

Soluzioni IBM® Client Security



Client Security Software versione 5.3

Guida per l'utente

Soluzioni IBM® Client Security



Client Security Software versione 5.3

Guida per l'utente

Nota

Prima di utilizzare questo prodotto e le relative informazioni, consultare la sezione Appendice B, “**Marchi e informazioni particolari**”, a pagina 57.

Indice

Prefazione v

A chi si rivolge questa guida	v
Modalità di utilizzo di questa guida	v
Ulteriori informazioni	vi

Capitolo 1. Introduzione 1

IBM Embedded Security Subsystem	1
IBM Embedded Security Chip	1
IBM Client Security Software	2
Relazione tra password e chiavi	2
Password del responsabile	2
Chiavi hardware pubbliche e private	3
Chiavi pubbliche e private del responsabile	4
Archivio ESS	4
Chiavi utente pubbliche e private	4
Gerarchia basata sullo scambio di chiavi IBM	4
Funzioni PKI (Public key Infrastructure) CSS	6

Capitolo 2. Cifratura e decifrazione di file e cartelle. 9

Cifratura con il tastino destro del mouse	9
Cifratura trasparente (FFE)	10
Stato di cifratura delle cartelle di FFE.	10
Suggerimenti per il programma di utilità File and Folder Encryption	11
Protezione dell'unità disco fisso	11
Eliminazione di cartelle e file protetti	11
Prima di aggiornare una versione precedente del programma di utilità IBM FFE	12
Prima della disinstallazione del programma di utilità IBM FFE	12
Limitazioni del programma di utilità FFE (File and Folder Encryption)	12
Limitazioni relative allo spostamento di cartelle e file protetti	12
Limitazioni relative all'esecuzione delle applicazioni	12
Limitazioni relative alla lunghezza del nome del percorso	12
Problemi relativi alla protezione delle cartelle	13

Capitolo 3. Roaming delle credenziali CSS 15

Requisiti per la rete di roaming delle credenziali CSS	15
Impostazione di un server di roaming	15
Configurazione di un server di roaming.	15
Registrazione dei client con il server di roaming	16
Completamento della procedura di registrazione dei client di roaming	17
Registrazione di un client di roaming utilizzando Administrator Utility	17
Registrazione di un client di roaming utilizzando User Configuration Utility	17

Registrazione di un client di roaming utilizzando la distribuzione di massa (non presidiata)	17
Gestione di una rete di roaming	19
Autorizzazione degli utenti	19
Sincronizzazione dei dati utente	20
Ripristino di un passphrase perduto in un ambiente di roaming	20
Importazione di un profilo utente	20
Rimozione e reintegrazione degli utenti in una rete di roaming	22
Rimozione e reintegro dei client registrati in una rete di roaming	22
Limitazione dell'accesso a client registrati in una rete di roaming	23
Ripristino di una rete di roaming	23
Modifica della coppia di chiavi del responsabile	24
Modifica della cartella di archivio	24
File and Folder Encryption (FFE)	24
IBM Password Manager	25
Termini e definizioni per il roaming	25

Capitolo 4. Istruzioni per gli utenti client 27

Utilizzo della protezione UVM per il collegamento al sistema	27
Procedure per sbloccare il client	27
User Configuration Utility	27
Funzioni User Configuration Utility	28
Limiti di User Configuration Utility con Windows XP	28
Utilizzo di User Configuration Utility	29
Utilizzo di un programma di navigazione sul web e di messaggi e-mail protetti	29
Utilizzo di Client Security Software con applicazioni Microsoft	30
Emissione di un certificato digitale per le applicazioni Microsoft	30
Trasferimento di certificati da Microsoft CSP	30
Aggiornamento dell'archivio di chiavi per le applicazioni Microsoft	31
Utilizzo del certificato digitale per le applicazioni Microsoft	32
Configurazione delle preferenze audio UVM	32

Capitolo 5. Risoluzione dei problemi . . . 33

Funzioni del responsabile.	33
Autorizzazione degli utenti	33
Rimozione di utenti	33
Impostazione della password del responsabile di BIOS (ThinkCentre).	33
Impostazione di una password del supervisore (ThinkPad)	34
Protezione della password del responsabile.	35
Annullamento di IBM embedded Security Subsystem (ThinkCentre).	35

Annullamento di IBM embedded Security Subsystem (ThinkPad)	36
Limitazioni note relative a CSS versione 5.2	36
Limitazioni di roaming	36
Limitazioni del badge di prossimità	38
Ripristino delle chiavi	38
Nomi di dominio e nomi utenti locali	38
Reinstallazione del software per le impronte digitali Targus	38
Passphrase del supervisore di BIOS	39
Utilizzo di 7.x	39
Utilizzo di un minidisco per l'archiviazione	39
Limitazioni delle Smart card.	39
Dopo la cifratura viene visualizzato il carattere più (+) sulle cartelle	39
Limitazioni di Windows XP con gli utenti limitati	40
Altre limitazioni	40
Utilizzo di Client Security Software con sistemi operativi Windows	40
Utilizzo di Client Security Software con applicazioni Netscape	40
Certificato IBM embedded Security Subsystem e algoritmi di cifratura	40
Utilizzo della protezione UVM per un ID utente Lotus Notes	41
Limiti di User Configuration Utility	41
Limitazioni relative a Tivoli Access Manager	42
Messaggi di errore	42
Prospetti per la risoluzione dei problemi.	42
Informazioni sulla risoluzione dei problemi relativi all'installazione	42
Informazioni sulla risoluzione dei problemi del programma Administrator Utility	43
Informazioni sulla risoluzione dei problemi del programma User Configuration Utility	44

Informazioni sulla risoluzione dei problemi specifici al ThinkPad	45
Informazioni sulla risoluzione dei problemi della Microsoft	46
Informazioni sulla risoluzione dei problemi dell'applicazione Netscape	48
Informazioni sulla risoluzione dei problemi relativi al certificato digitale	50
Informazioni sulla risoluzione dei problemi di Tivoli Access Manager.	50
Informazioni sulla risoluzione dei problemi relativi a Lotus Notes	51
Informazioni sulla risoluzione dei problemi relativi alla cifratura	52
Informazioni sulla risoluzione dei problemi relativi all'unità UVM	52

Appendice A. Informazioni sulle password e i passphrase 53

Regole per password e passphrase.	53
Regole per la password del responsabile.	53
Regole per passphrase UVM.	53
Conteggi errati su sistemi TCPA e non TCPA	55
Reimpostazione di un passphrase	55
Reimpostazione remota di un passphrase	55
Reimpostazione manuale di un passphrase	56

Appendice B. Marchi e informazioni particolari 57

Informazioni particolari	57
Marchi	58

Prefazione

Questa guida contiene informazioni sull'utilizzo di Client Security Software su elaboratori di rete, denominati anche client IBM, che dispongono di IBM embedded Security Chip.

La guida è organizzata nel modo seguente:

"Capitolo 1, "Introduzione"" contiene uno schema dei concetti di protezione di base, una panoramica dei componenti e delle applicazioni inclusi nel software ed una descrizione della funzioni PKI (Public Key Infrastructure).

"Capitolo 3, "Roaming delle credenziali CSS"," contiene informazioni su come utilizzare IBM Client Security Software per proteggere file e cartelle particolari.

"Capitolo 4, "Istruzioni per gli utenti client"," contiene istruzioni sulle diverse attività che l'utente del client può eseguire con Client Security Software. Questo capitolo comprende le istruzioni sull'utilizzo della la protezione del collegamento UVM, dello screen saver di Client Security, del servizio e-mail e del programma User Configuration Utility.

"Capitolo 5, "Risoluzione dei problemi"", contiene le informazioni utili per la risoluzione dei problemi che si possono verificare utilizzando le istruzioni fornite con questa guida.

"Appendice A, "Informazioni sulle password e i passphrase"," contiene i criteri relativi al passphrase applicabili alle regole e ad un passphrase UVM per le password del responsabile.

"Appendice B, "Marchi e informazioni particolari"," contiene le informazioni legali e le informazioni sui marchi.

A chi si rivolge questa guida

Questa guida è rivolta agli utenti finali di Client Security (utenti client). Prima di utilizzare le informazioni contenute nella guida, installare e configurare Client Security Software sull'elaboratore. E' richiesta la conoscenza sull'utilizzo di certificati digitali e l'utilizzo di applicazioni di collegamento e screen saver.

Modalità di utilizzo di questa guida

Utilizzare questa guida per configurare lo screen saver di Client Security, modificare i passphrase UVM e le password di Windows, le funzioni di cifratura di Client Security con le applicazioni Microsoft e Netscape. Questa guida si integra con *Guida all'installazione di Client Security Software*, *Utilizzo di Client Security con Tivoli Access Manager* e *Guida per il responsabile di Client Security Software*.

Alcune informazioni di questa guida vengono fornite anche nella *Guida per il responsabile di Client Security Software*. La *Guida per il responsabile* è stata progettata per i responsabili della protezione che installano e configurano Client Security Software sui client IBM.

E' possibile scaricare questa guida e tutta la documentazione relativa a Client Security dal sito web IBM all'indirizzo
<http://www.pc.ibm.com/us/security/index.html>.

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>.

Capitolo 1. Introduzione

Gli elaboratori ThinkPad™ e ThinkCentre™ dispongono di componenti hardware di cifratura, che operando con le tecnologie software scaricabili, forniscono un elevato livello di protezione alle piattaforme client. L'insieme di tali tecnologie hardware e software è denominato IBM Embedded Security Subsystem (ESS). Il componente hardware è IBM Embedded Security Chip, mentre quello software è IBM Client Security Software (CSS).

Client Security Software è stato progettato per elaboratori IBM che utilizzano IBM Embedded Security Chip per cifrare i file e memorizzarne le chiavi di cifratura. Questo software è costituito da applicazioni e componenti che consentono a sistemi client IBM di utilizzare funzioni di protezione client attraverso un rete locale, un'azienda o attraverso Internet.

IBM Embedded Security Subsystem

IBM ESS supporta soluzioni per la gestione delle chiavi, come ad esempio PKI (Public Key Infrastructure) e comprende le applicazioni logiche di seguito riportate:

- File and Folder Encryption (FFE)
- Password Manager
- Collegamento Windows protetto
- Vari metodi di autenticazione configurabile, compresi:
 - Password
 - Impronte digitali
 - Smart Card
 - Scheda di prossimità

Per utilizzare in modo efficiente le funzioni di IBM ESS, è necessario che un responsabile della protezione acquisisca alcuni concetti di base. Le sezioni di seguito riportate illustrano alcuni concetti di base sulla protezione.

IBM Embedded Security Chip

IBM Embedded Security Subsystem rappresenta la tecnologia hardware di cifratura integrata che fornisce un ulteriore livello di protezione alle piattaforme PC IBM. Con il sottosistema di protezione, le procedure di cifratura e autenticazione vengono trasferite dal software, più vulnerabile in un ambiente più protetto da hardware dedicato. L'incremento di protezione fornito da questa soluzione è tangibile.

IBM Embedded Security Subsystem supporta:

- Operazioni RSA3 PKI, come ad esempio la cifratura per riservatezza e le firme digitali per l'autenticazione
- Generazione chiave RSA
- Generazione numero casuale
- Computo funzione RSA in 200 millisecondi
- Memoria EEPROM per memorizzazione coppia chiavi RSA
- Tutte le funzioni TCPA definite nelle specifiche della versione 1.1

- Comunicazione con il processore principale mediante bus LPC (Low Pin Count)

IBM Client Security Software

IBM Client Security Software è costituito dalle applicazioni software e dai componenti di seguito riportati:

- **Administrator Utility:** Administrator Utility è l'interfaccia che un responsabile utilizza per attivare o disattivare IBM embedded Security Subsystem e per creare, archiviare e rigenerare le chiavi di cifratura e i passphrase. Inoltre, un responsabile può utilizzare questo programma di utilità per aggiungere utenti alla politica di protezione fornita da Client Security Software.
- **Administrator Console:** La console del responsabile di Client Security Software consente al responsabile di configurare una rete di roaming delle credenziali per creare e configurare file che consentono la distribuzione e per creare una configurazione non del responsabile e un profilo di ripristino.
- **User Configuration Utility:** Il programma User Configuration Utility consente ad un utente client di modificare il passphrase UVM, di abilitare le password di collegamento Windows affinché siano riconosciute da UVM, di aggiornare gli archivi delle chiavi e registrare le impronte digitali. Inoltre, un utente può effettuare le copie di backup dei certificati digitali creati con IBM embedded Security Subsystem.
- **UVM (User Verification Manager):** Client Security Software utilizza UVM per gestire passphrase e altri elementi che consentono l'autenticazione degli utenti del sistema. Ad esempio, un lettore di impronte digitali può essere utilizzato da UVM per l'autenticazione del collegamento. Client Security Software abilita alle funzioni di seguito riportate:
 - **Protezione della politica del client UVM:** Client Security Software consente al responsabile della protezione di impostare la politica di protezione del client, che stabilisce il modo in cui viene autenticato un utente client nel sistema.

Se la politica indica che è necessario fornire le impronte digitali per il collegamento e l'utente non ha registrato tali impronte digitali, verrà visualizzata l'opzione per la registrazione delle impronte digitali come parte del collegamento. Inoltre, se viene richiesta la verifica delle impronte digitali e non è collegato uno scanner, UVM restituirà un errore. Se la password di Windows non è registrata oppure è stata registrata in modo non corretto, con UVM, l'utente ha la possibilità di fornire la password corretta di Windows come parte del collegamento.
 - **Protezione del collegamento del sistema UVM:** Client Security Software consente ad un responsabile della protezione di controllare l'accesso all'elaboratore mediante un'interfaccia di collegamento. La protezione UVM verifica che solo gli utenti che sono riconosciuti dalla politica di protezione siano in grado di accedere al sistema operativo.

Relazione tra password e 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 relazione tra le password e le chiavi consente di comprendere il funzionamento di IBM Client Security Software.

Password del responsabile

La password del responsabile viene utilizzata per autenticare un responsabile per IBM Embedded Security Subsystem. La password, che deve essere costituita da

otto caratteri, viene conservata e autenticata nell'ambiente hardware protetto di Embedded Security Subsystem. Una volta autenticato, il responsabile può effettuare quanto di seguito riportato:

- Registrare gli utenti
- Avviare l'interfaccia per la politica di protezione
- Modificare la password del responsabile

La password del responsabile può essere impostata nei seguenti modi:

- Mediante la procedura guidata all'installazione di IBM Client Security
- Mediante il programma Administrator Utility
- Utilizzando gli script
- Mediante l'interfaccia BIOS (solo elaboratori ThinkCentre)

E' importante stabilire dei criteri per la creazione e la conservazione della password del responsabile. E' possibile modificare la password del responsabile se viene dimenticata o corrotta.

Per coloro che conoscono i concetti e la terminologia TCG (Trusted Computing Group), la password del responsabile è uguale al valore di autorizzazione dell'utente cui appartiene. Poiché la password del responsabile è associata a IBM Embedded Security Subsystem, talvolta viene denominata *password dell'hardware*.

Chiavi hardware pubbliche e private

La premessa principale di IBM Embedded Security Subsystem è di fornire una *root* ad elevata affidabilità ad un sistema di client. Questa *root* viene utilizzata per proteggere altre applicazioni e funzioni. La creazione di una chiave hardware pubblica ed una chiave hardware privata è parte della procedura di istituzione di una *root* affidabile. Le chiavi pubbliche e private, denominate *coppia di chiavi*, sono matematicamente correlate in modo che:

- I dati cifrati con la chiave pubblica possono essere decifrati solo con la chiave privata corrispondente.
- I dati cifrati con la chiave privata possono essere decifrati solo con la chiave pubblica corrispondente.

La chiave hardware privata viene creata, memorizzata ed utilizzata nell'ambiente hardware protetto del sottosistema di protezione. La chiave hardware pubblica viene resa disponibile per vari scopi (di qui il nome chiave pubblica), ma non è mai esposta fuori dell'ambiente hardware protetto del sottosistema di protezione. Le chiavi hardware pubbliche e private sono parti critiche della gerarchia basata sullo scambio di chiavi IBM descritta nella seguente sezione.

Le chiavi hardware pubbliche e private vengono create nei modi di seguito riportati:

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

Per coloro che conoscono i concetti e la terminologia TCGF (Trusted Computing Group), le chiavi hardware pubbliche e private sono denominate *SRK* (Storage Root Key).

Chiavi pubbliche e private del responsabile

Le chiavi pubbliche e private del responsabile sono parte integrante della gerarchia basata sullo scambio di chiavi IBM. Inoltre, consentono di effettuare copie di backup e il ripristino dei dati specifici per l'utente in caso di errore della scheda di sistema o del disco fisso.

Le chiavi pubbliche e private del responsabile possono essere uniche per tutti i sistemi oppure possono essere comuni a tutti i sistemi o gruppi di sistemi. Si noti che le chiavi del responsabile devono essere gestite stabilendo un criterio per l'utilizzo di chiavi uniche contro chiavi note.

Le chiavi pubbliche e private del responsabile possono essere create in uno dei modi di seguito riportati:

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

Archivio ESS

Le chiavi pubbliche e private del responsabile consentono di effettuare copie di backup e ripristino di dati specifici per l'utente in caso di errore della scheda di sistema o del disco fisso.

Chiavi utente pubbliche e private

IBM Embedded Security Subsystem crea chiavi utente pubbliche e private per proteggere dati specifici per l'utente stesso. Queste coppie di chiavi vengono create quando un utente è registrato in IBM Client Security Software. Queste chiavi vengono create e gestite in modo trasparente dal componente UVM (User Verification Manager) di IBM Client Security Software. Sono gestite in base all'utente Windows collegato al sistema operativo.

