IBM Client Security Solutions

Client Security Version 5.3 Administratorhandbuch

IBM Client Security Solutions

Client Security Version 5.3 Administratorhandbuch

Hinweis:
Vor Verwendung dieser Informationen und des darin beschriebenen Produkts sollten Sie die Informationen in Anhang C, „Bemerkungen und Marken", auf Seite 97 lesen.

- Die IBM Homepage finden Sie im Internet unter: **ibm.com**
- IBM und das IBM Logo sind eingetragene Marken der International Business Machines Corporation.
- Das e-business-Symbol ist eine Marke der International Business Machines Corporation.
- Infoprint ist eine eingetragene Marke der IBM.
- ActionMedia, LANDesk, MMX, Pentium und ProShare sind Marken der Intel Corporation in den USA und/oder anderen Ländern.
- C-bus ist eine Marke der Corollary, Inc. in den USA und/oder anderen Ländern.
- Java und alle auf Java basierenden Marken und Logos sind Marken der Sun Microsystems, Inc. in den USA und/oder anderen Ländern.
- Microsoft Windows, Windows NT und das Windows-Logo sind Marken der Microsoft Corporation in den USA und/oder anderen Ländern.
- PC Direct ist eine Marke der Ziff Communications Company in den USA und/oder anderen Ländern.
- SET und das SET-Logo sind Marken der SET Secure Electronic Transaction LLC.
- UNIX ist eine eingetragene Marke der Open Group in den USA und/oder anderen Ländern.
- Marken anderer Unternehmen/Hersteller werden anerkannt.

Erste Ausgabe (Mai 2004)

Diese Veröffentlichung ist eine Übersetzung des Handbuchs
IBM Client Security Solutions, Client Security Version 5.3 Administrator's Guide,
herausgegeben von International Business Machines Corporation, USA

Informationen, die nur für bestimmte Länder Gültigkeit haben und für Deutschland, Österreich und die Schweiz nicht zutreffen, wurden in dieser Veröffentlichung im Originaltext übernommen.

Möglicherweise sind nicht alle in dieser Übersetzung aufgeführten Produkte in Deutschland angekündigt und verfügbar; vor Entscheidungen empfiehlt sich der Kontakt mit der zuständigen IBM Geschäftsstelle.

Änderung des Textes bleibt vorbehalten.

Herausgegeben von:
SW TSC Germany
Kst. 2877
Mai 2004

Inhaltsverzeichnis

Vorwort

Dieses Handbuch enthält Informationen zur Konfiguration und zur Verwendung der Sicherheitsfunktionen von Client Security.

Das Handbuch ist wie folgt aufgebaut:

Kapitel 1, „Einführung", enthält eine Übersicht über die Anwendungen und Komponenten der Software sowie eine Beschreibung der PKI-Funktionen.

Kapitel 2, „Dateien und Ordner verschlüsseln und entschlüsseln", enthält Informationen zur Verwendung von Client Security für den Schutz sensibler Dateien und Ordner.

Kapitel 3, „Standortunabhängiger Zugriff mit Berechtigungsnachweis in CSS", enthält Informationen zur Konfiguration eines CSS-Netzwerks mit standortunabhängigem Zugriff mit Berechtigungsnachweis, zur Registrierung eines Clients mit standortunabhängigem Zugriff, zur Autorisierung und zum Import von Benutzern, zur Synchronisierung von Benutzerdaten sowie zur Wiederherstellung eines Netzwerks mit standortunabhängigem Zugriff.

Kapitel 4, „Client Security verwenden", enthält Beispiele zur Verwendung von Client Security-Komponenten für die Konfiguration der von IBM Clientbenutzern benötigten Sicherheitseinrichtungen.

Kapitel 5, „Benutzer autorisieren", enthält Informationen zur Authentifizierung von Clientbenutzern und erläutert das Autorisieren und Entfernen von Benutzern im User Verification Manager (UVM).

Kapitel 6, „Nach dem Autorisieren von Benutzern in UVM", enthält Anweisungen zum Einrichten des UVM-Schutzes für die Anmeldung am Betriebssystem, zur Verwendung des UVM-Schutzes für Lotus Notes und zur Verwendung von Client Security mit Netscape-Anwendungen.

Kapitel 7, „Mit der UVM-Policy arbeiten", enthält Anweisungen zum Bearbeiten einer lokalen UVM-Policy, zur Verwendung einer UVM-Policy für einen fernen Client und zum Ändern des Kennworts für eine UVM-Policy-Datei.

Kapitel 8, „Weitere Funktionen des Sicherheitsadministrators", enthält Anweisungen zum Ändern der Position des Schlüsselarchivs, zur Schlüsselwiederherstellung aus einem Archiv, zum Wiederherstellen eines UVM-Verschlüsselungstextes und zum Aktivieren oder Inaktivieren des integrierten IBM Security Chips mit Hilfe des Administratordienstprogramms.

Kapitel 9, „Anweisungen für den Clientbenutzer", enthält Anweisungen zu unterschiedlichen Tasks, die der Clientbenutzer mit Client Security ausführen kann. Dazu gehören Anweisungen zur Verwendung des UVM-Anmeldeschutzes, der sicheren E-Mail-Übertragung und des Benutzerkonfigurationsprogramms.

Kapitel 10, „Fehlerbehebung", enthält nützliche Informationen zum Umgehen bekannter Einschränkungen und Fehler, die möglicherweise beim Befolgen der Anweisungen in diesem Handbuch auftreten.

Anhang A, „Informationen zu Kennwörtern und Verschlüsselungstexten", enthält Kriterien für Kennwörter, die auf einen UVM-Verschlüsselungstext angewendet werden können, und Regeln für Kennwörter für den IBM Security Chip.

Anhang B, „Regeln für den UVM-Schutz für die Anmeldung am System", enthält Informationen zur Verwendung des UVM-Schutzes für die Anmeldung am Betriebssystem.

Anhang C, „Bemerkungen und Marken", enthält rechtliche Hinweise und Informationen zu Marken.

Zielgruppe

Dieses Handbuch ist für Sicherheitsadministratoren bestimmt, die folgende Vorgänge durchführen:

- Benutzerauthentifizierung für den IBM Client konfigurieren
- UVM-Sicherheitspolicy für IBM Clients konfigurieren und bearbeiten
- Mit Hilfe des Administratordienstprogramms das Sicherheits-Subsystem (integrierter IBM Security Chip) und den einzelnen IBM Clients zugeordnete Einstellungen verwalten.

Dieses Handbuch ist außerdem für Tivoli Access Manager-Administratoren konzipiert, die mit IBM Tivoli Access Manager Authentifizierungsobjekte verwalten, die sich in der UVM-Policy befinden. Tivoli Access Manager-Administratoren müssen Folgendes verwalten können:

- Objektbereich von Tivoli Access Manager
- Prozesse für die Authentifizierung, die Autorisierung und die Anforderung des Berechtigungsnachweises
- IBM Umgebung mit verteilter Datenverarbeitung (IBM Distributed Computing Environment - DCE)
- Protokoll "LDAP" (Lightweight Directory Access Protocol) von IBM SecureWay Directory

Benutzung des Handbuchs

Mit diesem Handbuch können Sie die Benutzerauthentifizierung und die UVM-Sicherheitspolicy für IBM Clients konfigurieren. Es wird ergänzt durch das *Client Security Installationshandbuch*, das Handbuch *Client Security mit Tivoli Access Manager verwenden* und das *Client Security Benutzerhandbuch*. Das vorliegende Handbuch und die gesamte Dokumentation zu Client Security kann von der IBM Website unter http://www.pc.ibm.com/us/security/secdownload.html heruntergeladen werden.

Verweise auf das *Client Security Installationshandbuch*

In diesem Dokument finden Sie Verweise auf das *Client Security Installationshandbuch*. Sie müssen Client Security auf einem IBM Client installieren, bevor Sie das vorliegende Handbuch verwenden können. Anweisungen zur Softwareinstallation finden Sie im *Client Security Installationshandbuch*.

Verweise auf das Handbuch *Client Security mit Tivoli Access Manager verwenden*

In diesem Dokument finden Sie Verweise auf das Handbuch *Client Security mit Tivoli Access Manager verwenden*. Sicherheitsadministratoren, die mit Tivoli Access Manager Authentifizierungsobjekte für die UVM-Policy verwalten, sollten das Handbuch *Client Security mit Tivoli Access Manager verwenden* lesen.

Verweise auf das *Client Security Benutzerhandbuch*

In diesem Dokument finden Sie Verweise auf das *Client Security Benutzerhandbuch*. Administratoren können mit diesem Handbuch UVM-Policies auf IBM Clients, auf denen Client Security eingesetzt wird, verwalten und warten. Nachdem ein Administrator die Benutzerauthentifizierung und die UVM-Sicherheitspolicy konfiguriert hat, kann ein Clientbenutzer im *Client Security Benutzerhandbuch* Informationen zu Client Security lesen.

Das Benutzerhandbuch enthält Informationen zur Ausführung von Tasks mit Client Security, wie z. B. zum UVM-Anmeldeschutz, zur Erstellung eines digitalen Zertifikats und zur Verwendung des Benutzerkonfigurationsprogramms.

Zusätzliche Informationen

Zusätzliche Informationen sowie Aktualisierungen für Sicherheitsprodukte können Sie, sobald sie verfügbar sind, von der IBM Website unter

http://www.pc.ibm.com/us/security/index.html

herunterladen.

Kapitel 1. Einführung

Select ThinkPad™- und ThinkCentre™-Computer sind mit integrierter Verschlüsselungshardware ausgestattet, die gemeinsam mit einer speziellen, für den Download verfügbaren Softwaretechnologie verwendet werden kann, um auf Client-PC-Plattformen erweiterte Sicherheitsfunktionen zu aktivieren.

Diese Hardware-/Softwarekombination wird allgemein als integriertes IBM Sicherheits-Subsystem (IBM Embedded Security Subsystem, ESS) bezeichnet. Dabei besteht die Hardwarekomponente aus dem integrierten IBM Security Chip und die Softwarekomponente aus der Software "IBM Client Security" (CSS).

Die Software "IBM Client Security" ist für IBM Computer konzipiert, die den integrierten IBM Security Chip zum Verschlüsseln von Dateien und zum Speichern von Chiffrierschlüsseln verwenden. Client Security besteht aus Anwendungen und Komponenten, mit denen IBM Clientsysteme die entsprechenden Sicherheitsfunktionen im lokalen Netzwerk, im Unternehmen oder im Internet gewährleisten können.

Integriertes IBM Sicherheits-Subsystem (ESS)

IBM ESS unterstützt Schlüsselverwaltungsfunktionen, wie z. B. eine PKI (Public Key Infrastructure). Es besteht aus folgenden lokalen Anwendungen:

- Verschlüsselung von Dateien und Ordnern (File and Folder Encryption, FFE)
- Password Manager
- Gesicherte Windows-Anmeldung
- Mehrere konfigurierbare Authentifizierungsmethoden, einschließlich:
  - Verschlüsselungstext
  - Registrierung über Fingerabdruck
  - Smartcard
  - Proximity Badge (berührungsloser Ausweis)

Damit die Funktionen von IBM ESS effektiv genutzt werden können, muss ein zuständiger Sicherheitsadministrator mit einigen grundlegenden Konzepten vertraut sein. In den folgenden Abschnitten werden diese grundlegenden Sicherheitskonzepte beschrieben.

Integrierter IBM Security Chip

Das integrierte IBM Sicherheits-Subsystem (IBM Embedded Security Subsystem) ist eine integrierte Verschlüsselungshardwarekomponente, die besondere Sicherheitsfunktionen für ausgewählte IBM PC-Plattformen bietet. Mit Hilfe dieses Sicherheits-Subsystems werden Verschlüsselungs- und Authentifizierungsprozesse von reinen Softwarelösungen, die relativ anfällig für Angriffe sind, in die gesicherte Umgebung einer speziellen Hardwarekomponente übertragen. Dieser Ansatz bietet eine bedeutend höhere Sicherheit.

Das integrierte IBM Sicherheits-Subsystem unterstützt Folgendes:

- RSA3-PKI-Operationen, wie z. B. Verschlüsselungen aus Datenschutzgründen und digitale Unterschriften zur Authentifizierung
- RSA-Schlüsselerstellung
- Generierung von Zufallszahlen
- RSA-Funktionsverarbeitung in 200 Millisekunden
- EEPROM-Speicher für die Speicherung von RSA-Schlüsselpaaren
- Alle in der Spezifikation Version 1.1 definierten TCPA-Funktionen
- Kommunikation mit dem Hauptprozessor über LPC-Bus (Low Pin Count)

Software ″IBM Client Security″

Die Software ″IBM Client Security″ setzt sich aus folgenden Softwareanwendungen und -komponenten zusammen:

- **Administratordienstprogramm:** Das Administratordienstprogramm ist die Schnittstelle, über die ein Administrator das integrierte IBM Sicherheits-Subsystem aktiviert oder inaktiviert sowie Chiffrierschlüssel und Verschlüsselungstexte erstellt, archiviert und erneut generiert. Darüber hinaus kann ein Administrator mit diesem Dienstprogramm der Sicherheits-Policy, die von Client Security bereitgestellt wird, Benutzer hinzufügen.
- **Administratorkonsole:** Über die Administratorkonsole von Client Security kann ein Administrator ein Netzwerk mit standortunabhängigem Zugriff mit Berechtigungsnachweis konfigurieren, Dateien für die Implementierung erstellen und konfigurieren und eine Konfiguration ohne Administratorberechtigungen sowie ein Wiederherstellungsprofil erstellen.
- **Benutzerkonfigurationsprogramm:** Das Benutzerkonfigurationsprogramm ermöglicht Clientbenutzern das Ändern des UVM-Verschlüsselungstextes, das Aktivieren von Windows-Anmeldekennwörtern, so dass sie von UVM erkannt werden, das Aktualisieren von Schlüsselarchiven und das Registrieren von Fingerabdrücken. Außerdem kann ein Benutzer Sicherungskopien der digitalen Zertifikate erstellen, die vom integrierten IBM Sicherheits-Subsystem erzeugt wurden.
- **User Verification Manager (UVM):** In Client Security werden mit UVM Verschlüsselungstexte und andere Elemente verwaltet, mit denen Systembenutzer authentifiziert werden. Mit einem Lesegerät für Fingerabdrücke kann UVM z. B. bei der Anmeldung Benutzer authentifizieren. Client Security bietet folgende Möglichkeiten:
  - **Schutz durch UVM-Client-Policy:** Mit Client Security kann ein Sicherheitsadministrator die Sicherheits-Policy für Clients festlegen, die bestimmt, wie auf dem System die Authentifizierung eines Clientbenutzers erfolgt.

    Wenn die Policy festlegt, dass Fingerabdrücke für die Anmeldung erforderlich sind, und der Benutzer keine Fingerabdrücke registriert hat, hat er die Möglichkeit, Fingerabdrücke bei der Anmeldung zu registrieren. Wenn die Überprüfung von Fingerabdrücken erforderlich ist und kein Scanner angeschlossen ist, meldet UVM einen Fehler. Wenn das Windows-Kennwort nicht oder nicht richtig in UVM registriert ist, hat der Benutzer die Möglichkeit, das richtige Windows-Kennwort als Teil der Anmeldung anzugeben.
  - **UVM-Systemanmeldeschutz:** Client Security ermöglicht es Sicherheitsadministratoren, den Zugriff auf die Computer über eine Anmeldeschnittstelle zu steuern. Der UVM-Schutz stellt sicher, dass nur Benutzer, die von der Sicherheits-Policy erkannt werden, auf das Betriebssystem zugreifen können.

Beziehung zwischen Kennwörtern und Schlüsseln

Kennwörter und Schlüssel werden gemeinsam, zusammen mit anderen optionalen Authentifizierungsgeräten zum Überprüfen der Identität von Systembenutzern verwendet. Das Verständnis der Beziehung zwischen Kennwörtern und Schlüsseln ist wichtig, um die Funktionsweise von IBM Client Security zu verstehen.

Administratorkennwort

Das Administratorkennwort dient zur Authentifizierung eines Administrators am integrierten IBM Sicherheits-Subsystem. Dieses Kennwort, das aus acht Zeichen bestehen muss, wird innerhalb der gesicherten Hardware, die in dem integrierten IBM Sicherheits-Subsystem enthalten ist, verwaltet und authentifiziert. Nach erfolgreicher Authentifizierung kann der Administrator folgende Aktionen ausführen:

- Benutzer registrieren
- Policy-Schnittstelle starten
- Administratorkennwort ändern

Das Administratorkennwort kann auf folgende Weise festgelegt werden:

- Über den Konfigurationsassistenten von IBM Client Security
- Über das Administratordienstprogramm
- Mit Hilfe von Scripts
- Über die BIOS-Schnittstelle (nur bei ThinkCentre-Computern)

Sie sollten eine Strategie für das Erstellen und Verwalten des Administratorkennworts festlegen. Das Administratorkennwort kann geändert werden, wenn es ausspioniert oder vergessen wurde.

Wenn Sie mit den Konzepten und der Terminologie der Trusted Computing Group (TCG) vertraut sind, ist Ihnen möglicherweise bekannt, dass das Administratorkennwort auch als ″Eignerberechtigungswert″ (Owner Authorization Value) bezeichnet wird. Da das Administratorkennwort mit dem integrierten IBM Sicherheits-Subsystem verbunden ist, wird es gelegentlich auch als *Hardwarekennwort* bezeichnet.

Öffentliche und private Hardwareschlüssel

Das grundlegende Konzept des integrierten IBM Sicherheits-Subsystems beruht auf einer starken *Sicherheitsbasis* auf dem Clientsystem. Diese Basis wird zur Sicherung der anderen Anwendungen und Funktionen verwendet. Dazu gehört auch das Erstellen eines öffentlichen und eines privaten Hardwareschlüssels. Ein öffentlicher Schlüssel und ein privater Schlüssel, die auch als *Schlüsselpaar* bezeichnet werden, sind mathematisch so miteinander verknüpft, dass folgende Aussagen gültig sind:

- Daten, die mit dem öffentlichen Schlüssel verschlüsselt wurden, können nur mit dem zugehörigen privaten Schlüssel entschlüsselt werden.
- Daten, die mit dem privaten Schlüssel verschlüsselt wurden, können nur mit dem zugehörigen öffentlichen Schlüssel entschlüsselt werden.

Der private Hardwareschlüssel wird im gesicherten Hardwarebereich des Sicherheits-Subsystems erstellt, gespeichert und verwendet. Der öffentlicher Hardwareschlüssel wird zu verschiedenen Zwecken zur Verfügung gestellt (daher die Bezeichnung ″öffentlicher Schlüssel″). Er ist jedoch außerhalb des gesicherten Hardwarebereichs des Sicherheits-Subsystems nicht verfügbar.

Die öffentlichen und privaten Schlüssel sind ein wichtiges Element in der IBM Schlüsselauslagerungshierarchie. Diese Hierarchie wird in einem der folgenden Abschnitte beschrieben.

Öffentliche und private Hardwareschlüssel werden auf eine der folgenden Arten erstellt:

- Über den Konfigurationsassistenten von IBM Client Security
- Über das Administratordienstprogramm
- Mit Hilfe von Scripts

Wenn Sie mit den Konzepten und der Terminologie der Trusted Computing Group (TCG) vertraut sind, ist Ihnen möglicherweise bekannt, dass die öffentlichen und privaten Hardwareschlüssel auch als *SRK (Speicherbasisschlüssel, Storage Root Key)* bezeichnet werden.

Öffentliche und private Administratorschlüssel

Die öffentlichen und privaten Administratorschlüssel sind integraler Bestandteil der IBM Schlüsselauslagerungshierarchie. Sie ermöglichen außerdem das Sichern und Wiederherstellen von benutzerspezifischen Daten im Fall eines Systemplatinen- oder Festplattenfehlers.

Ein öffentlicher und ein privater Administratorschlüssel kann entweder für die einzelnen Systeme eindeutig sein oder für alle Systeme oder Systemgruppen gelten. Da die Verwaltung dieser Administratorschlüssel ein wichtiger Punkt ist, sollten Sie eine Strategie festlegen und entweder eindeutige oder bekannte Schlüssel verwenden.

Öffentliche und private Administratorschlüssel können auf eine der folgenden Arten erstellt werden:

- Über den Konfigurationsassistenten von IBM Client Security
- Über das Administratordienstprogramm
- Mit Hilfe von Scripts

ESS-Archiv

Mit Hilfe der öffentlichen und privaten Administratorschlüssel können benutzerspezifische Daten gesichert und im Falle eines Systemplatinen- oder Festplattenfehlers wiederhergestellt werden.

Öffentliche und private Benutzerschlüssel

Das integrierte IBM Sicherheits-Subsystem erstellt öffentliche und private Benutzerschlüssel zum Schutz von benutzerspezifischen Daten. Diese Schlüsselpaare werden erstellt, wenn ein Benutzer bei IBM Client Security registriert wird. Die Schlüssel werden von der UVM-Komponente (User Verification Manager) von IBM Client Security transparent erstellt und verwaltet. Die Verwaltung der Schlüssel erfolgt abhängig von der Anmeldung der einzelnen Windows-Benutzer am Betriebssystem.

Die IBM Schlüsselauslagerungshierarchie

Ein grundlegendes Element der Architektur des integrierten IBM Sicherheits-Subsystems ist die IBM Schlüsselauslagerungshierarchie. Dabei stellen die öffentlichen und privaten Hardwareschlüssel die Basis der IBM Schlüsselauslagerungshierarchie dar. Die öffentlichen und privaten Hardwareschlüssel, die auch als *Hardwareschlüsselpaar* bezeichnet werden, werden von IBM Client Security erstellt und sind statistisch gesehen auf jedem einzelnen Client eindeutig.

Die nächsthöhere Ebene in der Schlüsselhierarchie (nach der Sicherheitsbasis) bildet das Schlüsselpaar aus öffentlichem und privaten Administratorschlüssel, das sog. *Administratorschlüsselpaar*. Das Administratorschlüsselpaar kann auf jeder Maschine eindeutig sein, oder es kann für alle Clients oder für eine Untergruppe von Clients dasselbe sein. Wie Sie dieses Schlüsselpaar verwalten, hängt davon ab, wie Sie Ihr Netzwerk verwalten möchten. Der private Administratorschlüssel ist in der Hinsicht eindeutig, dass er sich auf dem Clientsystem in einer vom Administrator festgelegten Position befindet (und durch den öffentlichen Hardwareschlüssel geschützt wird).

IBM Client Security registriert die Windows-Benutzer in der Umgebung des integrierten IBM Sicherheits-Subsystems. Bei der Registrierung eines Benutzers werden ein öffentlicher und ein privater Benutzerschlüssel (das *Benutzerschlüsselpaar*) sowie eine neue Schlüsselebene erstellt. Der private Benutzerschlüssel wird mit dem öffentlichen Administratorschlüssel verschlüsselt. Der private Administratorschlüssel wird mit dem öffentlichen Hardwareschlüssel verschlüsselt. Um den privaten Benutzerschlüssel verwenden zu können, muss demzufolge der private Administratorschlüssel (der mit dem öffentlichen Hardwareschlüssel verschlüsselt wird) in das Sicherheits-Subsystem geladen werden. Nachdem der private Administratorschlüssel in den Chip geladen wurde, wird er mit dem privaten Hardwareschlüssel entschlüsselt. Der private Administratorschlüssel im Sicherheits-Subsystem kann nun verwendet werden, um Daten, die mit dem zugehörigen öffentlichen Administratorschlüssel verschlüsselt wurden, in das Sicherheits-Subsystem zu laden, zu entschlüsseln und zu verarbeiten. Der private Benutzerschlüssel des gegenwärtig angemeldeten Windows-Benutzers (der mit dem öffentlichen Administratorschlüssel verschlüsselt wurde) wird in das Sicherheits-Subsystem geladen. Alle von einer Anwendung, die das integrierte IBM Sicherheits-Subsystem verwendet, angeforderten Daten werden ebenfalls in das Sicherheits-Subsystem geladen, entschlüsselt und innerhalb der gesicherten Umgebung des Sicherheits-Subsystems verarbeitet. Ein Beispiel für diesen Prozess ist ein privater Schlüssel, der für die Authentifizierung in einem festnetzunabhängigen Netz verwendet wird.

Wenn ein Schlüssel erforderlich ist, wird er in das integrierte Sicherheits-Subsystem geladen. Die verschlüsselten privaten Schlüssel werden in das Sicherheits-Subsystem geladen und können in der gesicherten Umgebung des Chips verwendet werden. Die privaten Schlüssel sind niemals ungeschützt; sie werden niemals außerhalb dieser Hardwareumgebung verwendet. Dadurch kann eine nahezu unbegrenzte Datenmenge mit Hilfe des integrierten IBM Security Chips geschützt werden.

Die privaten Schlüssel werden verschlüsselt, da für sie die höchste Sicherheitsstufe gilt und da im integrierten IBM Sicherheits-Subsystem nur eine begrenzte Speicherkapazität zur Verfügung steht. Es können immer nur einige Schlüssel gleichzeitig im Sicherheits-Subsystem gespeichert werden. Die öffentlichen und privaten Hardwareschlüssel sind die einzigen Schlüssel, die auch zwischen den einzelnen Bootvorgängen im Sicherheits-Subsystem gespeichert bleiben. Damit das Sicherheits-Subsystem für mehrere Schlüssel und verschiedene Benutzer verwendet werden kann, verwendet CSS die IBM Schlüsselauslagerungshierarchie. Wenn ein Schlüssel erforderlich ist, wird er in das integrierte IBM Sicherheits-Subsystem geladen. Die zugehörigen, verschlüsselten privaten Schlüssel werden in das Sicherheits-Subsystem geladen und können in der gesicherten Umgebung des Sicherheits-Subsystems verwendet werden. Die privaten Schlüssel sind niemals ungeschützt; sie werden niemals außerhalb dieser Hardwareumgebung verwendet.

Der private Administratorschlüssel wird mit dem öffentlichen Hardwareschlüssel verschlüsselt. Der private Hardwareschlüssel, der nur im Sicherheits-Subsystem verfügbar ist, wird zum Entschlüsseln des privaten Administratorschlüssels verwendet. Nach dem Entschlüsseln des privaten Administratorschlüssels im Sicherheits-Subsystem kann ein privater Benutzerschlüssel (der mit dem öffentlichen Administratorschlüssel verschlüsselt wurde), in das Sicherheits-Subsystem geladen und mit dem privaten Administratorschlüssel entschlüsselt werden. Mit dem öffentlichen Administratorschlüssel können verschiedene private Benutzerschlüssel verschlüsselt werden. Dadurch kann eine praktisch unbegrenzte Anzahl von Benutzern in einem System mit IBM ESS vorhanden sein. Es hat sich jedoch erwiesen, dass mit einer Beschränkung bei der Registrierung auf 25 Benutzer eine optimale Leistung erzielt werden kann.

IBM ESS verwendet eine Schlüsselauslagerungshierarchie, bei der die öffentlichen und privaten Hardwareschlüssel im Sicherheits-Subsystem zum Sichern von Daten verwendet werden, die außerhalb des Chips gespeichert sind. Der private Hardwareschlüssel wird im Sicherheits-Subsystem generiert und niemals außerhalb dieser gesicherten Umgebung verwendet. Der öffentliche Hardwareschlüssel ist außerhalb des Sicherheits-Subsystems verfügbar und wird zum Verschlüsseln oder Sichern von anderen Daten, wie z. B. der privaten Schlüssel, verwendet. Wenn diese Daten mit dem öffentlichen Hardwareschlüssel verschlüsselt werden, können sie nur mit dem privaten Hardwareschlüssel entschlüsselt werden. Da der private Hardwareschlüssel nur in der gesicherten Umgebung des Sicherheits-Subsystems verfügbar ist, können die verschlüsselten Daten nur in derselben gesicherten Umgebung entschlüsselt und verwendet werden. Beachten Sie, dass die einzelnen Computer jeweils über einen eindeutigen öffentlichen und privaten Schlüssel verfügen. Die Zufallszahlenfunktion des integrierten IBM Sicherheits-Subsystems gewährleistet, dass jedes einzelne Hardwareschlüsselpaar statistisch gesehen eindeutig ist.

CSS PKI-Funktionen

Client Security bietet alle erforderlichen Komponenten, um in Ihrem Unternehmen eine PKI (Public Key Infrastructure) aufzubauen, z. B.:

- **Steuerung der Client-Sicherheits-Policy durch Administratoren:** Die Authentifizierung von Endbenutzern auf Clientebene ist ein wichtiger Aspekt für Sicherheits-Policies. Client Security bietet die erforderliche Schnittstelle zur Verwaltung der Sicherheits-Policy eines IBM Clients. Diese Schnittstelle ist Teil der Authentifizierungssoftware UVM (User Verification Manager), der Hauptkomponente von Client Security.
- **Chiffrierschlüsselverwaltung für öffentliche Schlüssel:** Administratoren können mit Client Security Chiffrierschlüssel für die Computerhardware und für die Clientbenutzer erstellen. Bei der Erstellung von Chiffrierschlüsseln sind diese über eine Schlüsselhierarchie an den integrierten IBM Security Chip gebunden. In der Hierarchie wird ein Hardwareschlüssel der Basisebene verwendet, um die übergeordneten Schlüssel sowie die den einzelnen Clientbenutzern zugeordneten Benutzerschlüssel zu verschlüsseln. Die Verschlüsselung und Speicherung von Schlüsseln auf dem integrierten IBM Security Chip erweitert die Clientsicherheit um eine wesentliche zusätzliche Ebene, da die Schlüssel sicher an die Computerhardware gebunden sind.
- **Erstellung und Speicherung digitaler Signaturen, die durch den integrierten IBM Security Chip geschützt sind:** Wenn Sie ein digitales Zertifikat anfordern, das für die digitale Unterschrift und für die Verschlüsselung einer E-Mail verwendbar ist, können Sie mit Client Security das integrierte IBM Sicherheits-Subsystem zur Bereitstellung der Verschlüsselung für Anwendungen einsetzen, die mit der Microsoft CryptoAPI funktionieren. Zu diesen Anwendungen gehören Internet Explorer und Microsoft Outlook Express. Dadurch ist sichergestellt, dass der private Schlüssel des digitalen Zertifikats auf dem integrierten IBM Sicherheits-Subsystem mit dem öffentlichen Benutzerschlüssel verschlüsselt wird. Darüber hinaus können Netscape-Benutzer das integrierte IBM Sicherheits-Subsystem zum Generieren von privaten Schlüsseln für die zum Erhöhen der Systemsicherheit verwendeten digitalen Zertifikate auswählen. Anwendungen nach dem Standard PKCS #11 (Public-Key Cryptography Standard Nr. 11), wie z. B. Netscape Messenger, können sich über das integrierte IBM Sicherheits-Subsystem schützen.
- **Digitale Zertifikate an das integrierte IBM Sicherheits-Subsystem übertragen.** Mit dem Tool zur Übertragung von Zertifikaten von Client Security können Sie Zertifikate, die mit dem Standard-Microsoft-CSP erstellt wurden, an das CSP-Modul des integrierten IBM Sicherheits-Subsystems übertragen. Dadurch wird der notwendige Schutz für private Schlüssel, die zu Zertifikaten gehören, beträchtlich erhöht, da die Schlüssel nun statt in gefährdeter Software im integrierten IBM Sicherheits-Subsystem sicher gespeichert sind.

  Anmerkung: Durch das CSP-Modul des integrierten IBM Sicherheits-Subsystems geschützte digitale Zertifikate können nicht an ein anderes CSP-Modul übertragen werden.

- **Funktion zur Schlüsselarchivierung und -wiederherstellung:** Eine wichtige PKI-Funktion ist das Erstellen eines Schlüsselarchivs, aus dem Schlüssel bei Verlust oder Beschädigung der Originalschlüssel wiederhergestellt werden können. IBM Client Security bietet eine Schnittstelle, mit der Sie mit dem integrierten IBM Sicherheits-Subsystem erstellte Archive für Schlüssel und digitale Zertifikate erstellen und diese Schlüssel und Zertifikate bei Bedarf wiederherstellen können.
- **Verschlüsselung von Dateien und Ordnern:** Die Verschlüsselung von Dateien und Ordnern ermöglicht dem Benutzer das Ver- und Entschlüsseln von Dateien und Ordnern. This provides an So wird über die Sicherheitsmaßnahmen des CSS-Systems hinaus bereits eine höhere Stufe von Datensicherheit gewährleistet.
- **Authentifizierung über Fingerabdrücke:** IBM Client Security unterstützt das Lesegerät für Fingerabdrücke von Targus als PC-Karte oder über USB für die Authentifizierung. Die Client Security-Software muss installiert sein, bevor die Einheitentreiber für das Targus-Lesegerät für Fingerabdrücke installiert werden, damit ein ordnungsgemäßer Betrieb gewährleistet ist.
- **Smartcard-Authentifizierung:** IBM Client Security unterstützt bestimmte Smartcards als Authentifizierungseinheiten. Client Security ermöglicht die Verwendung von Smartcards zur Authentifizierung als Token, d. h., es kann sich jeweils nur ein Benutzer authentifizieren. Jede Smartcard ist systemgebunden, wenn nicht der standortunabhängige Zugriff (Roaming) mit Berechtigungsnachweis verwendet wird. Wenn eine Smartcard erforderlich ist, erhöht dies die Systemsicherheit, da neben einem Kennwort, das möglicherweise ausspioniert werden kann, auch die Smartcard geliefert werden muss.
- **Standortunabhängiger Zugriff mit Berechtigungsnachweis:** Der standortunabhängige Zugriff mit Berechtigungsnachweis ermöglicht es einem autorisierten Benutzer, jeden Computer im Netzwerk genau wie die eigene Workstation zu verwenden. Wenn ein Benutzer berechtigt ist, UVM auf einem beliebigen bei Client Security registrierten Client zu verwenden, kann er seine persönlichen Daten in alle anderen registrierten Clients in dem Netzwerk mit standortunabhängigem Zugriff mit Berechtigungsnachweis importieren. Die persönlichen Daten werden im CSS-Archiv und auf jedem Computer, in den sie importiert wurden, automatisch aktualisiert und verwaltet. Aktualisierungen dieser persönlichen Daten, wie z. B. neue Zertifikate oder Änderungen des Verschlüsselungstexts, werden sofort auf allen anderen Computer verfügbar, die über eine standortunabhängige Verbindung zum Netzwerk verfügen.
- **FIPS 140-1-Zertifizierung:** Client Security unterstützt FIPS 140-1-zertifizierte, verschlüsselte Bibliotheken. FIPS-zertifizierte RSA-BSAFE-Bibliotheken werden auf TCPA-Systemen verwendet.
- **Ablauf des Verschlüsselungstexts:** Client Security legt jeweils beim Hinzufügen eines Benutzers einen benutzerspezifischen Verschlüsselungstext und eine Policy für das Ablaufen des Verschlüsselungstexts fest.

