito decide di aggiungere IBM Password Manager, è possibile eseguire questa operazione eseguendo di nuovo il pacchetto di installazione di origine. Se eseguendo di nuovo l'installazione con un'interfaccia utente, viene visualizzato il pannello di manutenzione in cui è possibile scegliere il pulsante "Modifica" se Password Manager non è stato ancora installato. Quindi, viene visualizzato un pannello in cui è possibile scegliere di reinstallare solo Client Security o modificare la scelta per installare IBM Client Security Software e IBM Password Manager. Inoltre, l'utente può reinstallare il prodotto dall'origine senza interfaccia utente per aggiungere IBM Password Manager. Di seguito sono illustrati i comandi di esempio per effettuare questa operazione.

### Esempi di utilizzo di Setup.exe

La Tabella 1 illustra esempi di installazione utilizzando z046zis2018usaa.exe.

*Tabella 1. Esempi di installazione utilizzando z046zis2018usaa.exe*

| Tipo | Esempio |
|---|---|
| Installazione non presidiata con riavvio alla fine dell'installazione | `z046zis2018usaa.exe /s /v/qn` |
| Installazione non presidiata senza riavvio | `z046zis2018usaa.exe /s /v"/qn REBOOT="R""` |
| Installazione non presidiata senza riavvio e Password Manager non installato | `z046zis2018usaa.exe /s /v"/qn REBOOT="R" INSTALLPWM=0"` |

*Tabella 1. Esempi di installazione utilizzando z046zis2018usaa.exe (Continua)*

| Tipo | Esempio |
|---|---|
| Installazione non presidiata senza riavvio e specifica della directory di installazione | `z046zis2018usaa.exe /s /v"/qn REBOOT="R" INSTALLDIR=C:\ibmcss"` |
| Installazione non presidiata senza riavvio e specifica del file di configurazione | `z046zis2018usaa.exe /s /v"/qn REBOOT="R" CFGFILE=C:\csec.ini"` |
| Installazione amministrativa non presidiata | `z046zis2018usaa.exe /a` |
| Installazione amministrativa non presidiata con la specifica della posizione di estrazione | `z046zis2018usaa.exe /a /s /v"/qn TARGETDIR="F:\CSS""` |
| Installazione senza riavvio e creazione di un log di installazione in una directory temporanea | `z046zis2018usaa.exe /v"REBOOT="R" /L*v %temp%\css.log"` |
| Reinstallazione non presidiata del prodotto per aggiungere Password Manager | `z046zis2018usaa.exe /s /v"/qn ADDLOCAL=PWManager"` |

La Tabella 2 illustra esempi di installazione utilizzando msiexec.exe.

*Tabella 2. Installazione utilizzando msiexec.exe*

| Tipo | Esempio |
|---|---|
| Installazione con il file di log | `msiexec /i "C:\IBM Client Security Software.msi" /L*v %temp%\css.log` |
| Installazione non presidiata senza riavvio | `msiexec /i "C:\IBM Client Security Software.msi" /qn REBOOT="R"` |
| Installazione non presidiata senza riavvio e Password Manager non installato | `msiexec /i "C:\IBM Client Security Software.msi" /qn REBOOT="R" INSTALLPWM=0` |
| Reinstallazione non presidiata del prodotto per aggiungere Password Manager | `msiexec /i "C:\IBM Client Security Software.msi" /qn ADDLOCAL=PWManager` |

# Capitolo 3. ESC (Embedded Security Chip)- Istruzioni

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

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

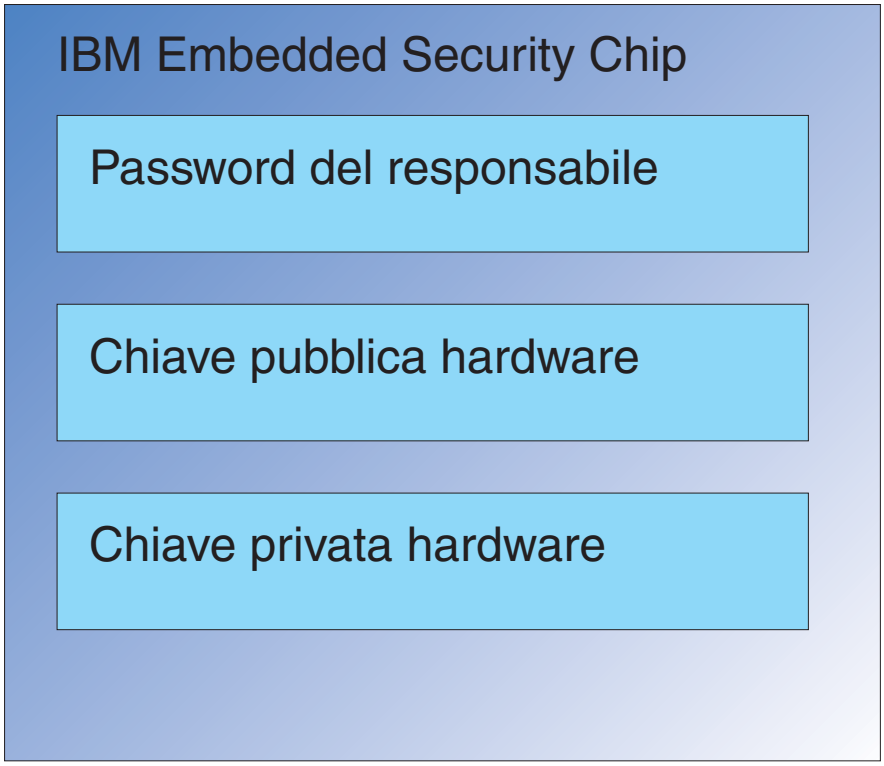


*Figura 2. Dati contenuti nell'ESC (Embedded Security Chip)IBM*

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.

La Figura 3 a pagina 11 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. La Figura 3 a pagina 11 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).

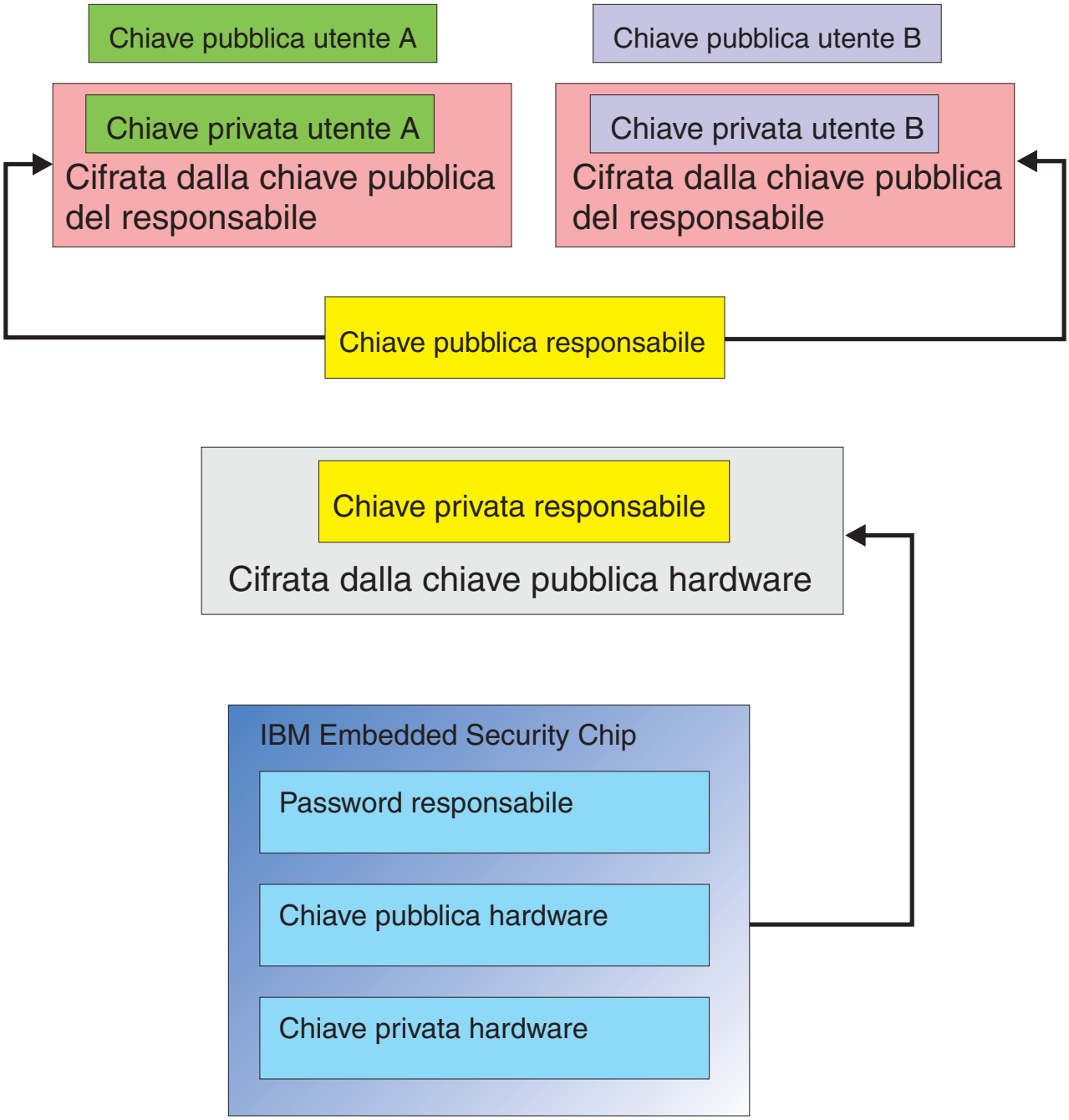


*Figura 3. Vari livelli di cifratura forniscono un alto livello di sicurezza*

## Gerarchia di scambio-chiavi

Parte dell'architettura ESSIBM è composta da una gerarchia di "scambio-chiavi". Informazioni dettagliate sul funzionamento verranno fornite nel manuale *IBM Client Security Software - Guida per l'utente e del responsabile*, tuttavia di seguito è riportata un'introduzione si concetti di applicazione, distribuzione e gestione di una configurazione di massa. 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 utente, descritto nel manuale *IBM Client Security Software - Guida per l'utente e del 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. Nella Figura 3 a pagina 11, 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. Nella Figura 3 a pagina 11, 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 4. Considerazioni sull'archiviazione delle chiavi

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

La Figura 4 mostra il modo in cui IBM Embedded Security Subsystem e Client Security Software funzionano insieme. Il collegamento di Windows richiede all'Utente A di collegarsi e il collegamento viene effettuato. 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.