Gerarchia basata sullo scambio di chiavi IBM

Un elemento essenziale di IBM Embedded Security Subsystem è costituito dalla gerarchia basata sullo scambio di chiavi IBM. La base (o root) della gerarchia basata sullo scambio di chiavi IBM è costituita dalle chiavi hardware pubbliche e private. Le chiavi hardware pubbliche e private, denominate *coppia di chiavi hardware*, vengono create da IBM Client Security Software e sono statisticamente uniche per ciascun client.

IL "livello" superiore della gerarchia (superiore alla root) è costituito dalle chiavi pubbliche e private del responsabile, denominate anche *coppia di chiavi del responsabile*. La coppia di chiavi del responsabile può essere unica per ciascuna macchina o può essere la stessa per tutti i client o sottoinsiemi di client. La gestione di questa coppia di chiavi è correlata alla gestione della rete. La chiave privata del responsabile è unica, in quanto si trova sul sistema client (protetto dalla chiave hardware pubblica) in una posizione definita dal responsabile.

IBM Client Security Software registra gli utenti Windows in ambiente Embedded Security Subsystem. Quando un utente viene registrato, vengono create le chiavi pubbliche e private (*coppia di chiavi utente*) oltre ad un nuovo "livello" di chiavi. La chiave utente privata viene cifrata con la chiave pubblica del responsabile. La chiave privata del responsabile viene cifrata con la chiave hardware pubblica. Quindi, per utilizzare la chiave privata utente, è necessario che venga caricata la chiave privata del responsabile (cifrata con la chiave hardware pubblica) nel

sottosistema di protezione. Una volta nel chip, la chiave hardware privata decifra la chiave privata del responsabile. La chiave privata del responsabile è ora pronta per l'utilizzo nel sottosistema di protezione, in modo che i dati cifrati con la corrispondente chiave pubblica del responsabile possano essere scambiati nel sottosistema di protezione, decifrati e utilizzati. La chiave privata dell'utente corrente di Windows (cifrata con la chiave pubblica del responsabile) viene passata nel sottosistema di protezione. I dati necessari ad un'applicazione che condizionano Embedded security Chip vengono passati nel chip, decifrati e gestiti nell'ambiente protetto del sottosistema di protezione. Un esempio potrebbe essere una chiave privata utilizzata per autenticare una rete senza fili.

Ogni volta che viene richiesta una chiave, lo scambio avviene nel sottosistema di protezione. Le chiavi private cifrate vengono scambiate nel sottosistema di protezione, quindi possono essere utilizzate nell'ambiente protetto del chip stesso. Le chiavi private non sono mai esposte o utilizzate fuori da questo ambiente hardware. Ciò consente di proteggere una quantità di dati illimitata mediante IBM Embedded Security Chip.

Le chiavi private vengono cifrate, sia per motivi di protezione sia per la quantità limitata di spazio disponibile in IBM Embedded Security Subsystem. E' possibile memorizzare solo una coppia di chiavi nel sottosistema di protezione in qualunque momento. Le chiavi hardware pubbliche e private sono le sole chiavi che restano memorizzate nel sottosistema di protezione durante l'avvio. Per consentire la memorizzazione di più chiavi e più utenti, CSS utilizza la gerarchia basata sullo scambio di chiavi IBM. Ogni volta che viene richiesta una chiave, lo scambio avviene in IBM Embedded Security Subsystem. Le chiavi private cifrate correlate vengono scambiate nel sottosistema di protezione, quindi possono essere utilizzate nell'ambiente protetto del chip stesso. Le chiavi private non sono mai esposte o utilizzate fuori da questo ambiente hardware.

La chiave privata del responsabile viene cifrata con la chiave hardware pubblica. La chiave hardware privata, disponibile solo nel sottosistema di protezione, viene utilizzata per decifrare la chiave privata del responsabile. Una volta decifrata la chiave privata del responsabile nel sottosistema di protezione, è possibile passare una chiave utente privata (cifrata con la chiave pubblica del responsabile) nel sottosistema di protezione e decifrarla con la chiave privata del responsabile. Con la chiave pubblica del responsabile, è possibile cifrare più chiavi utente private. Ciò consente di autenticare un numero virtualmente illimitato di utenti su un sistema con IBM ESS, tuttavia, per ottenere prestazioni ottimali, si consiglia di limitare la registrazione a 25 utenti per elaboratore.

IBM ESS utilizza una gerarchia basata sullo scambio di chiavi in cui le chiavi hardware pubbliche e private che si trovano nel sottosistema di protezione vengono utilizzate per proteggere i dati memorizzati fuori del chip stesso. La chiave hardware privata viene generata nel sottosistema di protezione e rimane sempre in questo ambiente protetto. La chiave hardware pubblica è disponibile fuori del sottosistema di protezione ed è utilizzata per cifrare o proteggere altri dati, come ad esempio una chiave privata. Una volta cifrati questi dati con la chiave hardware pubblica, è possibile decifrarli solo con la chiave hardware privata. Poiché la chiave hardware privata è disponibile solo nell'ambiente protetto del sottosistema di protezione, i dati cifrati possono essere solo decifrati ed utilizzati nello stesso ambiente protetto. Si noti che ciascun elaboratore dispone di una chiave hardware pubblica e privata unica. La capacità di numerazione casuale di IBM Embedded Security Subsystem assicura che ciascuna coppia di chiavi hardware sia statisticamente unica.

Funzioni PKI (Public key Infrastructure) CSS

Client Security Software fornisce tutti i componenti richiesti per creare una PKI (public key infrastructure) nella propria attività commerciale, quali:

- **Controllo responsabili sulla politica di protezione del client.** L'autenticazione degli utenti finali a livello di client rappresenta un problema di politica di protezione di rilevante importanza. Client Security Software fornisce l'interfaccia che è richiesta per gestire la politica di protezione di un client IBM. Questa interfaccia appartiene al software di autenticazione UVM (User Verification Manager), che rappresenta il componente principale di Client Security Software.
- **Gestione delle chiavi di cifratura per la cifratura delle chiavi pubbliche.** I responsabili creano le chiavi di codifica per l'hardware del computer e per gli utenti dei client con Client Security Software. Quando vengono create le chiavi di cifratura, esse risultano collegate a IBM embedded Security Chip tramite una gerarchia di chiavi, per cui una chiave hardware di livello base viene utilizzata per cifrare le chiavi dei livelli superiori, compreso le chiavi utente che sono associate ad ogni utente client. La cifratura e la memorizzazione delle chiavi su IBM embedded Security Chip aggiunge un ulteriore livello di protezione del client, poiché le chiavi vengono collegate in modo sicuro all'hardware del computer.
- **Creazione e memorizzazione del certificato digitale protetto da IBM embedded Security Chip.** Quando si applica un certificato digitale da poter utilizzare per firmare o cifrare digitalmente messaggi e-mail, Client Security Software consente di selezionare IBM embedded Security Subsystem come CSP (cryptographic service provider) per le applicazioni che utilizzano Microsoft CryptoAPI. Tali applicazioni includono Internet Explorer e Microsoft Outlook Express. Ciò assicura che la chiave privata del certificato digitale sia cifrata con la chiave pubblica dell'utente in IBM embedded Security Subsystem. Inoltre, gli utenti di Netscape possono selezionare IBM embedded Security Subsystem come creatore della chiave privata per i certificati digitali utilizzati per la protezione. Le applicazioni che utilizzano (PKCS) #11 (Public-Key Cryptography Standard), ad esempio Netscape Messenger si avvalgono della protezione fornita da IBM embedded Security Subsystem.
- **La capacità di trasferire certificati digitali a IBM embedded Security Subsystem.** IBM Client Security Software Certificate Transfer Tool consente di spostare i certificati creati con Microsoft CSP predefinito in IBM embedded Security Subsystem CSP. Ciò aumenta la protezione fornita alle chiavi private associate con i certificati poiché non sono memorizzate su IBM embedded Security Subsystem, invece del software.

Nota: I certificati digitali protetti da IBM embedded Security Subsystem CSP non possono essere esportati in un altro CSP.

- **Una soluzione per il recupero e l'archiviazione delle chiavi.** Una funzione PKI importante è la creazione di un archivio di chiavi da cui le chiavi possono essere ripristinate se le chiavi di origine risultano perse o danneggiate. IBM Client Security Software dispone di un'interfaccia che consente di stabilire un archivio per le chiavi e i certificati digitali creati con IBM embedded Security Subsystem e di ripristinare tali chiavi e certificati, se occorre.
- **Cifratura di file e cartelle.** Il programma di utilità FFE (File and folder encryption) consente a un utente client di cifrare e decifrare file e cartelle. Questa operazione implementa il livello di protezione dei dati ottimizzando le misure di protezione del sistema CSS.
- **Autenticazione delle impronte digitali.** IBM Client Security Software supporta per l'autenticazione l'utilità di lettura per le impronte digitali Targus PC Card e

Targus USB. Per un corretto funzionamento, è necessario installare Client Security Software prima dei driver di periferica dei programmi di utilità per la lettura delle impronte digitali Targus.

- **Autenticazione Smart card.** IBM Client Security Software supporta alcune smart card come dispositivi di autenticazione. Client Security Software consente l'utilizzo delle smart card come token di autenticazione per un solo utente alla volta. Ciascuna smart card è legata a un sistema se non viene utilizzato il roaming delle credenziali. La richiesta di una smart card protegge ulteriormente il sistema, in quanto quest'ultima deve essere fornita con una password, che può essere compromessa.
- **Roaming delle credenziali.** Il roaming delle credenziali consente ad un utente della rete autorizzato di utilizzare qualunque elaboratore della rete come propria stazione di lavoro. Una volta che l'utente è autorizzato ad utilizzare UVM su un qualunque client registrato Client Security Software, è possibile importare i dati personali su qualunque altro client registrato nella rete di roaming delle credenziali. I dati personali verranno aggiornati automaticamente e memorizzati nell'archivio di CSS e in ogni elaboratore in cui sono stati importati. L'aggiornamento dei dati personali come nuovi certificati o le modifiche dei passphrase saranno immediatamente disponibili su tutti gli elaboratori connessi alla rete di roaming.
- **Certificazione FIPS 140-1.** Client Security Software supporta le librerie cifrate certificate FIPS 140-1. Le librerie RSA BSAFE certificate FIPS vengono utilizzate sui sistemi TCPA.
- **Scadenza passphrase.** Client Security Software stabilisce un passphrase specifico per l'utente e una politica di scadenza del passphrase per ciascun utente aggiunto a UVM.

Capitolo 2. Cifratura e decifrazione di file e cartelle

La tecnologia di cifratura consente di proteggere i dati sensibile contenuti nell'elaboratore dell'utente. La cifratura dei file assicura che altri utenti non possano in alcun modo accedere alle informazioni contenute nel file cifrato senza adempiere ai requisiti di protezione specificati. Inoltre, la cifratura dei file consente di proteggere i dati sensibili contenuti nei file inviati mediante Internet mediante la rete.

IBM Client Security Software consente di cifrare e decifrare i file e le cartelle sensibili nei modi di seguito riportati:

- **Cifratura di un file singolo con il "tastino destro" del mouse utilizzando l'applicazione Client Security Software.**

Questa funzione è parte del pacchetto base di IBM Client Security Software.

- **Cifratura trasparente di file e cartelle utilizzando il programma di utilità IBM File and Folder Encryption.**

Nota: Affinché questa funzione sia abilitata, è necessario scaricare il programma di utilità IBM File and Folder Encryption (FFE). IBM Client Security Software deve essere installato *prima* di installare il programma di utilità IBM File and Folder Encryption.

Cifratura con il tastino destro del mouse

La funzione di cifratura di base mediante il tastino destro del mouse di Client Security Software consente di proteggere i file sensibili utilizzando il tastino destro del mouse. Per utilizzare questa funzione, non è necessario scaricare alcun software aggiuntivo. I file cifrati con questa funzione dispongono delle caratteristiche di seguito riportate:

- E' necessario decifrare manualmente un file cifrato ogni volta che si desidera utilizzarlo e cifrarlo di nuovo manualmente per proteggerlo a fine operazione. E' necessario richiamare la politica UVM ogni volta che si cifra o si decifra un file. Questi requisiti forniscono un elevato controllo manuale della cifratura e della decifrazione dei file selezionati, ma questa elevata protezione non è conveniente per gli utenti che non desiderano fornire una password, le impronte digitali o una smart card ogni volta che utilizzando un file cifrato.
- I file possono essere inviati ad una posizione remota cifrati, tuttavia possono essere decifrati solo sull'elaboratore utilizzato per cifrarli, poiché i tasti utilizzati per cifrare i file sono unici per IBM embedded Security Subsystem su un determinato elaboratore.

I file possono essere cifrati e decifrati manualmente con il menu contestuale che viene visualizzato facendo clic con il tastino destro del mouse. Quando i file vengono cifrati in questo modo, l'operazione di cifratura aggiunge un'estensione `.enc` ai file. Tali file cifrati possono quindi essere memorizzati in modo sicuro su server remoti. Restano, quindi cifrati e non disponibili per essere utilizzati da applicazioni fino a quando l'opzione con il tastino destro del mouse non viene utilizzata di nuovo per la decifrazione.

Cifratura trasparente (FFE)

La funzione di cifratura trasparente di Client Security Software viene abilitata scaricando il programma di utilità di IBM File and Folder Encryption (FFE), disponibile sul sito web di IBM Client Security. FFE fornisce una funzione di cifratura trasparente e più semplice rispetto alla funzione di cifratura con il "tastino destro" del mouse di CSS. Inoltre, la cifratura di file e cartelle con FFE può essere richiamata utilizzando il tastino destro del mouse. I file e le cartelle cifrate con FFE presentano le caratteristiche di seguito riportate:

- La politica UVM deve essere richiamata solo all'avvio. Quindi, ciò fornisce una forma di cifratura e decifrazione dei file selezionati più conveniente, poiché *non* è necessario fornire una password, le impronte digitali o una smart card ogni volta che si desidera utilizzare un file cifrato.
- Quando un file cifrato con il programma di utilità File and Folder Encryption viene aperto da un'applicazione, il file viene decifrato automaticamente. Quando un file cifrato con File and Folder Encryption viene salvato, è automaticamente cifrato.
- I file cifrati con FFE (File and Folder Encryption) possono essere inviati ad una posizione remota decifrati.

il programma di utilità Controllo disco potrebbe essere eseguito durante il riavvio del sistema operativo dopo aver protetto o rimosso la protezione delle cartelle. Verificare il sistema prima di utilizzare l'elaboratore.

Un utente registrato UVM che ha scaricato il programma di utilità FFE può selezionare una cartella da proteggere o da cui rimuovere la protezione mediante l'interfaccia visualizzata con il tastino destro del mouse. In tal modo, tutti i file contenuti nella cartella o nelle cartelle secondarie saranno cifrati. Quando i file vengono protetti in questo modo, non viene aggiunta alcuna estensione al nome file. Quando da un'applicazione si tenta di accedere ad un file contenuto in una cartella cifrata, il file viene decifrato in memoria e viene cifrato di nuovo prima di essere salvato sul disco fisso.

Tutte le operazioni che consentono l'accesso ad un file in una cartella protetta avranno accesso ai dati in forma decifrata. Questa funzione rende la cifratura più flessibile, poiché un file non deve essere decifrato ogni volta che è utilizzato oppure cifrato di nuovo ogni volta che il programma termina di utilizzarlo.

Stato di cifratura delle cartelle di FFE

Il programma di utilità File and Folder Encryption consente di proteggere il file e le cartelle sensibili utilizzando il tastino destro del mouse. Il modo in cui il software protegge un file e le cartelle differisce a seconda di come il file o la cartella viene cifrata inizialmente.

Una cartella può trovarsi in uno dei seguenti stati:

- **Cartella non protetta**

Questa cartella e tutte le relative cartelle secondarie sono state designate come protette. L'utente ha la possibilità di proteggere questa cartella.

- **Cartella protetta**

Una cartella protetta può trovarsi in uno dei seguenti stati:

- **Protetta dall'utente corrente**

L'utente corrente ha designato questa cartella come protetta. Tutti i file sono cifrati, compreso i file presenti nelle cartelle secondarie. L'utente ha la possibilità di annullare la protezione della cartella.

– **Una cartella secondaria di una cartella protetta dall'utente corrente**

L'utente corrente ha designato una di queste cartelle principali come protetta. Tutti i file sono cifrati. L'utente corrente non ha l'opzione del tastino destro.

– **Protetta da un utente diverso**

Un utente diverso ha designato questa cartella come protetta. Tutti i file sono cifrati, compreso i file presenti in tutte le cartelle secondarie e non sono disponibili all'utente corrente. L'utente corrente non ha l'opzione del tastino destro.

• **Cartella principale di una cartella protetta**

Una cartella principale di una cartella protetta può trovarsi in uno dei tre stati:

– **Può contenere una o più cartelle secondarie protette dall'utente corrente**

L'utente corrente ha designato una o più cartelle secondarie come protette. Tutti i file nelle cartelle secondarie protette sono cifrati. L'utente ha la possibilità di proteggere la cartella principale. E' necessario rimuovere la protezione da tutte le cartelle secondarie che si trovano nella cartella principale prima di proteggere la cartella principale stessa.

– **Può contenere una o più cartelle secondarie protette da uno o più utenti diversi.**

Un utente o più utenti diversi hanno designato una o più cartelle secondarie come protette. Tutti i file nelle cartelle secondarie protette sono cifrati e non sono disponibili all'utente corrente. L'utente corrente non ha l'opzione del tastino destro.

– **Può contenere cartelle secondarie protette dall'utente corrente e uno o più utenti diversi**

Sia l'utente corrente che uno o più utenti diversi hanno designato le cartelle secondarie come protette. L'utente corrente non ha l'opzione del tastino destro.

• **Cartella critica**

Una cartella critica è una cartella che si trova in un percorso critico e, quindi, non può essere protetto. Esistono due percorsi critici: il percorso Windows e il percorso di Client Security.

Ciascuno stato viene gestito in modo diverso mediante l'opzione con il tastino destro del mouse.

