IBM Client Security Solutions

Client Security Version 5.4 Installationshandbuch

IBM Client Security Solutions

Client Security Version 5.4 Installationshandbuch

Anmerkung:

- 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 (Oktober 2004)

Diese Veröffentlichung ist eine Übersetzung des Handbuchs
IBM Client Security Solutions Version 5.4 Installation Guide,
herausgegeben von International Business Machines Corporation, USA

Herausgegeben von:
SW TSC Germany
Kst. 2877
Oktober 2004

Inhaltsverzeichnis

Vorwort

Dieser Abschnitt enthält Hinweise zur Verwendung dieses Handbuchs.

Inhalt dieses Handbuchs

Das vorliegende Handbuch enthält Informationen zum Einsatz von IBM Client Security auf IBM Netzwerkcomputern bzw. IBM Clients, auf denen das integrierte IBM Sicherheits-Subsystem (IBM Embedded Security Subsystem) installiert ist. Außerdem finden Sie in diesem Handbuch Anweisungen zum Aktivieren des integrierten IBM Sicherheits-Subsystems sowie zum Festlegen des Administratorkennworts für das Sicherheits-Subsystem.

Das Handbuch umfasst folgende Inhalte:

Kapitel 1, „Einführung", enthält eine kurze Übersicht über grundlegende Sicherheitskonzepte, eine Übersicht über die in der Software enthaltenen Anwendungen und Komponenten sowie eine Beschreibung der PKI-Funkionen (Public Key Infrastructure).

Kapitel 2, „Erste Schritte", enthält Voraussetzungen für die Installation von Computerhardware und -software sowie Anweisungen zum Herunterladen der Software

Kapitel 3, „Vorbereitung der Softwareinstallation", enthält Anweisungen zu Voraussetzungen für die Installation von IBM Client Security.

Kapitel 4, „Software herunterladen, installieren und konfigurieren", enthält Anweisungen zum Installieren, Aktualisieren und Deinstallieren der Software.

Kapitel 5, „Fehlerbehebung", enthält nützliche Informationen zur Fehlerbehebung, die beim Befolgen der in diesem Handbuch enthaltenen Anweisungen auftreten können.

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

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

Zielgruppe

Dieses Handbuch ist für Netzwerk- und Systemadministratoren konzipiert, die für die Personal-Computing-Sicherheit auf IBM Clients sorgen. Vorausgesetzt werden Kenntnisse auf dem Gebiet der Sicherheitskonzepte, wie z. B. in PKI (Public Key Infrastructure) und in der Verwaltung von digitalen Zertifikaten in einer Netzwerkumgebung.

Benutzung des Handbuchs

Verwenden Sie dieses Handbuch, um die Personal-Computing-Sicherheit auf IBM Clients zu installieren und einzurichten. Dieses Handbuch dient als Ergänzung zum *Client Security Administrator- und Benutzerhandbuch*.

Dieses Handbuch und die gesamte weitere 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 Administrator- und Benutzerhandbuch*

Dieses Handbuch enthält Verweise auf das *Client Security Administrator- und Benutzerhandbuch*. Das *Administrator- und Benutzerhandbuch* umfasst Informationen zur Verwendung von User Verification Manager (UVM) und zum Arbeiten mit der UVM-Policy sowie Informationen zur Verwendung des Administratordienstprogramms und des Benutzerkonfigurationsprogramm.

Befolgen Sie nach der Installation der Software die Anweisungen im *Administrator- und Benutzerhandbuch* zum Einrichten und Verwalten der Sicherheitspolicy für die einzelnen Clients.

Zusätzliche Informationen

Zusätzliche Informationen sowie aktualisierte Fassungen der Sicherheitsprodukte erhalten Sie, sofern verfügbar, auf der IBM Website unter http://www.pc.ibm.com/us/security/index.html.

Kapitel 1. Einführung

Bestimmte ThinkPad™- und ThinkCentre™-Computer sind mit integrierter Verschlüsselungshardware ausgestattet, die mit für den Download verfügbaren Softwaretechnologien arbeitet und einen leistungsfähigen Schutz für Client-PC-Plattformen bietet. In der Gesamtheit wird diese Hardware und Software als das integrierte IBM Sicherheits-Subsystem oder abgekürzt als ESS (Embedded Security Subsystem) bezeichnet. Bei der Hardwarekomponente handelt es sich um den integrierten IBM Security Chip, bei der Softwarekomponente um IBM Client Security (abgekürzt CSS - Client Security Software).

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. Diese Software umfasst Anwendungen und Komponenten, die es IBM Clientsystemen ermöglichen, die Client-Sicherheitsfunktionen in einem lokalen Netzwerk, in einem Unternehmen oder im Internet zu nutzen.

IBM ESS

IBM ESS, das integrierte IBM Sicherheits-Subsystem, unterstützt Schlüsselverwaltungslösungen, wie z. B. die PKI-Infrastruktur, und besteht aus den folgenden lokalen Anwendungen:

- Verschlüsselung von Dateien und Ordnern (FFE - File and Folder Encryption)
- Password Manager
- Gesicherte Windows-Anmeldung
- Mehreren konfigurierbaren Authentifizierungsmethoden, wie z. B.:
  - Verschlüsselungstext
  - Fingerabdruck
  - Smartcard

Um die Funktionen von IBM ESS effizient nutzen zu können, muss der Sicherheitsadministrator mit einigen grundlegenden Konzepten vertraut sein. In den folgenden Abschnitten werden grundlegende Sicherheitskonzepte beschrieben.