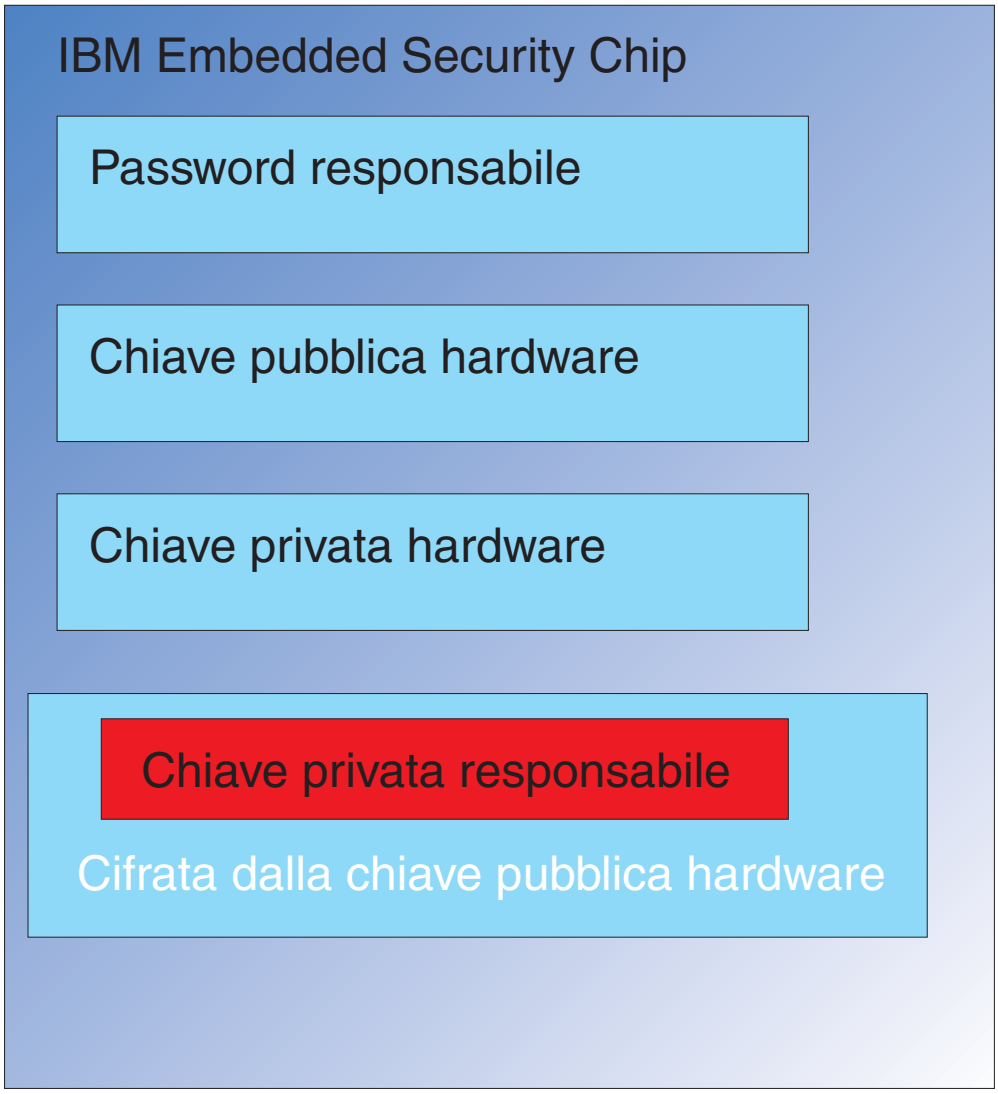


*Figura 4. La chiave privata del responsabile, cifrata dalla chiave hardware pubblica, viene caricata nel chip di Embedded Security.*

La chiave privata hardware (disponibile solo nel chip) decifra la chiave privata del responsabile. Ora, la chiave privata del responsabile è disponibile, come illustrato nella Figura 5.


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

Poiché l'Utente A è collegato all'elaboratore, la relativa chiave privata (cifrata con la chiave pubblica del responsabile) viene passata nel chip come illustrato nella Figura 6 a pagina 15.


*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 nella Figura 7 a pagina 16.

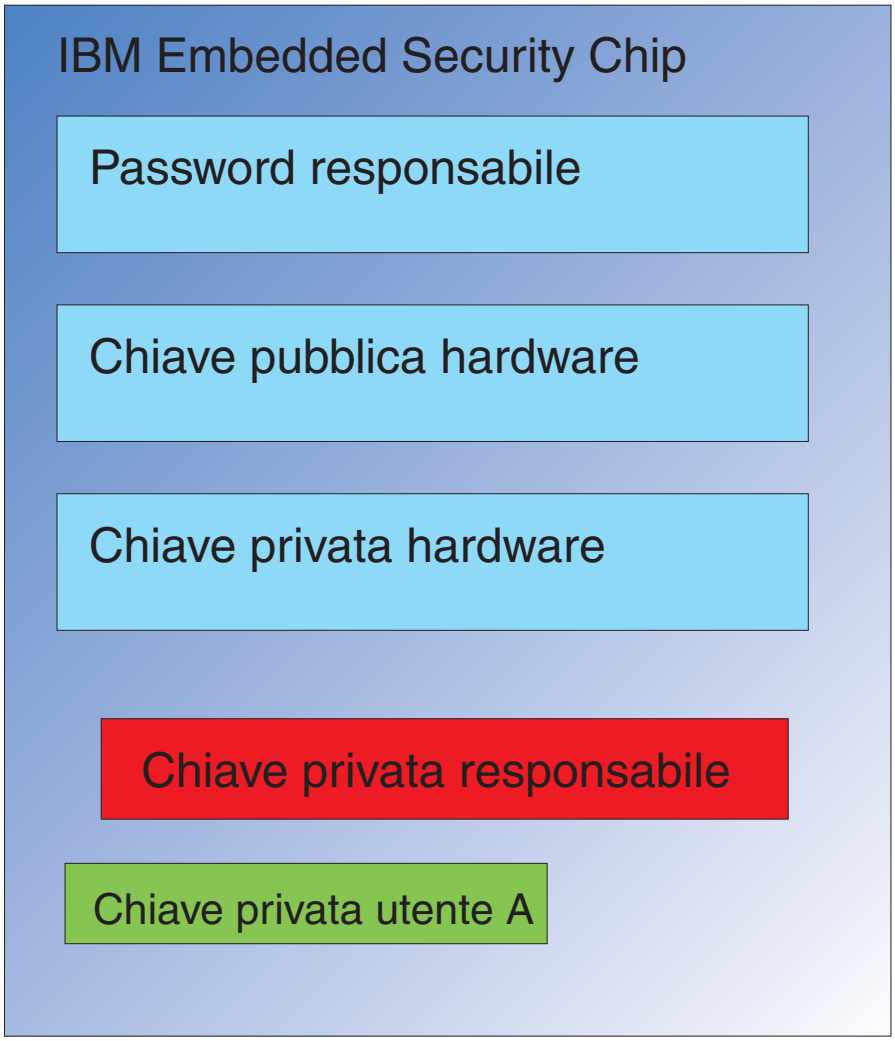


*Figura 7. La chiave privata dell'Utente A' è pronta per essere utilizzata.*

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 nella Figura 8 a pagina 17.

**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.

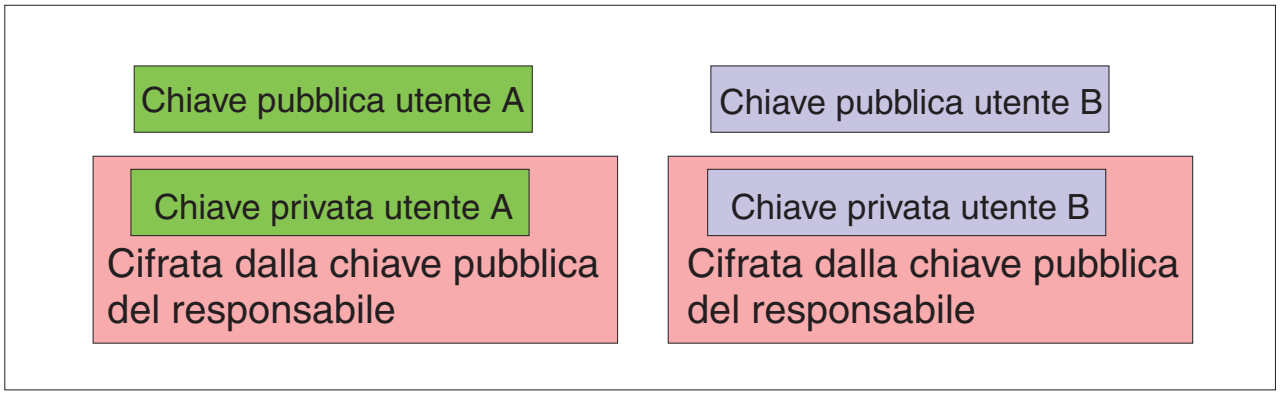


*Figura 8. Le informazioni sulla chiave privata specifica dell'utente vengono cifrate con la chiave pubblica del responsabile.*

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 nella Tabella 6 a pagina 41.

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 nella 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.

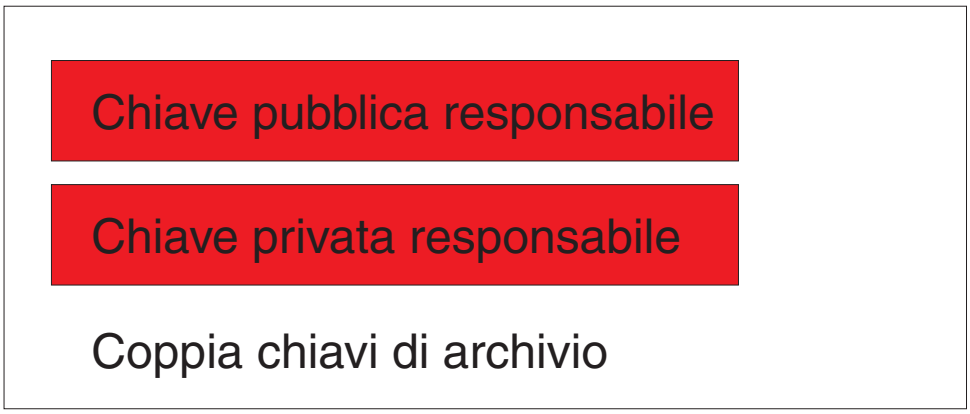


*Figura 9. Le chiavi pubblica e privata del responsabile formano la coppia di chiavi di archivio.*

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 funzione è compresa tra 10 e 15. 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 19.

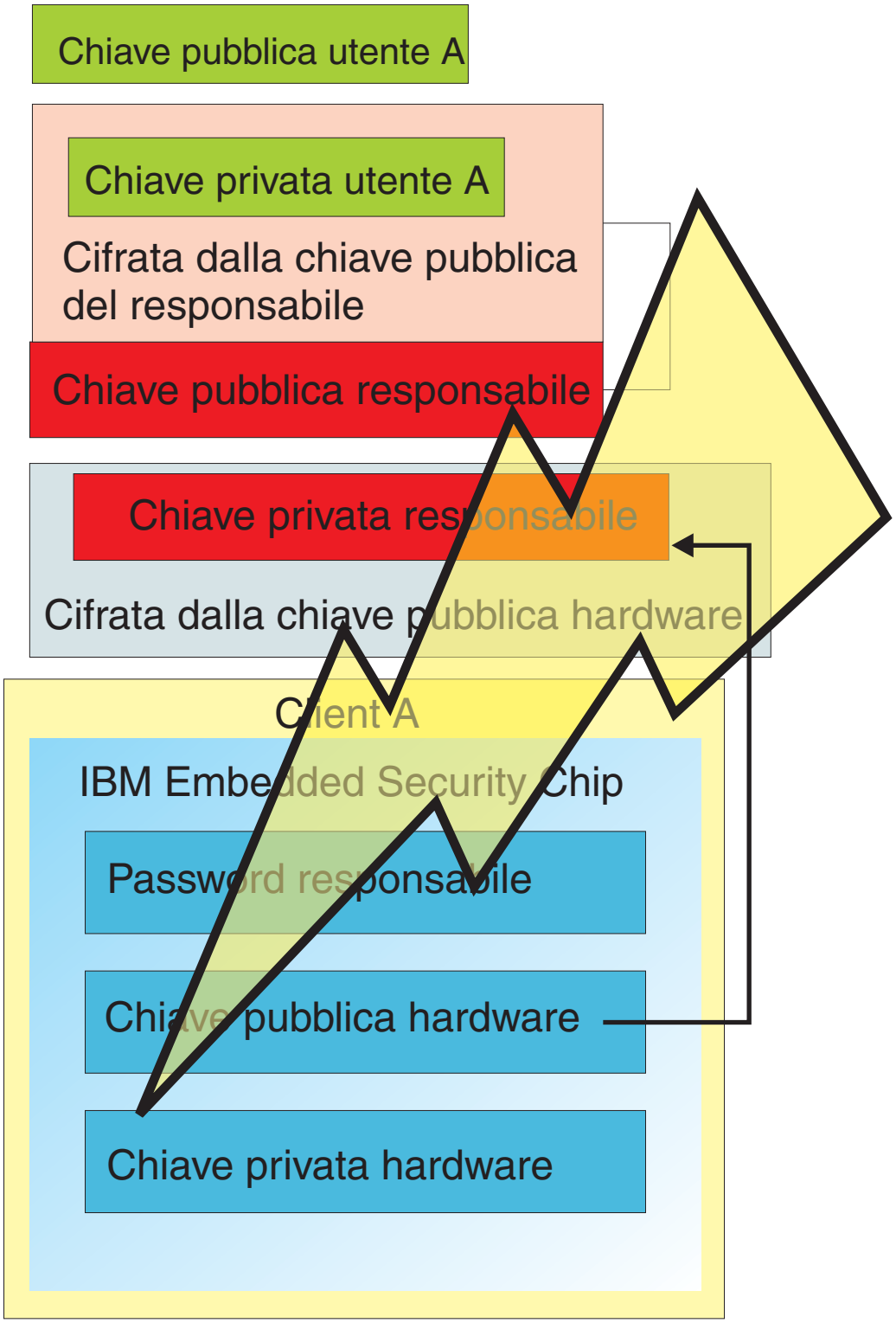


*Figura 10. Il computer dell'Utente A' viene colpito da un fulmine e reso quindi inutilizzabile.*

2. L'Utente A ne utilizza un computer IBM nuovo e più potente, denominato Client B come mostrato nella Figura 11 a pagina 20. 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.