Suggerimenti per il programma di utilità File and Folder Encryption

Le informazioni di seguito riportate potrebbero risultare utili per l'esecuzione di alcune funzioni relative al programma di utilità FFE.

Protezione dell'unità disco fisso

E' possibile utilizzare il programma di utilità IBM FFE per cifrare file e cartelle solo sull'unità C. Il programma di utilità IBM FFE non supporta la cifratura su altre partizioni del disco fisso o unità fisiche.

Eliminazione di cartelle e file protetti

Affinché i file o le cartelle sensibili non vengano lasciati non protetti nel Cestino, utilizzare la combinazione di tasti Maiusc+Canc per eliminare le cartelle e i file

protetti. La sequenza di tasti Maiusc+Canc effettua un'operazione di eliminazione incondizionata evitando di spostare i file nel cestino.

Prima di aggiornare una versione precedente del programma di utilità IBM FFE

Prima di aggiornare IBM FFE, se si dispone della versione 2.0 o precedente, scaricare ed utilizzare il programma di utilità ACL (Access Control List) Repair Tool dal sito web IBM Security. E' necessario utilizzare questo programma di utilità *prima* di disinstallare la versione di FFE precedente alla 2.0. In caso contrario, il processo di disinstallazione potrebbe non essere completato correttamente lasciando i file non accessibili.

Prima della disinstallazione del programma di utilità IBM FFE

Prima di disinstallare il programma di utilità IBM FFE, utilizzare IBM FFE per rimuovere la protezione dalle cartelle e dai file protetti.

Limitazioni del programma di utilità FFE (File and Folder Encryption)

Il programma di utilità IBM FFE presenta le limitazioni di seguito riportate:

Limitazioni relative allo spostamento di cartelle e file protetti

Il programma di utilità IBM FFE non supporta le operazioni di seguito riportate:

- Spostamento di file e cartelle che si trovano in cartelle protette
- Spostamento di file o cartelle tra cartelle protette e non protette

Se si tenta di eseguire tali operazioni di spostamento non supportate, viene visualizzato il messaggio del sistema operativo "Accesso negato". Questo messaggio è nella norma. Notifica solo che l'operazione di spostamento non è supportata. In alternativa all'operazione di spostamento, effettuare le operazioni di seguito riportate:

1. Copiare le cartelle e i file protetti nella nuova ubicazione.
2. Eliminare le cartelle e i file di origine utilizzando la combinazione di tasti Maiusc+Canc.

Limitazioni relative all'esecuzione delle applicazioni

Il programma di utilità IBM FFE non supporta l'esecuzione delle applicazioni da una cartella protetta. Ad esempio, se si dispone di un eseguibile denominato PROGRAM.EXE, non è possibile eseguire questa applicazione da una cartella protetta.

Limitazioni relative alla lunghezza del nome del percorso

Se si tenta di proteggere una cartella utilizzando il programma di utilità IBM FFE oppure di copiare o spostare un file o una cartella da una cartella non protetta a una cartella protetta, probabilmente verrà visualizzato il messaggio del sistema operativo "Uno o più nomi di percorso sono troppo estesi". Se si riceve questo messaggio, uno o più file o cartelle dispongono di un nome di percorso che eccede il numero massimo di caratteri consentiti. Per risolvere il problema, organizzare nuovamente la struttura della cartella, per ridurre la quantità di indirizzari o abbreviare i nomi dei file o delle cartelle.

Problemi relativi alla protezione delle cartelle

Se si tenta di proteggere una cartella e viene visualizzato il messaggio "Impossibile proteggere la cartella. Uno o più file potrebbero essere in uso," verificare quanto segue:

- Verificare che nessun file contenuto nella cartella sia al momento in uso.
- Se Esplora risorse visualizza una o più cartelle secondarie di una cartella che si sta tentando di proteggere, assicurarsi che la cartella da proteggere sia evidenziata e attiva, ma che non lo siano le cartelle secondarie.

Capitolo 3. Roaming delle credenziali CSS

La funzione di roaming delle credenziali di IBM Client Security Software abilita le credenziali degli utenti UVM per essere utilizzate su tutti gli elaboratori abilitati TCPA in una rete. Questa rete, denominata rete di roaming, potenzia la flessibilità utente la disponibilità delle applicazioni abilitando gli utenti a operare da qualunque elaboratore in rete.

Requisiti per la rete di roaming delle credenziali CSS

Una rete di roaming delle credenziali CSS è costituita dai componenti necessari di seguito riportati:

- Server di roaming
- Client di roaming
- Unità di rete mappata condivisa per memorizzare gli archivi utente UVM

Nota: Il server di roaming e i client di roaming autorizzati sono semplicemente elaboratori abilitati TCPA con password del responsabile stabilite e che dispongono di IBM Client Security Software 5.1 o versione successiva.

Impostazione di un server di roaming

Per configurare una rete di roaming delle credenziali CSS, è necessario designare un elaboratore TCPA come *server* di roaming (denominato sistema A). Gli altri elaboratori, una volta registrati mediante il server di roaming, diventano *client* registrati CSS autorizzati. (Il primo client registrato è denominato sistema B.)

L'elaboratore designato come server di roaming non è diverso dagli altri elaboratori. Quindi, è possibile utilizzare a tale scopo qualunque elaboratore designato come parte della rete di roaming. Il server di roaming è semplicemente l'elaboratore che viene designato per stabilire quali elaboratori sono "affidabili" nella rete di roaming. Una volta registrato un elaboratore con il server di roaming, quest'ultimo viene autenticato con tutti gli elaboratori in rete.

La configurazione di una rete di roaming è un processo costituito da sue fasi:

1. Configurazione di un sistema A (server) mediante l'istituzione di chiavi, archivi e utenti di roaming.
2. Registrazione di un sistema B e di tutti gli altri elaboratori come client di roaming nella rete di roaming delle credenziali CSS.

Il server di roaming definisce la rete di roaming delle credenziali CSS e inizia la registrazione dei client di roaming, ma il punto principale della rete di roaming delle credenziali CSS è costituito dall'unità di rete mappata in cui vengono memorizzati gli archivi utente. Questo archivio è il luogo in cui vengono memorizzati tutti gli aggiornamenti alle credenziali utente. E' necessario che l'archivio *non* sia ubicato nel server di roaming o su un qualunque client di roaming. Una volta inizializzati i client CSS, il server di roaming funziona come un qualsiasi client registrato CSS.

Configurazione di un server di roaming

Per configurare un server di roaming, completare la procedura di seguito riportata:

1. Sull'elaboratore designato, avviare Administrator Console, quindi fare clic su **Configura roaming delle credenziali**. Oppure, se l'elaboratore è già configurato per il roaming, selezionare **Riconfigura il sistema con server di roaming CSS**, fare clic su **Avanti** quindi su **OK**.
2. Creare la cartella c:\roaming sull'elaboratore designato come server di roaming.
3. Avviare Administrator Console, quindi fare clic su **Configura roaming delle credenziali**.
4. Selezionare **Configura il sistema come server di roaming delle credenziali CSS**, quindi fare clic su **Avanti**.
5. Fare clic su **Configura**.
6. Selezionare **Crea nuove chiavi di archivio**, quindi immettere il percorso della cartella in cui si trovano le nuove chiavi nel campo appropriato, dove la cartella delle chiavi di archivio è memorizzata nella cartella c:\roaming.
7. Scegliere di utilizzare una coppia di chiavi esistente o creare una nuova coppia di chiavi, quindi fare clic su **Avanti**.
8. Immettere la posizione della cartella di archivio, quindi fare clic su **Avanti**.

Nota: La cartella di archivio e la cartella delle chiavi devono essere accessibili agli elaboratori registrati per il roaming (client di roaming). La directory c:\roaming deve essere un'unità di rete mappata.

Se al momento esistono file nell'archivio, viene richiesto il modo in cui gestire tali file.

9. Fare clic su **Fine**.

Registrazione dei client con il server di roaming

Per registrare un client di roaming con il server di roaming, completare la procedura di seguito riportata:

1. Dopo aver completato la configurazione del server di roaming, viene visualizzato il pannello relativo alla configurazione della rete di roaming delle credenziali. Selezionare **Abilita registrazione client**, quindi fare clic su **Avanti**.
2. Immettere il nome dell'utente nel sistema B con privilegi da responsabile che completerà la registrazione del client.
3. Immettere e confermare una password costituita da 8 caratteri da utilizzare per tale utente. (Attenzione a non confondere questa procedura con quella per autorizzare un utente all'utilizzo di UVM, che deve essere effettuata in seguito.)
4. Se si desidera registrare il client utilizzando il programma User Configuration Utility, è necessario creare un file di configurazione del responsabile per quell'utente. Questa procedura genera un file unico per l'utente. Memorizzare questo file in una posizione accessibile all'utente e al sistema B.

Nota: Non è necessario generare questo file durante la registrazione di un client che utilizza il programma Administrator Utility.

5. Immettere la password del responsabile per il sistema B, quindi fare clic su **Avanti**.
6. Se viene creato un file di configurazione del responsabile, salvarlo in una posizione accessibile all'utente e al sistema B.

Una volta completate le procedure illustrate in precedenza, il server di roaming viene configurato. E' necessario completare la registrazione per ciascun client di roaming prima di poter utilizzare la rete di roaming.

Completamento della procedura di registrazione dei client di roaming

Una volta registrato l'elenco dei sistemi affidabili sul server di roaming, è necessario completare una delle procedure di seguito riportate sui sistemi client. E' necessario che il server di roaming sia in esecuzione e collegato all'archivio prima di poter completare la procedura di registrazione dei client di roaming.

Registrazione di un client di roaming utilizzando Administrator Utility

Per registrare un client di roaming utilizzando il programma Administrator Utility, completare la seguente procedura:

1. Fare clic su **Configurazione chiave**.
2. Fare clic su **No** se viene richiesto se si desidera ripristinare le chiavi dall'archivio.
3. Selezionare Registra questo sistema con un server di roaming CSS, quindi fare clic su **Avanti**.
4. Immettere la posizione dell'archivio creata dal sistema A, immettere la password di registrazione del sistema per quest'utente sul sistema A, quindi fare clic su **Avanti**.

Il completamento della registrazione richiede alcuni minuti.

Registrazione di un client di roaming utilizzando User Configuration Utility

Per registrare un client di roaming utilizzando il programma User Utility, completare la seguente procedura:

1. Dal separatore User Configuration, fare clic su **Registra con un server di roaming CSS**.
2. Selezionare il file di configurazione del responsabile generato sul sistema A, immettere la password di registrazione del sistema designata per il relativo utente sul sistema A, quindi fare clic su **Avanti**.
3. Immettere la posizione dell'archivio creata dal sistema A, quindi fare clic su **Avanti**.

Il completamento della registrazione richiede alcuni minuti.

Registrazione di un client di roaming utilizzando la distribuzione di massa (non presidiata)

Per registrare un client di roaming in modo non presidiato utilizzando una distribuzione di massa, completare la procedura di seguito riportata:

1. Creare il file csec.ini. Per ulteriori informazioni sulla creazione di un file CSS .ini, consultare la *Guida all'installazione di Client Security Software*.
2. Nella sezione csssetup del file, aggiungere "enableroaming=1". Questo indica che l'elaboratore dovrebbe essere registrato come client di roaming.
3. Nella stessa sezione, aggiungere la voce "username=OPTION". Sono disponibili tre opzioni per questo valore:
 - **Opzione 1: La stringa "[promptcurrent]" - parentesi quadre incluse.** La designazione dovrebbe essere utilizzata se viene generato un file .dat per l'utente al momento collegato sul server di roaming e se l'utente corrente conosce la password di registrazione del sistema. Questa opzione apre una finestra a comparsa che richiede all'utente di immettere la password di registrazione del sistema (sysregpwd) prima della distribuzione.

- **Opzione 2: La stringa "[current]" - parentesi quadre incluse.** Questa specifica dovrebbe essere utilizzata se è stato generato un file .dat sul server per l'utente al momento collegato. Il parametro sysregpwd viene gestito come descritto in seguito.
 - **Opzione 3: Un nome utente corrente come "joseph".** Se viene utilizzato tale nome utente, un file "joseph.dat" deve essere precedentemente generato dal server di roaming. La relativa stringa sysregpwd verrà gestita come descritto nel passo successivo.
4. Se vengono utilizzate le opzioni due e tre, è necessario fornire un'altra voce, vale a dire "sysregpwd=SYSREGPW". Questa è la password di registrazione del sistema costituita da otto caratteri associata all'utente corrente (se viene implementata l'opzione numero due) o all'utente designato (se viene implementata l'opzione numero tre).
 5. Per completare la registrazione dei client, collegare l'elaboratore all'archivio impostato dal server di roaming. Tale archivio è designato nel file csec.ini. Anche la cartella delle chiavi è impostata sul server di roaming delle credenziali è designata nel file csec.ini.
 6. Cifrare il file csec.ini utilizzando Administrator Console.

Esempi del file csec.ini

Gli esempi di seguito riportati illustrano un file csec.ini e le relative modifiche in base alle opzioni di roaming delle credenziali selezionata. Di seguito sono riportate le opzioni disponibili:

- **Nessun valore di roaming.** Questo file di base non è abilitato per il roaming delle credenziali.
- **Opzione di roaming 1.** Questo file è abilitato per il roaming con l'opzione 1 per la registrazione del client. È necessario che l'utente corrente immetta la password di registrazione del sistema prima della distribuzione.
- **Opzione di roaming 2.** Questo file è abilitato per il roaming con l'opzione 2 per la registrazione del client. È necessario che l'utente corrente immetta l'ID utente e la password di registrazione del sistema designati nel file .ini.
- **Opzione di roaming 3.** Questo file è abilitato per il roaming con l'opzione 3 per la registrazione del client. L'utente è designato nel file .ini. La password di registrazione del sistema per l'utente designato deve essere presente nel file .ini.

Di seguito sono illustrati gli esempi di quattro diversi file CSEC.INI:

[CSSSetup]	Opzione 1 [CSSSetup]	Opzione 2 [CSSSetup]	Opzione 3 [CSSSetup]
suppw=bootup	suppw=bootup	suppw=bootup	suppw=bootup
hwpw=11111111	hwpw=11111111	hwpw=11111111	hwpw=11111111
newkp=1	newkp=1	newkp=1	newkp=1
keysplit=1	keysplit=1	keysplit=1	keysplit=1
kpl=c:\jgk	kpl=c:\\computer name\jgk, dove "computer" è memorizzato nella coppia di chiavi sul server di roaming	kpl=c:\\computer name\jgk, dove "computer" è memorizzato nella coppia di chiavi sul server di roaming	kpl=c:\\computer name\jgk, dove "computer" è memorizzato nella coppia di chiavi sul server di roaming

kal=c:\jgk\archive pub= c:\jk\admin.key pri= c:\jk\private1.key wiz=0	kal=c:\\computer name\archive, dove "computer" è memorizzato nell'archivio del server di roaming pub= c:\jk\admin.key pri= c:\jk\private1.key wiz=0	kal=c:\\computer name\archive, dove "computer" è memorizzato nell'archivio del server di roaming pub= c:\jk\admin.key pri= c:\jk\private1.key wiz=0	kal=c:\\computer name\archive, dove "computer" è memorizzato nell'archivio del server di roaming pub= c:\jk\admin.key pri= c:\jk\private1.key wiz=0
clean=0	enableroaming=1 username=[promptcurrent] clean=0	enableroaming=1 username=[current] sysregpwd=12345678 clean=0	enableroaming=1 username=joseph sysregpwd=12345678 clean=0
[UVMEnrollment] enrollall=0 enrollusers=1 user1=joseph user1uvmpw= q1234r user1winpw= user1domain=0 user1ppchange=0 user1ppexppolicy=0 user1ppexppdays= 184	[UVMEnrollment] enrollall=0 enrollusers=1 user1=joseph user1uvmpw=q1234r user1winpw= user1domain=0 user1ppchange=0 user1ppexppolicy=0 user1ppexppdays=184	[UVMEnrollment] enrollall=0 enrollusers=1 user1=joseph user1uvmpw=q1234r user1winpw= user1domain=0 user1ppchange=0 user1ppexppolicy=0 user1ppexppdays=184	[UVMEnrollment] enrollall=0 enrollusers=1 user1=joseph user1uvmpw=q1234r user1winpw= user1domain=0 user1ppchange=0 user1ppexppolicy=0 user1ppexppdays=184
[UVMAppConfig] uvmlogon=0 entrust=0 notes=0 netscape=0 passman=0 folderprotect=0 autoprotect=0	[UVMAppConfig] uvmlogon=0 entrust=0 notes=0 netscape=0 passman=0 folderprotect=0 autoprotect=0	[UVMAppConfig] uvmlogon=0 entrust=0 notes=0 netscape=0 passman=0 folderprotect=0 autoprotect=0	[UVMAppConfig] uvmlogon=0 entrust=0 notes=0 netscape=0 passman=0 folderprotect=0 autoprotect=0

Gestione di una rete di roaming

Il responsabile di una rete di roaming deve autorizzare gli utenti e gestire l'accesso ai client e agli utenti stessi alla rete. Quindi l'importazione di un profilo utente, la sincronizzazione di dati utente o l'aggiunta e la rimozione di utenti e client è rapida e semplice in una rete di roaming CSS. Inoltre, potrebbe essere richiesto di ripristinare la rete di roaming, modificare la coppia di chiavi del responsabile o modificare la posizione di archivio.

Autorizzazione degli utenti

Una volta completate le procedure illustrate in precedenza, la rete di roaming delle credenziali CSS viene configurata e i client di roaming sono registrati per il roaming. Quindi, in seguito è possibile autorizzare gli utenti all'utilizzo del programma Administrator Utility.