Kapitel 2. Dateien und Ordner verschlüsseln und entschlüsseln

Mit Hilfe der Verschlüsselungstechnologie können Benutzer sensible Daten auf ihren Computern schützen. Durch das Verschlüsseln einer Datei wird sichergestellt, dass nur Benutzer, die die festgelegten Sicherheitsbestimmungen erfüllen, auf die Informationen in der verschlüsselten Datei zugreifen können. Durch das Verschlüsseln von Dateien können darüber hinaus auch sensible Daten in Dateien geschützt werden, die über das Internet oder ein Netzwerk gesendet werden.

Mit IBM Client Security können Benutzer sensible Dateien und Ordner mit Hilfe der folgenden Methoden verschlüsseln und entschlüsseln:

- **Einzelne Dateien mit Hilfe der Anwendung "Client Security" über die rechte Maustaste verschlüsseln.**

  Diese Funktion ist Teil des Basisdownloads von IBM Client Security.
- **Transparente Verschlüsselung von Dateien und Ordnern während des Betriebs mit Hilfe des Dienstprogramms "IBM File and Folder Encryption".**

  Anmerkung: Das Dienstprogramm "IBM File and Folder Encryption" (FFE) muss heruntergeladen werden, damit diese Funktion aktiviert werden kann. IBM Client Security muss *vor* der Installation des Dienstprogramms zur Verschlüsselung von Dateien und Ordnern installiert werden.

Verschlüsselung über die rechte Maustaste

Mit der Funktion von Client Security für die einfache Verschlüsselung über die rechte Maustaste können Benutzer mit der rechten Maustaste sensible Dateien schützen. Damit diese Funktion genutzt werden kann, muss keine zusätzliche Software heruntergeladen werden. Mit dieser Funktion verschlüsselte Dateien weisen die folgenden Merkmale auf:

- Eine verschlüsselte Datei muss für jede Verwendung manuell entschlüsselt und danach zum Schutz manuell wieder verschlüsselt werden. Die UVM-Policy muss bei jedem Ver- und Entschlüsseln der Datei aufgerufen werden. Diese Bestimmungen gewährleisten eine genaue, manuelle Steuerung der Verschlüsselung und Entschlüsselung der ausgewählten Dateien. Dieser strenge Schutz ist für Benutzer jedoch recht unbequem, die nicht bei jeder Nutzung einer verschlüsselten Datei ein Kennwort eingeben, einen Fingerabdruck abgeben oder eine Smartcard verwenden möchten.
- Dateien können in verschlüsselter Form an einen ferner Standort gesendet werden. Sie können jedoch nur auf dem Computer entschlüsselt werden, der zum Verschlüsseln verwendet wurde, da die zum Verschlüsseln der Dateien verwendeten Schlüssel im integrierten IBM Sicherheits-Subsystem (IBM Embedded Security Subsystem) auf diesem Computer eindeutig sind.

Sie können Dateien im Kontextmenü mit der rechten Maustaste manuell ver- und entschlüsseln. Wenn Sie Dateien auf diese Weise verschlüsseln, wird an den Dateinamen die Erweiterung `.$enc$` angehängt. Diese verschlüsselten Dateien können Sie anschließend auf fernen Servern sicher speichern. Sie bleiben so lange verschlüsselt und für Anwendungen nicht verfügbar, bis Sie sie mit der rechten Maustaste wieder entschlüsseln.

Transparente Verschlüsselung während des Betriebs (FFE, File and Folder Encryption)

Die Funktion von Client Security für transparente Verschlüsselung während des Betriebs wird durch das Herunterladen des Dienstprogramms zur Verschlüsselung von Dateien und Ordnern aktiviert. Dieses Programm steht auf der IBM Client Security-Website zur Verfügung. Das Dienstprogramm zur Verschlüsselung von Dateien und Ordnern stellt eine bequemere, transparentere Form der Verschlüsselung bereit als die einfache Verschlüsselung von CSS über die rechte Maustaste. Die Verschlüsselung von Dateien und Ordnern mit Hilfe dieses Dienstprogramms kann auch mit der rechten Maustaste durchgeführt werden. FFE-verschlüsselte Dateien und Ordner weisen die folgenden Merkmale auf:

- Die UVM-Policy muss nur beim Systemstart aufgerufen werden. Dies ist eine bequemere Form der Verschlüsselung und Entschlüsselung der ausgewählten Dateien, da zur Nutzung einer Datei *kein* Kennwort eingegeben, kein Fingerabdruck abgegeben und keine Smartcard verwendet werden muss.
- Wenn eine Anwendung eine Datei öffnet, die mit dem Dienstprogramm zur Verschlüsselung von Dateien und Ordnern verschlüsselt wurde, wird die Datei automatisch entschlüsselt. Wenn eine mit dem Dienstprogramm zur Verschlüsselung von Dateien und Ordnern verschlüsselte Datei gespeichert wird, wird sie automatisch verschlüsselt.
- Mit dem Dienstprogramm zur Verschlüsselung von Dateien und Ordnern verschlüsselte Dateien können an einen fernen Standort gesendet werden. Dies geschieht jedoch in verschlüsselter Form.

Das Dienstprogramm zur Plattenüberprüfung wird möglicherweise bei einem Neustart nach dem Schützen oder dem Aufheben des Schutzes von Ordnern ausgeführt. Warten Sie, bis das System geprüft ist, bevor Sie den Computer verwenden.

Ein in UVM registrierter Benutzer, der das Dienstprogramm zur Verschlüsselung von Dateien und Ordnern heruntergeladen hat, kann einen Ordner auswählen, um den Ordner mit der rechten Maustaste zu schützen oder den Schutz aufzuheben. Dadurch kann er alle Dateien innerhalb des Ordners oder alle untergeordneten Teilordner verschlüsseln. Wenn Sie Dateien auf diese Weise schützen, wird an deren Namen keine Erweiterung angehängt. Wenn Sie mit einer Anwendung auf eine Datei im verschlüsselten Ordner zugreifen, wird diese entschlüsselt, in den Speicher geladen und erneut verschlüsselt, bevor Sie sie auf der Festplatte speichern.

Alle Windows-Operationen, die auf eine Datei in einem geschützten Ordner zugreifen, erhalten Zugriff auf die Daten in entschlüsselter Form. Aufgrund dieses Merkmals ist die Verschlüsselung bequemer, da eine Datei nicht vor jeder Nutzung entschlüsselt und nach jeder Nutzung wieder verschlüsselt werden muss.

Status der FFE-Ordnerverschlüsselung

Mit dem Dienstprogramm zur Verschlüsselung von Dateien und Ordnern können Benutzer mit der rechten Maustaste sensible Dateien und Ordner schützen. Die Art des Datei- oder Ordnerschutzes hängt von der ursprünglichen Verschlüsselung der Datei bzw. des Ordners ab.

Ein Ordner kann sich in einem der folgenden Status befinden:

- **Ungeschützter Ordner**

  Weder dieser Ordner noch seine Teilordner noch einer seiner übergeordneten Ordner wurde geschützt. Der Benutzer erhält die Option, diesen Ordner zu schützen.

- **Geschützter Ordner**

  Ein geschützter Ordner kann sich in einem der folgenden drei Status befinden:

  – **Vom aktuellen Benutzer geschützt**

    Der aktuelle Benutzer schützt diesen Ordner. Alle enthaltenen Dateien werden verschlüsselt, einschließlich aller Dateien in Teilordnern. Der Benutzer erhält die Option, den Schutz dieses Ordners aufzuheben.

  – **Vom aktuellen Benutzer geschützter Teilordner eines Ordners**

    Der aktuelle Benutzer schützt einen der übergeordneten Ordner dieses Ordners. Alle Dateien werden verschlüsselt. Der aktuelle Benutzer erhält keine Optionen für die rechte Maustaste.

  – **Von einem anderen Benutzer geschützt**

    Ein anderer Benutzer schützt diesen Ordner. Alle enthaltenen Dateien werden verschlüsselt, einschließlich aller Dateien in Teilordnern, und sie sind für den aktuellen Benutzer nicht verfügbar. Der aktuelle Benutzer erhält keine Optionen für die rechte Maustaste.

- **Übergeordneter Ordner eines geschützten Ordners**

  Ein übergeordneter Ordner eines geschützten Ordners kann sich in einem der folgenden drei Status befinden:

  – **Enthält mindestens einen Teilordner, der vom aktuellen Benutzer geschützt wurde**

    Der aktuelle Benutzer schützt mindestens einen Teilordner. Alle Dateien in den verschlüsselten Teilordnern werden verschlüsselt. Der Benutzer erhält die Option, den übergeordneten Ordner zu schützen. Sämtliche Teilordner im übergeordneten Ordner müssen ungeschützt sein, damit der übergeordnete Ordner geschützt werden kann.

  – **Enthält mindestens einen Teilordner, der von mindestens einem anderen Benutzer geschützt wurde**

    Mindestens ein anderer Benutzer schützt mindestens einen Teilordner. Alle Dateien in den verschlüsselten Teilordnern werden verschlüsselt und sind für den aktuellen Benutzer nicht verfügbar. Der aktuelle Benutzer erhält keine Optionen für die rechte Maustaste.

  – **Enthält Teilordner, die vom aktuellen Benutzer und von mindestens einem anderen Benutzer geschützt wurden**

    Sowohl der aktuelle Benutzer als auch mindestens ein anderer Benutzer schützen Teilordner. Der aktuelle Benutzer erhält keine Optionen für die rechte Maustaste.

- **Kritischer Ordner**

  Ein kritischer Ordner ist ein Ordner in einem kritischen Pfad und kann daher nicht geschützt werden. Es gibt die beiden folgenden kritischen Pfade: den Pfad von Windows und den Pfad von Client Security.

Jeder Status wird von der Option zum Schützen eines Ordners durch Klicken mit der rechten Maustaste unterschiedlich gehandhabt.

Hinweise zur Verwendung des Dienstprogramms zur Verschlüsselung von Dateien und Ordnern (Dienstprogramm ″FFE″, File and Folder Encryption)

Die folgenden Informationen sind möglicherweise nützlich, wenn Sie bestimmte Funktionen des Dienstprogramms zur Verschlüsselung von Dateien und Ordnern durchführen.

Laufwerkbuchstabenschutz

Das IBM Dienstprogramm ″FFE″ kann ausschließlich zum Verschlüsseln von Dateien und Ordnern auf Laufwerk C verwendet werden. Dieses Dienstprogramm unterstützt keine Verschlüsselung auf anderen Festplattenpartitionen oder anderen physischen Laufwerken.

Geschützte Dateien und Ordner löschen

Damit sich keine sensiblen Dateien und Ordner ungeschützt im Papierkorb befinden, cmüssen Sie die Tastenkombination Umschalttaste+Entf verwenden, um geschützte Ordner und Dateien zu löschen. Durch diese Tastenkombination wird eine nicht an Bedingungen gebundene Löschoperation durchgeführt, und die gelöschten Dateien werden nicht im Papierkorb abgelegt.

Vor dem Upgrade von einer älteren Version des Dienstprogramms ″IBM FFE″

Bevor Sie das Dienstprogramm ″IBM FFE″ von Version 2.0 oder einer früheren Version aufrüsten, müssen Sie das ACL-Reparaturtool (Access Control List, Zugriffssteuerungsliste) von der IBM Security-Website herunterladen und verwenden. Verwenden Sie dieses Dienstprogramm, *bevor* Sie eine Vorversion von FFE Version 2.0 deinstallieren. Anderenfalls schlägt die Deinstallation möglicherweise fehl, und auf die betroffenen Dateien kann nicht zugegriffen werden.

Vor dem Deinstallieren des Dienstprogramms ″IBM FFE″

Heben Sie vor dem Deinstallieren des Dienstprogramms ″IBM FFE″ mit Hilfe dieses Dienstprogramms den Schutz für alle zuvor geschützten Dateien und Ordner auf.

Einschränkungen beim Dienstprogramm zur Verschlüsselung von Dateien und Ordnern (Dienstprogramm ″FFE″)

Das Dienstprogramm ″IBM FFE″ weist folgende Einschränkungen auf:

Einschränkungen beim Verschieben von geschützten Dateien und Ordnern

Das Dienstprogramm ″IBM FFE″ unterstützt folgende Aktionen nicht:

- Dateien und Ordner innerhalb geschützter Ordner verschieben
- Dateien oder Ordner zwischen geschützten und ungeschützten Ordnern verschieben

Wenn Sie versuchen, eine dieser nicht unterstützten Verschiebeoperationen durchzuführen, wird vom Betriebssystem eine Nachricht angezeigt, die besagt, dass der Zugriff verweigert wurde. Dies ist ein normaler Vorgang. Die Nachricht besagt lediglich, dass diese Verschiebeoperation nicht unterstützt wird. Alternativ zur Verschiebeoperation können Sie folgende Operation ausführen:

1. Kopieren Sie die geschützten Dateien oder Ordner an die neue Position.
2. Löschen Sie die ursprünglichen Dateien oder Ordner mit Hilfe der Tastenkombination Umschalttaste+Entf.

Einschränkungen beim Ausführen von Anwendungen

Das Dienstprogramm ″IBM FFE″ unterstützt nicht das Ausführen von Anwendungen von einem geschützten Ordner aus. Die ausführbare Datei PROGRAMM.EXE kann z. B. nicht von einem geschützten Ordner aus ausgeführt werden.

Längenbeschränkungen für Pfadnamen

Wenn Sie versuchen, einen Ordner mit Hilfe des Dienstprogramms ″IBM FFE″ zu schützen oder eine Datei oder einen Ordner von einem ungeschützten Ordner in einen geschützten Ordner zu verschieben, erhalten Sie möglicherweise eine Nachricht des Betriebssystems, die besagt, dass ein oder mehrere Pfadnamen zu lang sind. Wenn Sie diese Nachricht erhalten, überschreitet der Pfadname einer/eines oder mehrerer Dateien oder Ordner die maximal zulässige Zeichenlänge. Beheben Sie den Fehler, indem Sie entweder die Ordnerstruktur neu anordnen, so dass der Pfad verkürzt wird, oder indem Sie Ordner- oder Dateinamen kürzen.

Fehler beim Schützen eines Ordners

Wenn Sie versuchen, einen Ordner zu schützen und eine Nachricht mit folgendem (oder ähnlichem) Inhalt angezeigt wird: `"Der Ordner kann nicht geschützt werden. Mindestens eine Datei ist in Gebrauch."`, überprüfen Sie Folgendes:

- Überprüfen Sie, ob eine der Dateien im Ordner derzeit verwendet wird.
- Wenn im Windows Explorer ein oder mehrere Teilordner eines Ordners, den Sie schützen möchten, angezeigt werden, stellen Sie sicher, dass der Ordner, den Sie zu schützen versuchen, hervorgehoben und aktiv ist und nicht einer der Teilordner.

Kapitel 3. Standortunabhängiger Zugriff mit Berechtigungsnachweis in CSS

Mit Hilfe des standortunabhängigen Zugriffs mit Berechtigungsnachweis von IBM Client Security können Berechtigungsnachweise von UVM-Benutzern auf allen Computern in einem Netzwerk verwendet werden, auf denen TCPA aktiviert ist. Dieses Netzwerk mit standortunabhängigem Zugriff ermöglicht Benutzern eine größere Flexibilität. Außerdem sind die Anwendungen für Benutzer in diesem Netzwerk auf allen Computern gleichermaßen verfügbar.

Bedingungen für ein CSS-Netzwerk mit standortunabhängigem Zugriff mit Berechtigungsnachweis

Ein CSS-Netzwerk mit standortunabhängigem Zugriff mit Berechtigungsnachweis besteht aus den folgenden erforderlichen Komponenten:

- Roaming-Server
- Roaming-Clients
- Gemeinsam genutztes, zugeordnetes Netzlaufwerk zum Speichern der UVM-Benutzerarchive

Anmerkung: Bei dem Roaming-Server und den autorisierten Roaming-Clients handelt es sich einfach um Computer, für die TCPA aktiviert wurde, die über Administratorkennwörter verfügen und auf denen IBM Client Security ab Version 5.1 installiert ist.

Roaming-Server installieren

Um ein CSS-Netzwerk mit standortunabhängigem Zugriff mit Berechtigungsnachweis zu konfigurieren, müssen Sie einen TCPA-Computer als Roaming-*Server* definieren (dieser wird als ″System A″ bezeichnet). Die anderen Computer sind nach der Registrierung durch den Roaming-Server autorisierte, für CSS registrierte *Clients*. (Der erste registrierte Client wird als ″System B″ bezeichnet.)

Der Computer, den Sie als Roaming-Server definieren, kann ein ganz normaler Computer sein. Sie können für diese Funktion jeden beliebigen Computer verwenden, der Teil des Netzwerks mit standortunabhängigem Zugriff ist. Über den Roaming-Server wird nur bestimmt, welche Computer für den Zugriff auf das Netzwerk berechtigt sind. Nachdem ein Computer beim Roaming-Server registriert worden ist, ist er für Verbindungen zu allen Computern in diesem Netzwerk berechtigt.

Die Konfiguration eines Netzwerks mit standortunabhängigem Zugriff wird in zwei Schritten ausgeführt:

1. Konfigurieren Sie System A (den Server), indem Sie die Schlüssel, das Archiv und die Benutzer für den standortunabhängigen Zugriff definieren.
2. Registrieren Sie System B und alle weiteren Computer im CSS-Netzwerk mit standortunabhängigem Zugriff mit Berechtigungsnachweis als Roaming-Clients.

Der Roaming-Server definiert das CSS-Netzwerk mit standortunabhängigem Zugriff mit Berechtigungsnachweis und startet die Registrierung der Roaming-Clients. Das zentrale Element eines solchen Netzwerks ist jedoch das zugeordnete

Netzlaufwerk, auf dem Benutzerarchive gespeichert werden. In diesem Archiv werden alle Aktualisierungen der Benutzerberechtigungen gespeichert. Das Archiv darf sich *nicht* auf dem Roaming-Server oder auf einem der Roaming-Clients befinden. Nach der Initialisierung der CSS-Clients wird der Roaming-Server wie alle anderen für CSS registrierten Clients verwendet.

Roaming-Server konfigurieren

Gehen Sie wie folgt vor, um einen Roaming-Server zu konfigurieren:

1. Starten Sie auf dem ausgewählten Computer die Administratorkonsole, und klicken Sie auf **Standortunabhängigen Zugriff mit Berechtigungsnachweis konfigurieren**. Wenn der Computer bereits für einen standortunabhängigen Zugriff konfiguriert ist, wählen Sie die Option **Dieses System als CSS-Roaming-Server rekonfigurieren** aus, klicken Sie auf **Weiter**, und klicken Sie anschließend auf **OK**.
2. Erstellen Sie auf dem Computer, der als Roaming-Server eingerichtet werden soll, den Ordner `c:\roaming`.
3. Starten Sie die Administratorkonsole und klicken Sie auf **Standortunabhängigen Zugriff mit Berechtigungsnachweis konfigurieren**.
4. Wählen Sie die Option **Dieses System als CSS-Roaming-Server konfigurieren** aus, und klicken Sie auf **Weiter**.
5. Klicken Sie auf **Konfigurieren**.
6. Wählen Sie die Option **Neue Archivschlüssel erstellen** aus, und geben Sie den neuen Schlüsselordner im Feld "Ordner für Archivschlüssel" ein, wobei der Ordner für Archivschlüssel im Ordner `c:\roaming` gespeichert wird.
7. Wählen Sie aus, ob Sie ein vorhandenes Schlüsselpaar verwenden oder ein neues Schlüsselpaar erstellen möchten, und klicken Sie auf **Weiter**.
8. Geben Sie den Archivordner an und klicken Sie dann auf **Weiter**.

   Anmerkung: Die anderen Computer, die für den standortunabhängigen Zugriff registriert sind (Roaming-Clients), müssen über einen Zugriff auf den Archivordner und den Schlüsselordner verfügen. Beim Verzeichnis `c:\roaming` muss es sich um ein zugeordnetes Netzlaufwerk handeln.

   Wenn das Archiv gegenwärtig Dateien enthält, werden Sie auf der nächsten Seite des Assistenten aufgefordert anzugeben, wie mit den Dateien verfahren werden soll.
9. Klicken Sie auf **Fertig stellen**.

Clients beim Roaming-Server registrieren

Gehen Sie wie folgt vor, um einen Roaming-Client beim Roaming-Server zu registrieren:

1. Unmittelbar nachdem die Konfiguration des Roaming-Servers abgeschlossen ist, wird die Anzeige des Assistenten zum Konfigurieren des Netzwerks mit standortunabhängigem Zugriff mit Berechtigungsnachweis angezeigt. Wählen Sie die Option **Client-Registrierung aktivieren** aus, und klicken Sie dann auf **Weiter**.
2. Geben Sie den Namen des Benutzers mit Administratorberechtigung auf System B an, der die Clientregistrierung abschließen wird.
3. Geben Sie ein Kennwort für diesen Benutzer ein, das aus acht Zeichen besteht, und bestätigen Sie es. (Dieser Schritt bedeutet nicht, dass der Benutzer für die Verwendung von UVM berechtigt wird. Dieser Schritt wird später ausgeführt.)

4. Wenn Sie den Client mit Hilfe des Benutzerkonfigurationsprogramms registrieren möchten, müssen Sie eine Administratorkonfigurationsdatei für diesen Benutzer erstellen. Bei diesem Vorgang wird eine Datei generiert, die diesem Benutzer eindeutig zugeordnet ist. Speichern Sie diese Datei in einer Position, auf die der Benutzer und System B zugreifen können.

   Anmerkung: Diese Datei muss nicht generiert werden, wenn Sie einen Client mit Hilfe des Administratordienstprogramms registrieren.
5. Geben Sie das Administratorkennwort für System B ein und klicken Sie auf **Weiter**.
6. Wenn Sie eine Administratorkonfigurationsdatei erstellt haben, speichern Sie die Datei in einer Position, auf die der Benutzer und System B zugreifen können.

Nachdem Sie diese Schritte abgeschlossen haben, ist der Roaming-Server konfiguriert. Nun muss die Registrierung der Roaming-Clients wie im folgenden Abschnitt beschrieben durchgeführt werden, damit das Netzwerk mit standortunabhängigem Zugriff betriebsbereit ist.

Registrierung von Roaming-Clients

Nachdem Sie die Liste mit gesicherten Systemen beim Roaming-Server registriert haben, müssen Sie auf den Clientsystemen eines der folgenden Verfahren durchführen. Der Roaming-Server muss aktiviert werden, und es muss eine Verbindung zum Archiv hergestellt werden, bevor Sie die Registrierung der Clients durchführen können.

Roaming-Clients mit Hilfe des Administratordienstprogramms registrieren

Gehen Sie wie folgt vor, um einen Roaming-Client mit Hilfe des Administratordienstprogramms zu registrieren:

1. Klicken Sie auf **Schlüsselkonfiguration**.
2. Klicken Sie auf **Nein** auf die Frage, ob Sie Schlüssel aus dem Archiv wiederherstellen möchten.
3. Wählen Sie die Option "System beim CSS-Roaming-Server registrieren" aus, und klicken Sie auf **Weiter**.
4. Geben Sie die von System A erstellte Archivposition ein, geben Sie das Systemregistrierungskennwort ein, das für diesen Benutzer auf System A definiert wurde, und klicken Sie auf **Weiter**.

   Der Registrierungsprozess nimmt ungefähr eine Minute in Anspruch.

Roaming-Clients mit Hilfe des Benutzerkonfigurationsprogramms registrieren

Gehen Sie wie folgt vor, um einen Roaming-Client mit Hilfe des Benutzerkonfigurationsprogramms zu registrieren:

1. Klicken Sie auf der Registerkarte "Benutzerkonfiguration" auf **Beim CSS-Roaming-Server registrieren**.
2. Wählen Sie die auf System A generierte Administratorkonfigurationsdatei aus, geben Sie das Systemregistrierungskennwort ein, das für diesen Benutzer auf System A definiert wurde, und klicken Sie auf **Weiter**.
3. Geben Sie die von System A erstellte Archivposition an, und klicken Sie auf **Weiter**.

   Der Registrierungsprozess nimmt ungefähr eine Minute in Anspruch.

Roaming-Clients mit Hilfe von Massenimplementierung (im Hintergrund) registrieren

Führen Sie folgende Schritte aus, um einen Roaming-Client mit Hilfe von Massenimplementierung automatisch zu registrieren:

1. Erstellen Sie die Datei `csec.ini`. Weitere Informationen zum Erstellen einer CSS INI-Datei finden Sie im *Client Security Installationshandbuch*.
2. Fügen Sie im Abschnitt `csssetup` der Datei den Eintrag `"enableroaming=1"` hinzu. Dies bedeutet, dass der Computer als Client für den standortunabhängigen Zugriff registriert werden soll.
3. Fügen Sie im selben Abschnitt den Eintrag `"username=OPTION"` hinzu. Für diesen Wert gibt es drei Optionen:
   - **Option 1: Die Zeichenfolge `"[promptcurrent]"` - einschließlich der eckigen Klammern.** Diese Bezeichnung sollte verwendet werden, wenn eine .dat-Datei für den derzeit angemeldeten Benutzer auf dem Roaming-Server generiert wurde und der derzeitige Benutzer das Systemregistrierungskennwort kennt. Es wird ein Dialogfenster geöffnet, und der Benutzer wird aufgefordert, vor der Implementierung das Systemregistrierungskennwort (`sysregpwd`) einzugeben.
   - **Option 2: Die Zeichenfolge `"[current]"` - einschließlich der eckigen Klammern.** Diese Bezeichnung sollte verwendet werden, wenn für den derzeit angemeldeten Benutzer auf dem Server eine .dat-Datei generiert wurde. `sysregpwd` wird wie im nächsten Schritt beschrieben behandelt.
   - **Option 3: Ein tatsächlicher Benutzername, wie z. B. `"joseph"`.** Wenn ein solcher designierter Benutzername verwendet wird, muss die Datei `"joseph.dat"` zuvor durch den Roaming-Server generiert worden sein. Das Systemregistrierungskennwort (`sysregpwd`) wird in diesem Fall wie unter dem nächsten Punkt beschrieben behandelt.
4. Wenn die zuvor beschriebene Möglichkeit 2 oder 3 verwendet wird, muss als weiterer Eintrag `"sysregpwd=SYSREGPW"` hinzugefügt werden. Hierbei handelt es sich um das 8-stellige Systemregistrierungskennwort für den derzeitigen Benutzer (wenn Option 2 implementiert wird) oder für den designierten Benutzer (wenn Option 3 implementiert wird).
5. Um die Clientregistrierung abzuschließen, verbinden Sie den Computer mit dem vom Roaming-Server konfigurierten Archiv. Dieses Archiv wird in der Datei `csec.ini` benannt. Der Schlüsselordner, der auf dem CSS-Roaming-Server mit Berechtigungsnachweis festgelegt wurde, wird in der Datei `csec.ini` ebenfalls benannt.
6. Verschlüsseln Sie die Datei `csec.ini` mit Hilfe der Administratorkonsole.

Beispiele für die Datei csec.ini

In den folgenden Beispielen werden eine `csec.ini`-Datei und deren Veränderung, je nachdem, welche Option für standortunabhängigen Berechtigungsnachweis ausgewählt wird, angezeigt. Es gibt folgende Optionen:

- **Keine Werte für standortunabhängigen Zugriff.** Diese Basisdatei ist nicht für standortunabhängigen Zugriff mit Berechtigungsnachweis aktiviert.
- **Option 1 für standortunabhängigen Zugriff.** Diese Datei ist für standortunabhängigen Zugriff unter Verwendung der Option 1 für die Clientregistrierung aktiviert. Der derzeitige Benutzer muss vor der Implementierung das Systemregistrierungskennwort angeben.

- **Option 2 für standortunabhängigen Zugriff.** Diese Datei ist für standortunabhängigen Zugriff unter Verwendung der Option 2 für die Clientregistrierung aktiviert. Der derzeitige Benutzer muss die Benutzer-ID und das Systemregistrierungskennwort angeben, die in der INI-Datei benannt werden.
- **Option 3 für standortunabhängigen Zugriff.** Diese Datei ist für standortunabhängigen Zugriff unter Verwendung der Option 3 für die Clientregistrierung aktiviert. Der Benutzer wird in der INI-Datei benannt. Das Systemregistrierungskennwort für den benannten Benutzer muss in der INI-Datei gespeichert sein.

Im Folgenden finden Sie Beispiele für vier verschiedene CSEC.INI-Dateien:

[CSSSetup]	**Option 1** [CSSSetup]	**Option 2** [CSSSetup]	Option 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, wobei der Computer das Schlüsselpaar auf dem Roaming-Server speichert	kpl=c:\\computer name\jgk, wobei der Computer das Schlüsselpaar auf dem Roaming-Server speichert	kpl=c:\\computer name\jgk, wobei der Computer das Schlüsselpaar auf dem Roaming-Server speichert
kal=c:\jgk\archive pub= c:\jk\admin.key pri= c:\jk\private1.key wiz=0	kal=c:\\computer name\archive, wobei der Computer das Archiv auf dem Roaming-Server speichert pub= c:\jk\admin.key pri= c:\jk\private1.key wiz=0	kal=c:\\computer name\archive, wobei der Computer das Archiv auf dem Roaming-Server speichert pub= c:\jk\admin.key pri= c:\jk\private1.key wiz=0	kal=c:\\computer name\archive, wobei der Computer das Archiv auf dem Roaming-Server speichert 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]	[UVMEnrollment]	[UVMEnrollment]	[UVMEnrollment]
enrollall=0	enrollall=0	enrollall=0	enrollall=0
enrollusers=1	enrollusers=1	enrollusers=1	enrollusers=1
user1=joseph	user1=joseph	user1=joseph	user1=joseph
user1uvmpw= q1234r	user1uvmpw=q1234r	user1uvmpw=q1234r	user1uvmpw=q1234r
user1winpw=	user1winpw=	user1winpw=	user1winpw=
user1domain=0	user1domain=0	user1domain=0	user1domain=0
user1ppchange=0	user1ppchange=0	user1ppchange=0	user1ppchange=0
user1ppexppolicy=0	user1ppexppolicy=0	user1ppexppolicy=0	user1ppexppolicy=0
user1ppexpdays= 184	user1ppexpdays=184	user1ppexpdays=184	user1ppexpdays=184
[UVMAppConfig]	[UVMAppConfig]	[UVMAppConfig]	[UVMAppConfig]
uvmlogon=0	uvmlogon=0	uvmlogon=0	uvmlogon=0
entrust=0	entrust=0	entrust=0	entrust=0

notes=0	notes=0	notes=0	notes=0
netscape=0	netscape=0	netscape=0	netscape=0
passman=0	passman=0	passman=0	passman=0
folderprotect=0	folderprotect=0	folderprotect=0	folderprotect=0
autoprotect=0	autoprotect=0	autoprotect=0	autoprotect=0

Netzwerk mit standortunabhängigem Zugriff verwalten

Der Netzadministrator eines Netzwerks mit standortunabhängigem Zugriff muss Benutzer autorisieren und den Zugriff auf das Netzwerk durch Benutzer und Clients steuern. Zu seinen Aufgaben gehört das Importieren eines Benutzerprofils, das Synchronisieren von Benutzerdaten sowie das Hinzufügen und Entfernen von Benutzern und Clients. Diese Aufgaben lassen sich in einem CSS-Netzwerk mit standortunabhängigem Zugriff schnell und leicht durchführen. Zu den Aufgaben des Administrators kann auch das Wiederherstellen des Netzwerks mit standortunabhängigem Zugriff, das Ändern des Administratorschlüsselpaars oder das Ändern der Archivposition gehörten.

Benutzer autorisieren

Nachdem Sie diese Schritte abgeschlossen haben, ist das CSS-Netzwerk mit standortunabhängigem Zugriff mit Berechtigungsnachweis konfiguriert, und die Roaming-Clients sind für den standortunabhängigen Zugriff registriert. Nun können Benutzer mit Hilfe des Administratordienstprogramms autorisiert werden.

Benutzerdaten synchronisieren

Die Daten der einzelnen Benutzer werden in der Archivposition gespeichert. Eine Kopie dieser Daten wird außerdem lokal auf den Computern gespeichert, die der Benutzer für einen standortunabhängigen Zugriff verwendet hat. Wenn Änderungen vorgenommen werden, wie z. B. das Abrufen eines Zertifikats oder das Ändern eines Verschlüsselungstextes, werden die lokalen Daten aktualisiert. Wenn der Computer über eine Verbindung zum Archiv verfügt, werden die Benutzerdaten ebenfalls aktualisiert. Wenn sich der Benutzer auf einem anderen Computer anmeldet, werden die Aktualisierungen automatisch auf diesen Computer heruntergeladen, vorausgesetzt, der Computer verfügt ebenfalls über eine Verbindung zum Archiv.

Eine Verbindung zum Archiv kann jedoch nicht immer gewährleistet werden, d. h., dass die Benutzerdaten auf den Computern und im Archiv möglicherweise nicht konsistent sind. Wenn die Benutzerdaten auf einem Computer geändert werden, der nicht mit dem Archiv verbunden ist, werden diese Änderungen im Archiv und demzufolge auch auf den anderen Computern nicht übernommen. Wenn der Computer eine Verbindung zum Archiv herstellen kann, werden die Änderungen im Archiv aktualisiert, und die Dateninkonsistenzen auf allen anderen Computern, zu denen eine Verbindung besteht, werden behoben. Wenn jedoch Änderungen auf einem anderen Computer mit einer Verbindung zum Archiv vorgenommen werden, bevor der erste Computer, auf dem Änderungen vorgenommen wurden, eine Verbindung zum Archiv herstellen kann, entsteht eine nicht behebbare Dateninkonsistenz. Die Daten im Archiv enthalten Änderungen, die auf dem ersten Computer nicht vorhanden sind, während dieser Computer Änderungen enthält, die nicht im Archiv gespeichert wurden. Wenn dieser Fall eintritt, wird der Benutzer benachrichtigt, dass zwei unterschiedliche Konfigurationen vorhanden sind. Er wird aufgefordert, die Konfiguration auszuwählen, die er übernehmen möchte, die lokale oder die archivierte Konfiguration. Die Änderungen in der Konfiguration, die nicht ausgewählt wird, gehen verloren.

Aus diesem Grund ist es wichtig sicherzustellen, dass alle Änderungen in einer Benutzerkonfiguration im Archiv ebenfalls aktualisiert werden, bevor Änderungen auf einem anderen Computer vorgenommen werden.