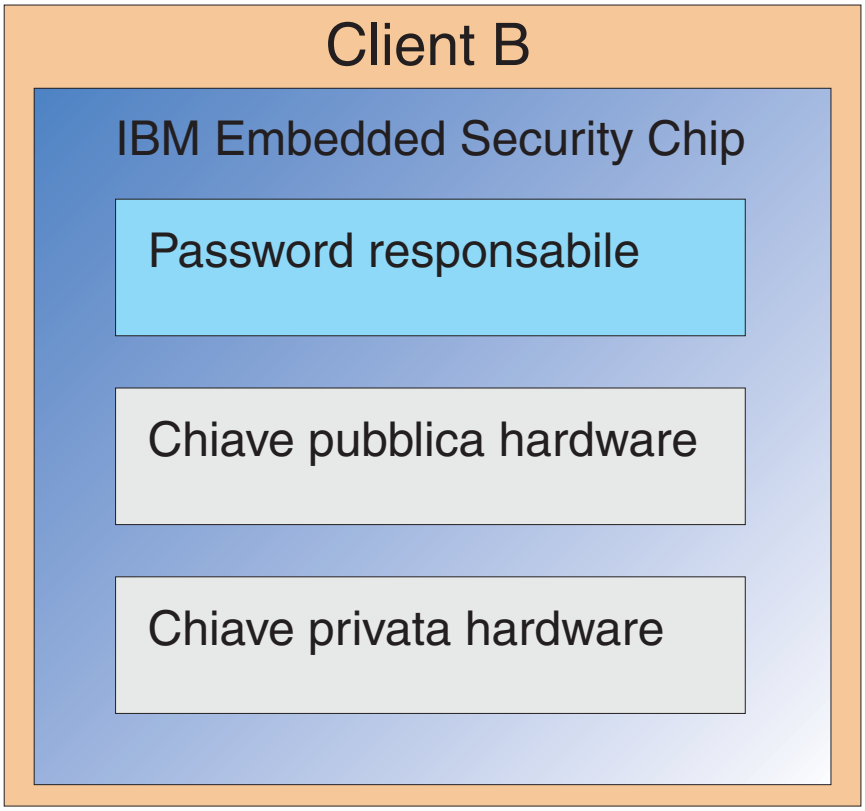


*Figura 11. L'Utente A riceve un computer nuovo, Client B, con un nuovo chip di Embedded Security.*

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 la Figura 8 a pagina 17, 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.

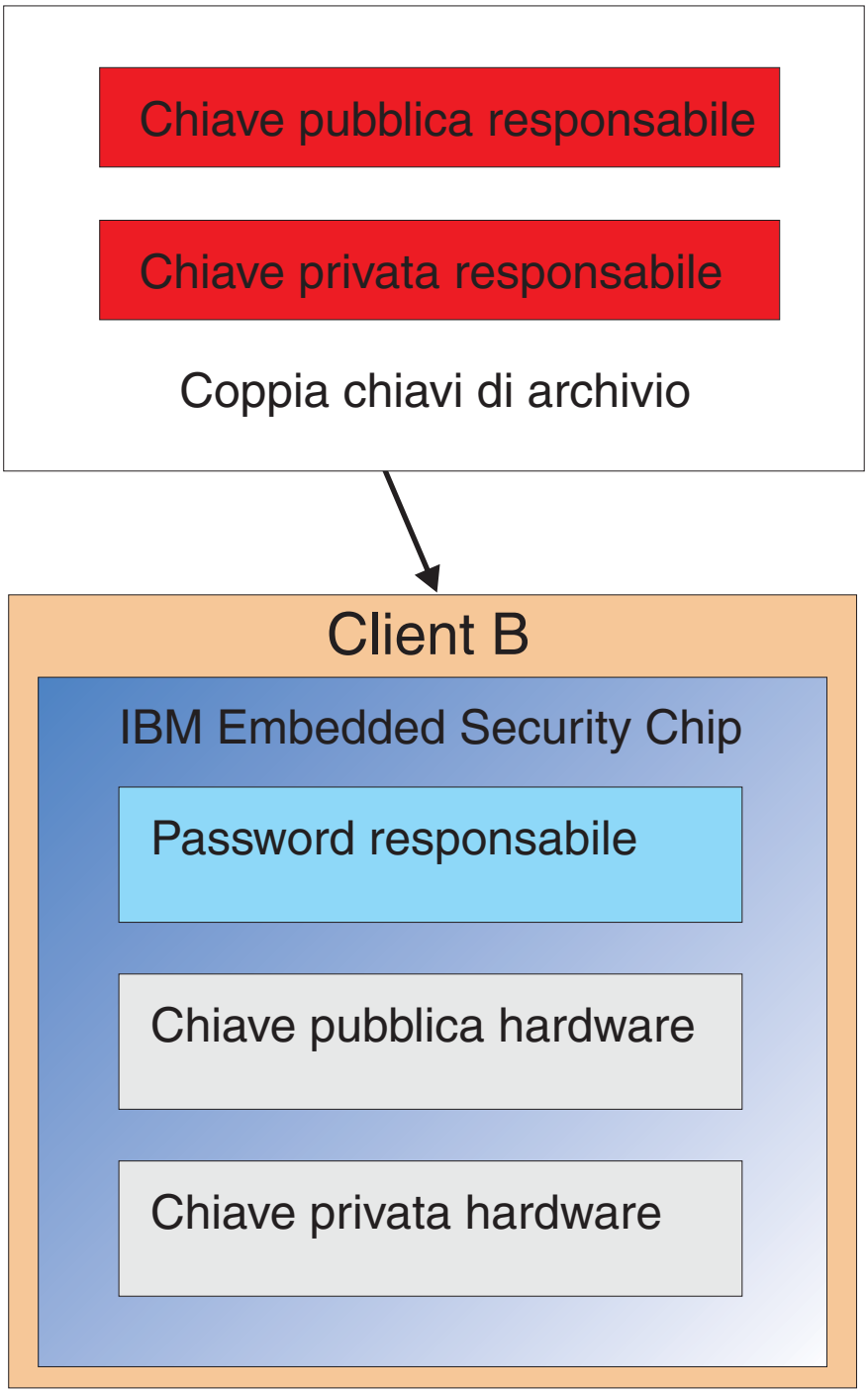


*Figura 12. Il Client B richiama le chiavi pubblica e privata del responsabile dall'ubicazione di archivio.*

4. La Figura 13 a pagina 22 mostra la chiave privata del responsabile che viene cifrata con la chiave hardware pubblica del Client B.

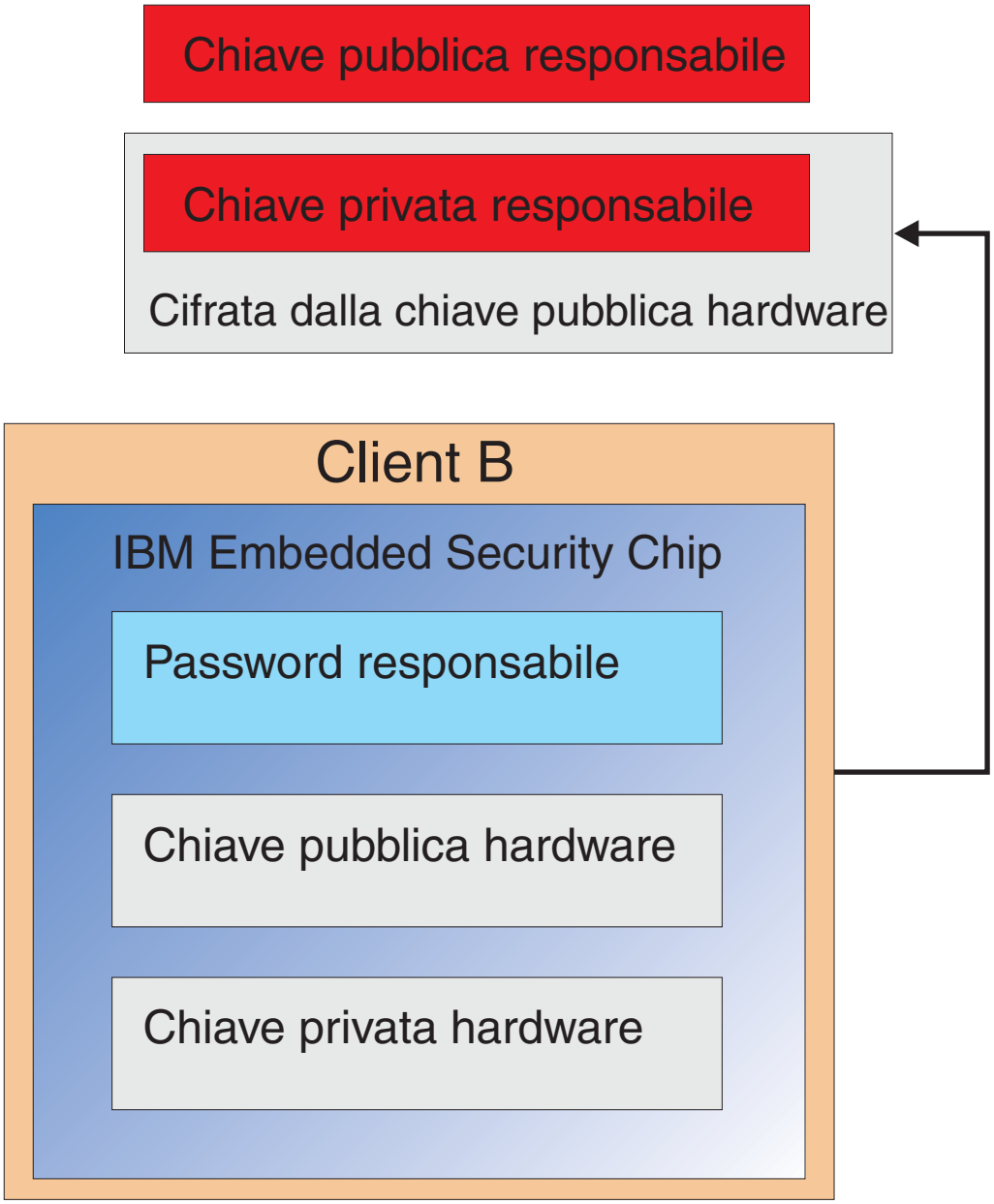


*Figura 13. La chiave privata del responsabile viene cifrata con la chiave hardware del Client B.*

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 nella Figura 14 a pagina 23.