Sincronizzazione dei dati utente

I dati per ciascun utente vengono memorizzati nella posizione dell'archivio. Una copia dei dati è memorizzata anche localmente su ogni elaboratore con cui è stato effettuato il roaming. Una volta effettuate le modifiche, come ad esempio ottenere un certificato o modificare un passphrase, vengono aggiornati i dati locali. Se l'elaboratore è collegato all'archivio, anche i dati utente vengono aggiornati. Quando l'utente si collega ad un altro elaboratore, gli aggiornamenti vengono automaticamente scaricati su quell'elaboratore, se è collegato all'archivio.

Il collegamento all'archivio non è sempre garantito, quindi talvolta i dati utente possono non corrispondere tra gli elaboratori e l'archivio. Se i dati utente vengono modificati su un elaboratore non collegato all'archivio, le modifiche non vengono aggiornate nell'archivio e di conseguenza neanche sugli altri elaboratori. Quando l'elaboratore è collegato all'archivio, le modifiche vengono aggiornate nell'archivio e l'eventuale non corrispondenza di dati viene risolta successivamente sugli altri elaboratori collegati. Tuttavia, se le modifiche vengono effettuate su un altro elaboratore collegato all'archivio prima che il primo elaboratore contenente le modifiche viene connesso all'archivio, si verifica un problema di inconsistenza dati. I dati contenuti nell'archivio contengono modifiche non presenti sul primo elaboratore, mentre il primo elaboratore contiene modifiche non contenute nell'archivio. Se ciò si verifica, all'utente vengono notificate le due configurazioni diverse e viene richiesto di scegliere quale conservare, la configurazione locale o quella archiviata. Le modifiche della configurazione che non vengono scelte andranno perdute. Quindi, è importante assicurarsi che le modifiche effettuate ad una configurazione utente siano aggiornate nell'archivio prima di effettuare modifiche su altri elaboratori.

Ripristino di un passphrase perduto in un ambiente di roaming

Quando viene perduto o dimenticato un passphrase, il responsabile può reimpostare il passphrase utente sul server di roaming o su un qualunque client registrato. Questa modifica viene aggiornata su tutti i sistemi di rete *escluso* i sistemi che l'utente ha importato per l'abilitazione del collegamento protetto UVM. In questi casi, l'aggiornamento del passphrase *non* viene riflesso sull'elaboratore. Per ottenere l'accesso all'elaboratore, è necessario che l'utente disponga di un file di sovrascrittura della password e che completi la procedura di sovrascrittura password.

Importazione di un profilo utente

È possibile importare un profilo utente in un nuovo elaboratore nella rete di roaming utilizzando il programma Administrator Utility, User Configuration Utility oppure UVM GINA. Se si desidera importare un utente che non dispone di account utente sul nuovo elaboratore, è necessario creare un account utente di Windows mediante il Pannello di controllo.

Nota: Per importare un utente in una rete di roaming, è necessario che tale utente sia autorizzato su un altro elaboratore che fa parte della rete di roaming.

Importazione di un profilo utente utilizzando User Configuration Utility

Per importare un profilo utente in un nuovo elaboratore della rete di roaming utilizzando User Configuration Utility, collegarsi al sistema con l'account utente da importare, quindi fare clic su **Start > Programmi > Access IBM > IBM Client**

Security Software > Modifica le impostazioni di protezione, quindi fare clic su **Importa configurazione esistente dall'archivio** nel separatore User Configuration.

Importazione di un profilo utente utilizzando Administrator Utility

Per importare un profilo utente in un nuovo elaboratore della rete di roaming utilizzando il programma Administrator Utility, selezionare l'utente, quindi fare clic su **Autorizza**. Fare clic su **Sì** quando viene richiesto di importare l'utente dall'archivio.

Importazione di un profilo utente utilizzando UVM GINA

E' possibile importare un profilo utente in un nuovo elaboratore nella rete di roaming utilizzando UVM GINA. La procedura inizia dal pannello di collegamento di UVM. Se un utente non è autorizzato all'utilizzo di UVM su un determinato sistema nella rete, viene visualizzata un messaggio nel quale si richiede se l'utente desidera essere importato dall'archivio.

Nota:

1. Se si desidera importare un utente che non dispone di un account utente nell'elaboratore, prima di continuare è necessario creare un account utente Windows utilizzando il Pannello di controllo.
2. Per accedere all'archivio sul server di roaming, è necessario che la directory sia un'unità di rete mappata.

Per importate un profilo utente in un nuovo elaboratore della rete di roaming utilizzando UVM GINA su un elaboratore che dispone di Windows 2000, completare la procedura di seguito riportata:

1. Al collegamento, immettere il nome utente ed il passphrase UVM dell'utente da importare. Viene visualizzato un messaggio che richiede se si desidera importare il profilo utente dall'archivio.
2. Fare clic su **Sì** alla richiesta di importazione dell'utente, quindi su **OK**.
3. Se la posizione dell'archivio si trova su un'unità di rete, fare clic su **Sì** indicando che deve essere fornita una condivisione di rete.
4. Immettere la password di Windows nel pannello standard di collegamento. Viene visualizzata una richiesta per il percorso di archivio.
5. Immettere il percorso di rete di archivio.
6. Immettere il nome utente e la password per il percorso di rete.
7. Fare clic su **OK**. Se l'operazione viene completata correttamente, viene visualizzato un messaggio indicante che l'importazione del profilo è riuscita.

Per importare un profilo utente in un nuovo elaboratore in una rete di roaming utilizzando UVM GINA su un elaboratore che dispone del sistema operativo Windows XP, completare la procedura di seguito riportata:

1. Al collegamento, immettere il nome utente ed il passphrase UVM dell'utente da importare. Viene visualizzato un messaggio che richiede se si desidera importare il profilo utente dall'archivio.
2. Fare clic su **Sì** alla richiesta di importazione dell'utente, quindi su **OK**.
3. Se la posizione dell'archivio si trova su un'unità di rete, fare clic su **Sì** indicando che deve essere fornita una condivisione di rete.
4. Alla richiesta dell'unità di rete mappata di Windows, immettere il percorso di rete dell'archivio.
5. Fare clic su **Fine**.

6. Immettere nome utente e password per il percorso di rete, quindi fare clic su **OK**. Se l'operazione viene completata correttamente, viene visualizzato un messaggio indicante che l'importazione del profilo è riuscita.

Nota: Per importare un utente in una rete di roaming, è necessario che tale utente sia autorizzato su un altro elaboratore che fa parte della rete di roaming.

Una volta importato il profilo utente, l'autenticazione con UVM è basata sulla politica di protezione dell'elaboratore. I requisiti per la protezione dell'elaboratore devono essere forniti correttamente prima che l'utente possa collegarsi.

Rimozione e reintegrazione degli utenti in una rete di roaming

Per rimuovere un utente da una rete di roaming, è necessario che il responsabile di rete completi la procedura di Administrator Console di seguito riportata:

1. Avviare il programma di utilità Administrator Console, quindi immettere la password del responsabile.
2. Fare clic su **Configura roaming delle credenziali**.
3. Selezionare **Rimuovi utenti da UVM e dalla rete di roaming delle credenziali**, quindi fare clic su **Avanti**. Ripetere i passi, se occorre.
4. Selezionare l'utente da rimuovere, quindi fare clic su **Rimuovi**.

Nota: Una volta rimosso un utente dalla rete, tutte le credenziali appartenenti a tale utente vengono perse definitivamente.

Gli utenti rimossi potrebbero non essere autorizzati ad utilizzare UVM e la rete di roaming fino a quando non vengono reintegrati dal responsabile di rete.

Per reintegrare un utente in una rete di roaming, è necessario che il responsabile di rete completi la procedura di Administrator Console di seguito riportata:

1. Avviare Console Utility, quindi immettere la password del responsabile.
2. Fare clic su **Configura roaming delle credenziali**.
3. Selezionare **Reintegra utenti rimossi**, quindi fare clic su **Avanti**.
4. Selezionare l'utente da reintegrare, quindi fare clic su **Reintegra**. Ripetere i passi, se occorre.

Una volta reintegrato l'utente, è necessario autorizzarlo di nuovo all'utilizzo di UVM. Il reintegro di un utente, dunque, non lo autorizza automaticamente all'utilizzo di UVM.

Rimozione e reintegro dei client registrati in una rete di roaming

Per rimuovere un client registrato da una rete di roaming, è necessario che il responsabile di rete completi la procedura di Administrator Console di seguito riportata:

1. Avviare Console Utility, quindi immettere la password del responsabile.
2. Fare clic su **Configura roaming delle credenziali**.
3. Selezionare **Rimuovi client registrati dalla rete di di roaming delle credenziali**, quindi fare clic su **Avanti**.
4. Selezionare il sistema da rimuovere, quindi fare clic su **Rimuovi**. Ripetere i passi, se occorre.

Nota: Una volta rimosso un client dalla rete, tutte le credenziali basate sulla macchina appartenenti al sistema andranno perse in modo definitivo.

I client rimossi non possono essere registrati con il server della rete di roaming fino a quando non vengono reintegrati dal responsabile di rete.

Per reintegrare un client registrato ad una rete di roaming, è necessario che il responsabile di rete completi la procedura di Administrator Console di seguito riportata:

1. Avviare Console Utility, quindi immettere la password del responsabile.
2. Fare clic su **Configura roaming delle credenziali**.
3. Selezionare **Reintegra client rimossi**, quindi fare clic su **Avanti**.
4. Selezionare il client da reintegrare, quindi fare clic su **Reintegra**. Ripetere i passi, se occorre.

Una volta reintegrato il client, quest'ultimo può essere registrato di nuovo con il server di roaming. La reintegrazione di un client non ne consente la registrazione automatica.

Nota: Tutti gli utenti le cui credenziali erano presenti nel sistema nel momento in cui il client è stato rimosso, potrebbero dover importare di nuovo le credenziali.

Limitazione dell'accesso a client registrati in una rete di roaming

Potrebbe verificarsi che il responsabile di rete desideri autorizzare l'accesso ad alcuni utenti ad un determinato client registrato, limitando l'accesso agli altri utenti.

Per gestire i privilegi di accesso degli utenti, è necessario che il responsabile di rete completi la procedura di Administrator Console di seguito riportata:

1. Avviare Console Utility, quindi immettere la password del responsabile.
2. Fare clic su **Configura roaming delle credenziali**.
3. Selezionare **Gestisci accesso utenti per i client registrati**, quindi fare clic su **Avanti**.
4. Selezionare il client registrato da gestire nella casella **Seleziona un sistema nella rete di roaming CSS**. Gli utenti che dispongono o meno dell'accesso sono elencati nelle due caselle ad elenco.
5. Effettuare una delle seguenti operazioni:
 - Per limitare l'accesso ad un utente, selezionare l'utente dall'elenco **Utenti con accesso**, quindi fare clic su **Limita**. Ripetere i passi, se occorre.
 - Per dare accesso ad un utente limitato, selezionare l'utente dall'elenco **Utenti senza accesso**, quindi fare clic su **Consenti**. Ripetere i passi, se occorre.

Per le funzioni di gestione degli accessi della rete di roaming è necessario creare una nuova cartella nell'archivio. La nuova cartella, denominata Protetta, deve disporre degli attributi di scrittura per il responsabile di rete di sola lettura per gli altri utenti. Se gli utenti dispongono degli attributi di scrittura per quella cartella, potrebbero reintegrare manualmente i loro profili sui sistemi.

Ripristino di una rete di roaming

In caso di errori software o hardware, potrebbe essere necessario ripristinare la rete di roaming. Se il server di roaming o i dati utilizzati da CSS sono corrotti su un

client registrato, ripristinare i dati utilizzando Administrator Utility allo stesso modo di un ambiente non di roaming. Se IBM embedded Security subsystem su un client registrato non funziona o viene annullato, è necessario registrare di nuovo il client con il server di roaming. Non è necessaria alcuna operazione aggiuntiva.

Modifica della coppia di chiavi del responsabile

Non è consigliato modificare la coppia di chiavi del responsabile di una rete di roaming.

Per modificare la coppia di chiavi del responsabile di una rete di roaming, è necessario procedere nel modo seguente affinché le modifiche siano effettuate ed attive su tutti gli elaboratori della rete:

1. Sul server di roaming, modificare la coppia di chiavi del responsabile utilizzando il programma Administrator Utility.
2. Registrare nuovamente tutti i client della rete.
3. Conservare i file esistenti quando viene richiesto.

Modifica della cartella di archivio

La modifica della cartella di archivio in un ambiente di roaming è leggermente diversa rispetto ad un ambiente non di roaming, in quanto ciascun elaboratore in rete accede alla stessa posizione di archivio.

Per modificare la cartella di archivio in una rete di roaming, completare la procedura di seguito riportata:

1. Copiare i file dalla cartella di archivio precedente a quella nuova con la procedura di seguito riportata:
 - a. Avviare il programma Administrator Utility, quindi immettere la password del responsabile.
 - b. Fare clic su **Configurazione chiave**.
 - c. Selezionare Modifica posizione dell'archivio, quindi fare clic su **Avanti**.
 - d. Immettere la nuova cartella dell'archivio, quindi fare clic su **Avanti**.
 - e. Fare clic su **Sì** quando viene richiesto di copiare tutti i file dalla cartella precedente a quella nuova.
2. Aggiornare tutti gli altri elaboratori in rete, affinché possano utilizzare la nuova cartella di archivio con la procedura di seguito riportata:
 - a. Avviare il programma Administrator Utility, quindi immettere la password del responsabile.
 - b. Fare clic su **Configurazione chiave**.
 - c. Selezionare Modifica posizione dell'archivio, quindi fare clic su **Avanti**.
 - d. Immettere la nuova cartella dell'archivio, quindi fare clic su **Avanti**.
 - e. Fare clic su **No** quando viene richiesto di copiare tutti i file dalla cartella precedente alla nuova.

File and Folder Encryption (FFE)

Le funzioni di File and Folder Encryption non sono condizionate da un ambiente di roaming. Tuttavia, le cartelle protette sono gestite su base elaboratore-elaboratore. In questo modo, se una cartella è protetta da un utente A su un sistema A, la stessa cartella sul sistema B non risulta protetta, se l'utente non l'ha protetta anche sul sistema B.

IBM Password Manager

Tutte le password protette utilizzando IBM Password Manager sono disponibili su tutti gli elaboratori nella rete di roaming.

Termini e definizioni per il roaming

Di seguito sono riportati termini che consentono di comprendere i concetti e le procedure relative alla configurazione di una rete di roaming:

Registrazione client di roaming

Il processo di registrazione di un elaboratore con un server di roaming.

Client di roaming

Tutti gli elaboratori affidabili TCPA in una rete di roaming.

Server di roaming

L'elaboratore TCPA utilizzato per inizializzare la rete di roaming.

Password di registrazione client di roaming

La password utilizzata per registrare l'elaboratore con il server di roaming.

Capitolo 4. Istruzioni per gli utenti client

Questa sezione fornisce informazioni che consentono ad un utente client di eseguire le attività riportate di seguito:

- Utilizzare la protezione UVM per il collegamento al sistema
- Utilizzare User Configuration Utility
- Utilizzare un programma di navigazione sul web e per i messaggi e-mail sicuro
- Configurare le preferenze audio UVM

Utilizzo della protezione UVM per il collegamento al sistema

Questa sezione contiene informazioni sull'utilizzo della protezione del collegamento UVM per il collegamento al sistema. Prima di utilizzare la protezione UVM, è necessario abilitarla per il computer.

La protezione UVM consente di controllare l'accesso al sistema operativo attraverso un'interfaccia di collegamento. La protezione al collegamento UVM sostituisce l'applicazione di collegamento a Windows, in modo che quando un utente sblocca il computer, viene visualizzata la finestra di collegamento a UVM e non la finestra di collegamento a Windows. Una volta abilitata la protezione UVM sul computer, all'avvio del computer verrà visualizzata l'interfaccia di collegamento a UVM.

Quando il computer è in esecuzione, è possibile accedere all'interfaccia di collegamento a UVM premendo **Ctrl + Alt + Canc** per arrestare o bloccare il computer oppure per aprire Task Manager o scollegare l'utente corrente.

Procedure per sbloccare il client

Per sbloccare un client Windows che utilizza la protezione UVM, procedere nel modo seguente:

1. Premere **Ctrl + Alt + Canc** per accedere all'interfaccia di collegamento UVM.
2. Immettere il nome utente e il dominio a cui si è collegati e, quindi, fare clic su **Sblocca**.

Viene visualizzata la finestra Passphrase UVM.

Nota: Anche se UVM riconosce molteplici domini, la password utente deve essere la stessa per tutti i domini.

3. Immettere il passphrase UVM, quindi fare clic su **OK** per accedere al sistema operativo.

Nota:

1. Se il passphrase UVM non corrisponde al nome utente e al dominio immessi, la finestra di collegamento a UVM viene visualizzata di nuovo.
2. A seconda dei requisiti di autenticazione della politica UVM per il client, è possibile che vengano richiesti ulteriori processi di autenticazione.

User Configuration Utility

Il programma User Configuration Utility abilita l'utente client ad eseguire le varie attività di gestione della protezione che non richiedono l'accesso con privilegi di responsabile.