Verloren gegangenen Verschlüsselungstext in einer Umgebung mit standortunabhängigem Zugriff wiederherstellen

Wenn ein Verschlüsselungstext verloren geht oder vergessen wird, kann der Administrator den Verschlüsselungstext des Benutzers auf dem Roaming-Server oder auf einem registrierten Client zurücksetzen. Diese Änderung wird bei allen Systemen im Netzwerk aktualisiert, *außer* bei den Systemen, in die das Benutzerprofil importiert wurde, und bei denen der sichere UVM-Anmeldeschutz aktiviert ist. In diesem Fall wird die Aktualisierung des Verschlüsselungstextes im Computer *nicht* übernommen. Um auf den Computer zugreifen zu können, benötigt der Benutzer eine Kennwortüberschreibungsdatei. Außerdem muss der den Vorgang zum Überschreiben dess Kennworts durchführen.

Benutzerprofil importieren

Sie können ein Benutzerprofil auf einen neuen Computer im Netzwerk mit standortunabhängigem Zugriff mit Hilfe des Administratordienstprogramms, des Benutzerkonfigurationsprogramms oder mit UVM GINA importieren. Wenn Sie einen Benutzer importieren möchten, der über keinen Benutzeraccount auf dem neuen Computer verfügt, müssen Sie über die Systemsteuerung von Windows einen Windows-Benutzeraccount erstellen.

Anmerkung: Damit ein Benutzer in ein Netzwerk mit standortunabhängigem Zugriff importiert werden kann, muss dieser Benutzer auf einem anderen Computer in diesem Netzwerk autorisiert sein.

Benutzerprofil mit Hilfe des Benutzerkonfigurationsprogramms importieren

Um ein Benutzerprofil mit Hilfe des Benutzerkonfigurationsprogramms auf einem neuen Computer im Netzwerk mit standortunabhängigem Zugriff zu importieren, klicken Sie auf **Start > Programme > Access IBM > IBM Client Security > Sicherheitseinstellungen ändern**, und klicken Sie anschließend auf der Registerkarte "Benutzerkonfiguration" auf **Vorhandene Konfiguration aus Archiv importieren**.

Benutzerprofil mit Hilfe des Administratordienstprogramms importieren

Um ein Benutzerprofil mit Hilfe des Administratordienstprogramms auf einen neuen Computer im Netzwerk mit standortunabhängigem Zugriff zu importieren, wählen Sie den Benutzer aus, und klicken Sie auf **Berechtigen**. Klicken Sie auf **Ja** auf die Frage, ob Sie den Benutzer aus dem Archiv importieren möchten.

Benutzerprofil mit Hilfe von UVM GINA importieren

Sie können ein Benutzerprofil auf einen neuen Computer in einem Netzwerk mit standortunabhängigem Zugriff mit Hilfe von UVM GINA importieren. Dazu müssen Sie die UVM-Anmeldeanzeige aufrufen. Wenn ein Benutzer noch nicht für die Verwendung von UVM auf einem System in dem Netzwerk autorisiert ist, wird eine entsprechende Nachricht mit der Frage angezeigt, ob der Benutzer aus dem Archiv importiert werden soll.

Anmerkungen:

1. Wenn Sie einen Benutzer importieren möchten, der über keinen Benutzeraccount auf dem neuen Computer verfügt, müssen Sie über die Systemsteuerung von Windows einen Windows-Benutzeraccount erstellen, bevor Sie fortfahren können.
2. Um auf das Archiv auf dem Roaming-Server zugreifen zu können, muss das Verzeichnis ein zugeordnetes Netzlaufwerk sein.

Gehen Sie wie folgt vor, um ein Benutzerprofil mit Hilfe von UVM GINA, das auf einem Computer mit Windows 2000 ausgeführt wird, auf einen neuen Computer im Netzwerk mit standortunabhängigem Zugriff zu importieren:

1. Geben Sie bei der Anmeldung den Benutzernamen und den UVM-Verschlüsselungstext des Benutzers ein, der importiert werden soll. Es wird eine Nachricht mit der Frage angezeigt, ob das Benutzerprofil aus dem Archiv importiert werden soll.
2. Klicken Sie auf **Ja**, wenn Sie dazu aufgefordert werden, um den Benutzer zu importieren, und klick en Sie anschließend auf **OK**.
3. Wenn sich die Archivposition auf einem Netzlaufwerk befindet, klicken Sie auf **Ja**, wenn angezeigt wird, dass eine Berechtigung für den Netzwerkzugriff benötigt wird.
4. Geben Sie in der Windows-Standardanmeldeanzeige Ihr Windows-Kennwort ein. Sie werden aufgefordert, den Pfad für das Archiv einzugeben.
5. Geben Sie den Netzpfad für das Archiv an.
6. Geben Sie den Benutzernamen und das Kennwort für den Netzpfad an.
7. Klicken Sie auf **OK**. Wenn der Vorgang ordnungsgemäß beendet wurde, wird eine Nachricht angezeigt, dass das Profil erfolgreich importiert wurde.

Gehen Sie wie folgt vor, um ein Benutzerprofil mit Hilfe von UVM GINA, das auf einem Computer mit Windows XP ausgeführt wird, auf einen neuen Computer im Netzwerk mit standortunabhängigem Zugriff zu importieren:

1. Geben Sie bei der Anmeldung den Benutzernamen und den UVM-Verschlüsselungstext des Benutzers ein, der importiert werden soll. Es wird eine Nachricht mit der Frage angezeigt, ob das Benutzerprofil aus dem Archiv importiert werden soll.
2. Klicken Sie auf **Ja**, wenn Sie dazu aufgefordert werden, um den Benutzer zu importieren, und klick en Sie anschließend auf **OK**.
3. Wenn sich die Archivposition auf einem Netzlaufwerk befindet, klicken Sie auf **Ja**, wenn angezeigt wird, dass eine Berechtigung für den Netzwerkzugriff benötigt wird.
4. Geben Sie bei der Windows-Standardaufforderung für die Zuordnung eines Netzlaufwerks den Netzpfad für das Archiv ein.
5. Klicken Sie auf **Fertig stellen**.
6. Geben Sie den Benutzernamen und das Kennwort für den Netzpfad an, und klicken Sie auf **OK**. Wenn der Vorgang ordnungsgemäß beendet wurde, wird eine Nachricht angezeigt, dass das Profil erfolgreich importiert wurde.

Anmerkung: Damit ein Benutzer in ein Netzwerk mit standortunabhängigem Zugriff importiert werden kann, muss dieser Benutzer auf einem anderen Computer in diesem Netzwerk autorisiert sein.

Nach dem Importieren des Benutzerprofils wird die Authentifizierung mit UVM entsprechend der auf diesem Computer definierten Sicherheits-Policy durchgeführt.

Der Benutzer muss über die Sicherheitsbestimmungen für diesen Computer informiert werden, bevor er sich anmelden kann.

Benutzer in einem Netzwerk mit standortunabhängigem Zugriff entfernen und wiederherstellen

Um einen Benutzer aus einem Netzwerk mit standortunabhängigem Zugriff zu entfernen, muss der Netzadministrator über die Administratorkonsole folgende Schritte ausführen:

1. Starten Sie das Dienstprogramm "Administratorkonsole", und geben Sie das Administratorkennwort ein.
2. Klicken Sie auf **Standortunabhängigen Zugriff mit Berechtigungsnachweis konfigurieren**.
3. Wählen Sie die Option **Benutzer von UVM und dem Netzwerk mit standortunabhängigem Zugriff mit Berechtigungsnachweis entfernen** aus, und klicken Sie auf **Weiter**. Wiederholen Sie diese Schritte bei Bedarf.
4. Wählen Sie den Benutzer aus, der entfernt werden soll, und klicken Sie auf **Entfernen**.

   Anmerkung: Wenn ein Benutzer aus dem Netzwerk entfernt wurde, gehen alle diesem Benutzer zugeordneten Berechtigungsnachweise für immer verloren.

Entfernte Benutzer sind erst wieder berechtigt, UVM und das Netzwerk mit standortunabhängigem Zugriff zu nutzen, wenn sie vom Netzadministrator wiederhergestellt wurden.

Um einen Benutzer in einem Netzwerk mit standortunabhängigem Zugriff wiederherzustellen, muss der Netzadministrator über die Administratorkonsole folgende Schritte ausführen:

1. Starten Sie das Dienstprogramm "Administratorkonsole", und geben Sie das Administratorkennwort ein.
2. Klicken Sie auf **Standortunabhängigen Zugriff mit Berechtigungsnachweis konfigurieren**.
3. Wählen Sie die Option **Entfernte Benutzer wiederherstellen** aus, und klicken Sie auf **Weiter**.
4. Wählen Sie den Benutzer aus, der wiederhergestellt werden soll, und klicken Sie auf **Wiederherstellen**. Wiederholen Sie diese Schritte bei Bedarf.

   Wenn der Benutzer wiederhergestellt ist, kann ihm die Berechtigung zur Verwendung von UVM erneut erteilt werden. Durch das Wiederherstellen eines Benutzers erhält dieser nicht automatisch die Berechtigung zur Verwendung von UVM.

Registrierte Clients in einem Netzwerk mit standortunabhängigem Zugriff entfernen und wiederherstellen

Um einen registrierten Client aus einem Netzwerk mit standortunabhängigem Zugriff zu entfernen, muss der Netzadministrator über die Administratorkonsole folgende Schritte ausführen:

1. Starten Sie das Dienstprogramm "Administratorkonsole", und geben Sie das Administratorkennwort ein.
2. Klicken Sie auf **Standortunabhängigen Zugriff mit Berechtigungsnachweis konfigurieren**.

3. Wählen Sie die Option **Registrierte Clients aus dem Netzwerk mit standortunabhängigem Zugriff mit Berechtigungsnachweis entfernen** aus, und klicken Sie auf **Weiter**.
4. Wählen Sie das System aus, das entfernt werden soll, und klicken Sie auf **Entfernen**. Wiederholen Sie diese Schritte bei Bedarf.

   Anmerkung: Wenn ein Client aus dem Netzwerk entfernt wurde, gehen alle diesem Client zugeordneten maschinenbasierten Berechtigungsnachweise für immer verloren.

Entfernte Clients können erst beim Roaming-Server registriert werden, nachdem sie vom Netzadministrator wiederhergestellt wurden.

Um einen registrierten Client in einem Netzwerk mit standortunabhängigem Zugriff wiederherzustellen, muss der Netzadministrator über die Administratorkonsole folgende Schritte ausführen:

1. Starten Sie das Dienstprogramm "Administratorkonsole", und geben Sie das Administratorkennwort ein.
2. Klicken Sie auf **Standortunabhängigen Zugriff mit Berechtigungsnachweis konfigurieren**.
3. Wählen Sie die Option **Entfernte Clients wiederherstellen** aus, und klicken Sie auf **Weiter**.
4. Wählen Sie den Client aus, der wiederhergestellt werden soll, und klicken Sie auf **Wiederherstellen**. Wiederholen Sie diese Schritte bei Bedarf.

   Wenn der Client wiederhergestellt ist, kann er beim Roaming-Server wieder registriert werden. Durch das Wiederherstellen eines Client wird dieser nicht automatisch neu registriert.

Anmerkung: Benutzer, deren Berechtigungsnachweis auf dem System vorhanden war, als der Client entfernt wurde, müssen ihren Berechtigungsnachweis möglicherweise erneut importieren.

Zugriff in einem Netzwerk mit standortunabhängigem Zugriff auf registrierte Clients beschränken

Es kann vorkommen, dass ein Netzadministrator einigen Benutzern den Zugriff auf einen bestimmten registrierten Client gewähren, anderen Benutzern den Zugriff jedoch entziehen möchte.

Um Benutzerzugriffsberechtigungen zu verwalten, muss der Netzadministrator über die Administratorkonsole folgende Schritte ausführen:

1. Starten Sie das Dienstprogramm "Administratorkonsole", und geben Sie das Administratorkennwort ein.
2. Klicken Sie auf **Standortunabhängigen Zugriff mit Berechtigungsnachweis konfigurieren**.
3. Wählen Sie die Option **Benutzerzugriff auf registrierte Clients verwalten** aus, und klicken Sie auf **Weiter**.
4. Wählen Sie im Fenster **Wählen Sie ein System im CSS-Netzwerk mit standortunabhängigem Zugriff mit Berechtigungsnachweis aus** den registrierten Client aus, den Sie verwalten möchten. In den beiden Listenfenstern sind Benutzer mit und ohne Zugriff aufgeführt.

5. Führen Sie einen der folgenden Schritte aus:
   - Um einem Benutzer den Zugriff zu entziehen, wählen Sie den Benutzer aus der Liste **Benutzer mit Zugriff** aus, und klicken Sie auf **Entziehen**. Wiederholen Sie diese Schritte bei Bedarf.
   - Um einem Benutzer den Zugriff zu gewähren, wählen Sie den Benutzer aus der Liste **Benutzer ohne Zugriff** aus, und klicken Sie auf **Zulassen**. Wiederholen Sie diese Schritte bei Bedarf.

Für die Zugriffsverwaltungsfunktionen des Netzwerks mit standortunabhängigem Zugriff muss im Archiv ein neuer Ordner erstellt werden. Für den neuen geschützten Ordner muss der Netzadministrator über Schreibzugriff, die anderen Benutzer nur über Lesezugriff verfügen. Wenn Benutzer über Schreibzugriff für diesen Ordner verfügen, können sie sich selbst oder ihre Systeme manuell wiederherstellen.

Netzwerk mit standortunabhängigem Zugriff wiederherstellen

Im Falle eines Software- oder Hardwarefehlers muss das Netzwerk mit standortunabhängigem Zugriff möglicherweise wiederhergestellt werden. Wenn der Roaming-Server beschädigt ist oder die von CSS verwendeten Daten auf einem registrierten Client beschädigt sind, können Sie die Daten mit Hilfe des Administratordienstprogramms genau so wiederherstellen, wie Sie es in einer Umgebung ohne standortunabhängigen Zugriff tun würden. Wenn das integrierte IBM Sicherheits-Subsystem (IBM Embedded Security Subsystem) auf einem registrierten Client beschädigt oder gelöscht wird, muss der Client erneut beim Roaming-Server registriert werden. Es ist keine weitere Maßnahme erforderlich.

Administratorschlüsselpaar ändern

Es ist nicht empfehlenswert, das Administratorschlüsselpaar in einem Netzwerk mit standortunabhängigem Zugriff zu ändern.

Um ein Administratorschlüsselpaar in einem Netzwerk mit standortunabhängigem Zugriff zu ändern, müssen Sie folgende Schritte ausführen, damit die Änderung an alle Computer im Netzwerk weitergeleitet wird.

1. Ändern Sie auf dem Roaming-Server das Administratorschlüsselpaar mit Hilfe des Administratordienstprogramms.
2. Registrieren Sie alle Clients im Netzwerk erneut.
3. Speichern bzw. übernehmen Sie bei allen entsprechenden Eingabeaufforderungen die vorhandenen Dateien.

Archivordner ändern

Der Prozess zum Ändern des Archivordners in einem Netzwerk mit standortunabhängigem Zugriff unterscheidet sich von dem Prozess in einem Netzwerk ohne standortunabhängigen Zugriff, da alle Computer in dem Netzwerk auf dieselbe Archivposition zugreifen.

Gehen Sie wie folgt vor, um den Archivordner in einem Netzwerk mit standortunabhängigem Zugriff zu ändern:

1. Kopieren Sie die Dateien aus dem alten Archivordner in den neuen Ordner. Gehen Sie dazu wie folgt vor:
   a. Starten Sie das Administratordienstprogramm, und geben Sie das Administratorkennwort ein.
   b. Klicken Sie auf **Schlüsselkonfiguration**.

c. Wählen Sie die Option "Archivposition ändern" aus, und klicken Sie auf **Weiter**.
d. Geben Sie den neuen Archivordner ein, und klicken Sie auf **Weiter**.
e. Klicken Sie auf **Ja** auf die Frage, ob Sie alle Dateien vom alten in den neuen Ordner kopieren möchten.

2. Gehen Sie wie folgt vor, um alle anderen Computer im Netzwerk für die Verwendung des neuen Archivordners zu aktualisieren:
   a. Starten Sie das Administratordienstprogramm, und geben Sie das Administratorkennwort ein.
   b. Klicken Sie auf **Schlüsselkonfiguration**.
   c. Wählen Sie die Option "Archivposition ändern" aus, und klicken Sie auf **Weiter**.
   d. Geben Sie den neuen Archivordner ein, und klicken Sie auf **Weiter**.
   e. Klicken Sie auf **Nein** auf die Frage, ob Sie alle Dateien vom alten in den neuen Ordner kopieren möchten.

FFE

Die FFE-Funktionalität (File and Folder Encryption, Verschlüsselung von Dateien und Ordnern) ist in einer Umgebung mit standortunabhängigem Zugriff nicht beeinträchtigt. Geschützte Ordner werden jedoch auf den einzelnen Computern gesondert verwaltet. Wenn z. B. ein Ordner von Benutzer A auf System A geschützt wird, ist ein Ordner mit demselben Namen auf System B - falls ein solches vorhanden ist - nicht geschützt, es sei denn, der Benutzer schützt diesen Ordner ebenfalls explizit auf System B.

IBM Password Manager

Alle mit Hilfe des IBM Password Managers geschützten Kennwörter sind auf allen Computern im Netzwerk mit standortunabhängigem Zugriff verfügbar.

Begriffe und Begriffsbestimmungen in Bezug auf standortunabhängigen Zugriff

Im Hinblick auf die Konzepte und Prozeduren in Verbindung mit der Konfiguration eines Netzwerks mit standortunabhängigem Zugriff ist es nützlich, die Definition der folgenden Begriffe zu kennen:

Roaming-Client-Registrierung
Das Registrieren eines Computers auf dem Roaming-Server.

Roaming-Clients
Alle gesicherten TCPA-Computer in dem Netzwerk mit standortunabhängigem Zugriff.

Roaming-Server
Der TCPA-Computer, der für die Initialisierung des Netzwerks mit standortunabhängigem Zugriff verwendet wird.

Kennwort für die Roaming-Client-Registrierung
Das Kennwort zum Registrieren des Computers auf dem Roaming-Server.

Kapitel 4. Client Security verwenden

Administratoren können mit den zahlreichen Komponenten von Client Security die Sicherheitsfunktionen einrichten, die für IBM Clientbenutzer erforderlich sind. Sie können sich an den folgenden Beispielen orientieren, wenn Sie die Policies und die Konfiguration mit Client Security planen. Windows 2000- und Windows XP-Anwender können z. B. für die Anmeldung am System den UVM-Schutz einrichten; dadurch werden unberechtigte Benutzer daran gehindert, sich am IBM Client anzumelden.

Beispiel 1 - Ein Client unter Windows 2000 und ein Client unter Windows XP, beide mit Outlook Express

In diesem Beispiel ist auf einem IBM Client (Client 1) Windows 2000 und Outlook Express installiert, auf dem anderen Client (Client 2) Windows XP und Outlook Express. Für drei Benutzer ist die Konfiguration der UVM-Authentifizierung auf Client 1 erforderlich; für einen Clientbenutzer ist eine Konfiguration der UVM-Benutzerauthentifizierung auf Client 2 erforderlich. Alle Clientbenutzer registrieren ihre Fingerabdrücke, so dass diese zur Authentifizierung verwendet werden können. In diesem Beispiel wird ein UVM-Sensor für Fingerabdrücke installiert. Außerdem wurde ermittelt, dass beide Clients den UVM-Schutz für die Windows-Anmeldung erfordern. Der Administrator hat entschieden, dass die UVM-Policy bearbeitet und von den einzelnen Clients verwendet werden soll.

Zum Einrichten von Client Security müssen Sie folgende Schritte ausführen:

1. Installieren Sie die Software auf Client 1 und Client 2. Weitere Informationen hierzu finden Sie im *Client Security Installationshandbuch*.
2. Installieren Sie die UVM-Sensoren für Fingerabdrücke und die zugehörige Software auf den einzelnen Clients.

   Weitere Informationen zu UVM-sensitiven Produkten finden Sie im World Wide Web unter der Adresse
   http://www.pc.ibm.com/us/security/secdownload.html.
3. Konfigurieren Sie die Benutzerauthentifizierung mit UVM für die einzelnen Clients. Gehen Sie wie folgt vor:
   a. Autorisieren Sie Benutzer für die Verwendung von UVM, indem Sie ihnen einen UVM-Verschlüsselungstext zuordnen. Da Client 1 drei Benutzer aufweist, müssen Sie das Autorisieren von Benutzern für die Verwendung von UVM wiederholen, bis alle Benutzer autorisiert sind.
   b. Konfigurieren Sie für die einzelnen Clients den UVM-Schutz für die Windows-Anmeldung.
   c. Registrieren Sie die Fingerabdrücke der Benutzer. Da in einer Policy festgelegt wird, dass drei Benutzer den Client 1 verwenden, müssen alle drei Benutzer ihre Fingerabdrücke auf Client 1 registrieren.

      Anmerkung: Wenn Sie als Authentifizierungsbestimmung in der UVM-Policy für den Client Fingerabdrücke konfigurieren, müssen die einzelnen Benutzer ihre Fingerabdrücke registrieren.
4. Bearbeiten und speichern Sie eine lokale UVM-Policy auf jedem Client, der die Authentifizierung für Folgendes erfordert:
   - Anmeldung am Windows-Betriebssystem

- Anfordern eines digitalen Zertifikats
- Verwenden einer digitalen Unterschrift für Outlook Express

5. Starten Sie die einzelnen Clients erneut, um den UVM-Anmeldeschutz für die Windows-Anmeldung zu aktivieren.
6. Informieren Sie die Benutzer über die UVM-Verschlüsselungstexte, die Sie für sie konfiguriert haben, und über die Authentifizierungsbestimmungen, die Sie für den IBM Client in der UVM-Policy konfiguriert haben.

Clientbenutzer können nun folgende Tasks ausführen:

- Sie können den UVM-Schutz zum Sperren und Entsperren von Windows verwenden.
- Sie können ein digitales Zertifikat anfordern und das integrierte IBM Sicherheits-Subsystem (IBM Embedded Security Subsystem, ESS) auswählen, um die zum Zertifikat gehörige Verschlüsselung bereitzustellen.
- Sie können das digitale Zertifikat zur Verschlüsselung von E-Mails verwenden, die mit Outlook Express erstellt wurden.

Beispiel 2 - Zwei IBM Clients unter Windows 2000 mit Lotus Notes

In diesem Beispiel ist auf zwei IBM Clients (Client 1 und Client 2) Windows 2000 und Lotus Notes installiert. Für zwei Benutzer ist die Konfiguration der UVM-Authentifizierung auf Client 1 erforderlich; für einen Benutzer ist die Konfiguration der UVM-Authentifizierung auf Client 2 erforderlich; für beide Clients ist der UVM-Anmeldeschutz für die Windows-Anmeldung erforderlich. Der Administrator hat entschieden, dass die UVM-Policy auf Client 1 bearbeitet und dann auf Client 2 kopiert wird.

Zum Einrichten von Client Security müssen Sie folgende Schritte ausführen:

1. Installieren Sie die Software auf Client 1 und Client 2. Da dieselbe UVM-Policy-Datei verwendet wird, müssen Sie denselben öffentlichen Administratorschlüssel verwenden, wenn Sie die Software auf Client 1 und auf Client 2 installieren. Weitere Informationen zur Softwareinstallation finden Sie im *Client Security Installationshandbuch*.
2. Konfigurieren Sie die Benutzerauthentifizierung mit UVM für die einzelnen Clients. Gehen Sie anschließend wie folgt vor:
   a. Autorisieren Sie Benutzer für die Verwendung von UVM, indem Sie ihnen einen UVM-Verschlüsselungstext zuordnen. Da Client 1 zwei Benutzer aufweist, müssen Sie das Autorisieren von Benutzern für die Verwendung von UVM wiederholen, bis beide Benutzer autorisiert sind.
   b. Konfigurieren Sie für die einzelnen Clients den UVM-Anmeldeschutz für die Windows-Anmeldung.
3. Aktivieren Sie die Lotus Notes-Unterstützung für den UVM-Schutz auf beiden Clients.
4. Bearbeiten und speichern Sie eine UVM-Policy auf Client 1, und kopieren Sie sie anschließend auf Client 2. Die UVM-Policy macht eine Benutzerauthentifizierung für das Entfernen des Bildschirmschoners, für die Anmeldung bei Lotus Notes und für die Windows-Anmeldung erforderlich. Weitere Informationen hierzu finden Sie im Abschnitt „UVM-Policy bearbeiten und verwenden" auf Seite 47.
5. Starten Sie die einzelnen Clients erneut, um den UVM-Anmeldeschutz für die Windows-Anmeldung zu aktivieren.
6. Informieren Sie die Clientbenutzer über die UVM-Verschlüsselungstexte und über die Policies, die für die einzelnen Clients festgelegt wurden.

Beispiel 3 - Mehrere IBM Clients unter Windows 2000 mit Tivoli Access Manager-Verwaltung und mit Netscape als E-Mail-Programm

Die Zielgruppe für das folgende Beispiel sind Unternehmensadministratoren, die planen, Tivoli Access Manager zur Verwaltung der mit der UVM-Policy konfigurierten Authentifizierungsobjekte zu verwenden. In diesem Beispiel ist auf mehreren IBM Clients Windows 2000 und Netscape installiert. Auf allen Clients ist der NetSEAT-Client, eine Komponente von Tivoli Access Manager, installiert. Auf allen Clients, die einen LDAP-Server verwenden, ist der LDAP-Client installiert. Mit der UVM-Policy kann Tivoli Access Manager ausgewählte Authentifizierungsobjekte für Clients steuern.

In diesem Beispiel ist für einen einzigen Benutzer auf jedem Client die Konfiguration der UVM-Authentifizierung erforderlich. Alle Benutzer registrieren ihre Fingerabdrücke, so dass diese zur Authentifizierung verwendet werden können. In diesem Beispiel wird ein UVM-Sensor für Fingerabdrücke installiert, und für alle Clients ist der UVM-Anmeldeschutz für die Windows-Anmeldung erforderlich.

Gehen Sie wie folgt vor, um Client Security einzurichten:

1. Installieren Sie Client Security auf dem Tivoli Access Manager-Server. Weitere Informationen hierzu finden Sie im Handbuch *Client Security mit Tivoli Access Manager verwenden*.
2. Installieren Sie Client Security auf allen Clients. Da eine UVM-Policy verwendet wird, müssen Sie denselben öffentlichen Administratorschlüssel verwenden, wenn Sie die Software auf allen Clients installieren. Weitere Informationen zur Softwareinstallation finden Sie im *Client Security Installationshandbuch*.
3. Installieren Sie die UVM-Sensoren für Fingerabdrücke und die zugehörige Software auf den einzelnen Clients. Weitere Informationen zu verfügbaren UVM-sensitiven Produkten finden Sie im World Wide Web unter der Adresse http://www.pc.ibm.com/us/security/index.html.
4. Konfigurieren Sie auf jedem Client die Benutzerauthentifizierung mit UVM. Weitere Informationen hierzu finden Sie im Abschnitt „Benutzer entfernen" auf Seite 33. Gehen Sie anschließend wie folgt vor:
   a. Autorisieren Sie Benutzer für die Verwendung von UVM, indem Sie ihnen einen UVM-Verschlüsselungstext zuordnen.
   b. Konfigurieren Sie für die einzelnen Clients den UVM-Anmeldeschutz für die Windows-Anmeldung.
   c. Registrieren Sie für die einzelnen Clientbenutzer die Fingerabdrücke. Wenn auf einem IBM Client die Authentifizierung über Fingerabdrücke erforderlich ist, müssen alle Benutzer dieses Clients ihre Fingerabdrücke registrieren.
5. Geben Sie die Informationen zur Tivoli Access Manager-Konfiguration auf den einzelnen Clients an. Weitere Informationen hierzu finden Sie im Handbuch *Client Security mit Tivoli Access Manager verwenden*.
6. Bearbeiten und speichern Sie auf einem der Clients eine UVM-Policy, und kopieren Sie diese anschließend auf die anderen Clients. Konfigurieren Sie die UVM-Policy so, dass Tivoli Access Manager die folgenden Authentifizierungsobjekte steuert:
   - Anmeldung am Windows-Betriebssystem
   - Anfordern eines digitalen Zertifikats
   - Verwenden einer digitalen Unterschrift für Outlook Express

Weitere Informationen hierzu finden Sie im Abschnitt „UVM-Policy bearbeiten und verwenden" auf Seite 47.

7. Starten Sie die einzelnen Clients erneut, um den UVM-Anmeldeschutz für die Windows-Anmeldung zu aktivieren.
8. Installieren Sie das PKCS #11-Modul des integrierten IBM Security Chips auf jedem Client. Dieses Modul unterstützt die Verschlüsselung auf Clients, die über Netscape E-Mails senden und empfangen, sowie das integrierte IBM Sicherheits-Subsystem für die Anforderung digitaler Zertifikate. Weitere Informationen hierzu finden Sie im *Client Security Installationshandbuch*.
9. Ermöglichen Sie Tivoli Access Manager die Steuerung der IBM Client Security Solutions-Objekte, die in der Verwaltungskonsole von Tivoli Access Manager angezeigt werden.
10. Informieren Sie die Clientbenutzer über die UVM-Verschlüsselungstexte und über die Policy, die für die einzelnen Clients festgelegt wurden.
11. Weisen Sie die Clientbenutzer an, im *Client Security Benutzerhandbuch* die Anweisungen zu folgenden Tasks zu lesen:
    - UVM-Schutz zum Sperren und Entsperren von Windows verwenden
    - Benutzerkonfigurationsprogramm verwenden
    - Ein digitales Zertifikat anfordern, das das integrierte IBM Sicherheits-Subsystem verwendet, um die zum Zertifikat gehörige Verschlüsselung bereitzustellen
    - Ein digitales Zertifikat zur Verschlüsselung von E-Mails verwenden, die mit Netscape erstellt wurden

Kapitel 5. Benutzer autorisieren

Folgende Informationen sind hilfreich bei der Autorisierung von Windows-Benutzern für die Verwendung von User Verification Manager (UVM).

Authentifizierung für Clientbenutzer

Die Authentifizierung von Endbenutzern auf Clientebene ist ein wichtiger Aspekt der Computersicherheit. Client Security bietet die erforderliche Schnittstelle zur Verwaltung der Sicherheitspolicy eines IBM Clients. Diese Schnittstelle ist Teil der Authentifizierungssoftware UVM (User Verification Manager), der Hauptkomponente von Client Security.

Die UVM-Sicherheitspolicy für einen IBM Client können Sie auf eine der zwei folgenden Arten verwalten:

- Lokal mit einem Policy-Editor, der sich auf dem IBM Client befindet
- Unternehmensweite Verwaltung über Tivoli Access Manager

Chiffrierschlüssel für die Hardware werden erzeugt, wenn Sie den ersten Benutzer hinzufügen.

Authentifizierungselemente

Authentifizierungselemente (z. B. UVM-Verschlüsselungstexte oder Fingerabdrücke von Benutzern) werden verwendet, um Benutzer mit dem IBM Client zu autorisieren. Wenn Sie einen Benutzer für die Verwendung von UVM autorisieren, ordnen Sie dem Clientbenutzer einen UVM-Verschlüsselungstext zu. Der UVM-Verschlüsselungstext kann bis zu 256 Zeichen lang sein und ist das wichtigste Element für die UVM-Authentifizierung. Wenn Sie einen UVM-Verschlüsselungstext zuordnen, werden für diesen Clientbenutzer Chiffrierschlüssel erstellt und in einer Datei gespeichert, die vom integrierten IBM Sicherheits-Subsystem (IBM Embedded Security Subsystem, ESS) verwaltet wird. Wenn der IBM Client eine UVM-sensitive Einheit zur Authentifizierung verwendet, z. B. Fingerabdrücke von Benutzern oder ein berührungsloser Ausweis (Proximity Badge), muss das Authentifizierungselement auch in UVM registriert sein.

Bei der Konfiguration der Benutzerauthentifizierung können Sie die folgenden Client Security-Funktionen auswählen:

- **UVM-Schutz für die Anmeldung am Betriebssystem:** Der UVM-Schutz stellt sicher, dass nur Benutzer, die von UVM erkannt werden, auf den Computer zugreifen können. Lesen Sie die wichtigen Informationen im Abschnitt ″UVM-Anmeldeschutz konfigurieren″, bevor Sie den UVM-Schutz für die Anmeldung am System aktivieren.
- **Client Security-Bildschirmschoner:** Nachdem Sie einen Clientbenutzer hinzugefügt haben, kann dieser Benutzer den Client Security-Bildschirmschoner konfigurieren und verwenden. Der Client Security-Bildschirmschoner wird mit Hilfe der Anzeigeoption in der Systemsteuerung von Windows konfiguriert. Sie müssen den UVM-Schutz für die Anmeldung am System aktivieren, um den Client Security-Bildschirmschoner verwenden zu können.

Vor dem Autorisieren von Benutzern

Wichtig: Autorisieren Sie nur Benutzeraccounts, mit denen eine Windows-Anmeldung möglich ist. Wenn ein Benutzeraccount autorisiert wird, der *nicht* zur Windows-Anmeldung verwendet werden kann, werden bei aktivierter gesicherter UVM-Anmeldung **alle** Benutzer für das System gesperrt.

Wichtig: Mindestens ein Clientbenutzer **muss** berechtigt sein, UVM während der Installation zu verwenden. Wenn bei der ersten Installation von Client Security kein Benutzer zur Verwendung von UVM berechtigt ist, werden die Sicherheitseinstellungen **nicht** angewendet, und Ihre Daten werden **nicht** geschützt.

Wenn Sie einen Clientbenutzer autorisieren, bietet das Administratordienstprogramm eine Liste mit Benutzernamen an, in der Sie eine Auswahl treffen können. Die in dieser Liste aufgeführten Namen sind Benutzeraccounts, die mit Hilfe von Windows hinzugefügt wurden. Erstellen Sie mit Hilfe von Windows Benutzeraccounts und Profile für die entsprechenden Benutzer, bevor Sie in UVM Clientbenutzer hinzufügen. Client Security funktioniert in Verbindung mit den Sicherheitseinrichtungen des Windows-Betriebssystems.

Mit dem Programm "Benutzer und Kennwörter" können Sie neue Benutzeraccounts erstellen und Benutzeraccounts oder Benutzergruppen verwalten. Weitere Informationen finden Sie in der Dokumentation von Microsoft.

Anmerkungen:

1. Wenn Sie mit Hilfe von Windows neue Benutzer erstellen, muss das Domänenkennwort für jeden neuen Benutzer gleich sein.
2. Autorisieren Sie keinen neuen Benutzer, dessen Windows-Benutzername zuvor geändert wurde. Andernfalls verweist UVM auf den früheren Benutzernamen, während Windows nur den neuen Benutzernamen erkennt.
3. Wenn ein Benutzeraccount, der autorisiert wurde, aus dem Windows-System gelöscht wird, listet die Schnittstelle für gesicherte UVM-Anmeldung fälschlicherweise weiterhin den Account als für die Anmeldung bei Windows geeignet auf. Dieser Account *kann nicht* zur Anmeldung bei Windows verwendet werden.
4. Nachdem ein Benutzer autorisiert wurde, dürfen Sie dessen Windows-Benutzernamen nicht ändern. Andernfalls müssen Sie den neuen Benutzernamen in UVM erneut autorisieren und alle neuen Berechtigungsnachweise anfordern.