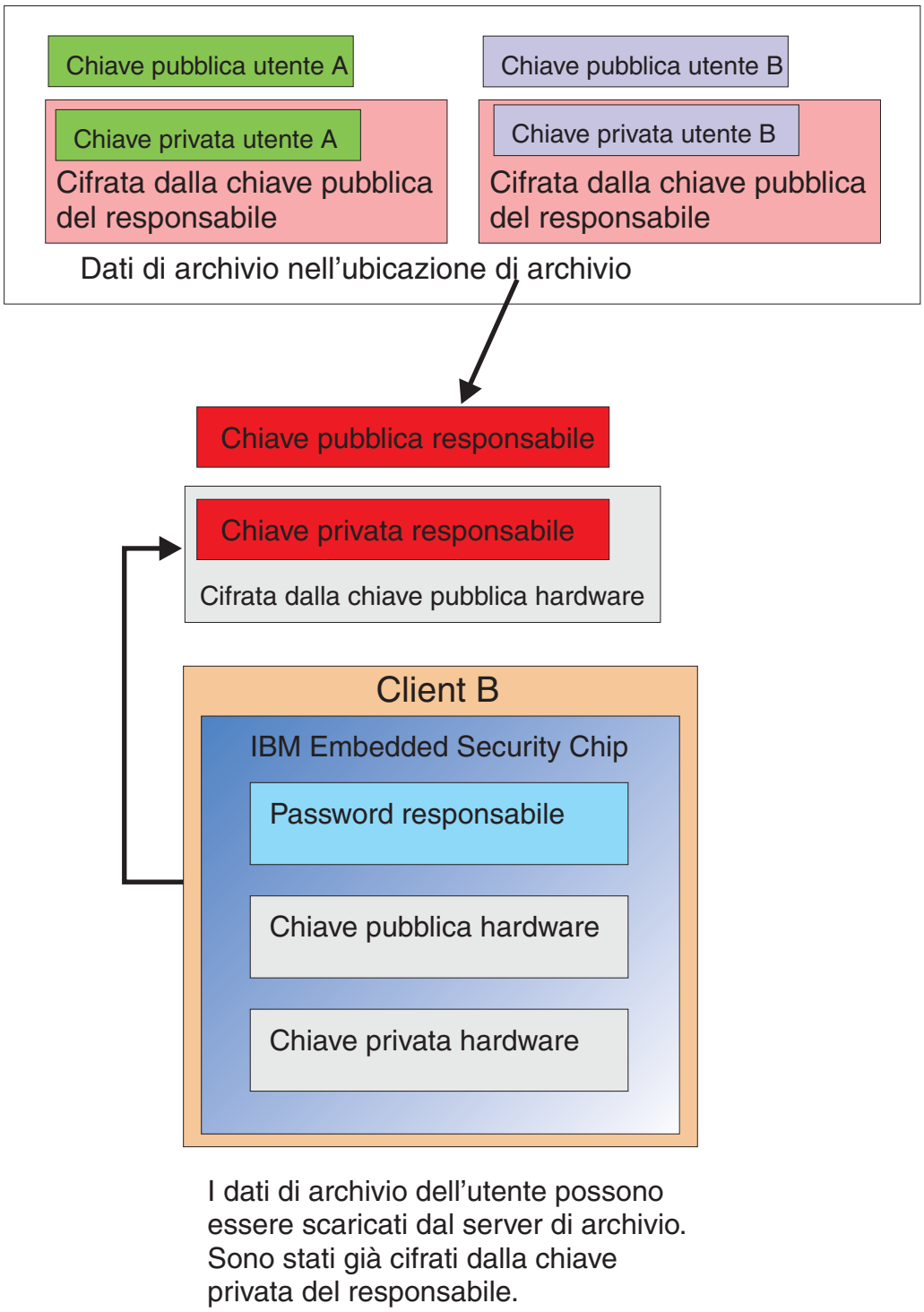


*Figura 14. E' possibile caricare le credenziali dell'Utente' A sul Client B dopo la cifratura della chiave privata del responsabile.*

La Figura 15 a pagina 24 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.

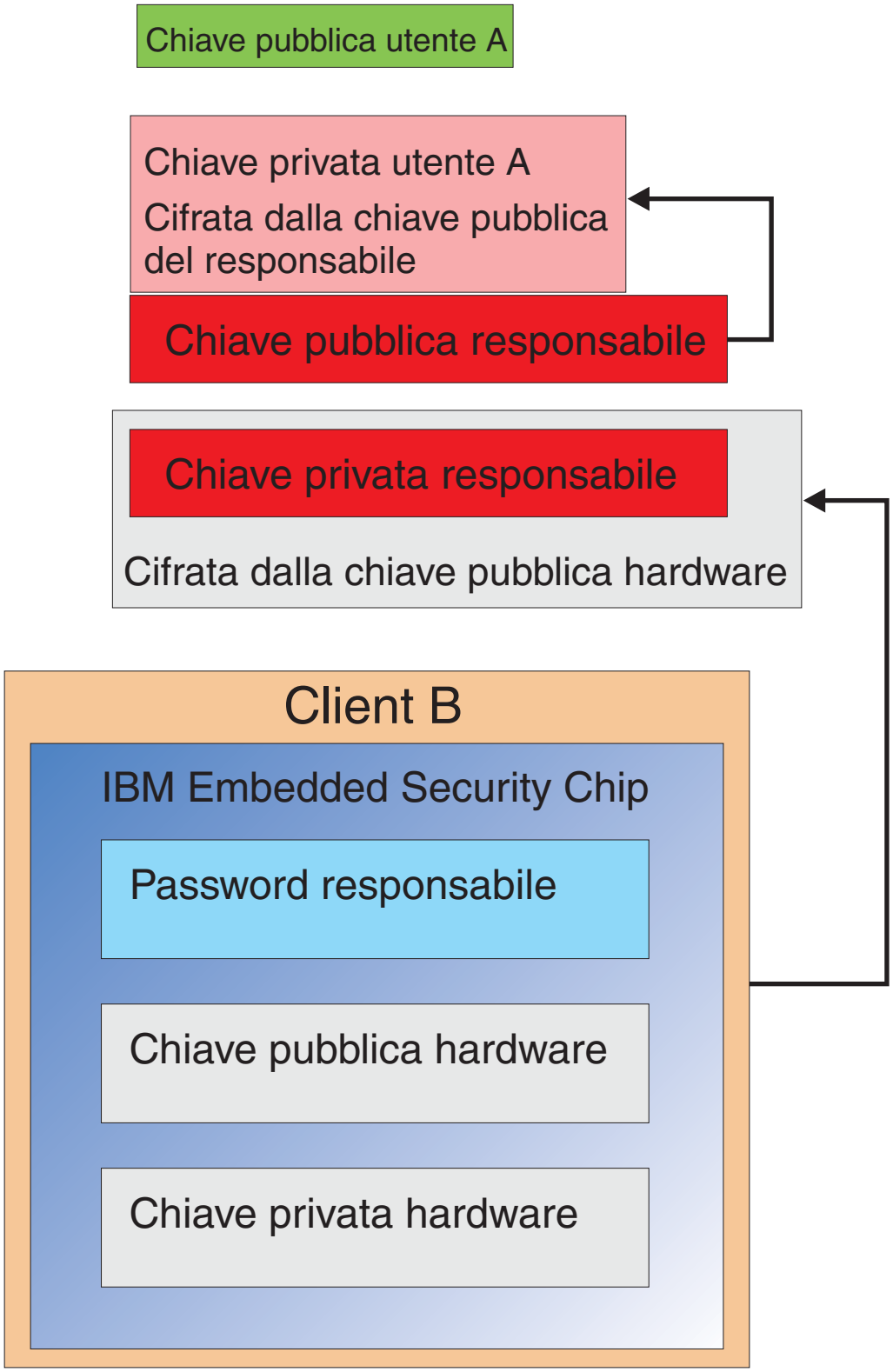


*Figura 15. L'Utente A è completamente ripristinato sul B.*

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.

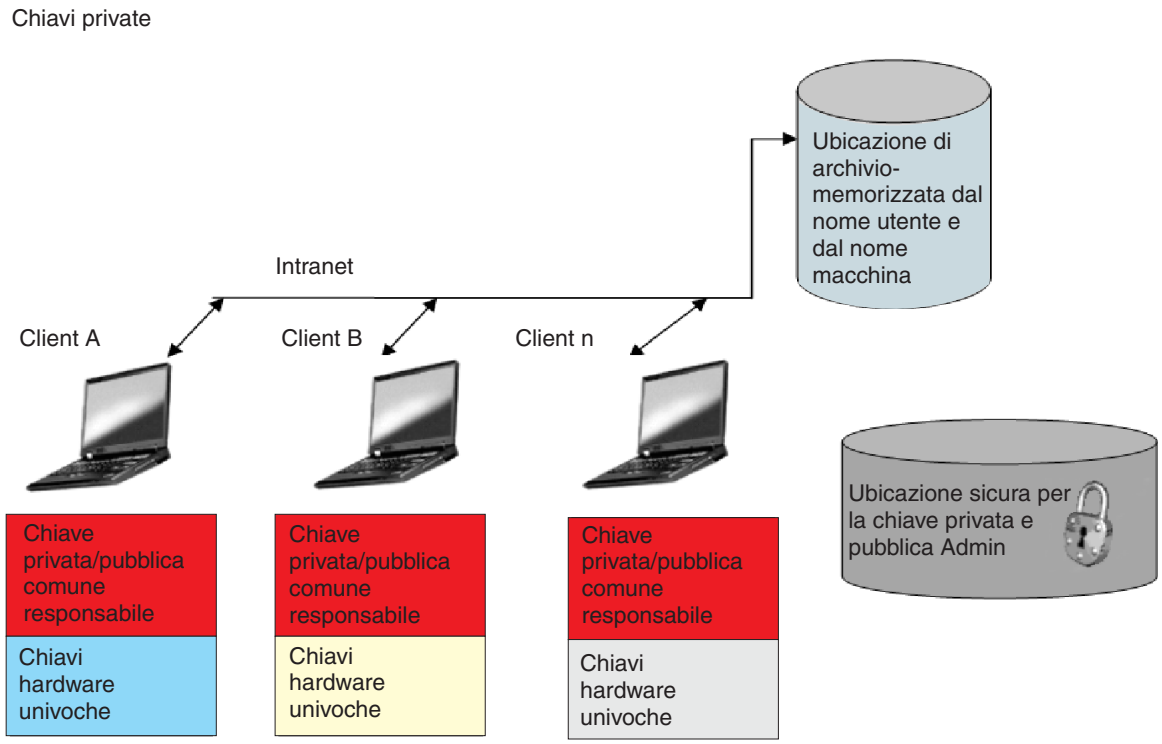


*Figura 16. Componenti principali dell'IBM Client Security System.*

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 5. 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 la passphrase o l'autenticazione delle impronte digitali. Se la persona collegata come Utente A non è in grado di fornire la 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 di IBM ESS sono Windows registrati nell'ambiente di 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 una 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 una passphrase che deve essere inserita come minimo una volta per ogni avvio del computer. Le seguenti sezioni illustreranno il perché viene utilizzato una passphrase, il modo di impostarne una e come utilizzarla.

## Richiesta di una passphrase

Inserire semplicemente, una 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. La passphrase richiesta da IBM ESS viene utilizzato per autenticare un utente prima che venga intrapresa qualsiasi azione con le credenziali dell'utente nell'hardware. La passphrase UVM può essere richiamata solo tramite la coppia di chiavi del responsabile, quindi non può essere recuperato da un sistema in modo illegale.

## Impostazione di una passphrase

Ogni utente seleziona una passphrase per proteggere le proprie credenziali. Nel Capitolo 3, "ESC (Embedded Security Chip)- Istruzioni", a pagina 9, si è visto che una chiave privata utente viene cifrata con la chiave pubblica del responsabile. Anche la chiave privata utente dispone di una passphrase associata. Tale passphrase viene utilizzata per autenticare l'utente con le proprie credenziali. La Figura 17 mostra la passphrase più il componente della chiave privata cifrato con la chiave pubblica del responsabile.