Funzioni User Configuration Utility

Il programma User Configuration Utility consente ad un utente client di procedere nel modo seguente:

- **Aggiornamento delle password e dell'archivio.** Questo separatore consente di eseguire le funzioni di seguito riportate:
 - **Cambiare il passphrase UVM.** Per migliorare la protezione, è possibile modificare periodicamente il passphrase UVM.
 - **Aggiornare la password di Windows.** Quando viene modificata la password di Windows per un client autorizzato UVM con il programma Windows User Manager, occorre modificare anche la password utilizzando IBM Client Security Software - User Configuration Utility. Se un responsabile utilizza Administrator Utility per modificare la password di collegamento a Windows per un utente, tutte le chiavi cifrate dell'utente create per quell'utente saranno eliminate e i certificati digitali associati non saranno più validi.
 - **Reimpostare la password Lotus Notes.** Per migliorare la protezione, è possibile modificare la password Lotus Notes.
 - **Aggiornare l'archivio delle chiavi.** Se si creano certificati digitali e si desidera creare copie della chiave privata memorizzata su IBM embedded Security Chip oppure se si desidera spostare l'archivio delle chiavi su un'altra ubicazione, aggiornare l'archivio delle chiavi.
- **Configurare le preferenze audio UVM.** User Configuration Utility consente di selezionare un file audio da riprodurre in caso di autenticazione riuscita o non riuscita.
- **Configurazione utente.** Questo separatore consente di eseguire le funzioni di seguito riportate:
 -
 - **Reimposta utente.** Questa funzione consente di reimpostare la configurazione di protezione. Quando si reimposta la configurazione di protezione, tutte le chiavi, i certificati, le impronte digitali precedenti vengono cancellati.
 - **Ripristinare la configurazione di protezione utente dall'archivio.** Questa funzione consente di ripristinare le impostazioni dall'archivio. Tale funzione è utile se i file sono stati corrotti o se si desidera ripristinare una configurazione precedente.
 - **Registra con un server di roaming CSS.** Questa funzione consente di registrare il sistema con un server di roaming CSS. Una volta registrato il sistema, è possibile importare la configurazione corrente in questo sistema.

Limiti di User Configuration Utility con Windows XP

Windows XP impone alcune restrizioni per l'accesso che limitano le funzioni disponibili ad un utente del client in determinate circostanze.

Windows XP Professional

In Windows XP Professional, le restrizioni dell'utente client potrebbero essere applicate nelle seguenti situazioni:

- Client Security Software è installato su una partizione che viene convertita successivamente in un formato NTFS
- La cartella Windows si trova su una partizione che viene convertita successivamente in un formato NTFS
- La cartella di archivio si trova su una partizione che viene convertita successivamente in un formato NTFS

Nelle situazioni precedenti, Windows XP Professional Limited Users potrebbe non essere in grado di eseguire le attività di User Configuration Utility di seguito riportate:

- Cambiare il passphrase UVM
- Aggiornare la password di Windows registrata con UVM
- Aggiornare l'archivio delle chiavi

Tali limitazioni vengono eliminate quando un responsabile avvia ed esce da Administrator Utility.

Windows XP Home

Windows XP Home Limited Users non sarà in grado di utilizzare User Configuration Utility in una delle seguenti situazioni:

- Client Security Software è installato su una partizione formattata NTFS
- La cartella Windows si trova su una partizione formattata NTFS
- La cartella di archivio si trova su una partizione formattata NTFS

Utilizzo di User Configuration Utility

Per utilizzare User Configuration Utility, procedere nel modo seguente:

1. Fare clic su **Avvio > Programmi > Access IBM > IBM Client Security Software > Modifica le impostazioni di protezione.**

Viene visualizzato il pannello principale di IBM Client Security Software User Configuration Utility.

2. Selezionare uno dei separatori di seguito riportati:

- **Aggiornamento delle password e dell'archivio.** Questo separatore consente di modificare il passphrase UVM, aggiornare la password di Windows in UVM, reimpostare la password Lotus Notes in UVM e aggiornare l'archivio di cifratura.
- **Configura suoni UVM.** Questo separatore consente di selezionare un file audio da riprodurre quando l'autenticazione è corretta o errata.
- **Configurazione utente.** Questo separatore consente all'utente di ripristinare la propria configurazione dall'archivio, reimpostarla oppure registrarsi con il server di roaming (se l'elaboratore può essere utilizzato come client di roaming).

3. Fare clic su **OK** per uscire.

Utilizzo di un programma di navigazione sul web e di messaggi e-mail protetti

Se si inviano transazioni non protette su Internet, tali transazioni possono essere intercettate e lette. E' possibile impedire gli accessi non autorizzati alle transazioni su Internet richiamando un certificato digitale e utilizzandolo per eseguire una firma digitale e per cifrare i propri messaggi e-mail o per rendere più sicuro il proprio browser web.

Un certificato digitale (definito anche ID digitale o certificato di protezione) è una credenziale elettronica immessa e inserita con una firma digitale da un'autorità certificata. Quando viene emesso un certificato digitale, l'autorità di certificazione convalida l'identità dell'utente in quanto possessore del certificato. Un'autorità di certificazione è un fornitore sicuro di certificati digitali e può essere un'azienda non IBM, come ad esempio VeriSign oppure tale autorità di certificazione può

essere configurata come server all'interno della propria azienda. Il certificato digitale contiene l'identità dell'utente, come ad esempio il nome e l'indirizzo e-mail, le date di scadenza del certificato, una copia della chiave pubblica, l'identità dell'autorità di certificazione e la firma digitale.

Utilizzo di Client Security Software con applicazioni Microsoft

Le istruzioni fornite in questa sezione sono specifiche per l'utilizzo di Client Security Software in relazione all'emissione e all'utilizzo di certificati digitali con le applicazioni che supportano Microsoft CryptoAPI, come ad esempio Outlook Express.

Per ulteriori dettagli su come creare le impostazioni di protezione e utilizzare applicazioni e-mail quali Outlook Express e Outlook, fare riferimento alla documentazione fornita con tali applicazioni.

Emissione di un certificato digitale per le applicazioni Microsoft

Quando si utilizza un'autorità di certificazione per creare un certificato digitale da utilizzare per le applicazioni Microsoft, verrà richiesto di selezionare un CSP (Cryptographic Service Provider) per il certificato.

Per utilizzare le funzioni di cifratura di IBM embedded Security Chip per le applicazioni Microsoft, assicurarsi di selezionare **IBM embedded Security Subsystem CSP** come provider di servizi di cifratura una volta ottenuto il certificato digitale. Questa operazione assicura che la chiave privata del certificato digitale venga memorizzata in IBM Security Chip.

Inoltre, selezionare la cifratura forte (o alta), se disponibile, per una ulteriore protezione. Poiché IBM embedded Security Chip consente una cifratura fino a 1024 bit della chiave privata del certificato digitale, selezionare questa opzione, se disponibile, nell'interfaccia relativa all'autorità di certificazione; la cifratura a 1024 bit è inoltre denominata cifratura forte.

Dopo aver selezionato **IBM embedded Security Subsystem CSP** come CSP, è possibile che venga richiesto di immettere il passphrase UVM, di eseguire una scansione delle impronte digitali o entrambi per soddisfare i requisiti di autenticazione per ottenere un certificato digitale. I requisiti di autenticazione vengono definiti nella politica UVM per il computer.

Trasferimento di certificati da Microsoft CSP

La procedura guidata per il trasferimento dei certificati di IBM CSS consente di trasferire certificati creati con il CSP predefinito della Microsoft sul CSP di IBM embedded Security System. Il trasferimento dei certificati aumenta la protezione fornita dalle chiavi private associate ai certificati, in quanto questi ultimi possono essere memorizzati in modo sicuro mediante IBM embedded Security Subsystem, invece di utilizzare il software, che è più vulnerabile.

Esistono due tipi di certificati di protezione che possono essere trasferiti:

- **Certificati utente:** lo scopo di un certificato utente è quello di autorizzare un determinato utente. In genere, il certificato si ottiene dalla CA (Certificate Authority), come ad esempio cssdesk. Una Certificate Authority è un'entità

affidabile che memorizza, rilascia e pubblica i certificati. Un certificato potrebbe essere necessario per firmare e cifrare e-mail o per collegarsi ad un determinato server.

- **Certificati della macchina:** lo scopo di un certificato macchina è quello di identificare un determinato elaboratore. Quando viene utilizzato un certificato macchina, l'autenticazione è basata sull'elaboratore utilizzato, non sul suo utente.

La procedura guidata per il trasferimento dei certificati di CSS trasferisce solo i certificati della Microsoft contrassegnati come esportabili ed è limitata ai certificati di dimensioni della chiave non superiori ai 1024 bit.

Se un utente deve trasferire un certificato macchina, ma non dispone di privilegi del responsabile del sistema, il responsabile può inviare un file di configurazione del responsabile che abilita l'utente al trasferimento del certificato evitando di fornire la password del responsabile. Per creare il file di configurazione del responsabile, utilizzare il programma di utilità Administrator Console, che si trova al seguente percorso `c:\program files\ibm\security`.

Per utilizzare la procedura guidata al trasferimento dei certificati CSS, completare la procedura di seguito riportata:

1. Fare clic su **Start > Access IBM > IBM Client Security Software > CSS Certificate Transfer Wizard**.
Viene visualizzato il pannello di benvenuto di IBM CSS Certificate Transfer Wizard.
2. Fare clic su **Avanti** per iniziare.
3. Selezionare i tipi di certificato da trasferire, quindi fare clic su **Avanti**. La procedura guidata al trasferimento dei certificati CSS consente di trasferire solo i certificati memorizzati della Microsoft contrassegnati come esportabili.
4. Selezionare i certificati da trasferire facendo clic sul nome del certificato visualizzato nell'area relativa ai certificati rilasciati dell'interfaccia, quindi fare clic su **Avanti**. Viene visualizzato un messaggio indicante che il certificato è stato trasferito correttamente.

Nota: Il trasferimento di un certificato macchina richiede la password del responsabile o un file di configurazione del responsabile.

5. Fare clic su **OK** per tornare alla procedura guidata al trasferimento dei certificati CSS.

Una volta trasferiti, i certificati vengono associati al CSP di IBM embedded Security Subsystem, quindi le chiavi private sono protette da IBM embedded Security Subsystem. Qualunque operazione che utilizza le chiavi private, come ad esempio la creazione di firme digitali o la decifrazione di e-mail, viene effettuata nell'ambiente protetto di IBM embedded Security Subsystem.

Aggiornamento dell'archivio di chiavi per le applicazioni Microsoft

Dopo aver creato un certificato digitale, eseguire una copia di backup del certificato aggiornando l'archivio di chiavi. È possibile aggiornare l'archivio delle chiavi utilizzando Administrator Utility.

Utilizzo del certificato digitale per le applicazioni Microsoft

Utilizzare le impostazioni di protezione nelle proprie applicazioni Microsoft per visualizzare e utilizzare certificati digitali. Per ulteriori informazioni, fare riferimento alla documentazione fornita dalla Microsoft.

Dopo aver creato il certificato digitale e averlo utilizzato per firmare un messaggio e-mail, UVM richiederà i requisiti di autenticazione la prima volta in cui si utilizza una firma digitale su un messaggio e-mail. E' possibile che risulti necessario inserire il passphrase UVM, eseguire una scansione delle proprie impronte digitali oppure entrambi per soddisfare i requisiti di autenticazione necessari per poter utilizzare il certificato digitale. I requisiti di autenticazione vengono definiti nella politica UVM per il computer.

Configurazione delle preferenze audio UVM

User Configuration Utility consente di configurare le preferenze audio utilizzando l'interfaccia fornita. Per modificare le preferenze audio predefinite, procedere nel modo seguente:

1. Fare clic su **Avvio > Programmi > Access IBM > IBM Client Security Software > Modifica le impostazioni di protezione**.
Viene visualizzato il pannello di IBM Client Security Software User Configuration Utility.
2. Selezionare il separatore **Configura suoni UVM**.
3. Nell'area relativa ai suoni di autenticazione UVM, immettere il percorso del file audio da associare ad un'autenticazione riuscita nel campo relativo all'autenticazione riuscita oppure fare clic su **Sfoglia** per selezionare il file.
4. Nell'area relativa ai suoni di autenticazione UVM, immettere il percorso del file audio da associare ad un'autenticazione non riuscita oppure fare clic su **Sfoglia** per selezionare il file.
5. Fare clic su **OK** per completare l'operazione.

Capitolo 5. Risoluzione dei problemi

La seguente sezione riporta informazioni utili a prevenire o identificare e correggere i problemi che potrebbero sorgere quando si utilizza Client Security Software.

Funzioni del responsabile

Questa sezione contiene informazioni che un responsabile potrebbe trovare utili quando si imposta e si utilizza Client Security Software.

IBM Client Security Software può essere utilizzato solo con elaboratori IBM su cui è installato IBM embedded Security Subsystem. Questo software è costituito da applicazioni e componenti che consentono ai client IBM di proteggere le informazioni sensibili mediante la protezione dell'hardware piuttosto che mediante un software, che è più vulnerabile.

Autorizzazione degli utenti

Prima di proteggere le informazioni dell'utente client, IBM Client Security Software **deve** essere installato sul client e gli utenti **devono** essere autorizzati ad utilizzare il software. Una procedura guidata rende più semplice il processo di installazione.

Importante: almeno un utente client **deve** essere autorizzato ad utilizzare UVM durante l'impostazione. Se non è autorizzato alcun utente all'utilizzo di UVM per l'impostazione iniziale di Client Security Software, le impostazioni di protezione **non** verranno applicate e le informazioni **non** verranno protette.

Se la procedura guidata all'installazione viene completata senza l'autorizzazione di alcun utente, chiudere e riavviare l'elaboratore, quindi eseguire la procedura guidata all'installazione di Client Security dal menu Start di Windows, quindi autorizzare un utente Windows all'utilizzo di UVM. Ciò consente a IBM Client Security Software di applicare le impostazioni di protezione alle informazioni sensibili.

Rimozione di utenti

Quando viene eliminato un utente, il nome utente viene eliminato dall'elenco degli utenti Administrator Utility.

Impostazione della password del responsabile di BIOS (ThinkCentre)

Le impostazioni di protezione disponibili in Configuration/Setup Utility consentono ai responsabili di:

- Abilitare o disabilitare IBM embedded Security Subsystem
- Eliminare IBM embedded Security Subsystem

Attenzione:

- Quando IBM embedded Security Subsystem viene eliminato, tutte le chiavi di cifratura e i certificati memorizzati nel sottosistema andranno persi.

Poiché alle impostazioni di protezione è possibile accedere tramite Configuration/Setup Utility, impostare una password di responsabile per evitare che utenti non autorizzati possano modificare le impostazioni.

Per impostare la password del responsabile di BIOS:

1. Chiudere e riavviare l'elaboratore.
2. Quando viene visualizzato sul pannello di Configuration/Setup Utility, premere **F1**.
Viene visualizzato il menu principale di Configuration/Setup Utility.
3. Selezionare **Protezione del sistema**.
4. Selezionare **Password responsabile**.
5. Immettere la password e premere freccia giù sulla tastiera.
6. Immettere di nuovo la password e premere freccia giù.
7. Selezionare **Modifica password responsabile** e premere Invio; premere di nuovo Invio.
8. Premere **Esc** per uscire e salvare le impostazioni.

Dopo aver impostato la password del responsabile di BIOS, viene visualizzata una richiesta ogni volta che si accede a Configuration/Setup Utility.

Importante: conservare un record della password del responsabile di BIOS in un luogo sicuro. Se si perde o si dimentica la password del responsabile di BIOS, non è possibile accedere a Configuration/Setup Utility, quindi non sarà possibile modificare o eliminare la password del responsabile di BIOS senza rimuovere il coperchio dell'elaboratore e spostare un cavallotto che si trova sulla scheda di sistema. Per ulteriori informazioni, consultare la documentazione sull'hardware fornita con il computer.

Impostazione di una password del supervisore (ThinkPad)

Le impostazioni di protezione disponibili nel programma di utilità di impostazione IBM BIOS consentono ai responsabili di:

- Abilitare o disabilitare IBM embedded Security Subsystem
- Eliminare IBM embedded Security Subsystem

Attenzione:

- E' necessario disabilitare temporaneamente la password del supervisore su alcuni modelli ThinkPad prima di installare o aggiornare Client Security Software.

Una volta impostato Client Security Software, impostare una password del supervisore per evitare che utenti non autorizzati possano modificare queste impostazioni.

Per impostare una password del supervisore, procedere nel modo seguente:

Esempio 1

1. Chiudere e riavviare l'elaboratore.
2. Quando viene visualizzata la finestra Setup Utility, premere il tasto F1.
Viene aperto il menu principale di Setup Utility.
3. Selezionare **Password**.
4. Selezionare **Password supervisore**.

5. Immettere la password e premere Invio.
6. Immettere di nuovo la password e premere Invio.
7. Fare clic su **Continua**.
8. Premere F10 per salvare e uscire.

Esempio 2

1. Chiudere e riavviare l'elaboratore.
2. Quando viene visualizzato il messaggio "To interrupt normal startup, press the blue Access IBM button", premere il pulsante blu Access IBM.
Viene aperta Access IBM Predesktop Area.
3. Fare doppio clic su **Start setup utility**.
4. Selezionare **Protezione** utilizzando i tasti di spostamento cursore per spostarsi nel menu.
5. Selezionare **Password**.
6. Selezionare **Password supervisore**.
7. Immettere la password e premere Invio.
8. Immettere di nuovo la password e premere Invio.
9. Fare clic su **Continua**.
10. Premere F10 per salvare e uscire.

Dopo aver impostato la password del supervisore, viene visualizzata una richiesta ogni volta che si accede a BIOS Setup Utility.

Importante: conservare la password del supervisore in un luogo sicuro. Se si perde o si dimentica la password del supervisore, non è possibile accedere al programma di utilità di impostazione IBM BIOS e non è possibile modificare o cancellare la password. Per ulteriori informazioni, consultare la documentazione sull'hardware fornita con il computer.

Protezione della password del responsabile

La password del responsabile limita l'accesso al programma Administrator Utility. Tenere in un luogo sicuro la password del responsabile per impedire agli utenti non autorizzati di modificare le impostazioni del programma Administrator Utility.

Annullamento di IBM embedded Security Subsystem (ThinkCentre)

Se si desidera cancellare tutte le chiavi di cifratura dell'utente da IBM embedded Security Subsystem ed eliminare la password del responsabile del sistema, è necessario azzerare le impostazioni del chip. Prima di riazzere IBM embedded Security Subsystem, leggere le informazioni di seguito riportate.

Attenzione:

- Quando IBM embedded Security Subsystem viene eliminato, tutte le chiavi di cifratura e i certificati memorizzati nel sottosistema andranno perduti.