Benutzer autorisieren

Benutzer müssen sich mit der Administratorberechtigung anmelden, wenn sie das Administratordienstprogramm verwenden möchten.

Gehen Sie wie folgt vor, um Benutzer in UVM zu autorisieren:

1. Klicken Sie auf dem Windows-Desktop des IBM Clients auf **Start > Einstellungen > Systemsteuerung > Integriertes IBM Sicherheits-Subsystem**.

   Die Anzeige "Administratorkennwort eingeben" wird angezeigt.
2. Geben Sie das Administratorkennwort ein, und klicken Sie auf **OK**.

   Das Hauptfenster des Administratordienstprogramms für das IBM Sicherheits-Subsystem wird angezeigt.
3. Wählen Sie im Bereich "Zu autorisierende Windows-Benutzer auswählen" in der Liste einen Benutzernamen aus.

Anmerkung: Die Benutzernamen in der Liste sind durch die Benutzeraccounts definiert, die in Windows erstellt wurden.

4. Klicken Sie auf **Autorisieren**.

   Die Anzeige "Konfiguration der Benutzerauthentifizierung" erscheint.

5. Geben Sie den UVM-Verschlüsselungstext für den neu berechtigten Benutzer ein, und bestätigen Sie diesen. Klicken Sie anschließend auf **Weiter**.

   Wenn der Verschlüsselungstext nicht die Bedingungen der Sicherheitspolicy erfüllt, erscheint eine Anzeige, die darauf hinweist, dass der eingegebene Verschlüsselungstext ungültig ist. Klicken Sie in diesem Fall auf **OK** und anschließend auf **Bedingungen für Verschlüsselungstext anzeigen**, um die Parameter anzuzeigen, die ein gültiger Verschlüsselungstext erfüllen muss.

   Wenn der Verschlüsselungstext akzeptiert wird, wird eine Nachricht angezeigt, die angibt, dass der Vorgang erfolgreich ausgeführt wurde.

6. Klicken Sie auf **OK**, um fortzufahren.

   Die Anzeige "Windows-Anmeldekennwort" erscheint. Wenn die gesicherte UVM-Anmeldung aktiviert ist, muss das aktuelle Windows-Kennwort dieses Benutzers gespeichert werden, damit sich der Benutzer am System anmelden kann. In dieser Anzeige stehen dem Administrator folgende Auswahlmöglichkeiten zur Verfügung:

   - **Benutzer soll Windows-Kennwort später mit dem Benutzerkonfigurationsprogramm speichern.** Soll der Benutzer das Windows-Kennwort später mit dem Benutzerkonfigurationsprogramm speichern, wählen Sie den entsprechenden Radioknopf aus, und klicken sie auf **Weiter**.
   - **Aktuelles Windows-Kennwort des Benutzers sofort speichern** Um das aktuelle Windows-Kennwort des Benutzers sofort zu speichern, geben Sie das Kennwort des Benutzers in das entsprechende Feld ein, und bestätigen Sie es. Klicken Sie dann auf **Weiter**.

     Anmerkung: Das hier eingegebene Kennwort muss mit dem aktuellen Windows-Kennwort des Benutzers übereinstimmen. Diese Einstellung hat keinen Einfluss auf das Kennwort, das im Windows-Betriebssystem gespeichert ist.

   Es erscheint eine Nachricht, in der mitgeteilt wird, dass der Vorgang erfolgreich ausgeführt wurde.

7. Klicken Sie auf **Fertig stellen**.

Benutzer entfernen

Benutzer müssen sich mit der Administratorberechtigung anmelden, wenn sie das Administratordienstprogramm einsetzen möchten.

Gehen Sie wie folgt vor, um die Autorisierung von Benutzern in UVM aufzuheben:

1. Klicken Sie auf dem Windows-Desktop des IBM Clients auf **Start > Einstellungen > Systemsteuerung > Integriertes IBM Sicherheits-Subsystem**.

   Die Anzeige "Administratorkennwort eingeben" erscheint.

2. Geben Sie das Administratorkennwort ein, und klicken Sie auf **OK**.

   Das Hauptfenster des Administratordienstprogramms für das IBM Sicherheits-Subsystem wird angezeigt.

3. Wählen Sie im Bereich "Für die Benutzung von UVM berechtigte Windows-Benutzer" in der Liste einen Benutzernamen aus.

4. Klicken Sie auf **Benutzer entfernen**.

   Es wird eine Warnung angezeigt, die darauf hinweist, dass die Sicherheitsdaten des ausgewählten Benutzers, einschließlich aller Schlüssel, Zertifikate, registrierter Fingerabdrücke und gespeicherter Kennwörter, gelöscht werden.
5. Klicken Sie auf **Ja**, um fortzufahren.

   Es wird eine Nachricht mit der Frage angezeigt, ob die archivierten Daten des Benutzers gelöscht werden sollen. Wenn diese Daten gelöscht werden, kann der Benutzer auf keinem System zuvor gespeicherte Einstellungen wiederherstellen.
6. Klicken Sie auf **Ja**, um den Vorgang auszuführen.

Neue Benutzer erstellen

Benutzer müssen sich mit der Administratorberechtigung anmelden, wenn sie das Administratordienstprogramm einsetzen möchten.

Gehen Sie wie folgt vor, um neue Benutzer zu erstellen:

1. Klicken Sie auf dem Windows-Desktop des IBM Clients auf **Start > Einstellungen > Systemsteuerung > Integriertes IBM Sicherheits-Subsystem**.

   Die Anzeige "Administratorkennwort eingeben" erscheint.
2. Geben Sie das Administratorkennwort ein, und klicken Sie auf **OK**.

   Das Hauptfenster des Administratordienstprogramms für das IBM Sicherheits-Subsystem wird angezeigt.
3. Klicken Sie im Bereich "Zu autorisierende Windows-Benutzer auswählen" auf **Neuen Windows-Benutzer erstellen**.

   Die Anzeige "Windows-Benutzeraccounts" erscheint.
4. Klicken Sie auf **Einen neuen Account erstellen**.
5. Geben Sie in das entsprechende Feld einen Namen für den neuen Account ein. Klicken Sie anschließend auf **Weiter**.
6. Wählen Sie mit Hilfe des entsprechenden Radioknopfs einen Accounttyp aus.
7. Klicken Sie auf **Account erstellen**.
8. Kehren Sie zum Administratordienstprogramms für das IBM Sicherheits-Subsystem zurück.

   Der neue Benutzeraccount wird im Bereich "Zu autorisierende Windows-Benutzer auswählen" angezeigt.

Kapitel 6. Nach dem Autorisieren von Benutzern in UVM

Nach dem Autorisieren der Benutzer können Sie zusätzliche Client Security-Funktionen ausführen, wie z. B. folgende:

- **UVM-Anmeldeschutz für Windows konfigurieren.** Weitere Informationen hierzu finden Sie im Abschnitt „Hinweise zur Konfiguration des UVM-Anmeldeschutzes".
- **Benutzerchiffrierschlüssel archivieren.** Weitere Informationen hierzu finden Sie im Abschnitt „Position des Schlüsselarchivs ändern" auf Seite 50.
- **Client Security-Bildschirmschoner konfigurieren.** Weitere Informationen hierzu finden Sie in Kapitel 9, „Anweisungen für den Clientbenutzer", auf Seite 59.
- **Fingerabdrücke von Benutzern in UVM registrieren.** Weitere Informationen hierzu finden Sie im Abschnitt „Fingerabdrücke von Benutzern in UVM registrieren" auf Seite 37.

  Wenn vor dem Hinzufügen von Benutzern in UVM ein UVM-Sensor für Fingerabdrücke installiert wurde, können Sie die Fingerabdrücke registrieren.

UVM-Anmeldeschutz für Windows

Der UVM-Anmeldeschutz für Windows erweitert die Kennwortfunktion, die von Windows bereitgestellt wird. Die UVM-Anmeldeschnittstelle ersetzt die Windows-Anmeldung, so dass immer wenn sich ein Benutzer am System anmelden möchte, das UVM-Anmeldefenster angezeigt wird.

Hinweise zur Konfiguration des UVM-Anmeldeschutzes

Lesen Sie die folgenden Informationen, bevor Sie den UVM-Anmeldeschutz für die Windows-Anmeldung konfigurieren und verwenden:

- Wenn die UVM-Policy angibt, dass die Authentifizierung über Fingerabdrücke für die Windows-Anmeldung erforderlich ist, und wenn für den Benutzer keine Fingerabdrücke registriert sind, muss der Benutzer Fingerabdrücke registrieren, um sich anmelden zu können.

  Wenn das Windows-Kennwort des Benutzers nicht oder falsch in UVM registriert wurde, muss der Benutzer das richtige Windows-Kennwort eingeben, um sich anzumelden.
- Löschen Sie den Inhalt des integrierten IBM Security Chips nicht bei aktiviertem UVM-Schutz. Andernfalls haben Sie keinen Zugriff mehr auf das System. Weitere Informationen hierzu finden Sie im Abschnitt "Administratorfunktionen" in Kapitel 10, „Fehlerbehebung", auf Seite 65.
- Wenn Sie im Administratordienstprogramm das Markierungsfeld **Die Windows-Standardanmeldung durch eine gesicherte UVM-Anmeldung ersetzen** inaktivieren, kehrt das System zum Windows-Anmeldungsprozess zurück, ohne die gesicherte UVM-Anmeldung zu verwenden.
- Wenn Sie die Windows-Standardanmeldung durch die gesicherte UVM-Anmeldung ersetzen und die Cisco LEAP-Funktion aktivieren, müssen Sie das Cisco Aironet Client Utility (ACU) erneut installieren.

UVM-Anmeldeschutz konfigurieren

Gehen Sie wie folgt vor, um den UVM-Anmeldeschutz für Windows zu konfigurieren:

1. Klicken Sie auf dem Windows-Desktop des IBM Clients auf **Start > Einstellungen > Systemsteuerung > Integriertes IBM Sicherheits-Subsystem**.

   Das Hauptfenster des Administratordienstprogramms wird angezeigt.
2. Klicken Sie auf **Anwendungsunterstützung und Policies konfigurieren**.

   Die Anzeige "Konfiguration der UVM-Anwendungen und -Policies" erscheint.
3. Wählen Sie das Markierungsfeld **Die Windows-Standardanmeldung durch eine gesicherte UVM-Anmeldung ersetzen** aus.
4. Klicken Sie auf **OK**.
5. Klicken Sie auf **Verlassen**.
6. Schließen Sie alle Anwendungen.
7. Starten Sie den Computer erneut.

Wenn der Computer erneut gestartet wird, werden Sie aufgefordert, sich am Computer anzumelden. Weitere Informationen zum UVM-Schutz finden Sie im Abschnitt „UVM-Anmeldeschutz für Windows" auf Seite 35.

UVM-Verschlüsselungstext wiederherstellen

Ein UVM-Verschlüsselungstext wird für jeden Benutzer erstellt, der durch die Sicherheitspolicy für den IBM Client autorisiert ist. Da Verschlüsselungstexte verloren gehen, vergessen werden oder vom Clientbenutzer geändert werden können, kann der Administrator mit Hilfe des Administratordienstprogramms einen vergessenen oder verlorenen Verschlüsselungstext wiederherzustellen oder ändern.

Gehen Sie wie folgt vor, um die Wiederherstellungsprozedur für einen UVM-Verschlüsselungstext einzuleiten:

1. Klicken Sie auf dem Windows-Desktop des IBM Clients auf **Start > Einstellungen > Systemsteuerung > Integriertes IBM Sicherheits-Subsystem**.

   Das Hauptfenster des Administratordienstprogramms wird angezeigt.
2. Wählen Sie im Bereich "Für die Benutzung von UVM berechtigte Windows-Benutzer" einen Benutzer aus.
3. Klicken Sie auf **Verschlüsselungstext ändern**.

   Die Anzeige "Verschlüsselungstext ändern" erscheint.
4. Geben Sie den Pfad und den Verzeichnisnamen des Schlüsselarchives ein, oder klicken Sie auf **Durchsuchen**, um das Verzeichnis auszuwählen.
5. Geben Sie in das Feld "Datei mit privatem Archivschlüssel" den Pfad und den Dateinamen des privaten Administratorschlüssels ein, oder klicken Sie auf **Durchsuchen**, um nach der Datei zu suchen.
6. Klicken Sie auf **OK**.

   Wenn der private Administratorschlüssel in mehrere Dateien aufgeteilt wurde, werden Sie in einer Nachricht aufgefordert, die Position und den Namen der einzelnen Dateien einzugeben. Klicken Sie, nachdem Sie die einzelnen Dateinamen in das Feld "Schlüsseldatei" eingegeben haben, auf die Option **Weiter lesen**.

7. Geben Sie in das Feld ″UVM-Verschlüsselungstext″ den neuen UVM-Verschlüsselungstext für den Benutzer ein, und bestätigen Sie den Verschlüsselungstext im Feld ″Bestätigen Sie den UVM-Verschlüsselungstext″. Klicken Sie auf **Bedingungen für Verschlüsselungstext anzeigen**, um eine Liste mit Regeln anzuzeigen, die durch die UVM-Sicherheitspolicy aktiviert wurden.
8. Wählen Sie im Bereich ″Ablauf von Verschlüsselungstexten″ die verfügbaren Regeln für das Ablaufen von Verschlüsselungstexten aus, und legen Sie sie fest.
9. Klicken Sie auf **Weiter**. Es erscheint eine Nachricht, die anzeigt, dass der Vorgang erfolgreich ausgeführt wurde.
10. Klicken Sie auf **Fertig stellen**.

Fingerabdrücke von Benutzern in UVM registrieren

Wenn die UVM-Policy so bearbeitet wurde, dass sie die Authentifizierung über Fingerabdrücke umfasst, muss jeder Benutzer in UVM Fingerabdrücke registrieren.

Gehen im Administratordienstprogramm wie folgt vor, um Fingerabdrücke von Benutzern in UVM zu registrieren:

1. Wählen Sie im Bereich ″Für die Benutzung von UVM berechtigte Windows-Benutzer″ in der Liste einen Benutzernamen aus.
2. Klicken Sie auf **Benutzer bearbeiten**.

   Das Fenster ″Benutzerkonfiguration von Client Security ändern - UVM-Benutzerattribute bearbeiten″ wird angezeigt.
3. Wählen Sie das Markierungsfeld **Fingerabdruck und/oder Smartcard registrieren** aus, und klicken Sie auf **Weiter**.

   Das Fenster ″Benutzerkonfiguration von Client Security ändern- UVM-gesicherte Einheiten″ wird angezeigt.
4. Klicken Sie auf **Fingerabdruck des Benutzers registrieren**.
5. Klicken Sie im Bereich für die Hand auf **Links** oder **Rechts**.
6. Klicken Sie auf den Bereich zur Fingerauswahl, um den zu scannenden Finger auszuwählen, und klicken Sie auf **Registrierung starten**.
7. Legen Sie den Finger auf den UVM-Sensor für Fingerabdrücke, und befolgen Sie die angezeigten Anweisungen.

   Je nach Scannermodell müssen Sie möglicherweise den Fingerabdruck viermal scannen. Klicken Sie auf **Brechen Sie den Vorgang für diesen Finger ab**, wenn Sie die Scannerabtastung des Fingerabdrucks abbrechen möchten.
8. Geben Sie einen anderen zu registrierenden Finger an, oder klicken Sie auf **Verlassen**, um das Programm zu beenden.

UVM-Anmeldeschutz für Lotus Notes verwenden

UVM bietet erweiterte Sicherheitseinrichtungen für Lotus Notes-Benutzer.

UVM-Anmeldeschutz für eine Lotus Notes-Benutzer-ID aktivieren und konfigurieren

Bevor Sie den UVM-Anmeldeschutz für Lotus Notes aktivieren können, muss Lotus Notes auf dem IBM Client installiert, eine Notes-Benutzer-ID und ein Kennwort für den Benutzer festgelegt und der Lotus Notes-Benutzer zum Verwenden von UVM autorisiert werden.

Gehen Sie wie folgt vor, um den UVM-Anmeldeschutz für Lotus Notes einzurichten:

1. Klicken Sie auf dem Windows-Desktop des IBM Clients auf **Start > Einstellungen > Systemsteuerung > Integriertes IBM Sicherheits-Subsystem**.

   Das Hauptfenster des Administratordienstprogramms wird angezeigt.
2. Klicken Sie auf **Anwendungsunterstützung und Policies konfigurieren**.

   Die Anzeige ″Konfiguration der UVM-Anwendungen und -Policies″ wird angezeigt.
3. Wählen Sie das Markierungsfeld **Lotus Notes-Unterstützung aktivieren** aus.

   Der UVM-Schutz für die Lotus Notes-Benutzer-ID ist jetzt aktiviert. Falls erforderlich, fahren Sie mit den folgenden Schritten fort, um die Policy für die Lotus Notes-Anmeldung zu konfigurieren.
4. Klicken Sie auf **Anwendungspolicy**.

   Die Anzeige ″Policy-Konfiguration von Client Security ändern″ wird angezeigt.
5. Klicken Sie auf **Policy bearbeiten**.
6. Geben Sie das Administratorkennwort ein, und klicken Sie auf **OK**. Die Anzeige ″IBM UVM-Policy: Lotus Notes-Anmeldung″ erscheint.
7. Wählen Sie auf der Registerkarte ″Objektauswahl″ im Dropdown-Menü ″Aktion″ den Eintrag **Lotus Notes-Anmeldung** aus.
8. Wählen Sie auf der Registerkarte ″Authentifizierungselemente″ die Authentifizierungselemente aus, die für die Lotus Notes-Anmeldung erforderlich sein sollen.
9. Klicken Sie auf **Übernehmen**, um Ihre Auswahl zu speichern.

   Die Anzeige ″Privater Administratorschlüssel erforderlich″ erscheint.
10. Geben Sie entweder durch Eingabe des Pfadnamens in das entsprechende Feld oder durch Klicken auf **Durchsuchen** und Auswählen des entsprechenden Ordners die Position des privaten Schlüssels an.
11. Klicken Sie auf **OK**.

    In der Anzeige ″IBM User Verification Manager: Zusammenfassung für Policy″ wird eine Zusammenfassung der Objekte angezeigt, die über die lokale Client-Policy gesteuert werden.
12. Starten Sie Lotus Notes.

    Wenn Lotus Notes gestartet wird, ist die UVM-Kennwortregistrierung beendet.

UVM-Schutz innerhalb von Lotus Notes verwenden

Bevor Sie den UVM-Schutz für Lotus Notes verwenden können, müssen Sie die Schritte im Abschnitt „UVM-Schutz innerhalb von Lotus Notes konfigurieren" befolgen.

UVM-Schutz innerhalb von Lotus Notes konfigurieren

Gehen Sie wie folgt vor, um den UVM-Schutz innerhalb von Lotus Notes zu konfigurieren:

1. Melden Sie sich bei Lotus Notes an.

   Das Fenster "IBM User Verification Manager" wird angezeigt.
2. Geben Sie in die verfügbaren Felder das Lotus Notes-Kennwort ein, und bestätigen Sie es.

   Nun ist das Lotus Notes-Kennwort in UVM registriert.

Lotus Notes-Kennwort neu festlegen

Gehen Sie wie folgt vor, um das Lotus Notes-Kennwort neu festzulegen:

1. Melden Sie sich bei Lotus Notes an.
2. Klicken Sie in der Menüleiste von Lotus Notes auf **Datei > Extras > Benutzersicherheit**.

   Das Fenster "IBM User Verification Manager" wird angezeigt.
3. Geben Sie den UVM-Verschlüsselungstext ein, und klicken Sie auf **OK**.

   Das Fenster "Benutzersicherheit" wird angezeigt.
4. Klicken Sie auf **Kennwort festlegen**.

   Das Fenster "IBM User Verification Manager" wird angezeigt.
5. Wählen Sie den Radioknopf **Eigenes Kennwort erstellen** aus.
6. Geben Sie in die verfügbaren Felder das neue Lotus Notes-Kennwort ein, und bestätigen Sie es. Klicken Sie anschließend auf **OK**.

Anmerkung: Wenn Sie das Kennwort innerhalb von Lotus Notes in einen bereits verwendeten Wert ändern, lehnt Notes die Kennwortänderung ab, teilt dies jedoch Client Security nicht mit. Folglich speichert UVM das Kennwort, das von Notes abgelehnt wurde.

Wird beim Ändern des Kennworts in Lotus Notes eine Nachricht angezeigt, die besagt, dass das Kennwort bereits zuvor verwendet wurde, müssen Sie Lotus Notes verlassen, das Benutzerkonfigurationsprogramm starten und das alte Notes-Kennwort wiederherstellen.

Wenn das Lotus Notes-Kennwort per Zufallsgenerator festgelegt wurde und Sie diese Fehlernachricht erhalten, haben Sie keine Möglichkeit, das alte Kennwort festzustellen, und können daher das Kennwort nicht manuell zurücksetzen. Sie müssen von Ihrem Administrator eine neue ID-Datei anfordern oder eine früher gesicherte Kopie der ID-Datei wiederherstellen.

UVM-Anmeldeschutz für eine Lotus Notes-Benutzer-ID inaktivieren

Gehen Sie wie folgt vor, um den UVM-Anmeldeschutz für eine Lotus Notes-Benutzer-ID zu inaktivieren:

1. Klicken Sie auf dem Windows-Desktop des IBM Clients auf **Start > Einstellungen > Systemsteuerung > Integriertes IBM Sicherheits-Subsystem**.

   Nachdem Sie das Administratorkennwort eingegeben haben, wird das Hauptfenster des Administratordienstprogramms angezeigt.
2. Klicken Sie auf **Anwendungsunterstützung und Policies konfigurieren**.

   Die Anzeige ″Konfiguration der UVM-Anwendungen und -Policies″ erscheint.
3. Inaktivieren Sie das Markierungsfeld **Lotus Notes-Unterstützung aktivieren**.
4. Klicken Sie auf **OK**.

   In der Anzeige ″Operationen zur Anwendungsunterstützung″ wird eine Nachricht angezeigt, die besagt, dass die Lotus Notes-Unterstützung inaktiviert ist.

UVM-Schutz für eine gewechselte Lotus Notes-Benutzer-ID konfigurieren

Gehen Sie wie folgt vor, um von einer Benutzer-ID mit aktiviertem UVM-Schutz zu einer anderen Benutzer-ID zu wechseln:

1. Verlassen Sie Lotus Notes.
2. Inaktivieren Sie den UVM-Schutz für die aktuelle Benutzer-ID. Weitere Informationen hierzu finden Sie im Abschnitt „UVM-Anmeldeschutz für eine Lotus Notes-Benutzer-ID inaktivieren”.
3. Rufen Sie Lotus Notes auf, und wechseln Sie die Benutzer-IDs. Weitere Informationen zum Wechseln von Benutzer-IDs finden Sie in der Dokumentation zu Lotus Notes.
4. Zur Konfiguration des UVM-Schutzes für die Benutzer-ID, zu der Sie gewechselt sind, rufen Sie das Tool zur Lotus Notes-Konfiguration auf (von Client Security bereitgestellt) und konfigurieren den UVM-Schutz. Weitere Informationen hierzu finden Sie im Abschnitt „UVM-Schutz innerhalb von Lotus Notes verwenden” auf Seite 39.

PKCS #11-Modul des integrierten IBM Security Chips verwenden

Die Anweisungen in diesem Abschnitt gelten speziell für die Verwendung von Client Security im Zusammenhang mit dem Anfordern und Anwenden digitaler Zertifikate bei Anwendungen, die den Standard PKCS #11 unterstützen, wie z. B. eine Netscape-Anwendung oder ein RSA SecurID Software Token.

Weitere Informationen zur Verwendung der Sicherheitseinstellungen für Netscape-Anwendungen finden Sie in der Dokumentation zu Netscape. IBM Client Security unterstützt nur Netscape Version 4.7x.

Anmerkung: Wenn Sie 128-Bit-Browser mit Client Security verwenden möchten, muss der integrierte IBM Security Chip 256-Bit-Verschlüsselung unterstützen. Den Grad der Verschlüsselung durch Client Security können Sie im Administratordienstprogramm feststellen, indem Sie auf die Schaltfläche **Chipeinstellungen** klicken.

PKCS #11-Modul des integrierten IBM Security Chips installieren

Bevor Sie ein digitales Zertifikat verwenden können, müssen Sie das PKCS #11-Modul des integrierten IBM Security Chips im Computer installieren. Da die Installation des PKCS #11-Moduls des integrierten IBM Security Chips einen UVM-Verschlüsselungstext erfordert, müssen Sie in die Sicherheitspolicy für den Computer mindestens einen Benutzer aufnehmen.

Gehen Sie wie folgt vor, um mit Hilfe von Netscape das PKCS #11-Modul des integrierten IBM Security Chips zu installieren:

1. Öffnen Sie Netscape und klicken Sie auf **Datei > Seite öffnen**.
2. Suchen Sie die Installationsdatei `ibmpkcsinstallt.html` bzw. `ibmpkcsinstalls.html`.

   (Falls bei der Installation das Standardverzeichnis übernommen wurde, befindet sich die Datei im Verzeichnis C:\Program Files\IBM\Security.)
3. Öffnen Sie die Installationsdatei `ibmpkcsinstallt.html` bzw. `ibmpkcsinstalls.html` in Netscape.

   Es wird eine Nachricht mit der Frage angezeigt, ob das Sicherheitsmodul tatsächlich installiert werden soll.
4. Klicken Sie auf **OK**.

   Das Fenster "UVM-Verschlüsselungstext" wird geöffnet.
5. Geben Sie den UVM-Verschlüsselungstext ein, und klicken Sie auf **OK**.

   In einer Nachricht wird Ihnen mitgeteilt, dass das Modul installiert wurde.

Integriertes IBM Sicherheits-Subsystem zum Generieren eines digitalen Zertifikats auswählen

Bei der Erstellung des digitalen Zertifikats werden Sie aufgefordert, die Karte oder die Datenbank auszuwählen, in der Sie den Schlüssel generieren möchten. Wählen Sie **IBM Embedded Security Subsystem Enhanced CSP** aus.

Weitere Informationen zum Generieren von digitalen Zertifikaten und zu deren Verwendung mit Netscape finden Sie in der Dokumentation zu Netscape.

Schlüsselarchiv aktualisieren

Sichern Sie das digitale Zertifikat nach seiner Erstellung, indem Sie das Schlüsselarchiv aktualisieren. Das Schlüsselarchiv können Sie mit Hilfe des Benutzerkonfigurationsprogramms aktualisieren.

Digitales Zertifikat für PKCS #11-Modul verwenden

Verwenden Sie zur Anzeige, zur Auswahl und zur Verwendung digitaler Zertifikate die Sicherheitseinstellungen in den Anwendungen. In den Sicherheitseinstellungen für Netscape Messenger müssen Sie z. B. das Zertifikat auswählen, bevor Sie es für digitale Unterschriften oder für die Verschlüsselung von E-Mails verwenden können. Weitere Informationen hierzu finden Sie in der Dokumentation von Netscape.

Nach der Installation des PKCS #11-Moduls des integrierten IBM Security Chips fordert Sie UVM bei jeder Verwendung des digitalen Zertifikats auf, die Authentifizierungsbestimmungen zu erfüllen. Möglicherweise müssen Sie den UVM-Verschlüsselungstext eingeben, die Fingerabdrücke scannen oder beides, damit Sie die Authentifizierungsbestimmungen erfüllen. Die Authentifizierungsbestimmungen sind in der UVM-Policy für den Computer definiert.

Wenn Sie die in der UVM-Policy festgelegten Authentifizierungsbestimmungen nicht erfüllen, wird eine Fehlernachricht angezeigt. Wenn Sie bei dieser Nachricht auf **OK** klicken, wird die Anwendung geöffnet. Sie können jedoch das vom integrierten IBM Security Chip generierte digitale Zertifikat erst verwenden, wenn Sie die Anwendung erneut starten und den richtigen UVM-Verschlüsselungstext, die Fingerabdrücke oder beides angeben.

Kapitel 7. Mit der UVM-Policy arbeiten

Anmerkung: Bevor Sie die UVM-Policy für den lokalen Client bearbeiten, müssen Sie sicherstellen, dass Schlüssel erstellt wurden. Andernfalls erhalten Sie beim Öffnen der lokalen Policy-Datei mit dem Policy-Editor eine Fehlernachricht.

Nachdem Benutzer für die Verwendung von UVM autorisiert sind, müssen Sie für jeden IBM Client eine Sicherheitspolicy bearbeiten und speichern. Die von Client Security bereitgestellte Sicherheitspolicy wird als UVM-Policy bezeichnet und kombiniert die Einstellungen, die Sie im Abschnitt "Benutzer autorisieren" vorgenommen haben, mit den Authentifizierungsbestimmungen auf Clientebene. Eine UVM-Policy-Datei kann über ein Netzwerk auf die Clients kopiert werden.

Das Administratordienstprogramm weist einen integrierten UVM-Policy-Editor auf, mit dem Sie die UVM-Policy für einen Client bearbeiten und speichern können. Tasks, die Sie am IBM Client ausführen, wie z. B. die Windows-Anmeldung oder das Entsperren des Bildschirmschoners, werden als Authentifizierungsobjekte bezeichnet, und diesen Objekten müssen in der UVM-Policy Authentifizierungsbestimmungen zugeordnet sein. Sie können z. B. eine UVM-Policy definieren, in der die folgenden Anforderungen festgelegt sind:

- Jeder Benutzer muss einen UVM-Verschlüsselungstext eingeben und sich mit einem berührungslosen Ausweis (Proximity Badge) authentifizieren, um sich am Windows-Betriebssystem anmelden zu können.

  Anmerkung: Zur Authentifizierung über einen berührungslosen Ausweis ist es nicht erforderlich, eine UVM-Policy zu bearbeiten.
- Jedes Mal, wenn ein digitales Zertifikat angefordert wird, muss jeder Benutzer einen UVM-Verschlüsselungstext eingeben.

Sie können auch mit Tivoli Access Manager einzelne Authentifizierungsobjekte so steuern, wie diese in der UVM-Policy festgelegt sind.

In der UVM-Policy sind die Bestimmungen für Authentifizierungsobjekte für den IBM Client, jedoch nicht für die einzelnen Benutzer festgelegt. Wenn Sie also in der UVM-Policy festlegen, dass für ein Objekt (z. B. für eine Windows-Anmeldung) eine Authentifizierung über Fingerabdrücke erforderlich ist, muss sich jeder Benutzer, der für die Verwendung von UVM autorisiert wird, mit einem Fingerabdruck registrieren, um dieses Objekt verwenden zu können. Weitere Informationen zum Autorisieren eines Benutzers finden Sie im Abschnitt „Benutzer entfernen" auf Seite 33.

Die UVM-Policy wird in einer Datei mit dem Namen `globalpolicy.gvm` gespeichert. Zur Verwendung von UVM über ein Netzwerk muss die UVM-Policy auf einem IBM Client gespeichert und anschließend auf die anderen Clients kopiert werden. Durch Kopieren der UVM-Policy-Datei auf andere Clients können Sie Zeit sparen, wenn Sie diese UVM-Policy auf diesen Clients konfigurieren.

UVM-Policy bearbeiten

Sie bearbeiten eine UVM-Policy und verwenden diese nur auf dem Client, für den Sie sie bearbeitet haben. Wenn Sie Client Security an seiner Standardposition installiert haben, wird die UVM-Policy-Datei im Pfad \Program Files\IBM\Security \UVM_Policy\globalpolicy.gvm gespeichert. Mit dem UVM-Policy-Editor können Sie eine UVM-Policy-Datei bearbeiten und speichern. Die Schnittstelle für den UVM-Policy-Editor wird im Administratordienstprogramm bereitgestellt.

Die Authentifizierung richtet sich nach Ihrer Auswahl im Policy-Editor. Wenn Sie z. B. die Option "Nach erstem Gebrauch auf diese Weise ist kein Verschlüsselungstext erforderlich" für die Lotus Notes-Anmeldung auswählen, werden Sie bei jeder Anmeldung bei Lotus Notes zur UVM-Authentifizierung aufgefordert. Solange Sie danach den Computer nicht warmstarten oder sich vom Computer abmelden, müssen Sie anschließend zum erneuten Zugriff auf Lotus Notes keinen Verschlüsselungstext eingeben.

Wenn Sie in der UVM-Policy festlegen, dass für ein Authentifizierungsobjekt Fingerabdrücke erforderlich sind (z. B. für die Windows-Anmeldung), muss sich jeder von UVM autorisierte Benutzer mit einem Fingerabdruck registrieren, um dieses Objekt verwenden zu können.

Beim Bearbeiten einer UVM-Policy können Sie die Zusammenfassungsinformationen der Policy anzeigen, indem Sie auf die Option **UVM-Policy-Zusammenfassung** klicken. Darüber hinaus können auf **Übernehmen** klicken, um Ihre Änderungen zu speichern. Wenn Sie auf **Übernehmen** klicken, werden Sie in einer Nachricht aufgefordert, den privaten Administratorschlüssel einzugeben. Geben Sie den privaten Administratorschlüssel ein, und klicken Sie auf **OK**, um die Änderungen zu speichern. Wenn Sie einen falschen privaten Administratorschlüssel eingeben, werden die Änderungen nicht gespeichert.

Objektauswahl

Mit Hilfe von UVM-Policy-Objekten können Sie für verschiedene Benutzeraktionen unterschiedliche Sicherheitspolicies aktivieren. Gültige UVM-Objekte sind auf der Registerkarte **Objektauswahl** der Anzeige "IBM UVM-Policy" im Administratordienstprogramm angegeben.

Es gibt folgende gültige UVM-Policy-Objekte:

Systemanmeldung
Mit diesem Objekt wird die Authentifizierung gesteuert, die zum Anmelden am System erforderlich ist.

Entsperren des Systems
Mit diesem Objekt wird die Authentifizierung gesteuert, die zum Ausblenden des Client Security-Bildschirmschoners erforderlich ist.

Lotus Notes-Anmeldung
Mit diesem Objekt wird die Authentifizierung gesteuert, die zum Anmelden bei Lotus Notes erforderlich ist.

Anmeldekennwort für Lotus Notes
Mit diesem Objekt wird die Authentifizierung gesteuert, die für UVM zum Generieren eines per Zufallsgenerator festgelegten Lotus Notes-Kennworts erforderlich ist.