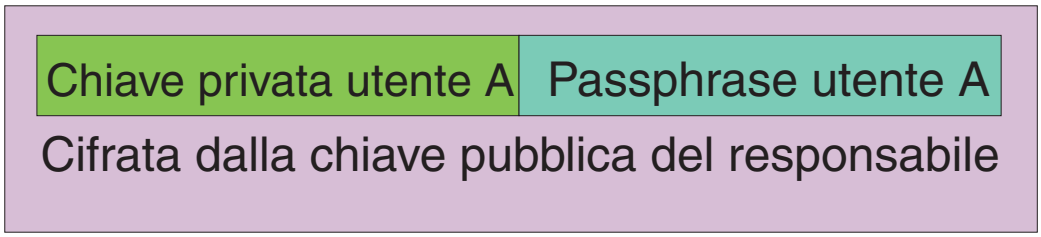


*Figura 17. E' necessario che l'Utente A fornisca la passphrase per eseguire qualsiasi funzione che richieda la chiave privata dell'Utente A'.*

La passphrase illustrata nella Figura 17 viene selezionata 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. La passphrase viene creata 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 la passphrase dell'Utente A, il responsabile può reimpostare una nuova passphrase.

## Utilizzo di una passphrase

La Figura 18 con la Figura 20 a pagina 31, mostra il modo in cui la passphrase dell'utente viene elaborata sul chip. E' sempre necessario utilizzare una passphrase all'inizio ed almeno una volta per sessione. E' sempre richiesta una passphrase. E' possibile scegliere di aggiungere ulteriori periferiche di autenticazione, ma nessuna di esse è in grado di sostituire il requisito della passphrase dell'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.

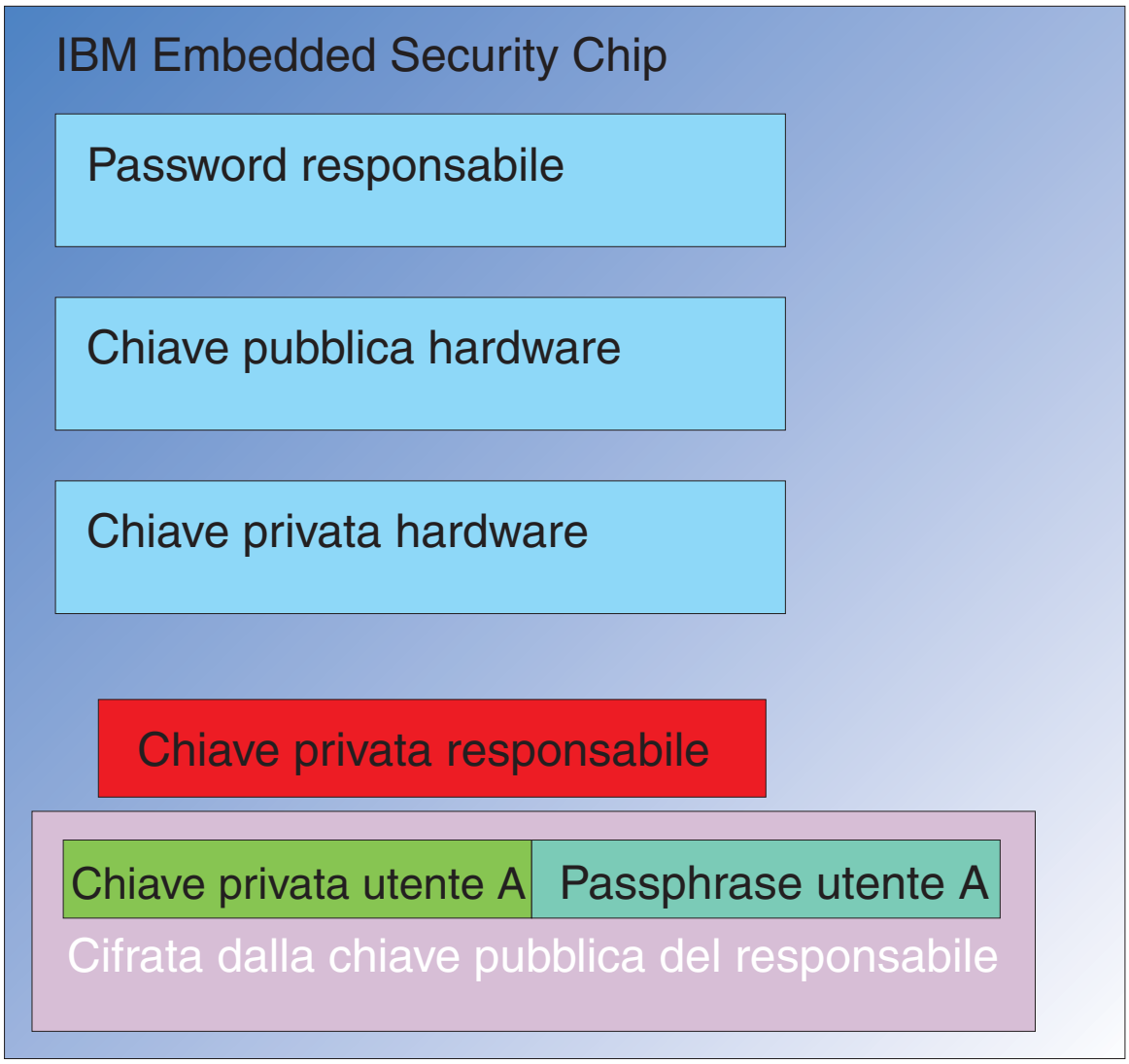


*Figura 18. La chiave privata del responsabile viene decifrata nel chip.*

Perciò, viene richiesto di fornire la passphrase almeno una volta per sessione per decifrare i dati aggiuntivi. Le credenziali che costituiscono la chiave privata e la 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 trasferite come descritto nella Figura 19 a pagina 30.

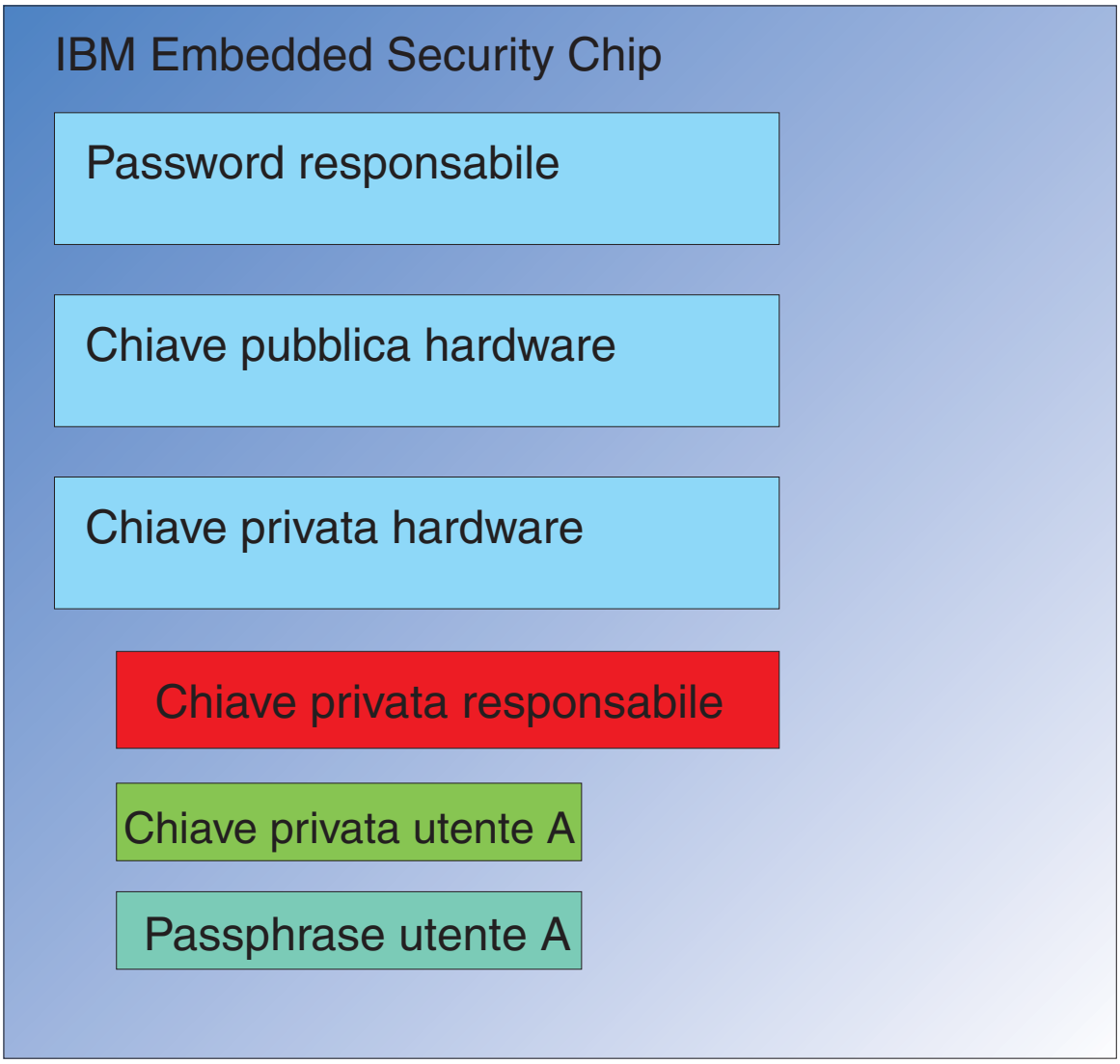


*Figura 19. La chiave privata e la passphrase dell'Utente A sono disponibili nel chip.*

Le credenziali vengono decifrate, rendendo disponibili nel chip sia la chiave privata che la passphrase dell'Utente A. Quando l'utente al momento collegato, identificato da IBM Client Security System come Utente A, tenta di utilizzare le credenziali dell'utente A, viene aperta una finestra di dialogo di richiesta passphrase, come illustrato nella Figura 20 a pagina 31.