Per eliminare IBM embedded Security Subsystem, completare la procedura di seguito riportata:

1. Chiudere e riavviare l'elaboratore.
2. Quando viene visualizzata la finestra Setup Utility, premere il tasto F1.
Viene aperto il menu principale di Setup Utility.

3. Selezionare **Security**.
4. Selezionare **IBM TCPA Setup**.
5. Selezionare **Clear IBM TCPA Security Feature**, quindi premere Invio.
6. Selezionare **Yes**.
7. Premere F10, quindi selezionare **Yes**.
8. Premere Invio. L'elaboratore viene riavviato.

Annullamento di IBM embedded Security Subsystem (ThinkPad)

Se si desidera cancellare tutte le chiavi di cifratura dell'utente da IBM embedded Security Subsystem ed eliminare la password del responsabile, è necessario azzerare le impostazioni del sottosistema. Prima di riavviare IBM embedded Security Subsystem, leggere le informazioni di seguito riportate.

Attenzione:

- Quando IBM embedded Security Subsystem viene eliminato, tutte le chiavi di cifratura e i certificati memorizzati nel sottosistema andranno persi.

Per eliminare IBM embedded Security Subsystem, completare la procedura di seguito riportata:

1. Chiudere l'elaboratore
2. Tenere premuto il tasto Fn durante il riavvio dell'elaboratore.
3. Quando viene visualizzata la finestra Setup Utility, premere il tasto F1. Viene aperto il menu principale di Setup Utility.
4. Selezionare **Config**.
5. Selezionare **IBM Security Chip**.
6. Selezionare **Clear IBM Security Chip**.
7. Selezionare **Yes**.
8. Premere Invio per continuare.
9. Premere F10 per salvare e uscire.

Limitazioni note relative a CSS versione 5.2

Le informazioni di seguito riportate potrebbero essere utili per le funzioni di Client Security Software versione 5.2.

Limitazioni di roaming

Utilizzo di un server di roaming CSS

La richiesta della password del responsabile di CSS viene visualizzata ogni volta che un utente tenta di collegarsi al server di roaming CSS. Tuttavia, l'elaboratore può essere utilizzato normalmente evitando di immettere la password.

Utilizzo di IBM Security Password Manager in un ambiente di roaming

Le password memorizzate in un sistema con IBM Client Security Password Manager possono essere utilizzate in altri sistemi che fanno parte dell'ambiente di roaming. Le nuove voci vengono automaticamente richiamate dall'archivio quando l'utente si collega ad un altro sistema (se l'archivio è disponibile) della rete di

roaming. Pertanto, se un utente è già collegato ad un sistema, è necessario che si scolleghi e si ricollegi prima che le nuove voci siano disponibili nella rete di roaming.

Certificati di Internet Explorer e intervallo di aggiornamento di roaming

I certificati di Internet Explorer vengono aggiornati nell'archivio ogni 20 secondi. Quando viene generato un nuovo certificato di Internet Explorer da un utente di roaming, tale utente deve attendere almeno 20 secondi prima di importare, ripristinare o modificare la configurazione CSS su un altro sistema. Se si tenta di effettuare una di queste operazioni prima dei 20 secondi di intervallo di aggiornamento, il certificato verrà perduto. Inoltre, se l'utente non era collegato all'archivio quando è stato generato il certificato, è necessario attendere 20 secondi dopo la connessione all'archivio per essere certi che il certificato sia stato aggiornato nell'archivio stesso.

Password di Lotus Notes e roaming delle credenziali

Se il supporto Lotus Notes è abilitato, la password utente di Lotus Notes viene memorizzata da UVM. Per accedere a Lotus Notes, non è necessario immettere la password Notes per collegarsi a Lotus Notes. Viene richiesto il passphrase, le impronte digitali, la smart card o altro (in base alle impostazioni di protezione).

Se un utente modifica la password Notes dall'ambiente Lotus Notes, il file contenente l'ID Notes ID viene aggiornato con la nuova password e viene aggiornata anche la copia UVM della nuova password Notes. In un ambiente di roaming, le credenziali utente UVM sono disponibili su altri sistemi sulla rete di roaming cui l'utente può accedere. E' possibile che la copia UVM della password di Notes possa non corrispondere alla password di Notes presente nel file contenente l'ID su altri sistemi nella rete di roaming se il file ID di Notes ID contenente la password aggiornata non è disponibile sugli altri sistemi. In questo caso, non sarà possibile accedere a Lotus Notes.

Se un file contenente l'ID Notes con una password aggiornata non è ancora disponibile su un altro sistema, tale file aggiornato dovrebbe essere copiato su altri sistemi della rete di roaming in modo che la password contenuta nel file corrisponda alla copia memorizzata da UVM. Altrimenti, è possibile eseguire Modify Your Security Settings dal menu Start, quindi modificare la password in modo che corrisponda a quella precedente. Quindi, la password Notes può essere aggiornata di nuovo con Lotus Notes.

Disponibilità delle credenziali al collegamento in un ambiente di roaming

Quando l'archivio è in condivisione, le serie più recenti di credenziali utente vengono scaricate dall'archivio quando l'utente vi accede. Al collegamento, gli utenti non dispongono ancora dell'accesso alle condivisioni di rete, quindi non è possibile scaricare le credenziali più recenti fino a quando non viene completato il collegamento. Ad esempio, se il passphrase UVM è stato modificato su un altro sistema nella rete di roaming o se sono state registrate le impronte digitali su un altro sistema, tali aggiornamenti non sono disponibili se non viene completata la procedura di collegamento. Se non sono disponibili le credenziali utente, è necessario immettere il passphrase precedente o altre impronte registrate per collegarsi al sistema. Dopo aver completato il collegamento, le credenziali utente aggiornate sono disponibili e i nuovi passphrase e impronte digitali verranno registrate con UVM.

Limitazioni del badge di prossimità

Abilitazione del collegamento protetto UVM con i badge di prossimità Xyloc

Per abilitare correttamente il collegamento protetto UVM per l'utilizzo con il badge di prossimità CSS, è necessario installare i componenti nell'ordine di seguito riportato:

1. Installare Client Security Software.
2. Abilitare il collegamento protetto UVM utilizzando CSS Administrator Utility.
3. Riavviare il computer.
4. Installare il software Xyloc per il supporto del badge di prossimità.

Nota: Se è installato prima il software del badge di prossimità Xyloc, l'interfaccia di collegamento di Client Security Software non viene visualizzata. In questo caso, è necessario disinstallare Client Security Software, quindi il software Xyloc e poi reinstallarli nell'ordine indicato in precedenza per ripristinare il collegamento protetto UVM.

Supporto Cisco LEAP e badge di prossimità

L'abilitazione della protezione del badge di prossimità e del supporto Cisco LEAP potrebbe causare un comportamento inaspettato. Si consiglia di non installare o utilizzare questi componenti sullo stesso sistema.

Supporto software Ensure

Client Security Software 5.2 richiede agli utenti dei badge di prossimità di aggiornare il software Ensure alla versione 7.41. Se si aggiorna una versione precedente di Client Security Software, aggiornare il software Ensure prima di installare Client Security Software 5.2.

Ripristino delle chiavi

Dopo aver eseguito un'operazione di ripristino delle chiavi, è necessario riavviare l'elaboratore prima di continuare ad utilizzare Client Security Software.

Nomi di dominio e nomi utenti locali

Se i nomi di dominio e nomi utente locali sono uguali, è necessario utilizzare la stessa password di Windows per entrambi gli account. IBM User Verification Manager memorizza solo una password di Windows per ID, in modo che gli utenti utilizzino la stessa password per il collegamento locale e di dominio. Altrimenti, viene richiesto di aggiornare la password Windows di IBM UVM quando si commuta tra il collegamento di dominio e quello locale quando è abilitata la sostituzione del collegamento Windows protetto IBM UVM.

CSS non dispone della possibilità di registrare utenti separati locali e di dominio a parte con lo stesso nome account. Se si tenta di registrare utenti locali e di dominio con lo stesso ID, viene visualizzato il seguente messaggio: L'ID utente selezionato è già stato configurato. CSS non consente una registrazione separata di ID utente locale e di dominio comuni su un sistema, in modo che l'ID utente comune disponga dell'accesso alla stessa serie di credenziali, come ad esempio i certificati, le impronte digitali memorizzate e altro.

Reinstallazione del software per le impronte digitali Targus

Se il software per le impronte digitali Targus viene rimosso e reinstallato, le voci di registro necessarie per l'abilitazione del supporto alle impronte digitali in Client

Security Software devono essere aggiunte manualmente affinché sia abilitato il relativo supporto. Scaricare il file di registro contenente le voci necessarie (atplugin.reg), quindi fare doppio clic per unire le voci al registro. Fare clic su Sì, quando viene richiesto, per confermare l'operazione. E' necessario riavviare il sistema affinché Client Security Software riconosca le modifiche e abiliti il supporto per le impronte digitali.

Nota: Per aggiungere queste voci di registro, è necessario disporre dei privilegi del responsabile del sistema.

Passphrase del supervisore di BIOS

IBM Client Security Software 5.2 e la versione precedente non supportano la funzione passphrase supervisore BIOS disponibile su alcuni sistemi ThinkPad. Se si abilita l'utilizzo del passphrase del supervisore di BIOS, è necessario effettuare qualunque abilitazione o disabilitazione del sottosistema di protezione dal Setup del BIOS.

Utilizzo di 7.x

Netscape 7.x funziona in modo differente da Netscape 4.x. La richiesta del passphrase non viene visualizzata all'avvio di Netscape. Il modulo PKCS#11 viene caricato solo quando necessario, in modo che la richiesta passphrase viene visualizzata solo quando si esegue un'operazione che richiede tale modulo.

Utilizzo di un minidisco per l'archiviazione

Se si specifica un minidisco come posizione di archivio durante la configurazione del software di protezione, potrebbe verificarsi un lungo intervallo di tempo di attesa corrispondente al processo di scrittura dei dati su minidisco. E' possibile considerare altri supporti di memorizzazione, come ad esempio la rete o una chiave USB.

Limitazioni delle Smart card

Registrazione delle smart card

E' necessario registrare le Smart card con UVM prima di autenticare correttamente un utente all'utilizzo della smart card. Se viene assegnata una sola smart card a più utenti, solo l'ultimo utente che l'ha registrata può utilizzarla. Di conseguenza, è necessario registrare le smart card per un solo account utente.

Autenticazione delle smart card

Se viene richiesta una smart card per l'autenticazione, viene visualizzato un dialogo in UVM che richiede la smart card. Quando la smart card viene inserita nel lettore, viene visualizzato un dialogo che richiede il PIN della smart card. Se viene immesso un PIN non corretto, UVM richiede di nuovo la smart card. E' necessario rimuovere la smart card e inserirla nuovamente prima di immettere di nuovo il PIN. E' necessario effettuare tale operazione fino a quando non viene immesso il PIN corretto per la smart card.

Dopo la cifratura viene visualizzato il carattere più (+) sulle cartelle

Dopo la cifratura di file e cartelle, Esplora risorse visualizza un segno più (+) prima dell'icona della cartella. Questo carattere aggiuntivo non viene più visualizzato quando il pannello di Esplora risorse viene aggiornato.

Limitazioni di Windows XP con gli utenti limitati

In Windows XP, con gli utenti limitati, non è possibile aggiornare i passphrase UVM, le password di Windows o aggiornare le chiavi di archivio con User Configuration Utility.

Altre limitazioni

Questa sezione contiene informazioni sulle limitazioni note relative a Client Security Software.

Utilizzo di Client Security Software con sistemi operativi Windows

Tutti i sistemi Windows presentano i seguenti limiti: se un utente client registrato con UVM modifica il nome utente di Windows, si perde la funzionalità Client Security. In caso contrario, sarà necessario registrare nuovamente il nuovo nome utente in UVM e richiedere tutte le nuove credenziali.

I sistemi operativi Windows XP presentano i seguenti limiti: gli utenti registrati in UVM che hanno modificato in precedenza il nome utente Windows non vengono riconosciuti da UVM. UVM punterà al primo nome utente mentre con Windows riconoscerà solo il nuovo nome utente. Questo problema si verifica anche se il nome utente di Windows è stato modificato prima di installare Client Security Software.

Utilizzo di Client Security Software con applicazioni Netscape

Netscape si apre dopo un errore di autorizzazione: se viene visualizzata la finestra Passphrase UVM, è necessario immettere il passphrase UVM, quindi fare clic su **OK** prima di continuare. Se viene immesso un passphrase UVM non corretto (o viene fornita un'impronta non corretta su un dispositivo di scansione impronte), viene visualizzato un messaggio di errore. Facendo clic su **OK**, viene aperto Netscape, ma non sarà possibile utilizzare il certificato digitale generato da IBM embedded Security Subsystem. Prima di poter utilizzare il certificato di IBM embedded Security Subsystem, è necessario uscire e riavviare Netscape, quindi immettere il passphrase UVM corretto.

Gli algoritmi non vengono visualizzati: tutti gli algoritmi supportati dal modulo PKCS#11 di IBM embedded Security Subsystem non sono selezionati se il modulo viene visualizzato in Netscape. I seguenti algoritmi sono supportati dal modulo IBM Security Subsystem PKCS#11 integrato, ma non sono considerati come supportati quando vengono visualizzati in Netscape:

- SHA-1
- MD5

Certificato IBM embedded Security Subsystem e algoritmi di cifratura

Le seguenti informazioni vengono fornite per identificare le emissioni sugli algoritmi di cifratura che possono essere utilizzati con il certificato di IBM embedded Security Subsystem. Consultare Microsoft o Netscape per informazioni sugli algoritmi di cifratura utilizzati con le proprie applicazioni e-mail.

Invio di posta elettronica da un client Outlook Express (128-bit) ad un altro client Outlook Express (128 bit): se risulta possibile utilizzare Outlook Express con la versione a 128 bit di Internet Explorer 4.0 o 5.0 per inviare posta elettronica ad

altri client utilizzando Outlook Express (128 bit), i messaggi di posta elettronica cifrati con certificato IBM embedded Security Subsystem possono utilizzare solo l'algoritmo 3DES.

Invio di posta elettronica tra un client Outlook Express (128-bit) e un client Netscape: al client Netscape con algoritmo RC2(40) viene sempre restituita una richiesta di cifratura RC2(40), RC2(64) o RC2(128) da un client Netscape a un client Outlook Express (128-bit).

Alcuni algoritmi potrebbero non essere disponibili per la selezione in un client Outlook Express (128 bit): in base alla configurazione o all'aggiornamento della versione di Outlook Express (128 bit), alcuni algoritmi RC2 o altri potrebbero non essere disponibili per essere utilizzati con il certificato di IBM embedded Security Subsystem. Consultare Microsoft per le informazioni correnti sugli algoritmi cifrati utilizzati con la versione di Outlook Express.

Utilizzo della protezione UVM per un ID utente Lotus Notes

La protezione UVM non opera se vengono attivati gli ID utente all'interno di una sessione Notes: è possibile impostare la protezione UVM solo per l'ID utente corrente di una sessione Notes. Per passare da un ID utente con protezione UVM abilitato ad un altro ID utente, procedere nel modo seguente:

1. Uscire da Notes.
2. Disabilitare la protezione UVM per l'ID utente corrente.
3. Aprire Notes e attivare gli ID utente. Consultare la documentazione Lotus Notes per informazioni su come attivare gli ID utente.
Per impostare la protezione UVM per l'ID utente attivato, procedere al passo 4.
4. Aprire il programma di configurazione Lotus Notes fornito da Client Security Software ed impostare la protezione UVM.

Limiti di User Configuration Utility

Windows XP impone restrizioni di accesso che limitano le funzioni disponibili ad un utente client in determinate circostanze.

Windows XP Professional

In Windows XP Professional, le restrizioni dell'utente client potrebbero essere applicate nelle seguenti situazioni:

- Client Security Software è installato su una partizione che viene convertita successivamente in un formato NTFS
- La cartella Windows si trova su una partizione che viene convertita successivamente in un formato NTFS
- La cartella di archivio si trova su una partizione che viene convertita successivamente in un formato NTFS

Nelle situazioni precedenti, Windows XP Professional Limited Users potrebbe non essere in grado di eseguire le attività di User Configuration Utility di seguito riportate:

- Modificare il passphrase UVM
- Aggiornare la password di Windows registrata con UVM
- Aggiornare l'archivio delle chiavi

Windows XP Home

Windows XP Home Limited Users non sarà in grado di utilizzare User Configuration Utility in una delle seguenti situazioni:

- Client Security Software è installato su una partizione formattata NTFS
- La cartella Windows si trova su una partizione formattata NTFS
- La cartella di archivio si trova su una partizione formattata NTFS

Limitazioni relative a Tivoli Access Manager

La casella di controllo **Nega tutti gli accessi all'oggetto selezionato** non risulta disabilitata quando viene selezionato il controllo Tivoli Access Manager. Nell'editor della politica UVM, se viene selezionato **Access Manager controlla l'oggetto selezionato** per consentire a Tivoli Access Manager di controllare un oggetto di autenticazione, la casella di controllo **Nega tutti gli accessi all'oggetto selezionato** non è disabilitata. Sebbene la casella di controllo **Nega tutti gli accessi all'oggetto selezionato** risulti disabilitata, non può essere selezionata per sovrascrivere il controllo di Tivoli Access Manager.

Messaggi di errore

I messaggi di errore relativi a Client Security Software sono registrati nel log di eventi: Client Security Software utilizza un driver di periferica che crea i messaggi di errore nel log di eventi. Gli errori associati con questi messaggi non influenzano il normale funzionamento del computer.

UVM richiama i messaggi di errore creati dal programma associato se l'accesso è negato per un oggetto di autenticazione: se la politica UVM è impostata per negare l'accesso per un oggetto di autenticazione, ad esempio la cifratura dell'e-mail, il messaggio che indica l'accesso negato varia in base al tipo di software utilizzato. Ad esempio, un messaggio di errore di Outlook Express che indica l'accesso negato ad un oggetto di autenticazione sarà diverso da un messaggio di errore Netscape, che indica che l'accesso è negato.