Digitale Unterschrift (E-Mail)
Mit diesem Objekt wird die Authentifizierung gesteuert, die beim Klicken auf die Schaltfläche zum Signieren in Microsoft Outlook oder in Outlook Express erforderlich ist.

Entschlüsselung (E-Mail)
Mit diesem Objekt wird die Authentifizierung gesteuert, die beim Klicken auf die Schaltfläche zum Entschlüsseln in Microsoft Outlook oder in Outlook Express erforderlich ist.

Schutz für Dateien und Ordner
Mit diesem Objekt wird die Authentifizierung gesteuert, die nach der Auswahl der Ver- und Entschlüsselung über die rechte Maustaste erforderlich ist.

Password Manager
Mit diesem Objekt wird die Authentifizierung gesteuert, die zum Verwenden des auf der IBM Website verfügbaren IBM Password Managers erforderlich ist. Wenn es aktiviert ist, sollten die meisten Benutzer die Einstellung ″Nach erstem Gebrauch auf diese Weise ist kein Verschlüsselungstext erforderlich″ beibehalten.

Netscape - PKCS #11-Anmeldung
Mit diesem Objekt wird die Authentifizierung gesteuert, die erforderlich ist, wenn vom PKCS #11-Modul der Aufruf ″PKCS#11 C_OpenSession″ empfangen wird. Die meisten Benutzer sollten die Einstellung “Nach erstem Gebrauch auf diese Weise ist kein Verschlüsselungstext erforderlich” beibehalten.

Entrust-Anmeldung
Mit diesem Objekt wird die Authentifizierung gesteuert, die erforderlich ist, wenn Entrust den Aufruf ″PKCS#11 C_OpenSession″ ausgibt, der vom PKCS #11-Modul empfangen werden soll. Die meisten Benutzer sollten die Einstellung “Nach erstem Gebrauch auf diese Weise ist kein Verschlüsselungstext erforderlich” beibehalten.

Entrust-Anmeldekennwort ändern
Mit diesem Objekt wird die Authentifizierung gesteuert, die zum Ändern des Entrust-Anmeldekennworts erforderlich ist. Dazu gibt Entrust den Aufruf ″PKCS#11 C_OpenSession″ aus, der vom PKCS #11-Modul empfangen werden soll. Die meisten Benutzer sollten die Einstellung “Nach erstem Gebrauch auf diese Weise ist kein Verschlüsselungstext erforderlich” beibehalten.

Authentifizierungselemente

Über die UVM-Policy wird festgelegt, welche verfügbaren Authentifizierungselemente für jedes aktivierte Objekt erforderlich sind. Auf diese Weise können Sie für verschiedene Benutzeraktionen unterschiedliche Sicherheitspolicies einrichten.

Auf der Registerkarte **Authentifizierungselemente** der Anzeige ″IBM UVM-Policy″ im Administratordienstprogramm können folgende Authentifizierungselemente ausgewählt werden:

Auswahl von Verschlüsselungstext
Über diese Auswahl kann ein Administrator den UVM-Verschlüsselungstext zur Authentifizierung eines Benutzers auf eine der drei folgenden Arten festlegen:

- Es ist immer ein neuer Verschlüsselungstext erforderlich.

- Nach erstem Gebrauch auf diese Weise ist kein Verschlüsselungstext erforderlich.
- Kein Verschlüsselungstext erforderlich, wenn Bereitstellung bei der Anmeldung am System erfolgt ist.

Fingerabdruck-Auswahl
Über diese Auswahl kann ein Administrator die Verwendung eines gescannten Fingerabdrucks zur Authentifizierung eines Benutzers auf eine der drei folgenden Arten festlegen:

- Es ist immer ein neuer Fingerabdruck erforderlich.
- Nach erstem Gebrauch auf diese Weise ist kein Fingerabdruck erforderlich.
- Kein Fingerabdruck erforderlich, wenn Bereitstellung bei der Anmeldung am System erfolgt ist.

Globale Einstellungen für Fingerabdrücke
Über diese Auswahl kann ein Administrator eine maximale Anzahl an Authentifizierungsversuchen festlegen, bis ein Benutzer vom System gesperrt wird. Über diesen Bereich kann der Administrator auch festlegen, dass der Schutz durch die Authentifizierung über Fingerabdrücke durch den UVM-Verschlüsselungstext außer Kraft gesetzt werden kann.

Smartcard-Auswahl
Über diese Auswahl kann ein Administrator festlegen, dass eine Smartcard als zusätzliche Authentifizierungseinheit erforderlich ist.

Globale Smartcard-Einstellungen
Über diese Auswahl kann ein Administrator die Policy so festlegen, dass Überschreibungen zugelassen werden, wenn der UVM-Verschlüsselungstext angegeben wird.

UVM-Policy-Editor verwenden

Führen Sie im Administratordienstprogramm die folgenden Schritte aus, um den UVM-Policy-Editor zu verwenden:

1. Klicken Sie auf die Schaltfläche **Anwendungsunterstützung und Policies konfigurieren**.

   Die Anzeige ″Konfiguration der UVM-Anwendungen und -Policies″ wird angezeigt.
2. Klicken Sie auf die Schaltfläche **Anwendungspolicy**.

   Die Anzeige ″Policy-Konfiguration von Client Security ändern″ wird angezeigt.
3. Klicken Sie auf die Schaltfläche **Policy bearbeiten**.

   Die Anzeige ″Administratorkennwort eingeben″ erscheint.
4. Geben Sie das Administratorkennwort ein, und klicken Sie auf **OK**.

   Die Anzeige ″IBM UVM-Policy″ erscheint.
5. Klicken Sie auf der Registerkarte ″Objektauswahl″ auf **Aktion** oder **Objekttyp**, und wählen Sie das Objekt aus, dem Authentifizierungsbestimmungen zugeordnet werden sollen.

   Zu den möglichen Aktionen gehören die Anmeldung am System, das Entsperren des Systems und die E-Mail-Entschlüsselung; ein Objekttyp ist z. B. ″Digitales Zertifikat anfordern″.

6. Führen Sie für jedes Objekt, das Sie auswählen, einen der folgenden Schritte aus:
   - Klicken Sie auf die Registerkarte **Authentifizierungselemente**, und bearbeiten Sie die Einstellungen für die verfügbaren Authentifizierungselemente, die Sie dem Objekt zuordnen möchten.
   - Zur Steuerung des ausgewählten Objekts über Tivoli Access Manager wählen Sie **Access Manager steuert ausgewähltes Objekt** aus. Wählen Sie diese Option nur aus, wenn Sie Tivoli Access Manager zum Steuern der Authentifizierungselemente für den IBM Client verwenden möchten. Weitere Informationen hierzu finden Sie im Handbuch *Client Security mit Tivoli Access Manager verwenden*.

     Wichtig: Wenn Sie Tivoli Access Manager zur Steuerung eines Objektes auswählen, übergeben Sie die Steuerung dem Tivoli Access Manager-Objektbereich. In diesem Fall müssen Sie Client Security erneut installieren, um die lokale Steuerung für dieses Objekt wiederherzustellen.
   - Wählen Sie **Keinen Zugriff auf ausgewähltes Objekt zulassen** aus, um den Zugriff für das von Ihnen ausgewählte Objekt zu verweigern.
7. Klicken Sie auf **OK**, um die Änderungen zu speichern und das Programm zu verlassen.

UVM-Policy bearbeiten und verwenden

Die UVM-Policy können Sie auf mehreren IBM Clients verwenden, indem Sie die UVM-Policy bearbeiten und speichern und anschließend die UVM-Policy-Datei auf andere IBM Clients kopieren. Wenn Sie Client Security an seiner Standardposition installieren, wird die UVM-Policy-Datei im Pfad \Program Files\IBM\Security\UVM_Policy\remote\globalpolicy.gvm gespeichert.

Kopieren Sie die folgenden Dateien auf andere ferne IBM Clients, die diese UVM-Policy verwenden:

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

Wenn Sie Client Security an seiner Standardposition installiert haben, lautet das Stammverzeichnis für den oben genannten Pfad \Program Files. Kopieren Sie beide Dateien in den Verzeichnispfad \IBM\Security\UVM_Policy\ auf den Clients.

Kapitel 8. Weitere Funktionen des Sicherheitsadministrators

Wenn Sie Client Security auf IBM Clients konfigurieren, verwenden Sie das Administratordienstprogramm, um den integrierten IBM Security Chip zu aktivieren, ein Kennwort für den IBM Security Chip festzulegen, Hardwareschlüssel zu generieren und die Sicherheitspoliy festzulegen. In diesem Abschnitt erhalten Sie Anweisungen zur Verwendung weiterer Funktionen des Administratordienstprogramms.

Gehen Sie wie folgt vor, um das Administratordienstprogramm zu öffnen:

1. Klicken Sie auf dem Windows-Desktop des IBM Clients auf **Start > Einstellungen > Systemsteuerung > Integriertes IBM Sicherheits-Subsystem**.

   Da der Zugriff auf das Administratordienstprogramm mit dem Administratorkennwort geschützt ist, werden Sie in einer Nachricht aufgefordert, das Administratorkennwort einzugeben. Dieses Kennwort muss genau acht Zeichen lang sein.
2. Geben Sie das Administratorkennwort ein, und klicken Sie auf **OK**.

Administratorkonsole verwenden

Über die Administratorkonsole von Client Security kann ein Sicherheitsadministrator administratorspezifische Tasks über Remotezugriff von seinem System aus ausführen.

Die Anwendung für die Administratorkonsole (console.exe) muss vom Verzeichnis `\program files\ibm\security` installiert und ausgeführt werden.

Die Administratorkonsole bietet einem Sicherheitsadministrator folgende Funktionen:

- **Authentifizierungselemente übergehen oder überschreiben.** Zu den Funktionen zum Übergehen und Überschreiben, die der Administrator durchführen kann, gehören die folgenden:
  - **UVM-Verschlüsselungstext übergehen.** Über diese Funktion kann der Administrator das Übergehen des UVM-Verschlüsselungstextes zulassen. Bei Verwendung dieser Funktion wird, zusammen mit einer Kennwortdatei, ein temporärer Verschlüsselungstext per Zufallsgenerator erstellt. Der Administrator schickt die Kennwortdatei an den Benutzer und übermittelt ihm dann das Kennwort auf einem anderen Weg. So ist die Sicherheit des neuen Verschlüsselungstextes gewährleistet.
  - **Kennwort zum Überschreiben des Fingerabdrucks/der Smartcard anzeigen/ändern.** Über diese Funktion kann der Administrator die Sicherheitspolicy auch dann außer Kraft setzen, wenn das Außerkraftsetzen von Verschlüsselungstexten für Fingerabdrücke oder Smartcard nicht erlaubt ist. Dies kann erforderlich werden, wenn das Lesegerät für Fingerabdrücke defekt oder die Smartcard nicht verfügbar ist. Der Administrator kann das Ersatzkennwort dem Benutzer mündlich mitteilen oder per E-Mail senden.
- **Auf Archivschlüsselinformationen zugreifen.** Der Administrator kann hier auf die folgenden Informationen zugreifen:
  - **Archivverzeichnis.** In diesem Feld kann der Administrator Archivschlüsselinformationen von einem fernen Standort aus suchen.

- **Position des öffentlichen Archivschlüssels.** In diesem Feld kann der Administrator den öffentlichen Administratorschlüssel suchen.
- **Position des privaten Archivschlüssels.** In diesem Feld kann der Administrator den privaten Administratorschlüssel suchen.

- **Andere Administratorfunktionen, die von einem fernen Standort aus durchgeführt werden können.** Über die Administratorkonsole kann der Sicherheitsadministrator von einem fernen Standort aus die folgenden Funktionen ausführen:
  - **Administratorkonfigurationsdatei erstellen.** Über diese Funktion kann der Administrator die Administratorkonfigurationsdatei generieren. Diese Datei wird benötigt, wenn ein Benutzer seinen Eintrag mit Hilfe des Clientdienstprogramms registrieren oder zurücksetzen möchte. Diese Datei wird vom Administrator in der Regel per E-Mail an den Benutzer gesendet.
  - **Konfigurationsdatei für Installationsprogramm verschlüsseln/entschlüsseln.** Über diese Funktion wird die Verschlüsselung der Konfigurationsdatei für das Installationsprogramm aktiviert und so zusätzliche Sicherheit gewährleistet. Mit dieser Funktion kann die Datei auch zur Bearbeitung entschlüsselt werden.
  - **Standortunabhängigen Zugriff mit Berechtigungsnachweis konfigurieren.** Über diese Funktion wird dieses System als CSS-Roaming-Server registriert. Nach der Registrierung können alle von UVM autorisierten Benutzer im Netzwerk auf ihre persönlichen Daten (Verschlüsselungstexte, Zertifikat, usw.) auf diesem System zugreifen.

Position des Schlüsselarchivs ändern

Wenn das Schlüsselarchiv zum ersten Mal erstellt wird, werden von allen Chiffrierschlüsseln Kopien erstellt und an der Position gespeichert, die bei der Installation angegeben wurde.

Anmerkung: Der Clientbenutzer kann auch die Position des Schlüsselarchivs mit dem Benutzerkonfigurationsprogramm ändern. Weitere Informationen hierzu finden Sie in Kapitel 9, „Anweisungen für den Clientbenutzer", auf Seite 59.

Gehen Sie im Administratordienstprogramm wie folgt vor, um die Position des Schlüsselarchivs zu ändern:

1. Klicken Sie auf die Schaltfläche **Schlüsselkonfiguration**. Die Anzeige "Schlüsselkonfiguration von Client Security ändern - Schlüssel konfigurieren" erscheint.
2. Klicken Sie auf den Radioknopf **Archivposition ändern** und anschließend auf **Weiter**. Die Anzeige "Schlüsselkonfiguration von Client Security ändern - Neue Position des Schlüsselarchivs" erscheint.
3. Geben Sie den neuen Pfad ein, oder klicken Sie auf **Durchsuchen**, um den Pfad auszuwählen.
4. Klicken Sie auf **OK**. Es erscheint eine Nachricht, die anzeigt, dass der Vorgang ausgeführt wurde.
5. Klicken Sie auf **Fertig stellen**.

Archivschlüsselpaar ändern

Wenn Sie die Administratorschlüssel in einer Archivposition speichern, werden die kopierten Schlüssel als Archivschlüsselpaar bezeichnet. Diese Schlüssel werden in der Regel auf einer Diskette oder in einem Netzwerkverzeichnis gespeichert.

Anmerkung: Aktualisieren Sie das Archiv unbedingt, bevor Sie das Archivschlüsselpaar ändern.

Gehen Sie im Administratordienstprogramm wie folgt vor, um die das Archivschlüsselpaar zu ändern:

1. Klicken Sie auf die Schaltfläche **Schlüsselkonfiguration**. Die Anzeige "Schlüsselkonfiguration von Client Security ändern - Schlüssel konfigurieren" wird angezeigt.
2. Klicken Sie auf den Radioknopf **Archivschlüssel ändern**, und klicken Sie anschließend auf **Weiter**. Die Anzeige "Schlüsselkonfiguration ändern - öffentlicher Schlüssel" wird angezeigt.
3. Geben Sie im Bereich "Neue Archivschlüssel" den Dateinamen für den neuen öffentlichen Archivschlüssel in das Feld "Öffentlicher Archivschlüssel" ein. Sie können auch auf **Durchsuchen** klicken, um nach der neuen Datei zu suchen, oder Sie können durch Klicken auf **Erstellen** einen neuen öffentlichen Archivschlüssel generieren.

   Anmerkung: Achten Sie darauf, dass Sie den neuen öffentlichen Schlüssel an einer anderen Position als die alten Archivschlüsseldateien erstellen.
4. Geben Sie im Bereich "Neue Archivschlüssel" den Dateinamen für den neuen privaten Archivschlüssel in das Feld "Privater Archivschlüssel" ein. Sie können auch auf **Durchsuchen** klicken, um die neue Datei zu suchen, oder Sie können durch Klicken auf **Erstellen** ein neues Archivschlüsselpaar generieren.

   Anmerkung: Achten Sie darauf, dass Sie das neue Schlüsselpaar an einer anderen Position als die alten Archivschlüsseldateien erstellen.
5. Geben Sie im Bereich "Alte Archivschlüssel" den Dateinamen für den alten öffentlichen Archivschlüssel im Feld "Öffentlicher Archivschlüssel" ein, oder klicken Sie auf **Durchsuchen**, um nach der Datei zu suchen.
6. Geben Sie im Bereich "Alte Archivschlüssel" den Dateinamen für den alten privaten Archivschlüssel im Feld "Privater Archivschlüssel" ein, oder klicken Sie auf **Durchsuchen**, um nach der Datei zu suchen.
7. Geben Sie im Bereich "Archivposition" den Dateipfad ein, in dem das Schlüsselarchiv gespeichert ist, oder klicken Sie auf **Durchsuchen**, um den Pfad auszuwählen.
8. Klicken Sie auf **Weiter**.

   Anmerkung: Wenn das Archivschlüsselpaar in mehrere Dateien aufgeteilt wurde, werden Sie in einer Nachricht aufgefordert, die Position und den Namen der einzelnen Dateien einzugeben. Klicken Sie auf die Option **Weiter lesen**, nachdem Sie die einzelnen Dateinamen in das Feld eingegeben haben.

   Es erscheint eine Nachricht, die anzeigt, dass der Vorgang erfolgreich ausgeführt wurde.
9. Klicken Sie auf **OK**. Es erscheint eine Nachricht, die anzeigt, dass der Vorgang ausgeführt wurde.
10. Klicken Sie auf **Fertig stellen**.

Schlüssel aus dem Archiv wiederherstellen

Sie müssen die Schlüssel wiederherstellen, wenn Sie eine Systemplatine austauschen oder wenn infolge eines Ausfalls des Festplattenlaufwerks die Integrität der Benutzerschlüssel beeinträchtigt ist. Bei der Wiederherstellung von Schlüsseln kopieren Sie die neuesten Schlüsseldateien für Benutzer aus dem Schlüsselarchiv und speichern diese im integrierten IBM Sicherheits-Subsystem (IBM Embedded Security Subsystem, ESS). Beim Wiederherstellen der Schlüssel werden alle derzeit im Security Chip gespeicherten Schlüssel überschrieben.

Wenn Sie die ursprüngliche Systemplatine im Computer durch eine neue Systemplatine mit dem integrierten IBM Sicherheits-Subsystem ersetzen und die Chiffrierschlüssel auf dem Festplattenlaufwerk weiterhin gültig bleiben, können Sie die Chiffrierschlüssel, die zuvor dem Computer zugeordnet waren, wiederherstellen, indem Sie diese mit dem integrierten IBM Sicherheits-Subsystem auf der neuen Systemplatine erneut verschlüsseln. *Nachdem* Sie den neuen Chip aktiviert und ein Administratorkennwort festgelegt haben, können Sie einen Schlüssel wiederherstellen.

Weitere Informationen zum Aktivieren des neuen Sicherheits-Subsystems und zum Festlegen eines Administratorkennworts finden Sie im Abschnitt „Integriertes IBM Sicherheits-Subsystem aktivieren und ein Administratorkennwort festlegen" auf Seite 57.

Anmerkung: Nach einer Schlüsselwiederherstellung wird die UVM-Anmeldung automatisch aktiviert. Wenn also für die UVM-Anmeldung auf dem System, das wiederhergestellt wird, die Authentifizierung über Fingerabdrücke erforderlich war, *müssen* Sie die Software zum Lesen von Fingerabdrücken installieren, *bevor* Sie nach einer Wiederherstellung das System erneut starten, damit Sie nicht vom System gesperrt werden.

In den folgenden Anweisungen wird davon ausgegangen, dass das Administratordienstprogramm nicht durch einen Ausfall des Festplattenlaufwerks beschädigt worden ist. Sollte ein Ausfall des Festplattenlaufwerks zur Beschädigung der Client Security-Dateien geführt haben, müssen Sie Client Security möglicherweise erneut installieren.

Voraussetzungen für Schlüsselwiederherstellung

Operationen zur Schlüsselwiederherstellung können nur unter folgenden Bedingungen erfolgreich durchgeführt werden:

- Der Name des wiederhergestellten Systemcomputers muss mit dem ursprünglichen Namen des Systemcomputers übereinstimmen.
- Das wiederhergestellte System muss auf das CSS-Administratorschlüsselpaar und auf die Archivposition des ursprünglichen Systems zugreifen können.
- Auf dem wiederhergestellten System muss sich ein gelöschtes und aktiviertes IBM Sicherheits-Subsystem befinden. (Aktivieren und löschen Sie den Chip mit Hilfe des BIOS.)
- Auf dem wiederhergestellten System muss sich dieselbe Version des IBM Sicherheits-Subsystems befinden wie auf dem ursprünglichen System (d. h. TCPA oder ein anderes System).

Wiederherstellungsszenarios

Die folgenden drei Szenarios bei der Wiederherstellung von IBM Client Security sind möglich:

- **Austausch der Systemplatine.** Ist ein Austausch der ursprünglichen Systemplatine erforderlich oder soll das Festplattenlaufwerk auf ein neues System versetzt werden, muss das IBM Sicherheits-Subsystem aus dem Schlüsselarchiv mit den Schlüsseln, die mit dem ursprünglichen System übereinstimmen, neu eingerichtet werden.
- **Austausch des gesamten Systems.** Geht das ursprüngliche System verloren oder wird es gestohlen, müssen sowohl das IBM Sicherheits-Subsystem als auch IBM Client Security aus den in der Archivposition gespeicherten Daten neu eingerichtet werden.
- **Austausch des Festplattenlaufwerks.** Wenn das Festplattenlaufwerk auf dem ursprünglichen System ausfällt und ein neues Festplattenlaufwerk im ursprünglichen System installiert wird, muss IBM Client Security aus der Archivposition wiederhergestellt werden.

Austausch der Systemplatine

Gehen Sie wie folgt vor, um die Systemplatine eines Computers auszutauschen, die ein aktiviertes integriertes IBM Sicherheits-Subsystem enthält:

1. Klicken Sie auf das Symbol **Subsystem von IBM Client Security** in der Windows-Systemsteuerung.
2. Geben Sie das Administratorkennwort ein, und bestätigen Sie es; klicken Sie anschließend auf **OK**.
3. Geben Sie die Archivposition und die Position des Administratorschlüssels des ursprünglichen Systems in den entsprechenden Feldern ein; klicken Sie anschließend auf **OK**.
4. Klicken Sie auf **OK**.
5. Klicken Sie auf **Verlassen**, um das Administratordienstprogramm zu schließen.

   Der Computer ist jetzt vollständig wiederhergestellt. Führen Sie einen Warmstart des Computers durch, bevor Sie fortfahren.

Austausch des gesamten Systems

Nach der Installation von IBM Client Security auf einem neuen System wird der CSS-Installationsassistent beim erneuten Starten des Systems automatisch ausgeführt. Gehen Sie wie folgt vor, um einen Austausch des gesamten Systems einzuleiten und um die in der Archivposition gespeicherten Daten wiederherzustellen:

1. Klicken Sie auf der Anfangsseite des CSS-Installationsassistenten auf **Weiter**.
2. Geben Sie das Administratorkennwort für das neue System ein, und bestätigen Sie es; klicken Sie anschließend auf **Weiter**.
3. Wählen Sie den Radioknopf **Einen vorhandenen Sicherheitsschlüssel verwenden** aus, und geben Sie die Position des archivierten öffentlichen Administratorschlüssels des ursprünglichen Systems in den entsprechenden Feldern ein.
4. Geben Sie im Bereich "Backup-Version der Sicherheitsdaten" eine temporäre Archivposition ein.

   Anmerkungen:

   a. Löschen Sie diese Position, nachdem das System in einem späteren Schritt aus dem Archiv des ursprünglichen Systems vollständig wiederhergestellt wurde.

b. Die restlichen Daten werden während der Wiederherstellung des Archivs des ursprünglichen Systems überschrieben. Verwenden Sie daher die Standardwerte.

5. Klicken Sie auf **Weiter**.
6. Klicken Sie auf der Seite "Anwendungen mit IBM Client Security schützen" auf **Weiter**.
7. Klicken Sie auf der Seite "Benutzer autorisieren" auf **Weiter**.
8. Klicken Sie auf der Seite "System Security-Stufe auswählen" auf **Weiter**.
9. Klicken Sie auf der Seite "Sicherheitseinstellungen prüfen" auf **Fertig stellen**.
10. Klicken Sie auf **OK**.
11. Fahren Sie fort, indem Sie die Prozedur „Austausch des Festplattenlaufwerks" ausführen.

Austausch des Festplattenlaufwerks

Gehen Sie wie folgt vor, um IBM Client Security nach dem Austausch eines Festplattenlaufwerks aus der Archivposition wiederherzustellen:

1. Klicken Sie in der Windows-Systemsteuerung auf das Symbol **Subsystem von IBM Client Security**.
2. Geben Sie das Administratorkennwort, das mit dem CSS-Installationsassistenten erstellt wurde, ein, und klicken Sie auf **OK**.
3. Klicken Sie auf **Schlüsselkonfiguration**.
4. Wählen Sie den Radioknopf **Schlüssel des IBM Sicherheits-Subsystems aus dem Archiv wiederherstellen** aus, und klicken Sie auf **Weiter**.
5. Geben Sie die Archivposition und die Positionen des Administratorschlüssels des ursprünglichen Systems in den entsprechenden Feldern ein, und klicken sie auf **Weiter**.
6. Klicken Sie auf **OK**.
7. Klicken Sie auf **Fertig stellen**, um zu der Hauptkonfigurationsseite zurückzukehren.
8. Klicken Sie auf **Verlassen**, um das Administratordienstprogramm zu schließen.

   Der Computer ist jetzt vollständig wiederhergestellt. Starten Sie den Computer erneut, bevor Sie fortfahren.

Zähler für fehlgeschlagene Authentifizierungsversuche zurücksetzen

Gehen Sie im Administratordienstprogramm wie folgt vor, um für einen Benutzer den Zähler für fehlgeschlagene Authentifizierungsversuche zurückzusetzen:

1. Wählen Sie im Bereich "Für die Benutzung von UVM berechtigte Windows-Benutzer" einen Benutzer aus.
2. Klicken Sie auf **Zähler für fehlgeschlagene Versuche zurücksetzen**.

   Die Anzeige "Zähler für fehlgeschlagene Versuche für BENUTZERNAME zurücksetzen" wird angezeigt.
3. Geben Sie für den ausgewählten Benutzer den UVM-Verschlüsselungstext ein, und klicken Sie auf **OK**.

   In einer Nachricht wird Ihnen mitgeteilt, dass der Vorgang erfolgreich ausgeführt wurde.
4. Klicken Sie auf **OK**.

Tivoli Access Manager-Einstellungsinformationen ändern

Die folgenden Informationen sind für Sicherheitsadministratoren vorgesehen, die Tivoli Access Manager zur Verwaltung von Authentifizierungsobjekten für die UVM-Sicherheitspolicy verwenden möchten. Weitere Informationen hierzu finden Sie im Handbuch *Client Security mit Tivoli Access Manager verwenden*.

Informationen zur Konfiguration von Tivoli Access Manager auf einem Client angeben

Nach dem Installieren von Tivoli Access Manager auf dem lokalen Client können Sie die Informationen zur Konfiguration von Tivoli Access Manager mit dem Administratordienstprogramm angeben. Für die Konfiguration von Tivoli Access Manager auf dem IBM Client verwendet Client Security eine Konfigurationsdatei. Über diese Konfigurationsdatei wird Tivoli Access Manager mit den Objekten verknüpft, an die die UVM-Policy die Steuerung übergibt.

Gehen Sie im Administratordienstprogramm wie folgt vor, um die Informationen zur Konfiguration von Tivoli Access Manager auf dem IBM Client anzugeben:

1. Klicken Sie auf die Schaltfläche **Anwendungsunterstützung und Policies konfigurieren**.

   Die Anzeige ″Konfiguration der UVM-Anwendungen und -Policies″ wird angezeigt.
2. Wählen Sie das Markierungsfeld **Die Windows-Standardanmeldung durch eine gesicherte UVM-Anmeldung ersetzen** aus.
3. Klicken Sie auf die Schaltfläche **Anwendungspolicy**. Die Anzeige ″Policy-Konfiguration von Client Security ändern″ wird angezeigt.
4. Wählen Sie im Bereich ″Informationen zur Konfiguration von Tivoli Access Manager″ den vollständigen Pfad zu der Konfigurationsdatei `TAMCSS.conf` aus. (z. B. `C:\TAMCSS\TAMCSS.conf`.) Tivoli Access Manager muss auf dem Client installiert sein, damit dieser Bereich verfügbar ist. Sie können auch auf **Durchsuchen** klicken, um nach der Konfigurationsdatei zu suchen.
5. Klicken Sie auf die Schaltfläche **Policy bearbeiten**, und geben Sie das Administratorkennwort ein.
6. Wählen Sie die Aktionen, die Tivoli Access Manager steuern soll, aus dem Dropdown-Menü ″Aktionen″ aus.
7. Wählen Sie das Markierungsfeld **Access Manager steuert ausgewähltes Objekt** aus, so dass ein Markierungszeichen im Feld angezeigt wird.
8. Klicken Sie auf die Schaltfläche **Übernehmen**. Die Änderungen werden bei der nächsten Cache-Aktualisierung wirksam. Wenn Sie möchten, dass die Änderungen sofort wirksam werden, klicken Sie auf die Schaltfläche **Lokalen Cache aktualisieren** in der Anzeige ″Policy-Konfiguration von Client Security ändern″.

Lokalen Cache aktualisieren

Auf dem IBM Client wird ein lokales Replikat der von Tivoli Access Manager verwalteten Sicherheitspolicy-Informationen verwaltet. Sie können die Aktualisierungsfrequenz des lokalen Caches in Inkrementen von einem Monat oder einem Tag festlegen oder durch Klicken auf eine Schaltfläche den lokalen Cache sofort aktualisieren.

Gehen Sie im Administratordienstprogramm wie folgt vor, um den lokalen Cache einzustellen oder zu aktualisieren:

1. Klicken Sie auf die Schaltfläche **Anwendungsunterstützung und Policies konfigurieren**.

   Die Anzeige ″Konfiguration der UVM-Anwendungen und -Policies″ erscheint.
2. Klicken Sie auf die Schaltfläche **Anwendungspolicy**. Die Anzeige ″Policy-Konfiguration von Client Security ändern″ erscheint.
3. Führen Sie im Bereich ″Aktualisierungsintervall für lokalen Cache″ einen der folgenden Schritte aus:
   - Klicken Sie auf **Lokalen Cache aktualisieren**, um den lokalen Cache jetzt zu aktualisieren.
   - Geben Sie zum Festlegen der Aktualisierungsfrequenz die Anzahl der Monate und Tage in die angezeigten Felder ein. Der Wert für die Monate und Tage gibt die Zeitspanne zwischen den geplanten Aktualisierungen an.

Administratorkennwort ändern

Sie müssen ein Administratorkennwort festlegen, um das integrierte IBM Sicherheits-Subsystem für einen Client zu aktivieren. Nachdem Sie ein Administratorkennwort festgelegt haben, ist der Zugriff auf das Administratordienstprogramm durch dieses Kennwort geschützt. Sie können die Sicherheit erhöhen, indem Sie das Administratorkennwort regelmäßig ändern. Wenn ein Kennwort längere Zeit gleich bleibt, ist es in geringerem Maße gegen unberechtigten Zugriff von außen geschützt. Schützen Sie das Administratorkennwort, um zu verhindern, dass Benutzer ohne Berechtigung Einstellungen im Administratordienstprogramm ändern können. Informationen zu den Regeln für das Administratorkennwort finden Sie in Anhang A, „Informationen zu Kennwörtern und Verschlüsselungstexten”, auf Seite 91.

Gehen Sie im Administratordienstprogramm wie folgt vor, um das Administratorkennwort zu ändern:

1. Klicken Sie auf die Schaltfläche **Chipeinstellungen**.

   Die Anzeige ″Einstellungen für IBM Security Chip ändern″ wird angezeigt.
2. Klicken Sie auf **Kennwort für Chip ändern**.

   Die Anzeige ″Kennwort für IBM Security Chip ändern″ wird angezeigt.
3. Geben Sie in das Feld ″Neues Kennwort″ das neue Kennwort ein.
4. Geben Sie das Kennwort in das Feld ″Bestätigung″ erneut ein.
5. Klicken Sie auf **OK**.

   In einer Nachricht wird Ihnen mitgeteilt, dass der Vorgang erfolgreich ausgeführt wurde.

   Achtung: Drücken Sie weder die Eingabetaste noch Tabulatortaste > Eingabetaste, um die Änderungen zu speichern. Andernfalls erscheint die Anzeige ″Chip inaktivieren″. Wenn das Fenster ″Chip inaktivieren″ geöffnet wird, inaktivieren Sie den Chip nicht, sondern schließen Sie das Fenster.
6. Klicken Sie auf **OK**.

Informationen zu Client Security anzeigen

Die folgenden Informationen zum integrierten IBM Sicherheits-Subsystem und Client Security werden angezeigt, indem Sie auf die Schaltfläche **Chipeinstellungen** klicken:

- Versionsnummer der Firmware, die mit Client Security verwendet wird
- Verschlüsselungsstatus des integrierten Security Chips
- Gültigkeit der Chiffrierschlüssel für die Hardware
- Status des integrierten IBM Security Chips

Integriertes IBM Sicherheits-Subsystem inaktivieren

Im Administratordienstprogramm gibt es eine Möglichkeit, das integrierte IBM Sicherheits-Subsystem zu inaktivieren. Da das Administratorkennwort erforderlich ist, um das Administratordienstprogramm zu starten und das Sicherheits-Subsystem zu inaktivieren, müssen Sie das Administratorkennwort schützen, um zu verhindern, dass unberechtigte Benutzer das Subsystem inaktivieren.

Wichtig: Löschen Sie bei aktivierten UVM-Schutz den Inhalt des integrierten IBM Sicherheits-Subsystems nicht. Andernfalls haben Sie keinen Zugriff mehr auf das System. Den UVM-Schutz können Sie entfernen, indem Sie das Administratordienstprogramm öffnen und das Markierungsfeld **Die Windows-Standardanmeldung durch eine gesicherte UVM-Anmeldung ersetzen** inaktivieren. Sie müssen den Computer erneut starten, damit der UVM-Schutz für die Anmeldung am System inaktiviert wird.

Gehen Sie im Administratordienstprogramm wie folgt vor, um das integrierte Sicherheits-Subsystem zu inaktivieren:

1. Klicken Sie auf die Schaltfläche **Chipeinstellungen**.
2. Klicken Sie auf die Schaltfläche **Chip inaktivieren**, und befolgen Sie die angezeigten Anweisungen.
3. Wenn für den Computer erweiterte Sicherheitseinrichtungen aktiviert sind, müssen Sie möglicherweise das BIOS-Administratorkennwort eingeben, das mit dem Programm "Configuration/Setup Utility" zum Inaktivieren des Chips festgelegt wurde.