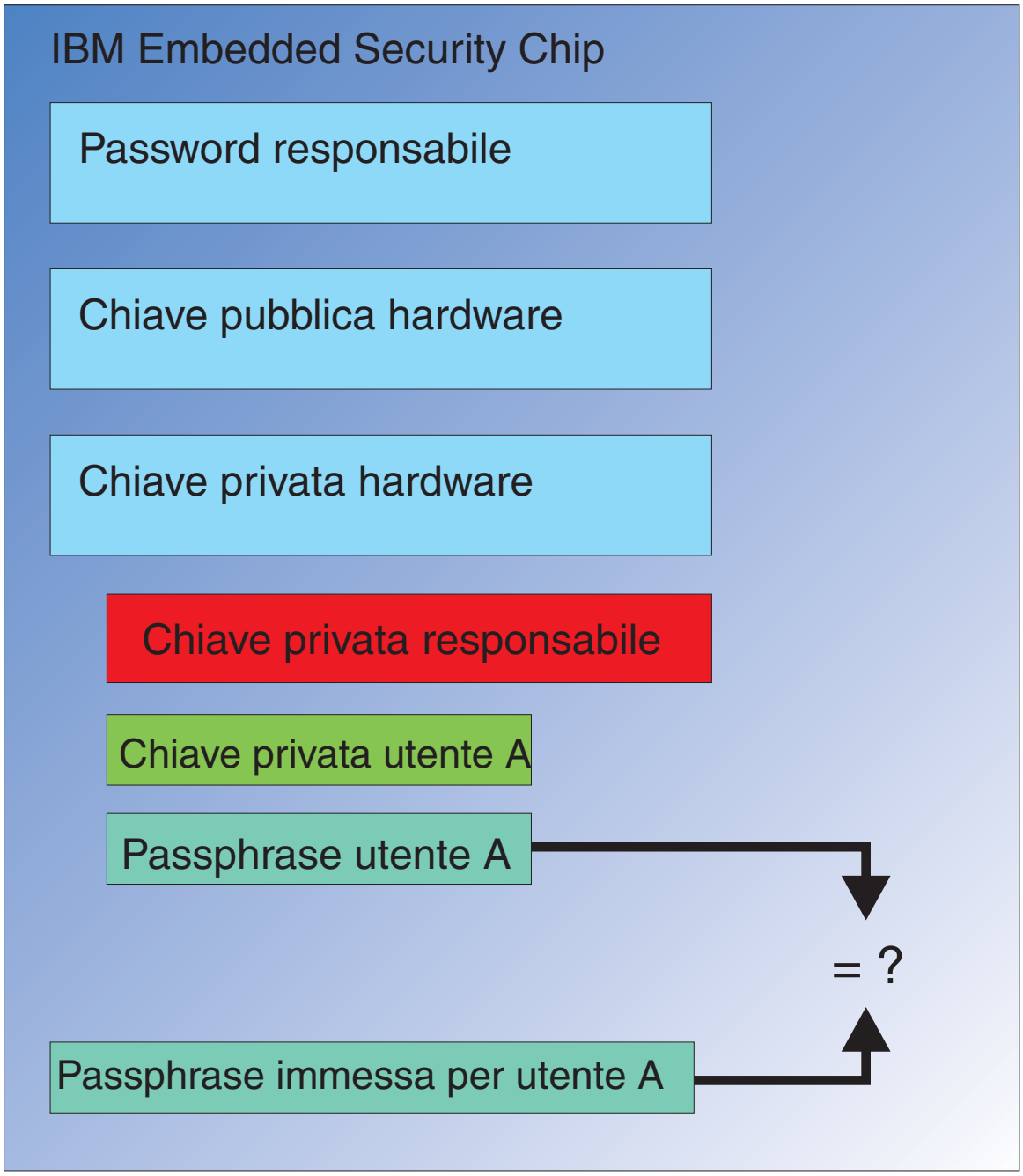


*Figura 20. Quando l'Utente A tenta di utilizzare le credenziali dell'Utente A viene visualizzata una finestra di dialogo passphrase.*

La passphrase immessa viene trasferita al chip e paragonata 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 una passphrase registrata 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 della passphrase dell'utente. Verrà illustrato dettagliatamente il modo in cui impostare questa passphrase e rafforzarne le regole.

La Figura 1 a pagina 1 mostra IBM Embedded Security Chip e IBM Client Security System. La Figura 1 a pagina 1 illustra 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 3. 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 |

La Tabella 3 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. La Tabella 4 riepiloga quanto consentito dalla password del responsabile e/o dalla chiave privata del responsabile.

*Tabella 4. 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 la 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 nella Tabella 3 a pagina 32 e nella Tabella 5 a pagina 36, 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 il Capitolo 8, “Distribuzione in remoto di file di politica della sicurezza nuovi o revisionati”, a pagina 59), 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 di passphrase dimenticate o malfunzionamento delle periferiche di autenticazione

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

**Passphrase dimenticata:** La passphrase utente’ non è memorizzata 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 una nuova passphrase all’utente.

Quando l’utente modifica la 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 la 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 alla 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 la passphrase.
2. Se non viene specificata un’ubicazione per l’archivio e l’ubicazione non è mappata sul computer client, non sarà possibile recuperare le 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 una 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. Nella 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 nella Figura 21, contiene i requisiti di

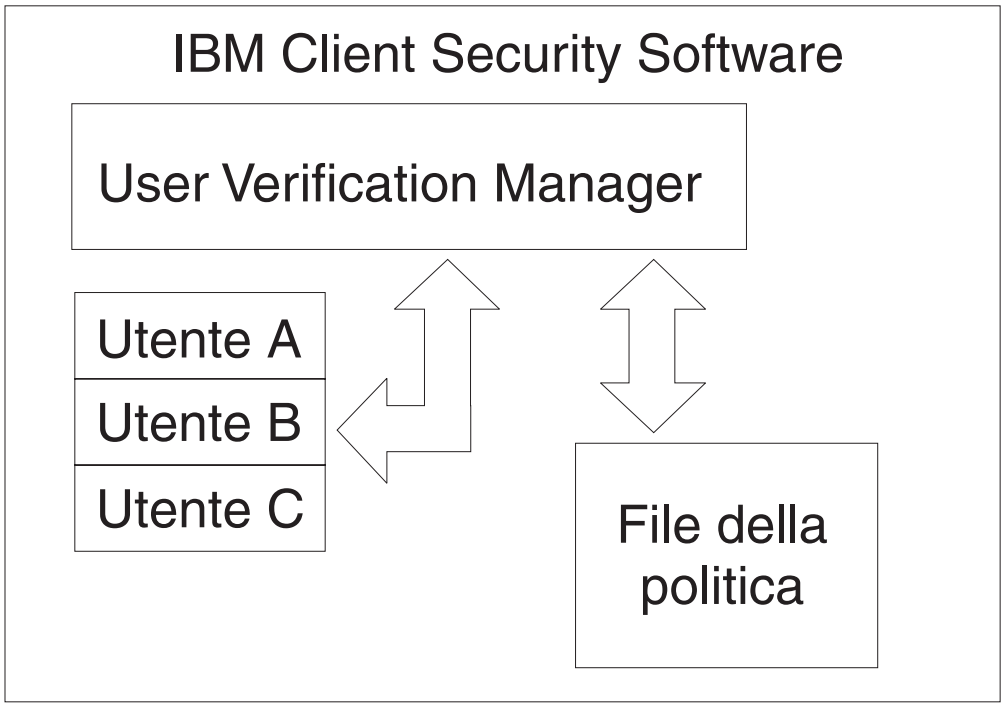


*Figura 21. UVM (User Verification Manager) controlla le credenziali di ciascun utente' ed applica le politiche di sicurezza.*

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 una passphrase deve essere autenticata prima di eseguire l'operazione. UVM richiederà all'utente la 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 una passphrase UVM singola. Le parti distinte del processo possono essere eseguite da persone diverse. La 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 la 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 la passphrase UVM venga associata 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 la passphrase in modo che nessuno possa eseguire transazioni sicure utilizzando la passphrase predefinita.

*Tabella 5. 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 la propria passphrase). Bob riceve il computer, avvia IBM Client Security Software e quindi imposta la 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:

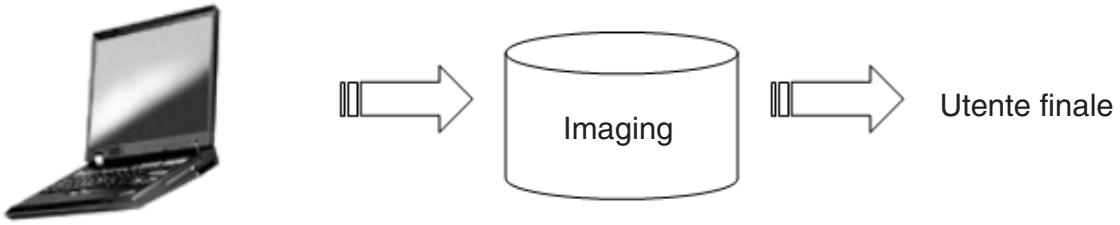


*Figura 22. Diagramma di flusso distribuzione PC tipico*

## 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 la Figura 23 a pagina 38.)
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 39.)
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 la Figura 24 a pagina 39.)
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 la passphrase utente e, se richiesto, fornisca altre informazioni sull'autenticazione come le impronte digitali o l'associazione smartcard. (Consultare la Figura 25 a pagina 40.)
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 la passphrase utente. Se viene richiesta una scansione delle impronte digitali o un'altra autenticazione, è necessario che l'utente fornisca tale personalizzazione. (Consultare la Figura 25 a pagina 40.)

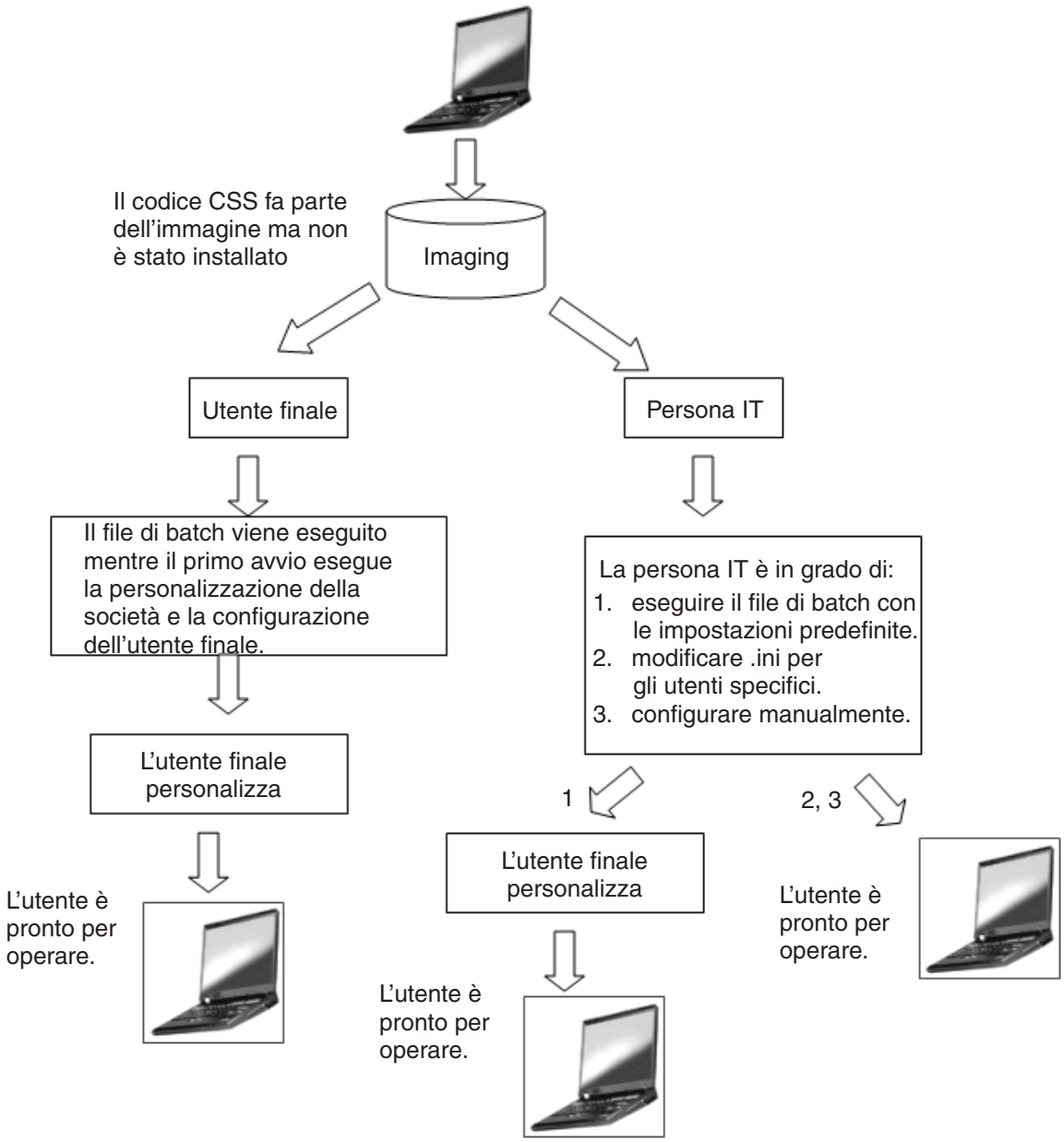


*Figura 23. Il codice dell'IBM Client Security Software è parte dell'immagine, ma non è installato.*