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 all'installazione

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

Problema	Possibile soluzione
Un messaggio di errore viene visualizzato durante l'installazione	Azione
Un messaggio viene visualizzato quando si installa il software che richiede di rimuovere l'applicazione selezionata e tutti i relativi componenti.	Per uscire dalla finestra, fare clic su OK . Iniziare di nuovo il processo di installazione per installare la nuova versione del programma Client Security Software.

Problema	Possibile soluzione
Viene visualizzato un messaggio durante l'installazione indicante che è necessario aggiornare o rimuovere il programma.	Eseguire una delle seguenti operazioni: <ul style="list-style-type: none"> • Se è installata una versione precedente a Client Security Software 5.0, selezionare Rimuovi, quindi azzerare il sottosistema di protezione utilizzando IBM BIOS Setup Utility. • In caso contrario, selezionare Aggiorna, quindi continuare con l'installazione.
L'accesso all'installazione viene negato a causa della password del responsabile sconosciuta	Azione
Durante l'installazione su un client IBM con IBM embedded Security Subsystem abilitato, la password del responsabile di IBM embedded Security Subsystem è sconosciuta.	Azzerare Security Subsystem per continuare con l'installazione.

Informazioni sulla risoluzione dei problemi del programma Administrator Utility

Le seguenti informazioni sulla risoluzione dei problemi possono essere utili se si conoscono i problemi quando si utilizza il programma Administrator Utility.

Problema	Possibile soluzione
Il pulsante Avanti non è disponibile in seguito all'immissione e alla conferma del passphrase UVM nel programma Administrator Utility	Azione
Quando si aggiungono utenti a UVM, il pulsante Avanti potrebbe non essere disponibile dopo aver immesso e confermato il passphrase UVM in Administrator Utility.	Fare clic sulla voce Informazioni nella barra delle applicazioni di Windows e continuare la procedura.
Viene visualizzato un messaggio di errore quando si modifica la chiave pubblica del responsabile	Azione
Quando si elimina embedded Security Subsystem e poi si ripristina l'archivio della chiave, è possibile che venga visualizzato un messaggio di errore se si modifica la chiave pubblica del responsabile.	Aggiungere gli utenti a UVM e richiedere i nuovi certificati, se validi.
Un messaggio di errore viene visualizzato quando si ripristina un passphrase UVM.	Azione
Quando si modifica la chiave pubblica del responsabile e si tenta di recuperare una passphrase UVM per un utente, potrebbe essere visualizzato un messaggio di errore.	Effettuare una delle seguenti operazioni: <ul style="list-style-type: none"> • Se il passphrase UVM per l'utente non è necessario, non viene richiesta alcuna azione. • Se il passphrase UVM per l'utente è necessaria, è necessario aggiungere l'utente a UVM e richiedere i nuovi certificati, se validi.
Un messaggio di errore viene visualizzato quando si salva il file di politica UVM	Azione

Problema	Possibile soluzione
Quando si tenta di salvare un file di politica UVM (globalpolicy.gvm) facendo clic su Applica o Salva , viene visualizzato un messaggio di errore.	Chiudere il messaggio di errore, modificare di nuovo il file di politica UVM per apportare le modifiche e salvare poi il file.
Un messaggio di errore viene visualizzato quando si tenta di aprire l'editor di politica UVM	Azione
Se l'utente corrente (collegato al sistema operativo) non è stato aggiunto a UVM, l'editor della politica UVM non sarà visualizzato.	Aggiungere l'utente a UVM ed visualizzare UVM Policy Editor.
Un messaggio di errore viene visualizzato quando si utilizza il programma Administrator Utility	Azione
Quando si utilizza il programma Administrator Utility, è possibile che sia visualizzato il seguente messaggio di errore: Si è verificato un errore I/O buffer durante l'accesso a IBM embedded Security Subsystem. E' possibile che questo problema sia risolto da un riavvio.	Uscire dal messaggio di errore e riavviare il computer.
Quando si modifica la password del responsabile, viene visualizzato un messaggio di errore	Azione
Quando si tenta di modificare la password del responsabile e si preme Invio o il tasto Tab > Invio in seguito all'immissione della password di conferma, viene abilitato il pulsante Disabilita chip , quindi viene visualizzato un messaggio di conferma della disabilitazione di tale chip.	Procedere nel modo seguente: 1. Uscire dalla finestra di conferma di disabilitazione del chip. 2. Per modificare la password del responsabile, immettere la nuova password, immetterla di nuovo per conferma, quindi fare clic su Modifica . Non premere Invio o il tasto di tabulazione > Invio dopo aver immesso la password di conferma.

Informazioni sulla risoluzione dei problemi del programma User Configuration Utility

Le seguenti informazioni sulla risoluzione dei problemi possono essere utili se si verificano problemi durante l'utilizzo del programma User Configuration Utility.

Problema	Possibile soluzione
Limited Users non è abilitato a eseguire alcune funzioni User Configuration Utility in Windows XP Professional	Azione

Problema	Possibile soluzione
Windows XP Professional Limited Users potrebbe non essere in grado di eseguire le attività User Configuration Utility di seguito riportate: <ul style="list-style-type: none"> • Modificare il passphrase UVM • Aggiornare la password di Windows registrata con UVM • Aggiornare l'archivio delle chiavi 	Questa è una limitazione nota con Windows XP Professional. Non esiste alcuna soluzione per questo problema.
Limited Users non è abilitato a utilizzare User Configuration Utility in Windows XP Home	Azione
Windows XP Home Limited Users non sarà in grado di utilizzare User Configuration Utility in una delle seguenti situazioni: <ul style="list-style-type: none"> • Client Security Software è installato su una partizione formattata NTFS • La cartella Windows si trova su una partizione formattata NTFS • La cartella di archivio si trova su una partizione formattata NTFS 	Si tratta di un limite conosciuto con Windows XP Home. Non esiste alcuna soluzione per questo problema.

Informazioni sulla risoluzione dei problemi specifici al ThinkPad

Le seguenti informazioni sulla risoluzione dei problemi possono risultare utili se si conoscono i problemi quando si utilizza il programma Client Security Software su computer ThinkPad.

Problema	Possibile soluzione
Viene visualizzato un messaggio di errore quando si tenta l'esecuzione di una funzione del responsabile di Client Security	Azione
Viene visualizzato un messaggio di errore durante l'esecuzione di una funzione da responsabile di Client Security.	E' necessario che la password del responsabile del ThinkPad sia disabilitata per effettuare determinate funzioni del responsabile di Client Security. Per disabilitare la password del supervisore, procedere nel modo seguente: <ol style="list-style-type: none"> 1. Premere il tasto F1 per accedere al programma IBM BIOS Setup Utility. 2. Inserire la password corrente del responsabile. 3. Inserire una nuova password vuota del responsabile e confermare una password vuota. 4. Premere Invio. 5. Premere F10 per salvare e uscire.
Un diverso sensore per le impronte digitali UVM non funziona correttamente	Azione

Problema	Possibile soluzione
Il computer IBM ThinkPad non supporta l'interscambio di più sensori per le impronte digitali UVM.	Non commutare i modelli del sensore per le impronte digitali. Utilizzare lo stesso modello durante il funzionamento remoto come durante il funzionamento da una stazione per espansione.

Informazioni sulla risoluzione dei problemi della Microsoft

I seguenti grafici sulla risoluzione dei problemi contengono informazioni che possono essere utili se si conoscono i problemi quando si utilizza il programma Client Security Software con le applicazioni o i sistemi operativi della Microsoft.

Problema	Possibile soluzione
Lo screen saver viene visualizzato solo sullo schermo locale	Azione
Durante l'utilizzo della funzione Windows Extended Desktop, lo screen saver di Client Security Software sarà visualizzato solo sullo schermo locale anche se l'accesso al sistema e la tastiera sono protetti.	Se vengono visualizzate le informazioni sensibili, ridurre le finestre del desktop esteso prima di richiamare lo screen saver Client Security.
Client Security non funziona correttamente per un utente registrato in UVM	Azione
E' possibile che l'utente client registrato non abbia modificato il proprio nome utente di Windows. Se si verifica tale situazione, la funzionalità del programma Client Security è persa.	Registrare di nuovo il nuovo nome utente in UVM e richiedere tutte le nuove credenziali.
Nota: In Windows XP, gli utenti registrati in UVM che precedentemente hanno modificato i relativi nomi utente di Windows, non saranno rilevati da UVM. Questo problema si verifica anche se il nome utente di Windows è stato modificato prima di installare Client Security Software.	
Problemi durante la lettura dell'e-mail cifrata mediante Outlook Express	Azione
Le e-mail cifrate non possono essere decifrate a causa delle differenze di cifratura dei browser Web utilizzati dal mittente e dal destinatario.	Verificare quanto segue: <ol style="list-style-type: none"> 1. La cifratura per il browser Web utilizzata dal mittente è compatibile con la cifratura del browser Web utilizzata dal destinatario. 2. La cifratura per il browser Web è compatibile con la cifratura fornita dal firmware del programma Client Security Software.
Problemi durante l'utilizzo di un certificato da un indirizzo dotato di più certificati associati	Azione
Outlook Express può elencare più certificati associati con un singolo indirizzo e-mail ed alcuni di questi certificati possono diventare non validi. Un certificato può diventare non valido se la chiave privata associata al certificato non esiste più in IBM embedded Security Subsystem dell'elaboratore del mittente su cui è stato creato il certificato.	Richiedere al destinatario di rinviare il proprio certificato digitale; quindi, selezionare tale certificato nella rubrica per Outlook Express.

Problema	Possibile soluzione
Messaggio di errore quando si firma un messaggio e-mail in modo digitale	Azione
Se il mittente di un messaggio e-mail prova a firmare un messaggio e-mail in modo digitale quando il mittente non ha già un certificato associato con il relativo account e-mail, viene visualizzato un messaggio di errore.	Utilizzare le impostazioni di protezione in Outlook Express per specificare un certificato da associare con l'account utente. Per ulteriori informazioni, consultare la documentazione fornita per Outlook Express.
Outlook Express (128 bit) cifratura i messaggi e-mail con l'algoritmo 3DES	Azione
Durante l'invio dell'e-mail cifrata tra i client che utilizzano Outlook Express con la versione a 128 bit di Internet Explorer 4.0 o 5.0, è possibile utilizzare solo l'algoritmo 3DES.	Consultare la Microsoft per le informazioni correnti sugli algoritmi di cifratura, utilizzati con Outlook Express.
I client Outlook Express restituiscono i messaggi e-mail con un diverso algoritmo	Azione
Un messaggio e-mail cifrato con l'algoritmo RC2(40), RC2(64) o RC2(128) viene inviato da un client su cui è in uso Netscape Messenger ad un client, su cui è in uso Outlook Express (a 128 bit). Un messaggio e-mail restituito dal client Outlook Express viene cifrato con l'algoritmo RC2(40).	Non è richiesta alcuna azione. Una richiesta di cifratura RC2(40), RC2(64) o RC2(128) da un client di Netscape ad un client di Outlook Express (a 128 bit) viene restituita sempre sul client di Netscape con l'algoritmo RC2(40). Consultare Microsoft per le informazioni correnti sugli algoritmi cifrati utilizzati con la versione di Outlook Express.
Messaggio di errore durante l'utilizzo di un certificato in Outlook Express in seguito ad un errore dell'unità disco fisso	Azione
I certificati possono essere ripristinati utilizzando la funzione per il ripristino della chiave nel programma Administrator Utility. E' possibile che alcuni certificati, ad esempio i certificati disponibili, forniti da VeriSign, non siano ripristinati in seguito ad un ripristino della chiave.	Una volta ripristinate le chiavi, procedere nel modo seguente: <ul style="list-style-type: none"> • reperire i nuovi certificati • registrare di nuovo l'autorizzazione del certificato in Outlook Express
Outlook Express non aggiorna la cifratura associata con un certificato	Azione
Quando un mittente seleziona la cifratura in Netscape ed invia un messaggio e-mail firmato ad un client su cui è in uso Outlook Express con Internet Explorer 4.0 (a 128 bit), è possibile che la cifratura dell'e-mail restituita non corrisponda.	Eliminare il certificato associato dalla rubrica di Outlook Express. Visualizzare di nuovo l'e-mail firmata ed aggiungere il certificato alla rubrica di Outlook Express.
Un messaggio di errore viene visualizzato in Outlook Express	Azione
E' possibile visualizzare un messaggio in Outlook Express quando si fa doppio clic. In alcuni casi, quando si fa doppio clic su un messaggio cifrato in modo rapido, viene visualizzato un messaggio di errore relativo alla decifrazione.	Chiudere il messaggio ed aprire nuovamente il messaggio e-mail cifrato.

Problema	Possibile soluzione
Inoltre, è possibile che un messaggio di errore relativo alla decifrazione sia visualizzato nel pannello precedente quando si seleziona un messaggio cifrato.	Se il messaggio di errore viene visualizzato nel pannello precedente, non è richiesta alcuna azione.
Un messaggio di errore viene visualizzato se si fa clic sul pulsante Invia due volte su e-mail cifrate	Azione
Quando si utilizza Outlook Express, se si fa doppio clic sul pulsante di invio per inviare un messaggio e-mail cifrato, viene visualizzato un messaggio di errore indicante che il messaggio non può essere inviato.	Chiudere questo messaggio di errore, quindi fare clic sul pulsante Invia .
Un messaggio di errore viene visualizzato quando viene richiesto un certificato	Azione
Quando si utilizza Internet Explorer, è possibile ricevere un messaggio di errore se si richiede un certificato che utilizza IBM embedded Security Subsystem CSP.	Richiedere di nuovo il certificato digitale.

Informazioni sulla risoluzione dei problemi dell'applicazione Netscape

I seguenti grafici sulla risoluzione dei problemi contengono informazioni che possono essere utili se si conoscono i problemi quando si utilizza il programma Client Security Software con le applicazioni di Netscape.

Problema	Possibile soluzione
Problemi durante la lettura dell'e-mail cifrata	Azione
Le e-mail cifrate non possono essere decifrate a causa delle differenze di cifratura dei browser Web utilizzati dal mittente e dal destinatario.	Verificare quanto segue: <ol style="list-style-type: none"> 1. Che la cifratura per il browser Web utilizzata dal mittente sia compatibile con la cifratura del browser Web utilizzata dal destinatario. 2. Che la cifratura per il browser Web sia compatibile con la cifratura fornita dal firmware del programma Client Security Software.
Messaggio di errore quando si firma un messaggio e-mail in modo digitale	Azione
Se il certificato di IBM embedded Security Subsystem non è stato selezionato in Netscape Messenger e il mittente del messaggio e-mail tenta di firmare tale messaggio con il certificato, viene visualizzato un messaggio di errore.	Utilizzare le impostazioni di protezione in Netscape Messenger per selezionare il certificato. Quando viene aperto Netscape Messenger, fare clic sull'icona Protezione, situata sulla barra degli strumenti. Viene visualizzata la finestra Info protezione. Fare clic su Messenger situato nel pannello sinistro e poi selezionare il certificato di IBM embedded Security Chip . Per ulteriori informazioni, fare riferimento alla documentazione fornita da Netscape.

Problema	Possibile soluzione
Un messaggio e-mail viene restituito al client con un diverso algoritmo	Azione
Un messaggio e-mail cifrato con l'algoritmo RC2(40), RC2(64) o RC2(128) viene inviato da un client su cui è in uso Netscape Messenger ad un client, su cui è in uso Outlook Express (a 128 bit). Un messaggio e-mail restituito dal client Outlook Express viene cifrato con l'algoritmo RC2(40).	Non è richiesta alcuna azione. Una richiesta di cifratura RC2(40), RC2(64) o RC2(128) da un client di Netscape ad un client di Outlook Express (a 128 bit) viene restituita sempre sul client di Netscape con l'algoritmo RC2(40). Consultare Microsoft per le informazioni correnti sugli algoritmi cifrati utilizzati con la versione di Outlook Express.
Impossibile utilizzare un certificato digitale generato da IBM embedded Security Subsystem	Azione
Il certificato digitale generato da IBM embedded Security Subsystem non è disponibile per l'utilizzo.	Verificare che il passphrase UVM corretto sia stato inserito quando viene visualizzato Netscape. Se si inserisce il passphrase UVM errata, viene visualizzato un messaggio di errore di autenticazione. Facendo clic su OK , viene aperto Netscape, ma non sarà possibile utilizzare il certificato generato da IBM embedded Security Subsystem. E' necessario uscire e riaprire Netscape, quindi inserire il passphrase corretto UVM.
I nuovi certificati digitali dallo stesso mittente non sono sostituiti all'interno di Netscape	Azione
Quando viene ricevuta un'e-mail firmata in modo digitale più di una volta dallo stesso mittente, il primo certificato digitale associato con l'e-mail non viene sovrascritto.	Se si ricevono più certificati e-mail, solo un certificato è quello predefinito. Utilizzare le funzioni di protezione di Netscape per eliminare il primo certificato, quindi riaprire il secondo certificato o richiedere al mittente di inviare un'altra e-mail firmata.
Impossibile esportare il certificato di IBM embedded Security Subsystem	Azione
Il certificato di IBM embedded Security Subsystem non può essere esportato in Netscape. La funzione di esportazione di Netscape può essere utilizzata per eseguire il backup dei certificati.	Passare al programma Administrator Utility o User Configuration Utility per aggiornare l'archivio chiave. Quando si aggiorna la chiave di archivio, vengono create le copie di tutti i certificati associati a IBM embedded Security Subsystem.
Un messaggio di errore viene visualizzato durante il tentativo di utilizzare un certificato ripristinato in seguito ad un errore del disco fisso	Azione
I certificati possono essere ripristinati utilizzando la funzione per il ripristino della chiave nel programma Administrator Utility. E' possibile che alcuni certificati, ad esempio i certificati disponibili, forniti da VeriSign, non siano ripristinati in seguito ad un ripristino della chiave.	Una volta ripristinate le chiavi, reperire un nuovo certificato.
L'agente di Netscape viene visualizzato e causa un errore relativo a Netscape	Azione

Problema	Possibile soluzione
L'agente di Netscape visualizza e chiude Netscape.	Disattivare l'agente di Netscape.
Netscape ritarda quando si tenta di aprirlo	Azione
Se si aggiunge il modulo PKCS#11 di IBM embedded Security Subsystem e si apre Netscape, quest'ultimo viene aperto dopo un intervallo di tempo maggiore rispetto alla norma.	Non è richiesta alcuna azione. Queste informazioni sono valide solo a scopo informativo.