Um das integrierte IBM Sicherheits-Subsystem und die Chiffrierschlüssel nach der Inaktivierung des Subsystems verwenden zu können, muss das Sicherheits-Subsystem erneut aktiviert werden.

Integriertes IBM Sicherheits-Subsystem aktivieren und ein Administratorkennwort festlegen

Wenn Sie nach der Softwareinstallation das integrierte IBM Sicherheits-Subsystem aktivieren müssen, können Sie mit Hilfe des Administratordienstprogramms das Administratorkennwort zurücksetzen und neue Chiffrierschlüssel konfigurieren.

Möglicherweise müssen Sie das integrierte IBM Sicherheits-Subsystem aktivieren, um das Schlüsselarchiv nach einem Austausch der Systemplatine oder nach der Inaktivierung des Subsystems wiederherzustellen.

Gehen Sie wie folgt vor, um das Sicherheits-Subsystem zu aktivieren und ein Administratorkennwort festzulegen:

1. Klicken Sie auf dem Windows-Desktop des IBM Clients auf **Start > Einstellungen > Systemsteuerung > Integriertes IBM Sicherheits-Subsystem**.

   In einer Nachricht werden Sie aufgefordert, das integrierte IBM Sicherheits-Subsystem für den IBM Client zu aktivieren.
2. Klicken Sie auf **Ja**.

   In einer Nachricht werden Sie aufgefordert, den Computer erneut zu starten. Sie müssen den Computer erneut starten, damit das integrierte IBM Sicherheits-Subsystem aktiviert wird. Wenn für den Computer erweiterte Sicherheitseinrichtungen aktiviert sind, müssen Sie möglicherweise das BIOS-Administratorkennwort eingeben, das mit dem Programm "Configuration/Setup Utility" zum Aktivieren des Chips festgelegt wurde.
3. Klicken Sie auf **OK**, um den Computer erneut zu starten.
4. Klicken Sie auf dem Windows-Desktop auf **Start > Einstellungen > Systemsteuerung > Integriertes IBM Sicherheits-Subsystem**.

   Da der Zugriff auf das Administratordienstprogramm mit dem Administratorkennwort geschützt ist, werden Sie in einer Nachricht aufgefordert, das Administratorkennwort einzugeben.
5. Geben Sie in das Feld "Neues Kennwort" ein neues Administratorkennwort ein; geben Sie es anschließend in das Feld "Bestätigung" erneut ein.
6. Klicken Sie auf **OK**.

Unterstützung für Entrust aktivieren

Der integrierte IBM Security Chip arbeitet mit Client Security zusammen, so dass die Sicherheitseinrichtungen von Entrust erweitert werden. Wenn Sie die Unterstützung für Entrust auf einem Computer mit Client Security aktivieren, werden die Sicherheitsfunktionen von Entrust auf den IBM Security Chip übertragen.

Client Security findet automatisch die Datei "entrust.ini", um die Unterstützung für Entrust zu aktivieren. Wenn sich jedoch die Datei "entrust.ini" nicht im normalen Pfad befindet, wird ein Dialogfenster geöffnet, in dem der Benutzer nach der Datei "entrust.ini" suchen kann. Sobald der Benutzer die Datei gefunden und ausgewählt hat, kann Client Security die Unterstützung für Entrust aktivieren. Nach Auswahl des Markierungsfelds **Entrust-Unterstützung aktivieren** ist ein Warmstart erforderlich, damit Entrust den integrierten IBM Security Chip verwenden kann.

Gehen Sie wie folgt vor, um die Entrust-Unterstützung zu aktivieren:

1. Klicken Sie auf dem Windows-Desktop des IBM Clients auf **Start > Einstellungen > Systemsteuerung > Integriertes IBM Sicherheits-Subsystem**.

   Das Hauptfenster des Administratordienstprogramms wird angezeigt.
2. Klicken Sie auf **Anwendungsunterstützung und Policies konfigurieren**.

   Die Anzeige "Konfiguration der UVM-Anwendungen und -Policies" erscheint.
3. Wählen Sie das Markierungsfeld **Entrust-Unterstützung aktivieren** aus.
4. Klicken Sie auf **Übernehmen**.

   In der Anzeige "Entrust-Unterstützung von IBM Client Security" wird eine Nachricht darüber ausgegeben, dass die Entrust-Unterstützung aktiviert ist.

Anmerkung: Sie müssen den Computer erneut starten, damit die Änderungen wirksam werden.

Kapitel 9. Anweisungen für den Clientbenutzer

Hier finden Sie Informationen zu den folgenden Tätigkeiten von Clientbenutzern:

- UVM-Schutz für die Anmeldung am System verwenden
- Benutzerkonfigurationsprogramm verwenden
- E-Mails sicher versenden und im World Wide Web sicher navigieren
- Einstellungen für UVM-Signaltöne konfigurieren

UVM-Schutz für die Anmeldung am System verwenden

In diesem Abschnitt finden Sie Informationen zur Verwendung der gesicherten UVM-Anmeldung für die Anmeldung am System. Bevor Sie den UVM-Schutz verwenden können, muss dieser für den Computer aktiviert sein.

Mit dem UVM-Schutz können Sie den Zugriff auf das Betriebssystem über eine Anmeldeschnittstelle steuern. Die gesicherte UVM-Anmeldung ersetzt die Anmeldeanwendung von Windows, so dass sich beim Entsperren des Computers durch einen Benutzer statt des Windows-Anmeldefensters das UVM-Anmeldefenster öffnet. Wenn der UVM-Schutz für den Computer aktiviert ist, wird die UVM-Anmeldeschnittstelle beim Start des Computers aufgerufen.

Während das System aktiv ist, können Sie die UVM-Anmeldeschnittstelle mit der Tastenkombination **Strg+Alt+Entf** aufrufen, um damit den Computer herunterzufahren, zu sperren, den Task-Manager zu öffnen oder den aktuellen Benutzer abzumelden.

Client entsperren

Einen Windows-Client mit aktiviertem UVM-Schutz können Sie folgendermaßen entsperren:

1. Drücken Sie die Tastenkombination **Strg+Alt+Entf**, um auf die UVM-Anmeldeschnittstelle zuzugreifen.
2. Geben Sie den Benutzernamen und die Domäne ein, an der Sie angemeldet sind, und klicken Sie anschließend auf **Entsperren**.

   Das Fenster "UVM-Verschlüsselungstext" wird geöffnet.

   Anmerkung: Obwohl UVM mehrere Domänen erkennt, muss das Benutzerkennwort für alle Domänen übereinstimmen.
3. Geben Sie den UVM-Verschlüsselungstext ein, und klicken Sie auf **OK**, um auf das Betriebssystem zuzugreifen.

Anmerkungen:

1. Wenn der UVM-Verschlüsselungstext für den eingegebenen Benutzernamen und für die eingegebene Domäne nicht der richtige ist, wird das UVM-Anmeldefenster erneut geöffnet.
2. Je nach den Authentifizierungsbestimmungen der UVM-Policy für den Client kann möglicherweise eine weiter reichende Authentifizierung erforderlich sein.

Benutzerkonfigurationsprogramm

Das Benutzerkonfigurationsprogramm ermöglicht es den Clientbenutzern, verschiedene Vorgänge zum Verwalten der Systemsicherheit auszuführen, für die keine Administratorberechtigungen erforderlich sind.

Funktionen des Benutzerkonfigurationsprogramms

Das Benutzerkonfigurationsprogramm bietet Clientbenutzern folgende Möglichkeiten:

- **Kennwörter und Archiv aktualisieren.** Auf dieser Registerkarte können die folgenden Funktionen ausgeführt werden:
  - **Den UVM-Verschlüsselungstext ändern:** Zum Erhöhen der Sicherheit können Sie den UVM-Verschlüsselungstext regelmäßig ändern.
  - **Windows-Kennwort aktualisieren:** Wenn Sie das Windows-Kennwort für einen UVM-berechtigten Clientbenutzer mit dem Benutzerverwaltungsprogramm von Windows ändern, müssen Sie das betreffende Kennwort auch über das Benutzerkonfigurationsprogramm von IBM Client Security ändern. Wenn ein Administrator das Administratordienstprogramm zum Ändern des Windows-Anmeldekennworts für einen Benutzer verwendet, werden alle zuvor für diesen Benutzer erstellten Chiffrierschlüssel gelöscht, und die zugeordneten digitalen Zertifikate werden ungültig.
  - **Lotus Notes-Kennwort zurücksetzen:** Zur Erhöhung der Sicherheit können Lotus Notes-Benutzer ihr Notes-Kennwort ändern.
  - **Das Schlüsselarchiv aktualisieren:** Wenn Sie digitale Zertifikate erstellen und von den privaten Schlüsseln, die auf dem integrierten IBM Security Chip gespeichert sind, Kopien erstellen möchten, oder wenn Sie das Schlüsselarchiv an eine andere Position versetzen möchten, aktualisieren Sie das Schlüsselarchiv.
- **Einstellungen für UVM-Signaltöne konfigurieren:** Mit dem Benutzerkonfigurationsprogramm können Sie eine Audiodatei auswählen, die bei erfolgreicher oder fehlgeschlagener Authentifizierung wiedergegeben werden soll.
- **Benutzerkonfiguration.** Auf dieser Registerkarte können die folgenden Funktionen ausgeführt werden:
-
  - **Benutzer zurücksetzen.** Mit dieser Funktion können Sie Ihre Sicherheitskonfiguration wiederherstellen. Beim Zurücksetzen der Sicherheitskonfiguration werden alle Schlüssel, Zertifikate und Fingerabdrücke gelöscht.
  - **Benutzerkonfiguration über Archiv wiederherstellen:** Mit dieser Funktion können Sie Einstellungen über das Archiv wiederherstellen. Dies ist nützlich, wenn Dateien beschädigt wurden oder Sie eine vorherige Konfiguration wiederherstellen möchten.
  - **Bein einem CSS-Roaming-Server registrieren.** Mit Hilfe dieser Funktion können Sie dieses System bei einem CSS-Roaming-Server registrieren. Wenn das System registriert ist, können Sie Ihre aktuelle Konfiguration in dieses System importieren.

Einschränkungen des Benutzerkonfigurationsprogramms unter Windows XP

Unter Windows XP gibt es für einen Clientbenutzer unter bestimmten Umständen Zugriffseinschränkungen für die verfügbaren Funktionen.

Windows XP Professional

Unter Windows XP Professional können die Einschränkungen für Clientbenutzer in den folgenden Situationen auftreten:

- Client Security ist auf einer Partition installiert, die später in das NTFS-Format konvertiert wird.
- Der Windows-Ordner befindet sich auf einer Partition, die später in das NTFS-Format konvertiert wird.
- Der Archivordner befindet sich auf einer Partition, die später in das NTFS-Format konvertiert wird.

In den vorgenannten Fällen können Benutzer von Windows XP Professional mit eingeschränkter Berechtigung möglicherweise folgende Tasks im Benutzerkonfigurationsprogramm nicht ausführen:

- Den UVM-Verschlüsselungstext ändern
- Das mit UVM registrierte Windows-Kennwort aktualisieren
- Das Schlüsselarchiv aktualisieren

Diese Einschränkungen gelten nicht mehr, nachdem ein Administrator das Administratordienstprogramm gestartet und beendet hat.

Windows XP Home

Benutzer von Windows XP Home mit eingeschränkter Berechtigung können in den folgenden Fällen das Benutzerkonfigurationsprogramm nicht verwenden:

- Client Security ist auf einer Partition im NTFS-Format installiert.
- Der Windows-Ordner befindet sich auf einer Partition im NTFS-Format.
- Der Archivordner befindet sich auf einer Partition im NTFS-Format.

Benutzerkonfigurationsprogramm verwenden

Gehen Sie wie folgt vor, um das Benutzerkonfigurationsprogramm zu verwenden:

1. Klicken Sie auf **Start > Programme > Access IBM > IBM Client Security > Sicherheitseinstellungen ändern**.

   Die Hauptanzeige des Benutzerkonfigurationsprogramms von IBM Client Security wird angezeigt.
2. Wählen Sie eine der folgenden Registerkarten aus:
   - **Kennwörter und Archiv aktualisieren.** Über diese Registerkarte können Sie Ihren UVM-Verschlüsselungstext ändern, Ihr Windows-Kennwort in UVM aktualisieren, Ihr Lotus Notes-Kennwort in UVM zurücksetzen und Ihr Verschlüsselungsarchiv aktualisieren.
   - **UVM-Signaltöne konfigurieren.** Über diese Registerkarte können Sie eine Audiodatei auswählen, die bei erfolgreicher oder fehlgeschlagener Authentifizierung wiedergegeben werden soll.
   - **Benutzerkonfiguration.** Über diese Registerkarte kann ein Benutzer seine Benutzerkonfiguration aus dem Archiv wiederherstellen, seine Sicherheitskonfiguration zurücksetzen oder den Computer beim Roaming-Server registrieren (sofern der Computer als Roaming-Client verwendet werden kann).
3. Klicken Sie auf **OK**, um die Konfiguration zu beenden.

E-Mails sicher versenden und im World Wide Web sicher navigieren

Wenn Sie über das Internet ungesicherte Transaktionen senden, können diese abgefangen und gelesen werden. Den unbefugten Zugriff auf Ihre Internet-Transaktionen können Sie verhindern, indem Sie sich ein digitales Zertifikat besorgen und damit die E-Mails signieren und verschlüsseln oder den Webbrowser sichern.

Ein digitales Zertifikat (auch digitale ID oder Sicherheitszertifikat genannt) ist ein elektronischer Berechtigungsnachweis, der von einer Zertifizierungsinstanz ausgestellt und digital signiert wird. Wenn Sie ein digitales Zertifikat erhalten, bescheinigt die Zertifizierungsinstanz dadurch Ihre Identität als Eigner des Zertifikats. Bei der Zertifizierungsinstanz handelt es sich um einen vertrauenswürdigen Anbieter von digitalen Zertifikaten, z. B. eine Firma wie VeriSign oder einen Server, der als Zertifizierungsinstanz innerhalb Ihres Unternehmens eingerichtet wird. Das digitale Zertifikat enthält Ihre Identität, d. h. Ihren Namen und Ihre E-Mail-Adresse, die Ablaufdaten des Zertifikats, eine Kopie des öffentlichen Schlüssels sowie die Identität der Zertifizierungsinstanz und deren digitale Unterschrift.

Client Security mit Microsoft-Anwendungen einsetzen

Die nachfolgenden Informationen beziehen sich auf die Verwendung von Client Security für das Anfordern und Anwenden digitaler Zertifikate im Zusammenhang mit Anwendungen, die die Schnittstelle Microsoft CryptoAPI (z. B. Outlook Express) unterstützen.

Weitere Informationen zur Erstellung der Sicherheitseinstellungen und zur Verwendung von E-Mail-Anwendungen wie Outlook Express und Outlook finden Sie in der Dokumentation, die mit diesen Anwendungen geliefert wird.

Digitales Zertifikat für Microsoft-Anwendungen beziehen

Wenn Sie über eine Zertifizierungsinstanz ein für Microsoft-Anwendungen zu verwendendes digitales Zertifikat erstellen, werden Sie aufgefordert, für das Zertifikat einen CSP (Cryptographic Service Provider) auszuwählen.

Damit Sie die Verschlüsselungsfunktionen des integrierten IBM Security Chips für Microsoft-Anwendungen nutzen können, müssen Sie bei Erhalt des digitalen Zertifikats als CSP das **CSP-Modul des integrierten IBM Sicherheits-Subsystems** auswählen. Dadurch ist sichergestellt, dass der private Schlüssel des digitalen Zertifikats auf dem IBM Security Chip gespeichert wird.

Wenn Sie die Sicherheit noch erhöhen möchten, können Sie den hohen Verschlüsselungsgrad auswählen. Da der integrierte IBM Security Chip einen Verschlüsselungsgrad von bis zu 1024 Bit für die Verschlüsselung des privaten Schlüssels des digitalen Zertifikats verarbeiten kann, sollten Sie diese Option auswählen, wenn sie von der Schnittstelle der Zertifizierungsinstanz angeboten wird; die 1024-Bit-Verschlüsselung wird hier auch als hochgradige Verschlüsselung bezeichnet.

Wenn Sie **CSP-Modul des integrierten IBM Sicherheits-Subsystems** als CSP ausgewählt haben, müssen Sie unter Umständen Ihren UVM-Verschlüsselungstext eingeben und/oder sich durch eine Sensorabtastung Ihrer Fingerabdrücke ausweisen, um die Authentifizierungsbestimmungen für das digitale Zertifikat zu erfüllen. Die Authentifizierungsbestimmungen sind in der UVM-Policy für den Computer definiert.

Zertifikate vom Microsoft-CSP übertragen

Mit dem Assistenten zur Übertragung von Zertifikaten von IBM CSS können Sie Zertifikate, die mit dem Standard-Microsoft-CSP erstellt wurden, an das CSP-Modul des integrierten IBM-Sicherheits-Subsystems (IBM Embedded Security Subsystem) übertragen. Durch die Übertragung der Zertifikate wird der Schutz für die den Zertifikaten zugeordneten privaten Schlüssel erheblich gesteigert, da diese sicher über das integrierte IBM Sicherheits-Subsystem gespeichert werden, und nicht mehr über die leicht zugängliche Software.

Es gibt zwei Arten von Sicherheitszertifikaten, die übertragen werden können:

- **Benutzerzertifikate:** Ein Benutzerzertifikat dient zum Autorisieren eines bestimmten Benutzers. In der Regel wird ein Benutzerzertifikat von einer Zertifizierungsstelle (CA, Certificate Authority), wie z. B. cssdesk, angefordert. Eine Zertifizierungsstelle ist ein vertrauenswürdiger Anbieter, der Zertifikate speichert, ausstellt und veröffentlicht. Benutzerzertifikate werden benötigt, um E-Mails zu unterzeichnen, E-Mails zu verschlüsseln oder um sich an bestimmten Servern anzumelden.
- **Maschinenzertifikate:** Ein Maschinenzertifikat dient der eindeutigen Bestimmung eines bestimmten Computers. Bei der Verwendung eines Maschinenzertifikats beruht die Authentifizierung nicht auf dem Benutzer, sondern auf dem Computer.

Der Assistent zur Übertragung von CSS-Zertifikaten überträgt nur Microsoft-Zertifikate, die als exportierbar gekennzeichnet sind und deren Schlüssel nicht mehr als 1024 Bit umfasst.

Wenn ein Benutzer ein Maschinenzertifikat übertragen muss, aber keine Administratorrechte für das System hat, kann ein Administrator eine Administratorkonfigurationsdatei senden, mit deren Hilfe ein Benutzer ein Zertifikat ohne Angabe des Administratorkennworts übertragen kann. Erstellen Sie mit Hilfe des Dienstprogramms "Administratorkonsole" eine Administratorkonfigurationsdatei. Das Dienstprogramm befindet sich im Ordner `c:\\Programme\ibm\security`.

Gehen Sie wie folgt vor, um den Assistenten zur Übertragung von CSS-Zertifikaten zu verwenden:

1. Klicken Sie auf **Start > Access IBM > IBM Client Security > Assistent zur Übertragung von CSS-Zertifikaten**.

   Die Eingangsanzeige des Assistenten zur Übertragung von CSS-Zertifikaten wird angezeigt.
2. Klicken Sie auf **Weiter**, um anzufangen.
3. Wählen Sie die Zertifikatstypen aus, die übertragen werden sollen, und klicken Sie auf **Weiter**. Der Assistent zur Übertragung von CSS-Zertifikaten kann nur Zertifikate im Microsoft-Zertifikatsspeicher übertragen, die als exportierbar gekennzeichnet sind.
4. Wählen Sie die zu übertragenden Zertifikate aus, indem Sie auf den Zertifikatnamen klicken, der im Bereich "Ausgegeben an" angezeigt wird, und klicken Sie dann auf **Weiter**. Eine Nachricht teilt mit, dass das Zertifikat erfolgreich übertragen wurde.

   Anmerkung: Zum Übertragen eines Maschinenzertifikats ist das Administratorkennwort oder eine Administratorkonfigurationsdatei erforderlich.

5. Klicken Sie auf **OK**, um zum Assistenten zur Übertragung von CSS-Zertifikaten zurückzukehren.

Nach dem Übertragen der Zertifikate werden diese dem CSP-Modul des integrierten IBM Sicherheits-Subsystems zugeordnet, und die privaten Schlüssel werden vom integrierten IBM Sicherheits-Subsystem geschützt. Alle Operationen, bei denen diese privaten Schlüssel verwendet werden, z. B. beim Erstellen digitaler Signaturen oder beim Entschlüsseln von E-Mails, werden innerhalb der geschützten Umgebung des integrierten IBM Sicherheits-Subsystems ausgeführt.

Schlüsselarchiv für Microsoft-Anwendungen aktualisieren

Sichern Sie das digitale Zertifikat nach seiner Erstellung, indem Sie das Schlüsselarchiv aktualisieren. Sie können das Schlüsselarchiv mit dem Administratordienstprogramm aktualisieren.

Digitales Zertifikat für Microsoft-Anwendungen verwenden

Verwenden Sie zur Anzeige und zur Verwendung digitaler Zertifikate die Sicherheitseinstellungen in den Microsoft-Anwendungen. Weitere Informationen hierzu finden Sie in der Dokumentation von Microsoft.

Nachdem Sie das digitale Zertifikat erstellt und damit eine E-Mail signiert haben, werden Sie von UVM aufgefordert, die Authentifizierungsbestimmungen beim ersten digitalen Signieren einer E-Mail zu erfüllen. Möglicherweise müssen Sie den UVM-Verschlüsselungstext eingeben, die Fingerabdrücke scannen oder beides, damit Sie die Authentifizierungsbestimmungen zur Verwendung des digitalen Zertifikats erfüllen. Die Authentifizierungsbestimmungen sind in der UVM-Policy für den Computer definiert.

Einstellungen für UVM-Signaltöne konfigurieren

Über die Schnittstelle des Benutzerkonfigurationsprogramms können Einstellungen für Signaltöne konfiguriert werden. Gehen Sie wie folgt vor, um die Standardeinstellung für Signaltöne zu ändern:

1. Klicken Sie auf **Start > Programme > Access IBM > IBM Client Security > Sicherheitseinstellungen ändern**.

   Die Anzeige des Benutzerkonfigurationsprogramms von IBM Client Security wird angezeigt.
2. Klicken Sie auf die Registerkarte **UVM-Signaltöne konfigurieren**.
3. Geben Sie im Abschnitt "UVM-Authentifizierungstöne" in das Feld "Erfolgreiche Authentifizierung" den Dateipfad zur Audiodatei ein, die bei erfolgreicher Authentifizierung wiedergegeben werden soll, oder klicken Sie auf **Durchsuchen**, wenn Sie eine Datei auswählen wollen.
4. Geben Sie im Abschnitt "UVM-Authentifizierungstöne" in das Feld "Authentifizierungsfehler" den Dateipfad zur Audiodatei ein, die bei nicht erfolgreicher Authentifizierung wiedergegeben werden soll, oder klicken Sie auf **Durchsuchen**, wenn Sie eine Datei auswählen wollen.
5. Klicken Sie auf **OK**, um den Vorgang abzuschließen.

Kapitel 10. Fehlerbehebung

Im Folgenden finden Sie Informationen zur Vermeidung, Erkennung und Behebung von Fehlern, die bei der Verwendung von Client Security auftreten können.

Administratorfunktionen

Dieser Abschnitt enthält Informationen für Administratoren zur Konfiguration und zur Verwendung von Client Security.

IBM Client Security kann nur auf IBM Computern verwendet werden, die über das integrierte IBM Sicherheits-Subsystem (IBM Embedded Security Subsystem) verfügen. Diese Software besteht aus Anwendungen und Komponenten, mit denen IBM Clients schutzwürdige Daten über sichere Hardware anstatt über leicht zugängliche Software sichern können.

Benutzer autorisieren

Bevor die Clientbenutzerinformationen geschützt werden können, **muss** IBM Client Security auf dem Client installiert sein, und die Benutzer **müssen** zur Nutzung der Software berechtigt werden. Ein benutzerfreundlicher Installationsassistent leitet Sie durch den gesamten Installationsprozess.

Wichtig: Mindestens ein Clientbenutzer **muss** bei der Installation für die Verwendung von UVM autorisiert werden. Wenn bei der ersten Installation von Client Security kein Benutzer für die Verwendung von UVM autorisiert wird, werden die Sicherheitseinstellungen **nicht** übernommen und Ihre Daten werden **nicht** geschützt.

Wenn Sie den Installationsassistenten beendet haben, ohne Benutzer autorisiert zu haben, fahren Sie den Computer herunter, und starten Sie ihn erneut; führen Sie dann den Installationsassistenten von Client Security über das Windows-Startmenü aus, und autorisieren Sie einen Windows-Benutzer für die Benutzung von UVM. Auf diese Weise wird IBM Client Security für das Übernehmen der Sicherheitseinstellungen und für den Schutz der schutzwürdigen Daten aktiviert.

Benutzer löschen

Wenn Sie einen Benutzer löschen, wird der Benutzername in der Benutzerliste des Administratordienstprogramms gelöscht.

BIOS-Administratorkennwort festlegen (ThinkCentre)

Über die Sicherheitseinstellungen im Programm "Configuration/Setup Utility" können Administratoren folgende Vorgänge durchführen:

- Das integrierte IBM Sicherheits-Subsystem aktivieren oder inaktivieren
- Den Inhalt des integrierten IBM Sicherheits-Subsystems löschen

Achtung:

- Wenn Sie den Inhalt des integrierten IBM Sicherheits-Subsystems löschen, gehen alle Chiffrierschlüssel und Zertifikate verloren, die auf dem Subsystem gespeichert sind.

Da auf Ihre Sicherheitseinstellungen über das Programm "Configuration/Setup Utility" des Computers zugegriffen werden kann, legen Sie ein Administratorkennwort fest, um zu verhindern, dass diese Einstellungen durch nicht autorisierte Benutzer geändert werden.

Gehen Sie wie folgt vor, um ein BIOS-Administratorkennwort festzulegen:

1. Fahren Sie das System herunter, und starten Sie es erneut.
2. Drücken Sie während der Eingabeaufforderung des Programms "Configuration/Setup Utility" die Taste **F1**.

   Das Hauptmenü des Programms "Configuration/Setup Utility" wird geöffnet.
3. Wählen Sie die Option **System Security** aus.
4. Wählen Sie die Option **Administrator Password** aus.
5. Geben Sie das Kennwort ein, und drücken Sie auf der Tastatur die Taste mit dem Abwärtspfeil.
6. Geben Sie das Kennwort erneut ein, und drücken Sie auf der Tastatur die Taste mit dem Abwärtspfeil.
7. Wählen Sie **Change Administrator password** aus, und drücken Sie die Eingabetaste. Drücken Sie danach erneut die Eingabetaste.
8. Drücken Sie die Taste **Esc**, um die Einstellungen zu speichern und das Programm zu verlassen.

Nach dem Festlegen eines BIOS-Administratorkennworts wird bei jedem Zugriff auf das Programm "Configuration/Setup Utility" eine Eingabeaufforderung angezeigt.

Wichtig: Bewahren Sie Ihr BIOS-Administratorkennwort an einem sicheren Ort auf. Sollten Sie das BIOS-Administratorkennwort verlieren oder vergessen, können Sie nicht auf das Programm "Configuration/Setup Utility" zugreifen und das Kennwort nicht ändern oder löschen, ohne die Computerabdeckung zu entfernen und auf der Systemplatine eine Brücke zu versetzen. Weitere Informationen hierzu finden Sie in der Hardwaredokumentation, die mit Ihrem Computer geliefert wurde.

Administratorkennwort festlegen (ThinkPad)

Mit den Sicherheitseinstellungen im Programm "IBM BIOS Setup Utility" können Administratoren folgende Vorgänge durchführen:

- Das integrierte IBM Sicherheits-Subsystem aktivieren oder inaktivieren
- Den Inhalt des integrierten IBM Sicherheits-Subsystems löschen

Achtung:

- Bei einigen ThinkPad-Modellen ist es vor der Installation oder dem Upgrade von Client Security notwendig, das Administratorkennwort vorübergehend zu inaktivieren.

Nach der Konfiguration von Client Security legen Sie ein Administratorkennwort fest, um nicht berechtigte Benutzer daran zu hindern, diese Einstellungen ändern.

Gehen Sie wie folgt vor, um ein Administratorkennwort festzulegen:

Beispiel 1

1. Fahren Sie das System herunter, und starten Sie es erneut.

2. Drücken Sie bei der Eingabeaufforderung des Programms ″Setup Utility″ die Taste F1.

   Das Hauptmenü des Programms ″Setup Utility″ wird geöffnet.
3. Wählen Sie die Option **Password** aus.
4. Wählen Sie die Option **Supervisor Password** aus.
5. Geben Sie das Kennwort ein, und drücken Sie die Eingabetaste.
6. Geben Sie das Kennwort erneut ein, und drücken Sie die Eingabetaste.
7. Klicken Sie auf **Continue**.
8. Drücken Sie die Taste F10, um die Einstellungen zu speichern und das Programm zu beenden.

Beispiel 2

1. Fahren Sie das System herunter, und starten Sie es erneut.
2. Wenn die Nachricht ″To interrupt normal startup, press the blue Access IBM button″ angezeigt wird, drücken Sie die blaue Taste ″Access IBM″.

   Die Access IBM Predesktop Area wird geöffnet.
3. Klicken Sie doppelt auf **Konfigurationsdienstprogramm starten**.
4. Wählen Sie mit Hilfe der Navigationstasten den Menüpunkt **Security** aus.
5. Wählen Sie die Option **Password** aus.
6. Wählen Sie die Option **Supervisor Password** aus.
7. Geben Sie das Kennwort ein, und drücken Sie die Eingabetaste.
8. Geben Sie das Kennwort erneut ein, und drücken Sie die Eingabetaste.
9. Klicken Sie auf **Continue**.
10. Drücken Sie die Taste F10, um die Einstellungen zu speichern und das Programm zu beenden.

Nach dem Festlegen eines Administratorkennworts wird bei jedem Zugriff auf das Programm ″BIOS Setup Utility″ eine Eingabeaufforderung angezeigt.

Wichtig: Bewahren Sie Ihr Administratorkennwort an einem sicheren Ort auf. Sollten Sie das Administratorkennwort verlieren oder vergessen, können Sie nicht auf das Programm ″IBM BIOS Setup Utility″ zugreifen und das Kennwort nicht ändern oder löschen. Weitere Informationen hierzu finden Sie in der Hardwaredokumentation, die mit Ihrem Computer geliefert wurde.

Administratorkennwort schützen

Das Administratorkennwort dient als Schutz für den Zugriff auf das Administratordienstprogramm. Halten Sie das Administratorkennwort geheim, um zu verhindern, dass Benutzer ohne Berechtigung Einstellungen im Administratordienstprogramm ändern können.

Inhalt des integrierten IBM Sicherheits-Subsystems löschen (ThinkCentre)

Wenn Sie alle Chiffrierschlüssel für Benutzer aus dem integrierten IBM Sicherheits-Subsystem sowie das Administratorkennwort für das Subsystem löschen möchten, müssen Sie den Inhalt des Chips löschen. Lesen Sie die nachfolgend aufgeführten Informationen, bevor Sie den Inhalt des integrierten IBM Sicherheits-Subsystems löschen.

Achtung:

- Wenn Sie den Inhalt des integrierten IBM Sicherheits-Subsystems löschen, gehen alle Chiffrierschlüssel und Zertifikate verloren, die auf dem Subsystem gespeichert sind.

Gehen Sie wie folgt vor, um den Inhalt des integrierten IBM Sicherheits-Systems zu löschen:

1. Fahren Sie das System herunter, und starten Sie es erneut.
2. Drücken Sie bei der Eingabeaufforderung des Programms ″Setup Utility″ die Taste F1.

   Das Hauptmenü des Programms ″Setup Utility″ wird geöffnet.
3. Wählen Sie die Option **Security** aus.
4. Wählen Sie **IBM TCPA Feature Setup** aus.
5. Wählen Sie **Clear IBM TCPA Security Feature** aus, und drücken Sie die Eingabetaste.
6. Wählen Sie **Yes** aus.
7. Drücken Sie die Taste F10, und wählen Sie **Yes** aus.
8. Drücken Sie die Eingabetaste. Der Computer startet neu.

Inhalt des integrierten IBM Sicherheits-Subsystems löschen (ThinkPad)

Wenn Sie alle Chiffrierschlüssel für Benutzer aus dem integrierten IBM Sicherheits-Subsystem sowie das Administratorkennwort löschen möchten, müssen Sie den Inhalt des Subsystems löschen. Lesen Sie die nachfolgend aufgeführten Informationen, bevor Sie den Inhalt des integrierten IBM Sicherheits-Subsystems löschen.

Achtung:

- Wenn Sie den Inhalt des integrierten IBM Sicherheits-Subsystems löschen, gehen alle Chiffrierschlüssel und Zertifikate verloren, die auf dem Subsystem gespeichert sind.

Gehen Sie wie folgt vor, um den Inhalt des integrierten IBM Sicherheits-Systems zu löschen:

1. Fahren Sie den Computer herunter.
2. Halten Sie beim Neustart des Computers die Taste Fn gedrückt.
3. Drücken Sie bei der Eingabeaufforderung des Programms ″Setup Utility″ die Taste F1.

   Das Hauptmenü des Programms ″Setup Utility″ wird geöffnet.
4. Wählen Sie **Config** aus.
5. Wählen Sie **IBM Security Chip** aus.
6. Wählen Sie **Clear IBM Security Chip** aus.
7. Wählen Sie **Yes** aus.
8. Drücken Sie die Eingabetaste, um fortzufahren.
9. Drücken Sie die Taste F10, um die Einstellungen zu speichern und das Programm zu beenden.

Bekannte Probleme oder Einschränkungen bei CSS Version 5.2

Die folgenden Informationen können bei der Verwendung der Funktionen von Client Security Version 5.2 hilfreich sein.

Einschränkungen bei standortunabhängigem Zugriff

CSS-Roaming-Server verwenden

Die Aufforderung zur Eingabe des CSS-Administratorkennworts erscheint immer dann, wenn jemand versucht, sich am CSS-Roaming-Server anzumelden. Normalerweise kann der Computer aber auch ohne die Eingabe dieses Kennworts benutzt werden.