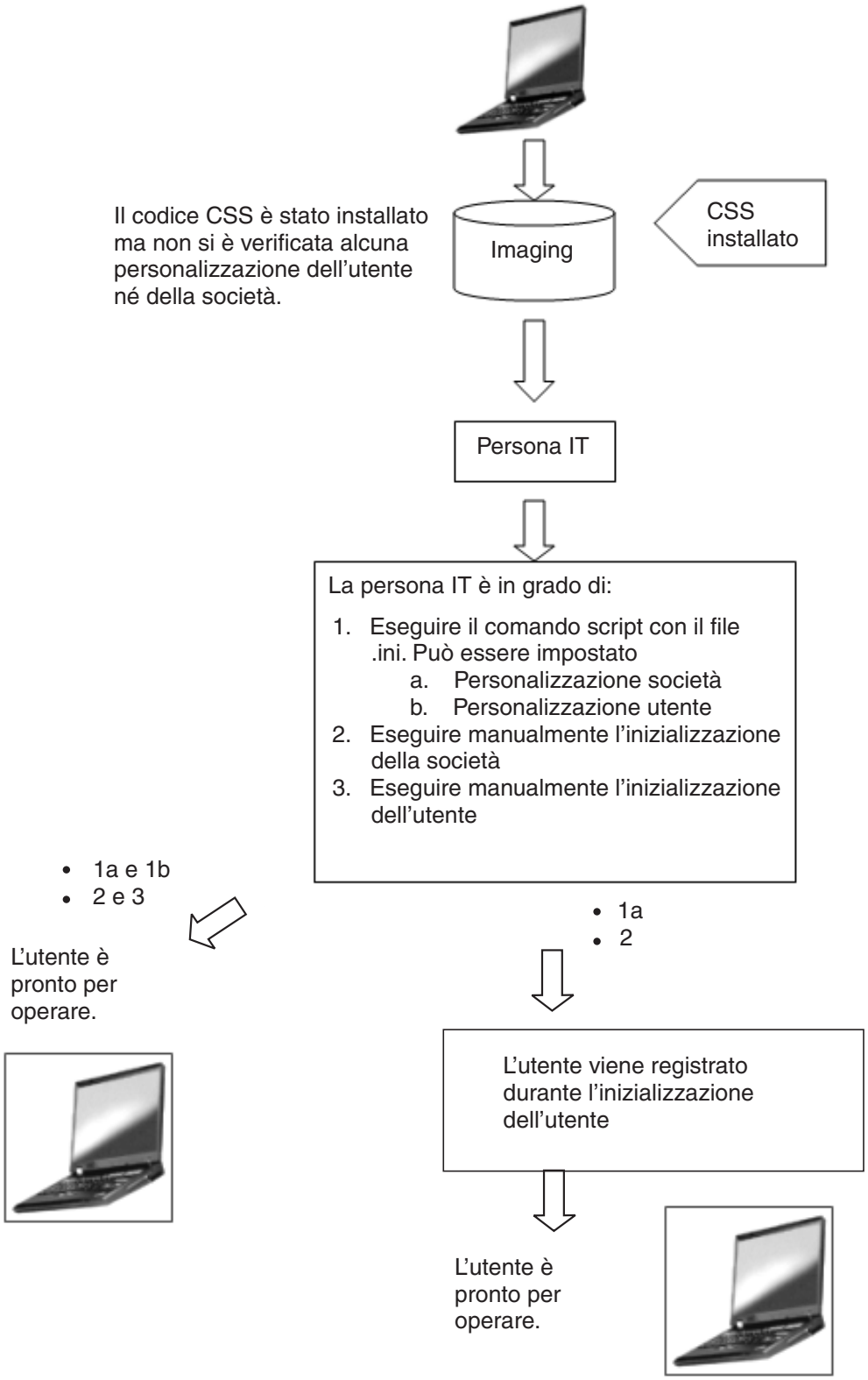


*Figura 24. Il codice dell'IBM Client Security Software è installato ma non si è verificata né la personalizzazione della società né quella dell'utente.*

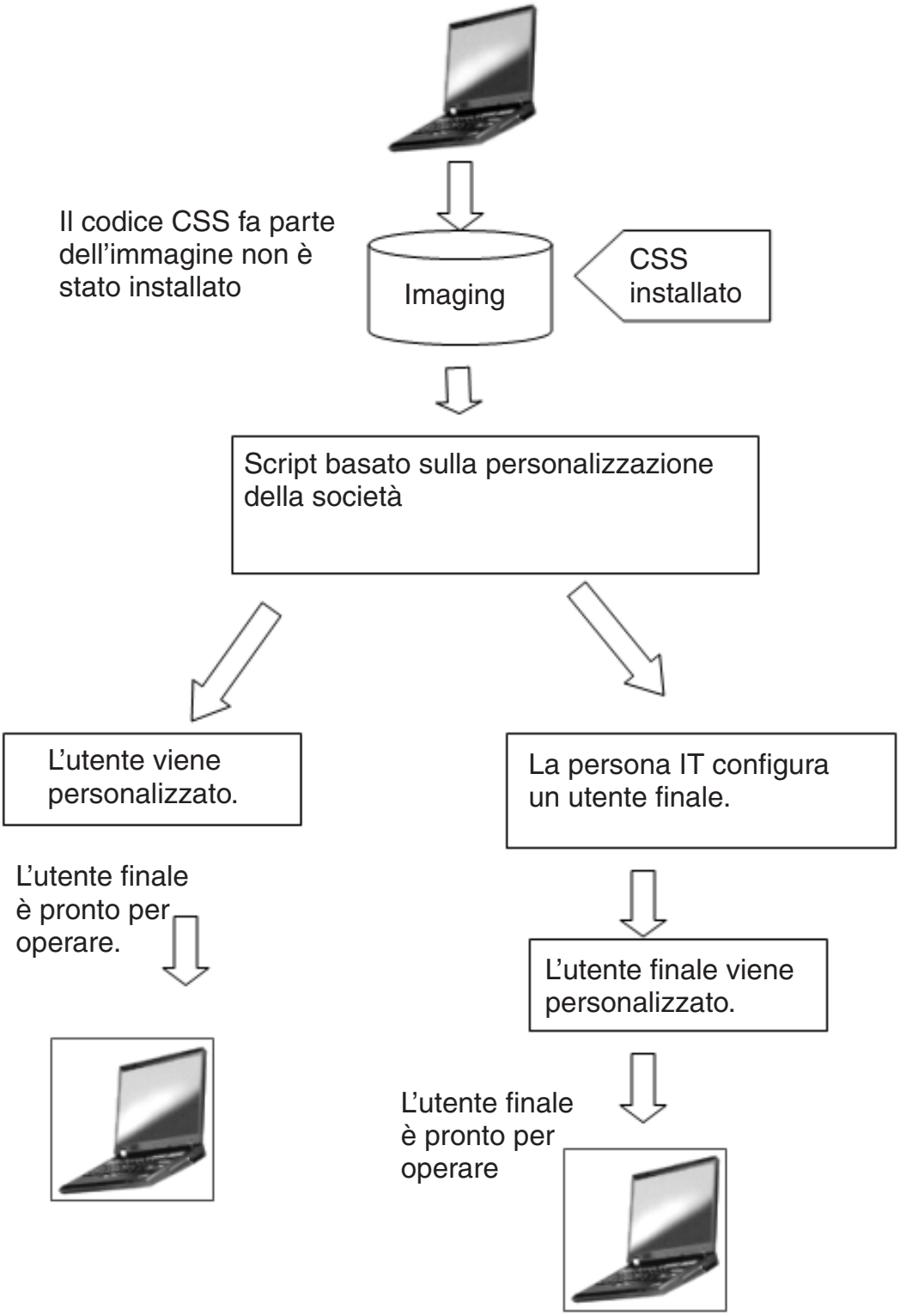


*Figura 25. IBM Client Security Software è installato e sono state impostate sia la personalizzazione della società che quella dell'utente.*

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.

## Dettagli file di configurazione

E' possibile creare il file CSEC.INI, utilizzando la procedura guidata Client security: 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)**.

### Configurazione

Il file cscc.ini è fondamentale durante 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.

*Tabella 6. Impostazioni di configurazione di Client Security System*

| | |
|---|---|
| [CSSSetup] | Intestazione della sezione per l'installazione CSS. |
| suppw=bootup | Password del Responsabile/supervisore BIOS.<br>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<br>0 per utilizzare una coppia di chiavi del responsabile. |
| keysplit=1 | Quando newkp è 1, determina il numero dei componenti delle chiavi private.<br>**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,<br>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,<br>se si tratta di un'unità di rete, è necessario che sia mappata. |
| pri=c:\jk\private1.key | Posizione della chiave privata del responsabile quando si utilizza una relativa coppia di chiavi esistente,<br>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. |

*Tabella 6. Impostazioni di configurazione di Client Security System (Continua)*

| | |
|---|---|
| clean=0 | 1 per eliminare il file .ini in seguito all'inizializzazione,<br>0 per lasciare il file .ini in seguito all'inizializzazione. |
| enableroaming=1 | 1 per abilitare il roaming per il client,<br>0 per disabilitare il roaming per il client. |
| username=<br>[promptcurrent] | [promptcurrent] per richiedere all'utente corrente la password di registrazione del sistema.<br>[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.<br>[<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.<br>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,<br>0 per registrare account utente specifici in UVM. |
| defaultuvmpw=top | Quando enrollall è 1, esso indica la 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.<br>1 per richiedere all'utente di modificare la passphrase UVM al collegamento successivo,<br>0 per non richiedere all'utente di modificare la passphrase UVM al successivo collegamento. |
| defaultppexppolicy=1 | Quando enrollall è 1, stabilisce la politica di scadenza della passphrase UVM per tutti gli utenti.<br>0 per indicare che la passphrase UVM scade<br>1 per indicare che la passphrase UVM non scade |
| defaultppexpdays=0 | Quando enrollall è 1, stabilisce la data di scadenza della passphrase UVM per tutti gli utenti.<br>Quando ppexppolicy è impostato su 0, immettere questo valore per stabilire la data di scadenza della 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.<br>Quando enrollall è 0, esso indica il numero degli utenti registrati in UVM. |

*Tabella 6. 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<br>1. Avviare Gestione computer (Gestione periferiche).<br>2. Espandere il nodo Utenti e gruppi locali.<br>3. Aprire la cartella Utenti.<br>Gli elementi elencati nella colonna Nome sono i nomi account. |
| user1uvmpw=chrome | Specificare la passphrase UVM dell'utente 1 UVM. |
| user1winpw=spinning | Specificare la passphrase Windows dell'utente 1 da registrare con UVM. |
| user1domain=0 | Specificare se l'account dell'utente 1 è locale o sul dominio.<br>0 per indicare che si tratta di un account locale,<br>1 per indicare che questo è presente sul dominio. |
| user1ppchange=0 | Specificare se all'utente 1 verrà richiesto di modificare la passphrase UVM al successivo collegamento.<br>1 per richiedere all'utente di modificare la passphrase UVM al collegamento successivo,<br>0 per non richiedere all'utente di modificare la passphrase UVM al successivo collegamento. |
| user1ppexppolicy=1 | Specificare se la passphrase UVM dell'utente 1 scade.<br>0 per indicare che la passphrase UVM scade.<br>1 per indicare che la passphrase UVM non scade. |
| user1ppexpdays=0 | Se user1ppexppolicy=0, impostare questo valore per indicare la data di scadenza dalla 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,<br>0 per utilizzare il collegamento Windows. |
| entrust=0 | 1 per utilizzare UVM per l'autenticazione entrust,<br>0 per utilizzare l'autenticazione entrust. |
| notes=1 | 1 per utilizzare la protezione UVM per Lotus Notes,<br>0 per utilizzare la protezione della password di Notes. |
| netscape=0 | 1 per firmare e cifrare e-mail con il modulo IBM PKCS#11,<br>0 per non firmare e cifrare e-mail con il modulo IBM PKCS#11. |

*Tabella 6. Impostazioni di configurazione di Client Security System (Continua)*

| | |
|---|---|
| passman=0 | 1 per utilizzare Password Manager,<br>0 per non utilizzare Password Manager |
| folderprotect=0 | 1 per utilizzare File and Folder Encryption,<br>0 per non utilizzare File and Folder Encryption. |

**Nota:**

1. Mentre IBM Client Security Software viene potenziato e aggiornato, i parametri *.ini potrebbero cambiare.
2. Se qualsiasi file o percorso si trovano su un'unità di rete, è necessario che l'unità venga associata ad una lettera.
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. (I doppi apici sono necessari per i nomi di percorsi lunghi): *Cartella di installazione di CSS*\console.exe /q /ini: *percorso completo di un file ini decifrato*
4. Il comando seguente esegue il file .ini dalla riga comandi quando la configurazione di massa non viene eseguita insieme ad un'installazione di massa:

   *Cartella di installazione di CSS*\acamucli /ccf:c:\csec.ini
5. 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.