Informazioni sulla risoluzione dei problemi relativi al certificato digitale

Le seguenti informazioni sulla risoluzione dei problemi possono essere utili se si conoscono i problemi relativi al reperimento di un certificato digitale.

Problema	Possibile soluzione
La finestra del passphrase UVM o la finestra di autenticazione delle impronte digitali viene visualizzata più volte durante una richiesta del certificato digitale.	Azione
La politica di protezione UVM indica che un utente fornisce il passphrase UVM o le impronte digitali prima di poter acquistare un certificato digitale. Se l'utente tenta di acquistare un certificato, la finestra di autenticazione richiede che la scansione delle impronte digitali o il passphrase UVM viene visualizzata più di una volta.	Inserire il passphrase UVM oppure eseguire la scansione delle impronte digitali ogni volta che viene visualizzata la finestra di autenticazione.
Viene visualizzato un messaggio di errore VBScript o JavaScript	Azione
Se si richiede un certificato digitale, è possibile che sia un messaggio di errore relativo a VBScript o JavaScript.	Riavviare il computer e reperire di nuovo il certificato.

Informazioni sulla risoluzione dei problemi di Tivoli Access Manager

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

Problema	Possibile soluzione
Le impostazioni sulla politica locali non corrispondono a quelle sul server	Azione
Tivoli Access Manager consente alcune configurazioni non supportate da UVM. Di conseguenza, i requisiti sulla politica locali possono ignorare le impostazioni del responsabile durante la configurazione del server PD.	Si tratta di un limite conosciuto.
Le impostazioni di Tivoli Access Manager non sono accessibili.	Azione

Problema	Possibile soluzione
Le impostazioni di Tivoli Access e della cache locale non sono accessibili dalla pagina relativa in Administrator Utility.	Installare Tivoli Access runtime Environment. Se Runtime Environment non è installato sul client IBM, le impostazioni di Tivoli Access sulla pagina relativa non saranno disponibili.
Il controllo utente è valido sia per l'utente che per il gruppo	Azione
Quando viene configurato il server di Tivoli Access, se si definisce l'utente di un gruppo, il controllo utente è valido sia per l'utente che per il gruppo.	Non è richiesta alcuna azione.

Informazioni sulla risoluzione dei problemi relativi a Lotus Notes

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

Problema	Possibile soluzione
Dopo l'abilitazione della protezione UVM per Lotus Notes, Notes non è in grado di terminare l'installazione	Azione
Lotus Notes non è in grado di terminare l'installazione dopo che viene abilitata la protezione UVM utilizzando il programma Administrator Utility.	Si tratta di un limite conosciuto. E' necessario che Lotus Notes sia configurato e sia in esecuzione prima che sia abilitato il supporto Lotus Notes nel programma Administrator Utility.
Un messaggio di errore viene visualizzato quando si tenta di modificare la password di Notes	Azione
E' possibile che la modifica della password di Notes durante l'utilizzo del programma Client Security Software visualizzi un messaggio di errore.	Riprovare la modifica della password. Se non funziona, riavviare il client.
Un messaggio di errore viene visualizzato in seguito ad una creazione casuale di una password	Azione
E' possibile che un messaggio di errore sia visualizzato quando si procede nel modo seguente: <ul style="list-style-type: none"> • Utilizzare lo strumento Configurazione di Lotus Notes per impostare la protezione UVM per un ID Notes • Visualizzare Notes ed utilizzare la funzione fornita da Notes per modificare la password per il file ID Notes • Chiudere Notes immediatamente dopo la modifica della password 	Fare clic su OK per chiudere il messaggio di errore. Non è richiesta ulteriore azione. Diversamente dal messaggio di errore, la password è stata modificata. La nuova password è una password creata in modo casuale dal programma Client Security Software. Il file ID Notes viene cifrato con la password creata in modo casuale e l'utente non necessita di un nuovo file ID utente. Se l'utente modifica di nuovo la password, UVM crea una nuova password casuale per ID Notes.

Informazioni sulla risoluzione dei problemi relativi alla cifratura

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

Problema	Possibile soluzione
I file cifrati precedentemente non saranno decifrati	Azione
I file cifrati con le versioni precedenti del programma Client Security Software non sono cifrati in seguito all'aggiornamento del programma Client Security Software 3.0 o successive.	Si tratta di un limite conosciuto. E' necessario decifrare tutti i file che sono stati cifrati, utilizzando versioni precedenti del programma Client Security Software, <i>prima</i> 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.

Informazioni sulla risoluzione dei problemi relativi all'unità UVM

Le seguenti informazioni sulla risoluzione dei problemi possono essere utili se si conoscono i problemi quando si utilizzano le unità UVM.

Problema	Possibile soluzione
Un'unità UVM interrompe il funzionamento correttamente	Azione
Una periferica protetta da UVM, come ad esempio una smart card, un lettore per smart card o per le impronte digitali non sta funzionando correttamente.	Confermare se la periferica è stata configurata correttamente. Una volta configurata la periferica, è necessario riavviare il sistema per avviarla correttamente. Per informazioni sulla risoluzione dei problemi per la periferica, consultare la documentazione fornita con la periferica stesso o rivolgersi al relativo fornitore.
Un'unità UVM interrompe il funzionamento correttamente	Azione
Quando un'unità UVM viene scollegata dalla porta USB (Universal Serial Bus) e poi l'unità viene collegata di nuovo alla porta USB, è possibile che l'unità non funzioni correttamente.	Riavviare il computer una volta collegata nuovamente l'unità alla porta USB.

Appendice A. Informazioni sulle password e i passphrase

L'appendice contiene informazioni sulle password e i passphrase.

Regole per password e passphrase

In un sistema protetto, sono presenti varie password e passphrase. Le varie password dispongono di regole diverse. Questa sezione contiene informazioni sulla password del responsabile e sui passphrase UVM.

Regole per la password del responsabile

Le regole per la password del responsabile non possono essere modificate dal responsabile della protezione.

Di seguito sono riportate le regole applicate alla password del responsabile:

Lunghezza

Le password devono essere costituite esattamente da otto caratteri.

Caratteri

La password deve contenere solo caratteri alfanumerici. E' consentita una combinazione di lettere e di numeri. Non è consentito alcun carattere aggiuntivo, come lo spazio, !, ?, %.

Proprietà

Impostare la password del responsabile per abilitare IBM Embedded Security Chip nell'elaboratore. E' necessario che questa password sia immessa ogni volta che si accede ai programmi Administrator Utility e Administrator Console.

Tentativi non corretti

Se si inserisce la password in modo non corretto per dieci volte, il computer viene bloccato per 1 ora e 17 minuti. Se trascorre tale periodo di tempo, inserire la password in modo non corretto per più di dieci volte, il computer viene bloccato per 2 ore e 34 minuti. L'intervallo di tempo della disabilitazione del computer raddoppia ogni volta che si inserisce in modo errato la password per dieci volte.

Regole per passphrase UVM

IBM Client Security Software consente ai responsabili della protezione di impostare le regole dei passphrase UVM per gli utenti. Per migliorare la protezione, il passphrase UVM è più lunga e può essere più univoca rispetto alla password tradizionale. La politica passphrase UVM è controllata da Administrator Utility.

L'interfaccia relativa alla politica passphrase UVM in Administrator Utility consente ai responsabili della protezione di controllare i criteri passphrase tramite una semplice interfaccia. L'interfaccia relativa alla politica passphrase UVM consente al responsabile di stabilire le regole passphrase di seguito riportate:

Nota: L'impostazione predefinita per ciascun criterio di passphrase viene fornita di seguito tra parentesi.

- stabilire se impostare un numero minimo di caratteri alfanumerici consentiti (si, 6)

Ad esempio, quando è impostato a "6" caratteri consentiti, 1234567xxx è una password non valida.

- stabilire se impostare un numero minimo di caratteri numerici consentiti (si, 1)
Ad esempio, quando è impostato a "1", questa è la password è una password non valida.
- stabilire se impostare un numero minimo di spazi consentiti (nessun minimo)
Ad esempio, quando è impostato a "2", non sono qui è una password non valida.
- stabilire se consentire che il passphrase inizi con un carattere numerico (no)
Ad esempio, per impostazione predefinita, 1password è una password non valida.
- stabilire se consentire che il passphrase termini con un carattere numerico (no)
Ad esempio, per impostazione predefinita, password8 è una password non valida.
- stabilire se consentire che il passphrase contenga un ID utente (no)
Ad esempio, per impostazione predefinita, Nome Utente è una password non valida, dove Nome Utente è un ID utente.
- stabilire se consentire che il nuovo passphrase sia diverso dagli ultimi x passphrase, dove x è un campo editabile (si, 3)
Ad esempio, per impostazione predefinita, password è una password non valida se qualcuna delle ultime tre password era password.
- stabilire se il passphrase può contenere più di tre caratteri consecutivi identici in qualunque posizione rispetto alla password precedente (no)
Ad esempio, per impostazione predefinita, paswor è una password non valida se la password precedente era pass o word.

Inoltre, l'interfaccia relativa alla politica passphrase UVM in Administrator Utility consente ai responsabili della protezione di controllare i criteri di scadenza dei passphrase. L'interfaccia relativa alla politica passphrase UVM consente al responsabile di scegliere tra le regole di scadenza passphrase di seguito riportate:

- Stabilire se il passphrase scade dopo un numero di giorni precedentemente impostato (si, 184)
Ad esempio, per impostazione predefinita il passphrase scade dopo 184 giorni. E' necessario che il nuovo passphrase sia conforme alla politica dei passphrase stabilita.
- stabilire se il passphrase scade (sì)
Quando viene selezionata questa opzione, il passphrase non scade.

La politica passphrase è controllata in Administrator Utility quando l'utente si iscrive, quindi viene anche controllato quando l'utente modifica il passphrase da Client Utility. Le due impostazioni utente collegate alla password precedente verranno reimpostate e verrà rimossa la cronologia dei passphrase.

Le seguenti regole si applicano al passphrase UVM:

Lunghezza

Il passphrase può contenere fino a 256 caratteri.

Caratteri

Il passphrase può contenere qualunque combinazione di caratteri prodotti dalla tastiera, compresi gli spazi e i caratteri non alfanumerici.

Proprietà

Il passphrase UVM è diverso da una password da utilizzare per collegarsi ad un sistema operativo. Il passphrase UVM può essere utilizzato insieme ad altre unità di autenticazione, ad esempio un sensore per le impronte digitali UVM.

Tentativi non corretti

Se si immette il passphrase UVM in modo non corretto per più volte durante una sessione, l'elaboratore sperimenta una serie di ritardi. Questi ritardi sono specificati nella sezione di seguito riportata.

Conteggi errati su sistemi TCPA e non TCPA

La tabella di seguito riportata illustra le impostazioni relative al ritardo per un sistema TCPA:

Tentativi	Ritardo al malfunzionamento successivo
15	1,1 minuti
31	2,2 minuti
47	4,4 minuti
63	8,8 minuti
79	17,6 minuti
95	35,2 minuti
111	1,2 ore
127	2,3 ore
143	4,7 ore

I sistemi TCPA non distinguono tra passphrase utente e password del responsabile. Qualunque autenticazione con IBM Embedded Security Chip è sottoposta alla stessa politica. Il timeout massimo è di 4,7. I sistemi TCPA non ritardano per un intervallo di tempo superiore alle 4,7.

I sistemi non TCPA distinguono tra password del responsabile e passphrase utente. Su sistemi non TCPA, la password del responsabile dispone di un ritardo di 77 dopo dieci tentativi non riusciti, quindi il tempo di blocco raddoppia dopo ogni 32 tentativi non riusciti.

Reimpostazione di un passphrase

Se un utente dimentica il passphrase, il responsabile può abilitare l'utente per riattivare tale passphrase.

Reimpostazione remota di un passphrase

Per impostare in remoto una password, completare la procedura di seguito riportata:

- **Responsabili**

E' necessario che un responsabile remoto effettui le operazioni di seguito riportate:

1. Creare e comunicare la nuova password temporanea all'utente.
2. Inviare un file di dati all'utente.

I file di dati possono essere inviati all'utente mediante e-mail, copiati su un supporto rimovibile, come ad esempio un minidisco o scritti direttamente nel file di archivio dell'utente (se l'utente dispone dell'accesso al sistema). Il file cifrato viene utilizzato come corrispondenza alla nuova password temporanea.

- **Utenti**

Gli utenti possono procedere nel modo seguente:

1. Collegarsi all'elaboratore.
2. Quando viene richiesto il passphrase, contrassegnare la casella di controllo "Passphrase dimenticato".
3. Immettere la password temporanea comunicata dal responsabile remoto, quindi fornire la posizione del file inviato da quest'ultimo.

Una volta che UVM ha verificato che le informazioni del file corrispondono alla password fornita, è concesso l'accesso all'utente. Viene richiesto di modificare immediatamente il passphrase dell'utente.

Questo è il modo consigliato per riassetare un passphrase dimenticato.

Reimpostazione manuale di un passphrase

Se il responsabile può collegarsi al sistema di un utente che ha dimenticato il passphrase, può anche collegarsi al sistema dell'utente come responsabile, fornire la chiave privata del responsabile in Administrator Utility, quindi modificare manualmente il passphrase dell'utente. Per modificare il passphrase, non è necessario che il responsabile conosca il passphrase precedente.

Appendice B. Marchi e informazioni particolari

La presente appendice contiene informazioni particolari relative ai prodotti IBM e le informazioni sui marchi.

Informazioni particolari

Queste informazioni sono state sviluppate per prodotti e servizi offerti negli Stati Uniti

I riferimenti contenuti in questa pubblicazione relativi a prodotti o servizi IBM non implicano che l'IBM intenda renderli disponibili in tutti i paesi in cui opera. Consultare il rappresentante IBM locale per informazioni relative a prodotti e servizi disponibili nel proprio paese. Qualsiasi riferimento a prodotti, programmi o servizi IBM non implica che possano essere utilizzati soltanto tali prodotti, programmi o servizi. 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

Il seguente paragrafo non è valido per il regno Unito o per tutti i paesi le cui leggi nazionali siano in contrasto con le disposizioni locali: 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 COMMERCIALIZZATA 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.

Coloro che detengono la licenza su questo programma e desiderano avere informazioni su di esso allo scopo di consentire (1) uno scambio di informazioni tra programmi indipendenti ed altri (compreso questo) e (ii) l'uso reciproco di tali informazioni, dovrebbero rivolgersi a IBM Corporation, Department 80D, P.O. Box 12195, 3039 Cornwallis, Research Triangle Park, NC 27709 U.S.A. Queste

informazioni possono essere rese disponibili secondo condizioni contrattuali appropriate, compreso, in alcuni casi, il pagamento di un addebito.

Il programma su licenza descritto in questo manuale e tutto il materiale su licenza ad esso relativo sono forniti dall'IBM nel rispetto dei termini dell'IBM Customer Agreement, dell'IBM International Program License Agreement o ad ogni altro accordo equivalente.

Marchi

IBM e SecureWay sono marchi IBM Corporation.

Tivoli è un marchio Tivoli Systems Inc.

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

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

Riservato ai commenti del lettore

Soluzioni IBM® Client Security
Client Security Software versione 5.3 Guida per l'utente

Commenti relativi alla pubblicazione in oggetto potranno contribuire a migliorarla. Sono graditi commenti pertinenti alle informazioni contenute in questo manuale ed al modo in cui esse sono presentate. Si invita il lettore ad usare lo spazio sottostante citando, ove possibile, i riferimenti alla pagina ed al paragrafo.

Si prega di non utilizzare questo foglio per richiedere informazioni tecniche su sistemi, programmi o pubblicazioni e/o per richiedere informazioni di carattere generale.

Per tali esigenze si consiglia di rivolgersi al punto di vendita autorizzato o alla filiale IBM della propria zona oppure di chiamare il "Supporto Clienti" IBM al numero verde 800-017001.

I suggerimenti ed i commenti inviati potranno essere usati liberamente dall'IBM e dalla Selfin e diventeranno proprietà esclusiva delle stesse.

Commenti:

Si ringrazia per la collaborazione.

Per inviare i commenti è possibile utilizzare uno dei seguenti modi.

- Spedire questo modulo all'indirizzo indicato sul retro.
- Inviare un fax al numero: +39-0823-353137
- Spedire una nota via email a: translationassurance@selfin.it

Se è gradita una risposta dalla Selfin, si prega di fornire le informazioni che seguono:

Nome

Indirizzo

Società

Numero di telefono

Indirizzo e-mail

Indicandoci i Suoi dati, Lei avrà l'opportunità di ottenere dal responsabile del Servizio di Translation Assurance della Selfin S.p.A. le risposte ai quesiti o alle richieste di informazioni che vorrà sottoporci. I Suoi dati saranno trattati nel rispetto di quanto stabilito dalla legge 31 dicembre 1996, n.675 sulla "Tutela delle persone e di altri soggetti rispetto al trattamento di dati personali". I Suoi dati non saranno oggetto di comunicazione o di diffusione a terzi; essi saranno utilizzati "una tantum" e saranno conservati per il tempo strettamente necessario al loro utilizzo.

Selfin S.p.A.
Translation Assurance

Via Pozzillo

Località Ponteselice
81100 CASERTA

IBM