IBM Client Security Password Manager in einer Umgebung mit standortunabhängigem Zugriff verwenden

Kennwörter, die in einem System gespeichert wurden, das IBM Client Security Password Manager verwendet, können auch in anderen Systemen innerhalb einer Umgebung mit standortunabhängigem Zugriff verwendet werden. Neue Einträge werden automatisch vom Archiv abgerufen, wenn sich der Benutzer bei einem anderen System im Netzwerk mit standortunabhängigem Zugriff anmeldet (wenn das Archiv verfügbar ist). Aus diesem Grund muss sich der Benutzer, wenn er bereits in einem System angemeldet ist, zunächst abmelden und erneut anmelden, bevor neue Einträge im Netzwerk mit standortunabhängigem Zugriff verfügbar sind.

Verzögerungen bei der Aktualisierung des Zertifikats für den Internet Explorer und des standortunabhängigen Zugriffs

Die Zertifikate für den Internet Explorer werden alle 20 Sekunden im Archiv aktualisiert. Wurde durch einen standortunabhängigen Benutzer ein neues Zertifikat für den Internet Explorer erstellt, muss der Benutzer mindestens 20 Sekunden warten, bis er seine CSS-Konfiguration auf einem anderen System importieren, wiederherstellen oder ändern kann. Bei dem Versuch, eine dieser Aktionen vor dem Ende des Aktualisierungsintervalls von 20 Sekunden durchzuführen, geht das Zertifikat verloren. Auch wenn der Benutzer keine Verbindung zum Archiv hatte, während das Zertifikat erstellt wurde, sollte er 20 Sekunden warten, nachdem die Verbindung zum Archiv hergestellt wurde, um sicherzustellen, dass das Zertifikat im Archiv aktualisiert wurde.

Lotus Notes-Kennwort und standortunabhängiger Zugriff mit Berechtigungsnachweis

Wenn die Lotus Notes-Unterstützung aktiviert ist, wird das Lotus Notes-Kennwort des Benutzers durch UVM gespeichert. Die Benutzer brauchen ihr Notes-Kennwort künftig nicht mehr einzugeben, um sich bei Lotus Notes anzumelden. Sie werden nach ihrem UVM-Verschlüsselungstext, dem Fingerabdruck, der Smartcard usw. (je nach Einstellungen der Sicherheitspolicy) gefragt, um auf Lotus Notes zugreifen zu können.

Wenn ein Benutzer sein Notes-Kennwort von Lotus Notes aus ändert, wird die Lotus Notes-ID-Datei mit dem neuen Kennwort aktualisiert und die UVM-Kopie des neuen Notes-Kennworts wird ebenfalls aktualisiert. In einer Umgebung mit standortunabhängigem Zugriff sind die UVM-Berechtigungsnachweise des Benutzers auch in anderen Systemen des Netzwerks mit standortunabhängigem Zugriff verfügbar, auf die der Benutzer zugreifen kann.

Es ist möglich, dass die Kopie des Notes-Kennworts von UVM nicht mit dem Notes-Kennwort in der ID-Datei auf anderen Systemen im Netzwerk mit standortunabhängigem Zugriff übereinstimmt, wenn die Notes-ID-Datei mit dem aktualisierten Kennwort nicht ebenfalls auf einem anderen System verfügbar ist. Wenn dies der Fall ist, kann der Benutzer nicht auf Lotus Notes zugreifen.

Wenn die Notes-ID-Datei mit dem aktualisierten Kennwort eines Benutzers nicht auch in einem anderen System verfügbar ist, sollte die ID-Datei in die anderen Systeme innerhalb des Netzwerks mit standortunabhängigem Zugriff kopiert werden, so dass das Kennwort in der ID-Datei mit der durch UVM gespeicherten Kopie übereinstimmt. Alternativ können die Benutzer im Startmenü auch die Anwendung 'Sicherheitseinstellungen ändern' ausführen und das Notes-Kennwort in den alten Wert ändern. Das Notes-Kennwort kann dann über Lotus Notes wieder aktualisiert werden.

Verfügbarkeit von Berechtigungsnachweisen bei der Anmeldung in einer Umgebung mit standortunabhängigem Zugriff

Befindet sich ein Archiv in einem gemeinsam benutzten Netzwerk, wird die aktuellste Gruppe von Benutzerberechtigungen aus dem Archiv heruntergeladen, sobald der Benutzer auf das Archiv zugreifen kann. Bei der Anmeldung haben die Benutzer nicht sofort Zugriff auf das gemeinsam benutzte Netzwerk, so dass die aktuellsten Berechtigungsnachweise erst heruntergeladen werden können, nachdem die Anmeldung am System abgeschlossen ist. Wenn z. B. der UVM-Verschlüsselungstext auf einem anderen System im Netzwerk mit standortunabhängigem Zugriff geändert wurde oder wenn neue Fingerabdrücke in einem anderen System registriert wurden, sind diese Aktualisierungen erst verfügbar, wenn der Anmeldeprozess beendet ist. Sind die aktualisierten Benutzerberechtigungen nicht verfügbar, sollten die Benutzer versuchen, sich mit dem früheren Verschlüsselungstext oder mit anderen registrierten Fingerabdrücken am System anzumelden. Sobald die Anmeldung beendet ist, sind die aktualisierten Benutzerberechtigungen verfügbar, und das neue Kennwort sowie der Fingerabdruck sind bei UVM registriert.

Einschränkungen bei berührungslosem Ausweis (Proximity Badge)

Sicheren UVM-Anmeldeschutz mit berührungslosem Ausweis (Proximity Badge) von XyLoc aktivieren

Um die Unterstützung des sicheren UVM-Anmeldeschutzes für die Verwendung eines berührungslosen Ausweises (Proximity Badge) bei CSS erfolgreich zu aktivieren, müssen Sie die Komponenten in folgender Reihenfolge installieren:

1. Installieren Sie Client Security.
2. Aktivieren Sie den sicheren UVM-Anmeldeschutz mit Hilfe des CSS-Administratordienstprogramms.
3. Starten Sie den Computer erneut.
4. Installieren Sie die Software von XyLoc für die Unterstützung von berührungslosen Ausweisen (Proximity Badges).

Anmerkung: Wenn die Software von XyLoc für den berührungslosen Ausweis zuerst installiert wird, wird die Anmeldeschnittstelle für Client Security nicht angezeigt. Wenn dies eintritt, müssen Sie Client Security und XyLoc deinstallieren und anschließend in der oben genannten Reihenfolge erneut installieren, um den sicheren UVM-Anmeldeschutz wiederherzustellen.

Unterstützung von berührungslosem Ausweis (Proximity Badge) und Cisco LEAP

Durch das Aktivieren der Unterstützung von Zugriffsschutz mit berührungslosem Ausweis (Proximity Badge) und von Cisco LEAP können unerwartete Ergebnisse auftreten. Es wird empfohlen, diese Komponenten nicht zusammen auf demselben System zu installieren oder zu verwenden.

Ensure-Software unterstützen

Bei Client Security 5.2 ist es erforderlich, dass die Benutzer eines berührungslosen Ausweises (Proximity Badge) ihre Ensure-Software auf die Ensure-Softwareversion 7.41 aufrüsten. Wenn Sie einen Upgrade von einer früheren Version von Client Security aus durchführen, müssen Sie zuerst die Ensure-Software aufrüsten, bevor Sie auf Client Security 5.2 aufrüsten können.

Schlüssel wiederherstellen

Nach der Durchführung einer Wiederherstellungsoperation für die Schlüssel müssen Sie den Computer erneut starten, bevor Sie Client Security weiterhin verwenden können.

Namen des lokalen Benutzers und des Domänenbenutzers

Wenn die Namen des Domänenbenutzers und des lokalen Benutzers gleich sind, sollten Sie für beide Accounts dasselbe Windows-Kennwort verwenden. IBM User Verification Manager speichert nur ein Windows-Kennwort pro ID. Die Benutzer sollten daher dasselbe Kennwort für die lokale Anmeldung und für die Domänenanmeldung verwenden. Wenn dies nicht der Fall ist, werden die Benutzer dazu aufgefordert, das IBM UVM Windows-Kennwort zu aktualisieren, wenn sie zwischen lokaler und Domänenanmeldung umschalten, wenn die Ersetzung der gesicherten Windows-Standardanmeldung durch eine gesicherte UVM-Anmeldung aktiviert ist.

CSS ist nicht in der Lage, getrennte Domänenbenutzer und lokale Benutzer mit demselben Accountnamen zu registrieren. Wenn Sie versuchen, lokale Benutzer und Domänenbenutzer mit derselben ID zu registrieren, wird folgende Nachricht angezeigt: Die ausgewählte Benutzer-ID wurde bereits konfiguriert. Bei CSS ist es nicht möglich, allgemeine IDs von Domänen- und von lokalen Benutzern einzeln in einem System zu registrieren, so dass mit der allgemeinen Benutzer-ID auf dieselbe Gruppe von Berechtigungsnachweisen, wie z. B. Zertifikate, gespeicherte Fingerabdrücke usw., zugegriffen werden kann.

Targus-Software zum Lesen von Fingerabdrücken erneut installieren

Wurde die Targus-Software zum Lesen von Fingerabdrücken entfernt und anschließend erneut installiert, müssen die erforderlichen Registrierungseinträge zum Aktivieren der Unterstützung für das Lesen von Fingerabdrücken bei Client Security manuell aktiviert werden. Laden Sie die Registrierungsdatei mit den erforderlichen Einträgen (atplugin.reg) herunter, und klicken Sie doppelt darauf, um die Registrierungseinträge der Registrierungsdatenbank hinzuzufügen. Klicken Sie bei entsprechender Aufforderung auf "Ja", um diese Operation zu bestätigen. Das System muss erneut gestartet werden, damit die Änderungen von Client Security erkannt werden und die Unterstützung für das Lesen von Fingerabdrücken aktiviert wird.

Anmerkung: Für das Hinzufügen dieser Registrierungseinträge ist die Administratorberechtigung auf dem System erforderlich.

Administratorverschlüsselungstext für das BIOS

IBM Client Security 5.2 und frühere Versionen unterstützen nicht die auf einigen ThinkPad-Systemen verfügbare Funktion für den Administratorverschlüsselungstext für das BIOS. Wenn Sie die Verwendung des Administratorverschlüsselungstextes für das BIOS aktivieren, muss jede Aktivierung und Inaktivierung des Sicherheits-Subsystems über das Programm "IBM BIOS Setup Utility" vorgenommen werden.

Netscape 7.x verwenden

Netscape 7.x unterscheidet sich von Netscape 4.x. Die Eingabeaufforderung für den Verschlüsselungstext erscheint nicht, sobald Netscape gestartet wurde. Stattdessen wird das PKCS#11-Modul nur bei Bedarf geladen, so dass die Eingabeaufforderung für den Verschlüsselungstext nur dann angezeigt wird, wenn eine Operation ausgeführt wird, bei der das PKCS#11-Modul erforderlich ist.

Diskette zum Archivieren verwenden

Wenn Sie bei der Konfiguration der Sicherheitssoftware eine Diskette als Archivposition angegeben haben, müssen Sie mit langen Verzögerungen rechnen, wenn die Daten während des Konfigurationsprozesses auf die Diskette geschrieben werden. Ein anderer Datenträger, wie z. B. ein gemeinsam benutztes Netzwerk oder ein USB Memory Key, eignet sich möglicherweise besser als Archivposition.

Smartcard-Einschränkungen

Smartcards registrieren

Smartcards müssen erst bei UVM registriert werden, bevor ein Benutzer eine Authentifizierung mit Hilfe der Karte erfolgreich durchführen kann. Wenn eine Karte mehreren Benutzern zugeordnet ist, kann nur der letzte Benutzer, der die Karte registrieren ließ, diese auch verwenden. Aus diesem Grund sollten Smartcards nur für einen Benutzeraccount registriert werden.

Smartcards authentifizieren

Ist für die Authentifizierung eine Smartcard erforderlich, zeigt UVM ein Dialogfeld an, in dem die Smartcard angefordert wird. Wenn die Smartcard in die Leseeinheit eingelegt wird, erscheint ein Dialogfenster, in dem die PIN-Nummer der Smartcard angefordert wird. Gibt der Benutzer eine falsche PIN-Nummer ein, fordert UVM die Smartcard noch einmal an. Die Smartcard muss entnommen und erneut eingelegt werden, bevor die PIN-Nummer erneut eingegeben werden kann. Die Benutzer müssen die Smartcard so oft entnehmen und erneut einlegen, bis die richtige PIN-Nummer für die Karte eingegeben wurde.

Pluszeichen (+) wird auf Ordnern nach der Verschlüsselung angezeigt

Nach der Verschlüsselung von Dateien oder Ordnern zeigt der Windows Explorer möglicherweise ein Pluszeichen (+) vor dem Ordnersymbol an. Dieses zusätzliche Zeichen wird nicht mehr angezeigt, wenn das Explorer-Fenster aktualisiert wird.

Einschränkungen für Benutzer mit eingeschränkter Berechtigung unter Windows XP

Benutzer mit eingeschränkter Berechtigung unter Windows XP können ihren UVM-Verschlüsselungstext, das Windows-Kennwort oder ihr Schlüsselarchiv nicht mit Hilfe des Benutzerkonfigurationsprogramms aktualisieren.

Andere Einschränkungen

Dieser Abschnitt enthält Informationen zu anderen bekannten Problemen und Einschränkungen in Bezug auf Client Security.

Client Security mit Windows-Betriebssystemen einsetzen

Alle Windows-Betriebssysteme weisen die folgende bekannte Einschränkung auf: Wenn ein in UVM registrierter Clientbenutzer seinen Windows-Benutzernamen ändert, geht die gesamte Funktionalität von Client Security verloren. Der Benutzer muss den neuen Benutzernamen erneut in UVM registrieren und alle neuen Berechtigungsnachweise anfordern.

Windows XP-Betriebssysteme weisen die folgende bekannte Einschränkung auf: In UVM registrierte Benutzer, deren Windows-Benutzername zuvor geändert wurde, werden von UVM nicht erkannt. UVM verweist auf den früheren Benutzernamen, während Windows nur den neuen Benutzernamen erkennt. Diese Einschränkung gilt selbst dann, wenn der Windows-Benutzername vor der Installation von Client Security geändert wurde.

Client Security mit Netscape-Anwendungen einsetzen

Netscape wird nach einem Berechtigungsfehler geöffnet: Wenn das Fenster "UVM-Verschlüsselungstext" geöffnet wird, müssen Sie den UVM-Verschlüsselungstext eingeben und auf **OK** klicken, bevor Sie fortfahren können. Wenn Sie einen falschen UVM-Verschlüsselungstext eingeben (oder bei einer Scannerabtastung von Fingerabdrücken einen falschen Fingerabdruck liefern), wird eine Fehlernachricht angezeigt. Wenn Sie auf **OK** klicken, wird Netscape geöffnet. Sie können aber das vom integrierten IBM Sicherheits-Subsystem generierte digitale Zertifikat nicht verwenden. Sie müssen Netscape verlassen, erneut aufrufen und den richtigen UVM-Verschlüsselungstext eingeben, bevor Sie das Zertifikat für das integrierte IBM Sicherheit-Subsystem verwenden können.

Algorithmen werden nicht angezeigt: Beim Anzeigen des Moduls in Netscape ist keiner der vom PKCS #11-Modul des integrierten IBM Sicherheits-Subsystems unterstützten Hashverfahren-Algorithmen ausgewählt. Die folgenden Algorithmen werden vom PKCS #11-Modul des integrierten IBM Sicherheits-Subsystems unterstützt, jedoch nicht als unterstützt erkannt, wenn sie in Netscape angezeigt werden:

- SHA-1
- MD5

Zertifikat des integrierten IBM Sicherheits-Subsystems und Verschlüsselungsalgorithmen

Im Folgenden finden Sie Informationen zu Verschlüsselungsalgorithmen, die Sie mit dem Zertifikat des integrierten IBM Sicherheits-Subsystems verwenden können. Aktuelle Informationen zu Verschlüsselungsalgorithmen für die jeweilige E-Mail-Anwendung erhalten Sie von Microsoft oder Netscape.

Beim Senden von E-Mails von einem Outlook Express-Client (128 Bit) an einen anderen Outlook Express-Client (128 Bit): Wenn Sie Outlook Express mit der 128-Bit-Version von Internet Explorer 4.0 oder 5.0 verwenden, um verschlüsselte E-Mails an andere Clients mit Outlook Express (128 Bit) zu senden, können mit dem Zertifikat des integrierten IBM Sicherheits-Subsystems verschlüsselte E-Mails nur mit dem 3DES-Algorithmus verschlüsselt werden.

Beim Senden von E-Mails zwischen einem Outlook Express-Client (128 Bit) und einem Netscape-Client: Eine Verschlüsselungsanforderung gemäß RC2(40), RC2(64) oder RC2(128) von einem Netscape-Client an einen Outlook Express-Client (128 Bit) wird an den Netscape-Client immer mit dem RC2(40)-Algorithmus zurückgesendet.

Möglicherweise stehen einige Algorithmen im Outlook Express-Client (128 Bit) nicht zur Auswahl: Je nachdem, wie die Version von Outlook Express (128 Bit) konfiguriert oder aktualisiert wurde, sind möglicherweise einige RC2-Algorithmen und andere Algorithmen für die Verwendung mit dem Zertifikat des integrierten IBM Sicherheits-Subsystems nicht verfügbar. Aktuelle Informationen zu den Verschlüsselungsalgorithmen, die mit den verschiedenen Versionen von Outlook Express verwendet werden, erhalten Sie von Microsoft.

UVM-Schutz für eine Lotus Notes-Benutzer-ID verwenden

Der UVM-Schutz funktioniert nicht, wenn Sie innerhalb einer Notes-Sitzung die Benutzer-ID wechseln: Sie können den UVM-Schutz nur für die aktuelle Benutzer-ID einer Notes-Sitzung konfigurieren. Gehen Sie wie folgt vor, um von einer Benutzer-ID, für die UVM-Schutz aktiviert wurde, zu einer anderen Benutzer-ID zu wechseln:

1. Verlassen Sie Lotus Notes.
2. Inaktivieren Sie den UVM-Schutz für die aktuelle Benutzer-ID.
3. Rufen Sie Lotus Notes auf, und wechseln Sie die Benutzer-ID. Weitere Informationen zum Wechseln von Benutzer-IDs finden Sie in der Dokumentation zu Lotus Notes.

   Wenn Sie den UVM-Schutz für die Benutzer-ID, zu der Sie gewechselt haben, konfigurieren möchten, fahren Sie mit Schritt 4 fort.
4. Rufen Sie das von Client Security bereitgestellte Tool zur Lotus Notes-Konfiguration auf, und konfigurieren Sie den UVM-Schutz.

Einschränkungen für das Benutzerkonfigurationsprogramm

Unter Windows XP gibt es für einen Clientbenutzer unter bestimmten Umständen Zugriffseinschränkungen für die verfügbaren Funktionen.

Windows XP Professional

Unter Windows XP Professional können die Einschränkungen für Clientbenutzer in den folgenden Situationen auftreten:

- Client Security ist auf einer Partition installiert, die später in das NTFS-Format konvertiert wird.
- Der Windows-Ordner befindet sich auf einer Partition, die später in das NTFS-Format konvertiert wird.
- Der Archivordner befindet sich auf einer Partition, die später in das NTFS-Format konvertiert wird.

In den vorgenannten Fällen können Benutzer von Windows XP Professional mit eingeschränkter Berechtigung möglicherweise folgende Tasks im Benutzerkonfigurationsprogramm nicht ausführen:

- Den UVM-Verschlüsselungstext ändern
- Das mit UVM registrierte Windows-Kennwort aktualisieren
- Das Schlüsselarchiv aktualisieren

Windows XP Home

Benutzer von Windows XP Home mit eingeschränkter Berechtigung können in den folgenden Fällen das Benutzerkonfigurationsprogramm nicht verwenden:

- Client Security ist auf einer Partition im NTFS-Format installiert.
- Der Windows-Ordner befindet sich auf einer Partition im NTFS-Format.
- Der Archivordner befindet sich auf einer Partition im NTFS-Format.

Tivoli Access Manager-Einschränkungen

Das Markierungsfeld **Keinen Zugriff auf ausgewähltes Objekt zulassen** ist nicht inaktiviert, wenn die Tivoli Access Manager-Steuerung ausgewählt wurde. Wenn Sie im UVM-Policy-Editor die Option **Access Manager steuert ausgewähltes Objekt** auswählen, um ein Authentifizierungsobjekt über Tivoli Access Manager zu steuern, wird das Markierungsfeld **Keinen Zugriff auf ausgewähltes Objekt zulassen** nicht inaktiviert. Auch wenn das Markierungsfeld **Keinen Zugriff auf ausgewähltes Objekt zulassen** weiterhin aktiviert ist, kann die Tivoli Access Manager-Steuerung nicht über dieses Markierungsfeld außer Kraft gesetzt werden.

Fehlernachrichten

Fehlernachrichten für Client Security werden in Ereignisprotokoll geschrieben: Client Security verwendet einen Einheitentreiber, der möglicherweise Fehlernachrichten in das Ereignisprotokoll schreibt. Die Fehler, auf denen diese Nachrichten basieren, wirken sich auf den normalen Betrieb des Computers nicht aus.

UVM ruft Fehlernachrichten auf, die vom zugeordneten Programm generiert werden, wenn für ein Authifizierungsobjekt der Zugriff verweigert wird: Wenn in der UVM-Policy die Verweigerung des Zugriffs für ein Authentifizierungsobjekt, z. B. für die E-Mail-Verschlüsselung festgelegt ist, variiert die Nachricht über den verweigerten Zugriff je nach verwendeter Software. Eine Fehlernachricht von Outlook Express über die Verweigerung des Zugriffs auf ein Authentifizierungsobjekt unterscheidet sich somit von einer Netscape-Fehlernachricht über verweigerten Zugriff.

Fehlerbehebungstabellen

Im folgenden Abschnitt finden Sie Tabellen, die Ihnen bei der Behebung von Fehlern in Verbindung mit Client Security weiterhelfen können.

Fehlerbehebungsinformationen zur Installation

Im folgenden Abschnitt finden Sie Informationen, die Ihnen bei der Behebung von Fehlern bei der Installation von Client Security weiterhelfen können.

Fehlersymptom	**Mögliche Lösung**
Während der Softwareinstallation wird eine Fehlernachricht angezeigt.	**Maßnahme**
Bei der Softwareinstallation werden Sie in einer Nachricht gefragt, ob Sie die ausgewählte Anwendung und alle zugehörigen Komponenten entfernen möchten.	Klicken Sie auf **OK**, um das Fenster zu verlassen. Beginnen Sie erneut mit dem Installationsprozess, um die neue Version von Client Security zu installieren.
Während der Installation wird eine Nachricht angezeigt, die besagt, dass Sie das Programm aufrüsten oder entfernen müssen.	Führen Sie einen der folgenden Schritte aus: • Wenn eine Version von Client Security installiert ist, die älter als Version 5.0 ist, wählen Sie **Entfernen** aus, und löschen Sie das Sicherheits-Subsystem mit Hilfe des Programms "IBM BIOS Setup Utility". • Andernfalls wählen Sie **Upgrade** aus, und fahren mit der Installation fort.
Der Installationszugriff wird verweigert, da das Administratorkennwort unbekannt ist	**Maßnahme**
Wenn Sie die Software auf einem IBM Client mit aktiviertem integrierten IBM Sicherheits-Subsystem installieren, ist das Administratorkennwort für das integrierte IBM Sicherheits-Subsystem unbekannt.	Löschen Sie das Sicherheits-Subsystem, um mit der Installation fortzufahren.

Fehlerbehebungsinformationen zum Administratordienstprogramm

Im folgenden Abschnitt finden Sie Informationen, die Ihnen bei der Behebung von Fehlern bei der Verwendung des Administratordienstprogramms weiterhelfen können.

Fehlersymptom	**Mögliche Lösung**
Die Schaltfläche "Weiter" ist nicht verfügbar, nachdem Sie im Administratordienstprogramm den UVM-Verschlüsselungstext eingegeben und bestätigt haben.	**Maßnahme**
Wenn Sie neue Benutzer in UVM aufnehmen, ist die Schaltfläche **Weiter** möglicherweise nicht mehr verfügbar, nachdem Sie Ihren UVM-Verschlüsselungstext im Administratordienstprogramm eingegeben und bestätigt haben.	Klicken Sie in der Windows-Taskleiste auf **Informationen**, und fahren Sie mit dem Vorgang fort.

Fehlersymptom	Mögliche Lösung
Beim Ändern des öffentlichen Administratorschlüssels wird eine Fehlernachricht angezeigt.	**Maßnahme**
Wenn Sie den Inhalt des integrierten Sicherheits-Subsystems löschen und anschließend das Schlüsselarchiv wiederherstellen, wird bei der Änderung des öffentlichen Administratorschlüssels möglicherweise eine Fehlernachricht angezeigt.	Fügen Sie in UVM die Benutzer hinzu, und fordern Sie ggf. neue Zertifikate an.
Beim Versuch, einen UVM-Verschlüsselungstext wiederherzustellen, wird eine Fehlernachricht angezeigt.	**Maßnahme**
Wenn Sie einen öffentlichen Administratorschlüssel ändern und anschließend versuchen, einen UVM-Verschlüsselungstext für einen Benutzer wiederherzustellen, wird möglicherweise eine Fehlernachricht angezeigt.	Führen Sie einen der folgenden Schritte aus: • Sollte für den Benutzer der UVM-Verschlüsselungstext nicht benötigt werden, ist keine Maßnahme erforderlich. • Wenn der UVM-Verschlüsselungstext für den Benutzer erforderlich ist, müssen Sie ihn in UVM aufnehmen und ggf. neue Zertifikate anfordern.
Beim Versuch, die UVM-Policy-Datei zu speichern, wird eine Fehlernachricht angezeigt.	**Maßnahme**
Wenn Sie versuchen, eine UVM-Policy-Datei (globalpolicy.gvm) durch Klicken auf **Übernehmen** oder **Speichern** zu speichern, wird eine Fehlernachricht angezeigt.	Schließen Sie die Fehlernachricht, bearbeiten Sie die UVM-Policy-Datei erneut, und speichern Sie die Datei.
Beim Versuch, den UVM-Policy-Editor zu öffnen, wird eine Fehlernachricht angezeigt.	**Maßnahme**
Wenn der aktuelle Benutzer, der am Betriebssystem angemeldet ist, nicht in UVM aufgenommen wurde, wird der UVM-Policy-Editor nicht geöffnet.	Nehmen Sie den Benutzer in UVM auf, und öffnen Sie den UVM-Policy-Editor.

Fehlersymptom	Mögliche Lösung
Bei der Verwendung des Administratordienstprogramms wird eine Fehlernachricht angezeigt.	**Maßnahme**
Während Sie das Administratordienstprogramm verwenden, wird möglicherweise die folgende Fehlernachricht angezeigt: Beim Versuch, auf das IBM Sicherheits-Subsystem zuzugreifen, ist ein Puffer-E/A-Fehler aufgetreten. Der Fehler kann möglicherweise durch einen Warmstart behoben werden.	Schließen Sie die Fehlernachricht, und starten Sie den Computer erneut.
Beim Ändern des Administratorkennworts wird eine Nachricht über die Inaktivierung des Chips angezeigt.	**Maßnahme**
Wenn Sie versuchen, das Administratorkennwort zu ändern, und nach der Eingabe des Bestätigungskennworts die Eingabetaste oder die Tabulatortaste zusammen mit der Eingabetaste drücken, wird die Schaltfläche **Chip inaktivieren** aktiviert, und es wird eine Bestätigungsnachricht für das Inaktivieren des Chips angezeigt.	Gehen Sie wie folgt vor: 1. Schließen Sie das Bestätigungsfenster für die Inaktivierung des Chips. 2. Geben Sie zum Ändern des Administratorkennworts das neue Kennwort ein, geben Sie das Bestätigungskennwort ein, und klicken Sie anschließend auf **Ändern**. Drücken Sie, nachdem Sie das Bestätigungskennwort eingegeben haben, nicht die Eingabetaste oder die Tabulatortaste zusammen mit der Eingabetaste.

Fehlerbehebungsinformationen zum Benutzerkonfigurationsprogramm

Die folgenden Informationen zur Fehlerbehebung können hilfreich sein, wenn bei der Verwendung des Benutzerkonfigurationsprogramms Fehler auftreten.

Fehlersymptom	**Mögliche Lösung**
Benutzer mit eingeschränkter Berechtigung können gewisse Funktionen des Benutzerkonfigurationsprogramms unter Windows XP Professional nicht ausführen	**Maßnahme**
Benutzer von Windows XP Professional mit eingeschränkter Berechtigung können möglicherweise folgende Tasks im Benutzerkonfigurationsprogramm nicht ausführen: • Den UVM-Verschlüsselungstext ändern • Das mit UVM registrierte Windows-Kennwort aktualisieren • Das Schlüsselarchiv aktualisieren	Dies ist eine bekannte Einschränkung unter Windows XP Professional. Für dieses Problem gibt es keine Lösung.
Benutzer mit eingeschränkter Berechtigung können das Benutzerkonfigurationsprogramm unter Windows XP Home nicht ausführen	**Maßnahme**
Benutzer von Windows XP Home mit eingeschränkter Berechtigung können in den folgenden Fällen das Benutzerkonfigurationsprogramm nicht verwenden: • Client Security ist auf einer Partition im NTFS-Format installiert. • Der Windows-Ordner befindet sich auf einer Partition im NTFS-Format. • Der Archivordner befindet sich auf einer Partition im NTFS-Format.	Dies ist eine bekannte Einschränkung unter Windows XP Home. Für dieses Problem gibt es keine Lösung.

Fehlerbehebungsinformationen zum ThinkPad

Im folgenden Abschnitt finden Sie Informationen, die Ihnen bei der Behebung von Fehlern bei der Verwendung von Client Security auf ThinkPads weiterhelfen können.

Fehlersymptom	**Mögliche Lösung**
Beim Versuch, eine Administratorfunktion von Client Security aufzurufen, wird eine Fehlernachricht angezeigt.	**Maßnahme**
Nach dem Versuch, eine Administratorfunktion von Client Security aufzurufen, wird eine Fehlernachricht angezeigt.	Das ThinkPad-Administratorkennwort muss inaktiviert sein, damit Sie bestimmte Administratorfunktionen von Client Security ausführen können. Gehen Sie wie folgt vor, um das Administratorkennwort zu inaktivieren: 1. Rufen Sie mit ″F1″ das Programm ″IBM BIOS Setup Utility″ auf. 2. Geben Sie das aktuelle Administratorkennwort ein. 3. Geben Sie ein leeres neues Administratorkennwort ein, und bestätigen Sie das leere Kennwort. 4. Drücken Sie die Eingabetaste. 5. Drücken Sie die Taste F10, um die Einstellungen zu speichern und das Programm zu beenden.
Ein anderer UVM-Sensor für Fingerabdrücke funktioniert nicht ordnungsgemäß.	**Maßnahme**
Der IBM ThinkPad unterstützt den Wechsel zwischen mehreren UVM-Sensoren für Fingerabdrücke nicht.	Wechseln Sie die Modelle der Sensoren für Fingerabdrücke nicht. Verwenden Sie bei der Arbeit von einem fernen Standort aus stets das gleiche Modell wie bei der Arbeit an einer Andockstation.

Fehlerbehebungsinformationen zu Microsoft-Anwendungen und -Betriebssystemen

Die folgenden Fehlerbehebungstabellen enthalten Informationen zur Fehlerbehebung bei der Verwendung von Client Security mit Microsoft-Anwendungen oder -Betriebssystemen.

Fehlersymptom	**Mögliche Lösung**
Bildschirmschoner wird nur auf lokaler Anzeige angezeigt	**Maßnahme**
Bei Verwendung des erweiterten Windows-Desktops wird der Client Security-Bildschirmschoner nur auf der lokalen Anzeige angezeigt, obwohl der Zugriff auf das System und die Tastatur geschützt wird.	Wenn sensible Informationen angezeigt werden, verkleinern Sie die Fenster auf Ihrem erweiterten Desktop auf Symbolgröße, bevor Sie den Client Security-Bildschirmschoner aufrufen.
Client Security funktioniert für einen in UVM registrierten Benutzer nicht ordnungsgemäß.	**Maßnahme**
Der registrierte Clientbenutzer hat möglicherweise seinen Windows-Benutzernamen geändert. Wenn dies zutrifft, geht die gesamte Funktionalität von Client Security verloren.	Registrieren Sie den neuen Benutzernamen in UVM erneut, und fordern Sie alle neuen Berechtigungsnachweise an.
Anmerkung: Unter Windows XP werden in UVM registrierte Benutzer, deren Windows-Benutzername zuvor geändert wurde, von UVM nicht erkannt. Diese Einschränkung gilt selbst dann, wenn der Windows-Benutzername vor der Installation von Client Security geändert wurde.	
Fehler beim Lesen verschlüsselter E-Mails mit Outlook Express	**Maßnahme**
Verschlüsselte E-Mails können nicht entschlüsselt werden, da sich die Verschlüsselungsgrade der Webbrowser, die vom Sender und vom Empfänger verwendet werden, unterscheiden.	Überprüfen Sie Folgendes: 1. Der Verschlüsselungsgrad des Webbrowsers beim Sender muss mit dem Verschlüsselungsgrad des Webbrowsers des Empfängers kompatibel sein. 2. Der Verschlüsselungsgrad des Webbrowsers muss mit dem Verschlüsselungsgrad der Firmware von Client Security kompatibel sein.
Fehler bei der Verwendung eines Zertifikats von einer Adresse, der mehrere Zertifikate zugeordnet sind	**Maßnahme**
Outlook Express kann mehrere Zertifikate zu einer einzigen E-Mail-Adresse auflisten, und einige dieser Zertifikate können ungültig werden. Ein Zertifikat wird ungültig, wenn der dem Zertifikat zugeordnete private Schlüssel auf dem integrierten IBM Sicherheits-Subsystem des Sendercomputers, auf dem das Zertifikat generiert wurde, nicht mehr vorhanden ist.	Bitten Sie den Empfänger, sein digitales Zertifikat erneut zu senden; wählen Sie anschließend dieses Zertifikat im Adressbuch von Outlook Express aus.