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 7. Impostazioni di configurazione Client Security System alla seconda esecuzione*

| | |
|---|---|
| [CSSSetup] | Intestazione della sezione per l'installazione CSS. |
| suppw= | Password del Responsabile/supervisore BIOS.<br>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.<br>**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,<br>se si tratta di un'unità di rete, è necessario che sia mappata. |

*Tabella 7. Impostazioni di configurazione Client Security System alla seconda esecuzione (Continua)*

| | |
|---|---|
| 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. |
| [UVMEnrollment] | Intestazione della sezione per la registrazione dell'utente. |
| enrollall=0 | 1 per registrare tutti gli account utente locale in UVM,<br>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 la passphrase UVM dell'utente 1 UVM. |
| user1winpw= | Specificare la passphrase Windows dell'utente 1 da registrare con UVM. |
| user1domain=0 | Specificare se l'account dell'utente 1 è locale o sul dominio.<br>0 per indicare che si tratta di un account locale,<br>1 per indicare che questo è presente sul dominio. |
| user1ppchange=0 | Specificare se all'utente 1 verrà richiesto di modificare la passphrase UVM al successivo collegamento.<br>1 per richiedere all'utente di modificare la passphrase UVM al collegamento successivo,<br>0 per non richiedere all'utente di modificare la passphrase UVM al successivo collegamento. |
| user1ppexppolicy=1 | Specificare se la passphrase UVM dell'utente 1 scade.<br>0 per indicare che la passphrase UVM scade.<br>1 per indicare che la passphrase UVM non scade. |
| user1ppexpdays=0 | Se user1ppexppolicy=0, impostare questo valore per indicare la data di scadenza dalla passphrase UVM. |

# Capitolo 6. 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 protezione UVM per un client IBM può essere gestita in due modi:

- Localmente, utilizzando un editor che si trova sul client IBM
- In tutta l'azienda, utilizzando Tivoli Access Manager

Prima di utilizzare Client Security con Tivoli Access Manager, deve essere installato il componente Client Security di Tivoli Access Manager. Questo componente può essere scaricato dall'indirizzo http://www.pc.ibm.com/us/security/index.html del sito web IBM.

## 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
- Tivoli Access Manager Runtime Environment

Per informazioni dettagliate sull'installazione e l'utilizzo di Tivoli Access Manager, consultare la documentazione che si trova sul sito web IBM all'indirizzo http://www.tivoli.com/products/index/secureway_policy_dir/index.htm.

## Scaricamento e installazione del componente Client Security

Il componente Client Security è disponibile come download gratuito dal sito web IBM.

Per scaricare ed installare il componente Client Security sul server Tivoli Access Manager e il client IBM, completare la procedura di seguito riportata.

1. Utilizzando le informazioni che si trovano sul sito web, verificare che IBM integrated security chip sia presente sul sistema controllando il numero di modello corrisponda con uno di quelli forniti nella tabella dei 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, registrarlo IBM compilando il modulo in linea, quindi visualizzare di nuovo l'Accordo di licenza e fare clic su **Accetto**.

   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 di Benvenuto della 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. Quando viene riavviato l'elaboratore, dal desktop di Windows, fare clic su **Start > Esegui.** .
7. Nel campo Esegui, immettere *d:\directory*`\TAMCSS.exe`, dove *d:\directory* è la lettera corrispondente all'unità e la directory in cui si trova il file oppure fare clic su **Sfogli** per trovare 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 dei componenti di Client Security sul server 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 ]nome percorso-file
```

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

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

Fare riferimento al manuale *Tivoli Access Manager Base Administrator Guide* per ulteriori informazioni sull'utilità pdadmin e la relativa sintassi del comando.

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

Il client IBM deve stabilire la sua identità autenticata all'interno del dominio protetto di Tivoli Access Manager per richiedere decisioni di autorizzazione da parte di Tivoli Access Manager Authorization Service.

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 Tivoli Access Manager Management Server and Authorization Server.

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

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 server_name** Il nome utente/UVMWindows corrente dell'utente client IBM.
- **-P admin_pwd** La password del 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 port_num** Impostare il numero della porta di ascolto per il client IBM. Si tratta del parametro specificato nella porta server SSL della variabile PDRE Tivoli Access Manager Runtime.
- **-e pwd_life** Impostare la scadenza della password in numero di giorni.

Per stabilire una connessione protetta tra il client IBM e il server Tivoli Access Manager, completare la seguente 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 <server_name> con il nome utente UVM e il nome host del client IBM. Ad esempio: –n DemoUser/MyHostName. Il nome host del client IBM può essere trovato immettendo "hostname" dalla riga comandi MSDOS. Il

programma svrsslcfg crea una voce valida nel server di Tivoli Access Manager e fornisce un file della chiave univoca SSL per la comunicazione cifrata.

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 definiti come: **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 autenticazione per i client IBM, è necessario configurare ciascun client utilizzando Administrator Utility, un componete 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 nell'ordine di seguito riportato:

1. Sistema operativo **Microsoft Windows supportato.** E' possibile utilizzare Tivoli Access Manager per controllare i requisiti di autenticazione per i client IBM in esecuzione su 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 Client Security Administrator Utility per configurare l'autenticazione utente e modificare la politica di protezione 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 Tivoli Access Manager

Una volta installato Tivoli Access Manager sul client locale, è possibile configurare le informazioni di impostazione di Access Manager utilizzando 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 di controllo **Sostituisci il collegamento standard di Windows con il collegamento protetto 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 Access Manager sia installato sul client di questa area per essere 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 visualizzato il pannello di IBM UVM Policy.
9. Selezionare le azioni che si desidera controllare dal menu a discesa di Tivoli Access Manager.
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 protezione nel modo in cui viene gestita da Tivoli Access Manager viene conservata nel 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 Tivoli Access Manager per controllare gli oggetti client IBM

La politica UVM viene controllata tramite un file globale della politica. Il file della politica globale, denominato file di politica UVM, contiene i requisiti di autenticazione per le azioni che vengono eseguite sul sistema client IBM, come ad esempio il collegamento al sistema, l'impostazione dello screen saver o la firma dei messaggi di posta elettronica.

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

**Importante:** L'abilitazione di Tivoli Access Manager per controllare un oggetto consente il controllo degli oggetti allo spazio oggetti 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 visualizzato il pannello di IBM UVM Policy.
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 gli oggetti selezionati** per abilitare Tivoli Access Manager per quell'oggetto.

   **Importante:** Se si abilita Tivoli Access Manager per controllare un oggetto, si cede il controllo dello spazio di oggetti a 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 tra più client IBM, modificare e salvare la politica UVM per un client remoto, quindi copiare il file di 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 utilizzando la 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 della 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 la 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 la passphrase UVM viene visualizzata più di una volta. | Inserire la passphrase UVM oppure eseguire la scansione delle impronte digitali ogni volta in cui viene visualizzata la finestra di autenticazione. |
| Viene visualizzato un messaggio di errore **VBScript o JavaScript** | **Azione** |

| Problema | Possibile soluzione |
| --- | --- |
| Se si richiede un certificato digitale, potrebbe essere visualizzato un messaggio di errore relativo a VBScript o JavaScript. | Riavviare il computer e reperire di nuovo il certificato. |

## Tivoli Access Manager - Informazioni sulla risoluzione dei problemi

Le seguenti informazioni sulla risoluzione dei pproblemi protrebbero 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 configurazione 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 Manager e le relative impostazioni della cache locale non sono accessibili nella pagine di configurazione della politica in Administrator Utility. | Installare Tivoli Access Manager runtime Environment. Se Runtime Environment non è installato sul client IBM, le impostazioni di IBM Tivoli Access Manager non saranno disponibili nella pagina di configurazione della politica. |
| **Il controllo utente è valido sia per l'utente che per il gruppo** | **Azione** |
| Quando viene configurato il server Tivoli Access Manager, se si definisce un gruppo utenti, il controllo utenti è valido per utente e gruppo se è attivo **Traverse bit**. | Non è richiesta alcuna azione. |

## Lotus Notes - Informazioni sulla risoluzione dei problemi

Le seguenti informazioni sulla risoluzione dei problemi possono essere utili se si verificano problemi utilizzando Lotus Notes con Client Security Software.

| Problema | Possibile soluzione |
| --- | --- |
| **Una volta abilitata la protezione UVM per Lotus Notes, Notes non è in grado di completare la configurazione.** | **Azione** |
| Lotus Notes non è in grado di completare la configurazione una volta abilitata la protezione UVM utilizzando Administrator Utility. | Si tratta di un limite conosciuto.<br><br>Lotus Notes deve essere configurato ed in esecuzione prima che sia abilitato il supporto Lotus Notes in Administrator Utility. |
| **Viene visualizzato un messaggio di errore quando si tenta di modificare la password di Notes.** | **Azione** |

| Problema | Possibile soluzione |
| --- | --- |
| E' possibile che con la modifica della password di Notes quando si utilizza Client Security Software venga visualizzato 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:<br>• Utilizzare lo strumento di configurazione di Lotus Notes per impostare la protezione UVM per un ID Notes<br>• Aprire Notes e utilizzare la funzione fornita da Notes per modificare la password del file di ID Notes<br>• Chiudere immediatamente Notes dopo la modifica della password | Fare clic su **OK** per chiudere il messaggio di errore. Non è richiesta ulteriore azione.<br><br>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 di ID di Notes è ora cifrato con una password generata casualmente e l'utente non necessita di un nuovo file di ID utente. Se l'utente finale modifica di nuovo la password, UVM genera una nuova password casuale per l'ID Notes ID. |

## 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.<br><br>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 7. 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 8. 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 delle passphrase in remoto dopo la distribuzione. L'aggiornamento del file di politica di passphrase consente di cambiare i requisiti della passphrase quando (o se) l'utente modifica successivamente la passphrase. Il responsabile può stabilire un periodo di tempo, dopo il quale l'utente è obbligato a modificare la 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 la 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" della passphrase con scadenza a 30 giorni. Un nuovo file di politica viene inviato al computer client che specifica che è necessario che la passphrase venga cambiata ogni 15 giorni. Quando scadrà la passphrase in 5 giorni o in 20? La passphrase scadrà in 20 giorni come specificato dalla politica originale. La politica di scadenza delle passphrase diviene effettiva al momento dell'impostazione della passphrase. La politica di modifica a 15 giorni di scadenza inizierà quando Jane cambierà la passphrase dopo i 20 giorni

Se si desidera modificare le caratteristiche richieste della 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:

*Director of Commercial Relations*
*IBM Europe*
*Shoenaicher Str. 220*
*D-7030 Boeblingen*
*Deutschland*

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. Nessuna parte di questo documento può essere utilizzata coma licenza esplicita o implicita o come indennità nei diritti di autore dell'IBM o di 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.