Fehlersymptom	Mögliche Lösung
Beim Versuch, eine E-Mail digital zu signieren, wird eine Fehlernachricht angezeigt.	**Maßnahme**
Wenn der Verfasser einer E-Mail versucht, eine E-Mail digital zu signieren, jedoch seinem E-Mail-Account noch kein Zertifikat zugeordnet ist, wird eine Fehlernachricht angezeigt.	Verwenden Sie die Sicherheitseinstellungen in Outlook Express, um ein Zertifikat anzugeben, das dem Benutzeraccount zugeordnet werden soll. Weitere Informationen hierzu finden Sie in der Dokumentation zu Outlook Express.
Outlook Express (128 Bit) verschlüsselt E-Mails nur mit dem 3DES-Algorithmus.	**Maßnahme**
Beim Senden verschlüsselter E-Mails zwischen Clients, die Outlook Express mit der 128-Bit-Version von Internet Explorer 4.0 oder 5.0 verwenden, kann nur der 3DES-Algorithmus verwendet werden.	Aktuelle Informationen zu den Verschlüsselungsalgorithmen, die mit Outlook Express verwendet werden, erhalten Sie bei Microsoft.
Outlook Express-Clients senden E-Mails mit einem anderen Algorithmus zurück.	**Maßnahme**
Eine mit dem RC2(40)-, RC2(64)- oder RC2(128)-Algorithmus verschlüsselte E-Mail wird von einem Client mit Netscape Messenger an einen Client mit Outlook Express (128 Bit) gesendet. Eine vom Outlook Express-Client zurückgesendete E-Mail wird mit dem Algorithmus RC2(40) verschlüsselt.	Es ist keine Maßnahme erforderlich. Eine Verschlüsselungsanforderung gemäß RC2(40), RC2(64) oder RC2(128) von einem Netscape-Client an einen Outlook Express-Client (128 Bit) wird an den Netscape-Client immer mit dem RC2(40)-Algorithmus zurückgesendet. Aktuelle Informationen zu den Verschlüsselungsalgorithmen, die mit den verschiedenen Versionen von Outlook Express verwendet werden, erhalten Sie von Microsoft.
Bei der Verwendung eines Zertifikats in Outlook Express wird nach dem Ausfall eines Festplattenlaufwerks eine Fehlernachricht angezeigt.	**Maßnahme**
Zertifikate können im Administratordienstprogramm mit der Wiederherstellungsfunktion für Schlüssel wiederhergestellt werden. Möglicherweise sind einige Zertifikate, wie z. B. die kostenfreien Zertifikate von VeriSign, nach einer Schlüsselwiederherstellung nicht wiederhergestellt.	Führen Sie nach der Wiederherstellung der Schlüssel einen der folgenden Schritte aus: • Fordern Sie neue Zertifikate an. • Registrieren Sie die Zertifizierungsinstanz erneut in Outlook Express.
Outlook Express aktualisiert den dem Zertifikat zugeordneten Verschlüsselungsgrad nicht.	**Maßnahme**
Wenn ein Sender den Verschlüsselungsgrad in Netscape auswählt und eine signierte E-Mail an einen Outlook Express-Client mit Internet Explorer 4.0 (128 Bit) sendet, stimmt möglicherweise der Verschlüsselungsgrad der zurückgesendeten E-Mail nicht überein.	Löschen Sie das zugeordnete Zertifikat aus dem Adressbuch von Outlook Express. Öffnen Sie die signierte E-Mail erneut, und fügen Sie dem Adressbuch von Outlook Express das Zertifikat hinzu.

Fehlersymptom	Mögliche Lösung
In Outlook Express wird eine Nachricht über Entschlüsselungsfehler angezeigt.	**Maßnahme**
Sie können in Outlook Express eine Nachricht öffnen, indem Sie doppelt darauf klicken. Wenn Sie zu schnell auf eine verschlüsselte Nachricht klicken, wird in einigen Fällen eine Nachricht über Entschlüsselungsfehler angezeigt.	Schließen Sie die Nachricht, und öffnen Sie die verschlüsselte E-Mail erneut.
Darüber hinaus wird möglicherweise in der Voranzeige eine Fehlernachricht angezeigt, wenn Sie eine verschlüsselte Nachricht auswählen.	Wenn in der Voranzeige eine Fehlernachricht angezeigt wird, ist keine Maßnahme erforderlich.
Wenn Sie bei verschlüsselten E-Mails zwei Mal auf die Schaltfläche "Senden" klicken, wird eine Fehlernachricht angezeigt.	**Maßnahme**
Wenn Sie in Outlook Express zweimal auf die Schaltfläche zum Senden klicken, um eine verschlüsselte E-Mail zu senden, wird eine Fehlernachricht darüber angezeigt, dass die Nachricht nicht gesendet werden konnte.	Schließen Sie die Fehlernachricht, und klicken Sie einmal auf die Schaltfläche **Senden**.
Beim Anfordern eines Zertifikats wird eine Fehlernachricht angezeigt.	**Maßnahme**
Bei Verwendung von Internet Explorer erhalten Sie möglicherweise eine Fehlernachricht, wenn Sie ein Zertifikat anfordern, das das CSP-Modul des integrierten IBM Sicherheits-Subsystems verwendet.	Fordern Sie das digitale Zertifikat erneut an.

Fehlerbehebungsinformationen zu Netscape-Anwendungen

Die folgenden Fehlerbehebungstabellen enthalten Informationen zur Fehlerbehebung bei der Verwendung von Client Security mit Netscape-Anwendungen.

Fehlersymptom	Mögliche Lösung
Fehler beim Lesen verschlüsselter E-Mails	**Maßnahme**
Verschlüsselte E-Mails können nicht entschlüsselt werden, da sich die Verschlüsselungsgrade der Webbrowser, die vom Sender und vom Empfänger verwendet werden, unterscheiden.	Überprüfen Sie Folgendes: 1. Der Verschlüsselungsgrad des vom Sender verwendeten Webbrowsers ist mit dem Verschlüsselungsgrad des vom Empfänger verwendeten Webbrowsers kompatibel. 2. Der Verschlüsselungsgrad des Webbrowsers ist mit dem Verschlüsselungsgrad kompatibel, der von der Firmware von Client Security bereitgestellt wird.

Fehlersymptom	Mögliche Lösung
Beim Versuch, eine E-Mail digital zu signieren, wird eine Fehlernachricht angezeigt.	**Maßnahme**
Wenn das Zertifikat des integrierten IBM Sicherheits-Subsystems in Netscape Messenger nicht ausgewählt wurde und der Verfasser der E-Mail versucht, diese mit dem Zertifikat zu signieren, wird eine Fehlernachricht angezeigt.	Verwenden Sie zur Auswahl des Zertifikats die Sicherheitseinstellungen in Netscape Messenger. Wenn Netscape Messenger geöffnet ist, klicken Sie in der Symbolleiste auf das Sicherheitssymbol. Das Fenster mit den Sicherheitsinformationen wird geöffnet. Klicken Sie im linken Teilfenster auf **Netscape Messenger**, und wählen Sie anschließend **Zertifikat des integrierten IBM Security Chips** aus. Weitere Informationen hierzu finden Sie in der Dokumentation von Netscape.
Eine E-Mail wird mit einem anderen Algorithmus an den Client zurückgesendet.	**Maßnahme**
Eine mit dem RC2(40)-, RC2(64)- oder RC2(128)-Algorithmus verschlüsselte E-Mail wird von einem Client mit Netscape Messenger an einen Client mit Outlook Express (128 Bit) gesendet. Eine vom Outlook Express-Client zurückgesendete E-Mail wird mit dem Algorithmus RC2(40) verschlüsselt.	Es ist keine Maßnahme erforderlich. Eine Verschlüsselungsanforderung gemäß RC2(40), RC2(64) oder RC2(128) von einem Netscape-Client an einen Outlook Express-Client (128 Bit) wird an den Netscape-Client immer mit dem RC2(40)-Algorithmus zurückgesendet. Aktuelle Informationen zu den Verschlüsselungsalgorithmen, die mit den verschiedenen Versionen von Outlook Express verwendet werden, erhalten Sie von Microsoft.
Die Verwendung des digitalen Zertifikats, das vom integrierten IBM Sicherheits-Subsystem erstellt wurde, ist nicht möglich	**Maßnahme**
Das vom integrierten IBM Sicherheits-Subsystem generierte digitale Zertifikat ist nicht verfügbar.	Überprüfen Sie, ob Sie beim Öffnen von Netscape den richtigen UVM-Verschlüsselungstext eingegeben haben. Wenn Sie den falschen UVM-Verschlüsselungstext eingeben, wird eine Fehlernachricht über einen Authentifizierungsfehler angezeigt. Wenn Sie auf **OK** klicken, wird Netscape geöffnet, Sie können aber das vom integrierten IBM Sicherheits-Subsystem generierte Zertifikat nicht verwenden. Sie müssen Netscape verlassen und erneut öffnen und anschließend den richtigen UVM-Verschlüsselungstext eingeben.
Neue digitale Zertifikate vom selben Sender werden innerhalb von Netscape nicht ausgetauscht.	**Maßnahme**
Wenn eine digital signierte E-Mail vom selben Sender mehrmals empfangen wird, wird das erste digitale Zertifikat, das der E-Mail zugeordnet ist, nicht überschrieben.	Wenn Sie mehrere E-Mail-Zertifikate empfangen, ist das einzige Zertifikat das Standardzertifikat. Löschen Sie mit den Sicherheitseinrichtungen in Netscape das erste Zertifikat, und öffnen Sie anschließend das zweite Zertifikat erneut, oder bitten Sie den Sender, eine weitere signierte E-Mail zu senden.

Fehlersymptom	Mögliche Lösung
Das Zertifikat des integrierten IBM Sicherheits-Subsystems kann nicht exportiert werden.	**Maßnahme**
Das Zertifikat des integrierten IBM Sicherheits-Subsystems kann in Netscape nicht exportiert werden. Die Exportfunktion in Netscape können Sie zum Sichern von Zertifikaten verwenden.	Rufen Sie das Administratordienstprogramm oder Benutzerkonfigurationsprogramm auf, um das Schlüsselarchiv zu aktualisieren. Wenn Sie das Schlüsselarchiv aktualisieren, werden von allen Zertifikaten, die dem integrierten IBM Sicherheits-Subsystem zugeordnet sind, Kopien erstellt.
Beim Versuch, ein wiederhergestelltes Zertifikat nach dem Ausfall eines Festplattenlaufwerks zu verwenden, wird eine Fehlernachricht angezeigt.	**Maßnahme**
Zertifikate können im Administratordienstprogramm mit der Wiederherstellungsfunktion für Schlüssel wiederhergestellt werden. Möglicherweise sind einige Zertifikate, wie z. B. die kostenfreien Zertifikate von VeriSign, nach einer Schlüsselwiederherstellung nicht wiederhergestellt.	Fordern Sie nach dem Wiederherstellen der Schlüssel ein neues Zertifikat an.
Der Netscape-Agent wird geöffnet und verursacht einen Fehler in Netscape.	**Maßnahme**
Das Öffnen des Netscape-Agenten führt zum Schließen von Netscape.	Schalten Sie den Netscape-Agenten aus.
Netscape wird mit zeitlicher Verzögerung geöffnet.	**Maßnahme**
Wenn Sie das PKCS #11-Modul des integrierten IBM Sicherheits-Subsystems hinzufügen und anschließend Netscape öffnen, verzögert sich das Öffnen von Netscape um kurze Zeit.	Es ist keine Maßnahme erforderlich. Dies dient lediglich zu Ihrer Information.

Fehlerbehebungsinformationen zu digitalen Zertifikaten

Die folgenden Informationen zur Fehlerbehebung können hilfreich sein, wenn bei der Anforderung eines digitalen Zertifikats Fehler auftreten.

Fehlersymptom	**Mögliche Lösung**
Das Fenster "UVM-Verschlüsselungstext" oder das Fenster für die Authentifizierung über Fingerabdrücke wird bei der Anforderung eines digitalen Zertifikats mehrmals angezeigt.	**Maßnahme**
In der UVM-Sicherheitspolicy ist festgelegt, dass ein Benutzer sich mit einem UVM-Verschlüsselungstext oder über Fingerabdrücke authentifizieren muss, bevor er ein digitales Zertifikat erhalten kann. Wenn der Benutzer versucht, ein Zertifikat zu erhalten, wird das Authentifizierungsfenster, in dem er aufgefordert wird, den UVM-Verschlüsselungstext anzugeben oder die Fingerabdrücke abtasten zu lassen, mehrmals angezeigt.	Geben Sie bei jedem Öffnen des Authentifizierungsfensters den UVM-Verschlüsselungstext ein bzw. lassen Sie ihre Fingerabdrücke abtasten.
Eine Nachricht über einen VBScript- oder JavaScript-Fehler wird angezeigt.	**Maßnahme**
Wenn Sie ein digitales Zertifikat anfordern, wird möglicherweise eine Fehlernachricht angezeigt, die sich auf VBScript oder JavaScript bezieht.	Starten Sie den Computer erneut, und beziehen Sie das Zertifikat erneut.

Fehlerbehebungsinformationen zu Tivoli Access Manager

Die folgenden Informationen zur Fehlerbehebung können hilfreich sein, wenn bei der Verwendung von Tivoli Access Manager in Verbindung mit Client Security Fehler auftreten.

Fehlersymptom	**Mögliche Lösung**
Die lokalen Policy-Einstellungen entsprechen nicht denen auf dem Server.	**Maßnahme**
Tivoli Access Manager lässt bestimmte Bit-Konfigurationen zu, die von UVM nicht unterstützt werden. Folglich können lokale Policy-Anforderungen Einstellungen überschreiben, die ein Administrator bei der Konfiguration eines PD-Servers vorgenommen hat.	Dies ist eine bekannte Einschränkung.
Kein Zugriff auf die Konfigurationseinstellungen von Tivoli Access Manager	**Maßnahme**
Im Administratordienstprogramm kann auf der Seite zur Policy-Installation weder auf die Konfigurationseinstellungen von Tivoli Access Manager noch auf die entsprechenden Einstellungen zur lokalen Cache-Einrichtung zugegriffen werden.	Installieren Sie Tivoli Access Manager Runtime Environment. Wenn die Laufzeitumgebung (Runtime Environment) auf dem IBM Client nicht installiert ist, sind auf der Seite zur Policy-Installation auch keine Einstellungen für Tivoli Access Manager verfügbar.
Eine Benutzersteuerung gilt sowohl für den Benutzer als auch für die Gruppe.	**Maßnahme**
Wenn Sie beim Konfigurieren des Tivoli Access Manager-Servers einen Benutzer für eine Gruppe definieren, gilt die Benutzersteuerung sowohl für den Benutzer als auch für die Gruppe, wenn die Option **Traverse-bit** aktiviert wurde.	Es ist keine Maßnahme erforderlich.

Fehlerbehebungsinformationen zu Lotus Notes

Im folgenden Abschnitt finden Sie Informationen, die Ihnen bei der Behebung von Fehlern bei der Verwendung von Lotus Notes mit Client Security weiterhelfen können.

Fehlersymptom	**Mögliche Lösung**
Nach dem Aktivieren des UVM-Schutzes für Lotus Notes kann Lotus Notes die Konfiguration nicht fertig stellen.	**Maßnahme**
Lotus Notes kann nach dem Aktivieren des UVM-Schutzes mit dem Administratordienstprogramm die Konfiguration nicht fertig stellen.	Dies ist eine bekannte Einschränkung. Lotus Notes muss konfiguriert werden und aktiv sein, bevor die Lotus Notes-Unterstützung im Administratordienstprogramm aktiviert wird.
Beim Versuch, das Notes-Kennwort zu ändern, wird eine Fehlernachricht angezeigt.	**Maßnahme**
Wenn Sie das Notes-Kennwort bei Verwendung von Client Security ändern, wird dies in einer Fehlernachricht angezeigt.	Wiederholen Sie die Kennwortänderung. Wurde der Fehler dadurch nicht behoben, starten Sie den Client neu.
Nach dem Festlegen eines Kennworts per Zufallsgenerator wird eine Fehlernachricht angezeigt.	**Maßnahme**
Wenn Sie folgende Vorgänge ausführen, wird möglicherweise eine Fehlernachricht angezeigt: • Verwenden des Tools zur Lotus Notes-Konfiguration zur Einstellung des UVM-Schutzes für eine Notes-ID • Öffnen von Notes und Verwenden der Notes-Funktion zur Kennwortänderung für die Datei mit der Notes-ID • Schließen von Notes sofort nach der Kennwortänderung	Klicken Sie auf **OK**, um die Fehlernachricht zu schließen. Es ist keine weitere Maßnahme erforderlich. Entgegen der Fehlernachricht wurde das Kennwort geändert. Das neue Kennwort wurde von Client Security per Zufallsgenerator festgelegt. Die Datei mit der Notes-ID wird nun mit dem per Zufallsgenerator festgelegten Kennwort verschlüsselt, und der Benutzer benötigt keine neue Benutzer-ID-Datei. Wenn der Endbenutzer das Kennwort erneut ändert, generiert UVM ein neues, per Zufallsgenerator festgelegtes Kennwort für die Notes-ID.

Fehlerbehebungsinformationen zur Verschlüsselung

Im folgenden Abschnitt finden Sie Informationen, die Ihnen bei der Behebung von Fehlern bei der Verschlüsselung von Dateien unter Verwendung von Client Security ab Version 3.0 weiterhelfen können.

Fehlersymptom	**Mögliche Lösung**
Bereits verschlüsselte Dateien werden nicht entschlüsselt.	**Maßnahme**
Dateien, die mit früheren Versionen von Client Security verschlüsselt wurden, werden nach dem Upgrade auf Client Security ab Version 3.0 nicht entschlüsselt.	Dies ist eine bekannte Einschränkung. Sie müssen alle mit früheren Versionen von Client Security verschlüsselten Dateien entschlüsseln, *bevor* Sie Client Security ab Version 3.0 installieren. Client Security 3.0 kann Dateien, die von früheren Versionen von Client Security verschlüsselt wurden, nicht entschlüsseln, da in dieser Version die Implementierung der Dateiverschlüsselung geändert wurde.

Fehlerbehebungsinformationen zu UVM-sensitiven Einheiten

Im folgenden Abschnitt finden Sie Informationen, die Ihnen bei der Behebung von Fehlern bei der Verwendung UVM-sensitiver Einheiten weiterhelfen können.

Fehlersymptom	**Mögliche Lösung**
Eine UVM-sensitive Einheit funktioniert nicht mehr ordnungsgemäß.	**Maßnahme**
Eine UVM-sensitive Sicherheitseinheit, wie z. B. eine Smartcard, ein Kartenlesegerät für Smartcards oder ein Lesegerät für Fingerabdrücke, funktioniert nicht ordnungsgemäß.	Überprüfen Sie, ob die Einheit ordnungsgemäß vom System konfiguriert wurde. Nachdem die Einheit konfiguriert wurde, müssen Sie möglicherweise das System erneut starten, damit der Service richtig ausgeführt wird. Weitere Informationen zur Fehlerbehebung finden Sie auch in der Dokumentation zu der entsprechenden Einheit. Sie können sich auch an die Verkaufsstelle wenden, bei der Sie die Einheit erworben haben.
Eine UVM-sensitive Einheit funktioniert nicht mehr ordnungsgemäß.	**Maßnahme**
Wenn Sie eine UVM-sensitive Einheit vom USB-Anschluss (Universal Serial Bus) trennen und die Einheit danach erneut am USB-Anschluss anschließen, funktioniert die Einheit möglicherweise nicht ordnungsgemäß.	Starten Sie nach dem erneuten Anschluss der Einheit an den USB-Anschluss den Computer erneut.

Anhang A. Informationen zu Kennwörtern und Verschlüsselungstexten

Dieser Anhang enthält Informationen zu Kennwörtern und Verschlüsselungstexten.

Regeln für Kennwörter und Verschlüsselungstexte

Bei einem gesicherten System wird eine Vielzahl verschiedener Kennwörter und Verschlüsselungstexte verwendet. Für die verschiedenen Arten von Kennwörtern gelten unterschiedliche Regeln. Dieser Abschnitt enthält Informationen zum Administratorkennwort und zum UVM-Verschlüsselungstext.

Regeln für Administratorkennwörter

Die Regeln für das Administratorkennwort können nicht von einem Sicherheitsadministrator geändert werden.

Für Administratorkennwörter gelten folgende Regeln:

Länge Das Kennwort muss genau acht Zeichen lang sein.

Zeichen
Das Kennwort darf nur alphanumerische Zeichen enthalten. Die Kombination von Buchstaben und Ziffern ist zulässig. Es sind keine speziellen Zeichen wie das Leerzeichen und die Zeichen !, ?, % zulässig.

Merkmale
Sie können das Administratorkennwort festlegen, um den integrierten IBM Security Chip im Computer zu aktivieren. Dieses Kennwort müssen Sie bei jedem Zugriff auf das Administratordienstprogramm oder die Administratorkonsole eingeben.

Fehlversuche
Wenn Sie das Kennwort zehnmal falsch eingegebenen haben, wird der Computer 1 Stunde und 17 Minuten lang gesperrt. Wenn Sie nach diesem Zeitraum das Kennwort zehn weitere Male falsch eingeben, wird der Computer 2 Stunden und 34 Minuten lang gesperrt. Die Dauer der Computersperrung verdoppelt sich jedes Mal, wenn Sie das Kennwort zehnmal falsch eingeben.

Regeln für UVM-Verschlüsselungstexte

IBM Client Security bietet Sicherheitsadministratoren die Möglichkeit, Regeln für die UVM-Verschlüsselungstexte von Benutzern festzulegen. Die Sicherheit wird dadurch erhöht, dass der UVM-Verschlüsselungstext länger und eindeutiger ist als ein herkömmliches Kennwort. Die Policy für den UVM-Verschlüsselungstext wird über das Administratordienstprogramm gesteuert.

Das Fenster ″Policy für UVM-Verschlüsselungstext″ des Administratordienstprogramms stellt Sicherheitsadministratoren eine einfache Schnittstelle zur Steuerung von Kriterien für Verschlüsselungstexte bereit. Über das Fenster ″Policy für UVM-Verschlüsselungstext″ kann der Administrator folgende Regeln für Verschlüsselungstexte festlegen:

Anmerkung: Die Standardeinstellung für jedes Kriterium ist unten in Klammern angegeben.

- ob eine Mindestanzahl an alphanumerischen Zeichen festgelegt werden soll (ja, 6)

  Wenn z. B. der Wert ″6″ festgelegt ist, ist der Verschlüsselungstext `1234567xxx` ungültig.
- ob eine Mindestanzahl an Ziffern festgelegt werden soll (ja, 1)

  Wenn z. B. der Wert ″1″ festgelegt ist, ist der Verschlüsselungstext `thisismypassword` ungültig.
- ob eine Mindestanzahl an Leerzeichen festgelegt werden soll (keine Mindestanzahl)

  Wenn z. B. der Wert ″2″ festgelegt ist, ist der Verschlüsselungstext `i am not here` ungültig.
- ob der Verschlüsselungstext mit einer Ziffer beginnen darf (nein)

  Standardmäßig ist z. B. der Verschlüsselungstext `1password` ungültig.
- ob der Verschlüsselungstext mit einer Ziffer enden darf (nein)

  Standardmäßig ist z. B. der Verschlüsselungstext `password8` ungültig.
- ob der Verschlüsselungstext eine Benutzer-ID enthalten darf (nein)

  Standardmäßig ist z. B. der Verschlüsselungstext `Benutzername` ungültig, wobei es sich bei `Benutzername` um eine Benutzer-ID handelt.
- ob der neue Verschlüsselungstext sich von den letzten x Verschlüsselungstexten unterscheiden muss (ja, 3)

  Standardmäßig ist z. B. der Verschlüsselungstext `mypassword` ungültig, wenn einer der drei vorherigen Verschlüsselungstexte `mypassword` war.
- ob der Verschlüsselungstext mehr als drei identische aufeinander folgende Zeichen des letzten Kennworts enthalten darf (nein)

  Standardmäßig ist z. B. der Verschlüsselungstext `password` ungültig, wenn einer der drei vorherigen Verschlüsselungstexte `pass` oder `word` war.

Das Fenster ″Policy für UVM-Verschlüsselungstext″ des Administratordienstprogramms ermöglicht Sicherheitsadministratoren zudem eine Steuerung des Ablaufs der Verschlüsselungstexte. Über das Fenster ″Policy für UVM-Verschlüsselungstext″ kann der Administrator aus den folgenden Regeln für Verschlüsselungstexte auswählen:

- Verschlüsselungstext ist nicht mehr gültig nach (ja, 184).

  In diesem Beispiel läuft der Verschlüsselungstext standardmäßig nach 184 Tagen ab. Der neue Verschlüsselungstext muss der vorhandenen Policy für den Verschlüsselungstext entsprechen.
- Verschlüsselungstext läuft ab (ja).

  Wenn diese Option ausgewählt ist, läuft der Verschlüsselungstext nie ab.

Die Policy für den Verschlüsselungstext wird vom Administratordienstprogramm bei der Registrierung des Benutzers und bei der Änderung des Verschlüsselungstextes durch den Benutzer über das Clientdienstprogramm überprüft. Die beiden Benutzereinstellungen zum vorherigen Kennwort werden zurückgesetzt, und Protokolle zum Verschlüsselungstext werden entfernt.

Folgende allgemeine Regeln gelten für UVM-Verschlüsselungstexte:

Länge Der Verschlüsselungstext kann bis zu 256 Zeichen lang sein.

Zeichen

Der Verschlüsselungstext kann jede beliebige Kombination von Zeichen enthalten, die die Tastatur erzeugt, einschließlich Leerzeichen und nicht alphanumerische Zeichen.

Merkmale

Der UVM-Verschlüsselungstext unterscheidet sich von einem Kennwort, das Sie zur Anmeldung am Betriebssystem verwenden können. Der UVM-Verschlüsselungstext kann in Verbindung mit anderen Authentifizierungseinheiten verwendet werden, z. B. mit einem UVM-Sensor für Fingerabdrücke.

Fehlversuche

Wenn der UVM-Verschlüsselungstext mehrere Male während einer Sitzung falsch eingegeben wird, führt der Computer eine Reihe entsprechender Verzögerungsaktionen (eine so genannte Anti-Hammering-Verzögerung) durch. Diese Aktionen werden im folgenden Abschnitt beschrieben.

Anzahl der Fehlversuche auf TCPA-Systemen und anderen Systemen

In der folgenden Tabelle sind die Einstellungen für die Verzögerungsaktionen in einem TCPA-System dargestellt:

Versuche	Verzögerung beim nächsten Fehlversuch
15	1,1 Minuten
31	2,2 Minuten
47	4,4 Minuten
63	8,8 Minuten
79	17,6 Minuten
95	35,2 Minuten
111	1,2 Stunden
127	2,3 Stunden
143	4,7 Stunden

Auf TCPA-Systemen findet keine Unterscheidung zwischen Benutzerverschlüsselungstexten und Administratorkennwort statt. Alle Authentifizierungsmethoden unter Verwendung des integrierten IBM Security Chips richten sich nach derselben Policy. Die maximale Zeitsperre beträgt 4,7 Stunden. TCPA-Systeme führen keine Verzögerungsaktionen durch, die länger als 4,7 Stunden dauern.

Bei anderen Systemen findet eine Unterscheidung zwischen Administratorkennwort und Benutzerverschlüsselungstexten statt. Auf diesen Systemen wird für das Administratorkennwort nach 10 fehlgeschlagenen Versuchen eine Verzögerungsaktion von 77 Minuten ausgeführt. Für Benutzerkennwörter gilt nur eine einminütige Verzögerung nach 32 fehlgeschlagenen Versuchen. Nach weiteren 32 fehlgeschlagenen Versuchen wird die Sperrzeit jeweils verdoppelt.

Verschlüsselungstext zurücksetzen

Wenn ein Benutzer seinen Verschlüsselungstext vergisst, kann der Administrator den Benutzer dazu berechtigen, seinen Verschlüsselungstext zurückzusetzen.

Verschlüsselungstext über Remotezugriff zurücksetzen

Gehen Sie wie folgt vor, um ein Kennwort über Remotezugriff zurückzusetzen:

- **Administrator**

  Ein Administrator sollte über Remotezugriff wie folgt vorgehen:

  1. Erstellen Sie ein neues Kennwort zur einmaligen Verwendung für den Benutzer, und teilen Sie es dem Benutzer mit.
  2. Senden Sie eine Datendatei an den Benutzer.

     Sie können dem Benutzer diese Datendatei per E-Mail senden, auf einen austauschbaren Datenträger (wie z. B. eine Diskette) kopieren oder sie direkt in die Archivdatei des Benutzers schreiben (vorausgesetzt, der Benutzer verfügt über einen Zugriff auf dieses System). Diese verschlüsselte Datei ist zum Abgleich mit dem neuen Kennwort für eine einmalige Verwendung erforderlich.

- **Benutzer**

  Der Benutzer muss wie folgt vorgehen:

  1. Melden Sie sich auf dem Computer an.
  2. Wenn die Aufforderung zur Eingabe eines Verschlüsselungstextes angezeigt wird, aktivieren Sie das Markierungsfeld "Verschlüsselungstext vergessen".
  3. Geben Sie das Kennwort ein, das Ihnen der Administrator zur einmaligen Verwendung mitgeteilt hat, und geben Sie die Position der Datei an, die Sie vom Administrator erhalten haben.

     Nachdem UVM bestätigt hat, dass die Informationen in der Datei mit dem eingegebenen Kennwort übereinstimmen, erhält der Benutzer die Zugriffsberechtigung. Der Benutzer wird daraufhin sofort aufgefordert, seinen Verschlüsselungstext zu ändern.

Hierbei handelt es sich um die empfohlene Vorgehensweise zum Zurücksetzen eines verloren gegangenen Verschlüsselungstextes.

Verschlüsselungstext manuell zurücksetzen

Wenn der Administrator den Arbeitsplatz des Benutzers, der seinen Verschlüsselungstext vergessen hat, auf einfache Weise erreichen kann, kann er sich am System des Benutzers als Administrator anmelden, den privaten Administratorschlüssel im Administratordienstprogramm angeben und den Verschlüsselungstext des Benutzers manuell ändern. Zum Ändern des Verschlüsselungstextes ist es nicht erforderlich, dass der Administrator den alten Verschlüsselungstext des Benutzers kennt.

Anhang B. Regeln für den UVM-Schutz für die Anmeldung am System

Mit dem UVM-Schutz wird sichergestellt, dass nur Benutzer, die in UVM für einen bestimmten IBM Client hinzugefügt wurden, auf das Betriebssystem zugreifen können. Windows-Betriebssysteme umfassen Anwendungen, die einen Anmeldeschutz bieten. Auch wenn UVM-Schutz parallel mit diesen Windows-Anmeldeanwendungen verwendet werden kann, funktioniert er je nach Betriebssystem etwas anders.

Die UVM-Anmeldeschnittstelle ersetzt die Anmeldung am Betriebssystem, so dass immer wenn sich ein Benutzer am System anmelden möchte, das UVM-Anmeldefenster angezeigt wird.

Lesen Sie die folgenden Hinweise, bevor Sie den UVM-Anmeldeschutz für das System konfigurieren und verwenden:

- Löschen Sie den Inhalt des integrierten IBM Security Chips nicht bei aktiviertem UVM-Schutz. Andernfalls wird der Inhalt der Festplatte unbrauchbar, und Sie müssen die Festplatte neu formatieren und die gesamte Software neu installieren.
- Wenn Sie im Administratordienstprogramm das Markierungsfeld **Die Windows-Standardanmeldung durch eine gesicherte UVM-Anmeldung ersetzen** inaktivieren, kehrt das System zum Windows-Anmeldungsprozess zurück, ohne die gesicherte UVM-Anmeldung zu verwenden.
- Sie haben die Option, die maximale Anzahl der Versuche für die Eingabe des richtigen Kennworts für die Windows-Anmeldeanwendung anzugeben. Diese Option steht bei UVM-Anmeldeschutz *nicht* zur Verfügung. Für die Anzahl der zulässigen Fehlversuche bei der Eingabe des UVM-Verschlüsselungstextes können Sie keine Grenze festlegen.

Anhang C. Bemerkungen und Marken

Dieser Anhang enthält rechtliche Hinweise zu IBM Produkten und Informationen zu Marken.

Bemerkungen

Die vorliegenden Informationen wurden für Produkte und Services entwickelt, die auf dem deutschen Markt angeboten werden.

Möglicherweise bietet IBM die in diesem Dokument beschriebenen Produkte, Services oder Funktionen in anderen Ländern nicht an. Informationen über die gegenwärtig im jeweiligen Land verfügbaren Produkte und Services sind beim IBM Ansprechpartner erhältlich. Hinweise auf IBM Lizenzprogramme oder andere IBM Produkte bedeuten nicht, dass nur Programme, Produkte oder Dienstleistungen von IBM verwendet werden können. Anstelle der Produkte, Programme oder Dienstleistungen können auch andere, ihnen äquivalente Produkte, Programme oder Dienstleistungen verwendet werden, solange diese keine gewerblichen oder andere Schutzrechte von IBM verletzen. Die Verantwortung für den Betrieb von Fremdprodukten, Fremdprogrammen und Fremddienstleistungen liegt beim Kunden.

Für in diesen Dokument beschriebene Erzeugnisse und Verfahren kann es IBM Patente oder IBM Patentanmeldungen geben. Mit der Auslieferung dieses Handbuchs ist keine Lizenzierung dieser Patente verbunden. Lizenzanfragen sind schriftlich an folgende Adresse zu richten (Anfragen an diese Adresse müssen auf Englisch formuliert werden):

IBM Europe
Director of Licensing
92066 Paris
La Defense Cedex
France

Trotz sorgfältiger Bearbeitung können technische Ungenauigkeiten oder Druckfehler in dieser Veröffentlichung nicht ausgeschlossen werden. Die Angaben in diesem Handbuch werden in regelmäßigen Zeitabständen aktualisiert. Die Änderungen werden in Überarbeitungen oder in Technical News Letters (TNLs) bekannt gegeben. IBM kann jederzeit ohne Vorankündigung Verbesserungen und/oder Änderungen an den in dieser Veröffentlichung beschriebenen Produkten und/oder Programmen vornehmen.

Lizenznehmer des Programms, die Informationen zu diesem Produkt wünschen mit der Zielsetzung: (i) den Austausch von Informationen zwischen unabhängigen, erstellten Programmen und anderen Programmen (einschließlich des vorliegenden Programms) sowie (ii) die gemeinsame Nutzung der ausgetauschten Informationen zu ermöglichen, wenden sich an folgende Adresse: IBM Corporation, Department 80D, P.O. Box 12195, 3039 Cornwallis, Research Triangle Park, NC 27709, U.S.A. Die Bereitstellung dieser Informationen kann unter Umständen von bestimmten Bedingungen - in einigen Fällen auch von der Zahlung einer Gebühr - abhängig sein.

Die Lieferung des in diesem Dokument aufgeführten Lizenzprogramms sowie des zugehörigen Lizenzmaterials erfolgt im Rahmen der Allgemeinen Geschäftsbedingungen der IBM, der Internationalen Nutzungsbedingungen der IBM für Programmpakete oder einer äquivalenten Vereinbarung.

Marken

IBM und SecureWay sind in gewissen Ländern Marken der IBM Corporation.

Tivoli ist in gewissen Ländern eine Marke von Tivoli Systems Inc.

Microsoft, Windows und Windows NT sind in gewissen Ländern Marken der Microsoft Corporation.

Andere Namen von Unternehmen, Produkten und Dienstleistungen können Marken oder Dienstleistungsmarken anderer Unternehmen sein.