Integrierter IBM Security Chip

Beim integrierten IBM Sicherheits-Subsystem (IBM Embedded Security Subsystem) handelt es sich um die integrierte Verschlüsselungshardware-Technologie, die eine zusätzliche Schutzebene für ausgewählte IBM PC-Plattformen bietet. Durch die Einführung dieses Sicherheits-Subsystems werden Verschlüsselungs- und Authentifizierungsprozesse von der Software, die relativ fehleranfällig ist, auf die sichere Umgebung einer dedizierten Hardware übertragen. So wird die Sicherheit deutlich erhöht.

Das integrierte IBM Sicherheits-Subsystem unterstützt folgende Funktionen:

- RSA3-PKI-Vorgänge, wie z. B. Verschlüsselung aus Datenschutzgründen sowie digitale Unterschriften zur Authentifizierung
- RSA-Schlüsselerstellung
- Erstellung von Zufallszahlen

- Berechnung von RSA-Funktionen in 200 Millisekunden
- EEPROM-Speicher für RSA-Schlüsselpaarspeicherung
- Alle TCG-Funktionen (Trusted Computing Group), die in der TCG-Hauptspezifikation Version 1.1 definiert sind
- Kommunikation mit dem Hauptprozessor über den LPC-Bus (LPC - Low Pin Count)

IBM Client Security

IBM Client Security beinhaltet folgende Softwareanwendungen und Komponenten:

- **Administratordienstprogramm:** Das Administratordienstprogramm ist die Schnittstelle, die vom Administrator zum Aktivieren oder Inaktivieren des integrierten IBM Sicherheits-Subsystems sowie zum Erstellen, Archivieren und Neugenerieren von Chiffrierschlüsseln und Verschlüsselungstexten verwendet wird. Außerdem kann ein Administrator in diesem Dienstprogramm Benutzer in die von Client Security bereitgestellte Sicherheitspolicy aufnehmen.
- **Administratorkonsole:** Die Administratorkonsole von Client Security ermöglicht es einem Administrator, ein Netzwerk mit standortunabhängigem Zugriff mit Berechtigungsnachweis zu konfigurieren, Dateien zu erstellen und zu konfigurieren, die Implementierung ermöglichen, und eine Konfiguration und ein Konfigurations- und Wiederherstellungsprofil ohne Administratorberechtigung zu erstellen.
- **Benutzerkonfigurationsprogramm:** Das Benutzerkonfigurationsprogramm ermöglicht es Clientbenutzern, den UVM-Verschlüsselungstext zu ändern, Windows-Anmeldekennwörter für die Erkennung durch UVM zu aktivieren, Schlüsselarchive zu aktualisieren sowie Fingerabdrücke zu registrieren. Außerdem kann ein Benutzer Sicherungskopien der digitalen Zertifikate erstellen, die vom integrierten IBM Sicherheits-Subsystem erzeugt wurden.
- **User Verification Manager (UVM):** Client Security verwendet UVM, um Verschlüsselungstexte und andere Elemente zur Authentifizierung von Systembenutzern zu verwalten. So kann z. B. ein Lesegerät für Fingerabdrücke von UVM für die Anmeldungsauthentifizierung verwendet werden. Client Security unterstützt die folgenden Funktionen:
  - **UVM-Client-Policy-Schutz:** Client Security ermöglicht es Sicherheitsadministratoren, die Client-Sicherheitspolicy einzurichten, die festlegt, wie ein Clientbenutzer auf dem System authentifiziert wird.

    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 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-Schutz bei der Anmeldung am System:** Client Security ermöglicht es Administratoren, den Zugriff auf Computer über eine Anmeldeschnittstelle zu steuern. Der UVM-Schutz stellt sicher, dass nur Benutzer, die von der Sicherheitspolicy erkannt werden, auf das Betriebssystem zugreifen können.

Beziehung zwischen Kennwörtern und Schlüsseln

Kennwörter und Schlüssel dienen, zusammen mit weiteren optionalen Authentifizierungsgeräten, zur Prüfung der Identität von Systembenutzern. Zum Verständnis der Funktionsweise von IBM Client Security ist es entscheidend, die Beziehung zwischen Kennwörtern und Schlüsseln zu verstehen.

Administratorkennwort

Das Administratorkennwort wird zur Authentifizierung des Administrators beim integrierten IBM Sicherheits-Subsystem verwendet. Dieses Kennwort wird innerhalb der sicheren Hardware des integrierten IBM Sicherheits-Subsystems verwaltet und authentifiziert. Wenn es authentifiziert ist, kann der Administrator folgende Aktionen ausführen:

- Benutzer registrieren
- Die Policy-Schnittstelle starten
- Das Administratorkennwort ändern

Das Administratorkennwort kann auf eine der folgenden Arten definiert werden:

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

Es ist wichtig, zum Erstellen und Verwalten des Administratorkennworts nach einer Strategie vorzugehen. Das Administratorkennwort kann geändert werden, wenn es beschädigt oder vergessen wurde.

Im Vergleich mit TCG-Begriffen und TCG-Terminologie entspricht das Administratorkennwort dem OAV (Owner Authorization Value). Da das Administratorkennwort mit dem integrierten IBM Sicherheits-Subsystem verknüpft ist, wird es manchmal auch als das *Hardwarekennwort* bezeichnet.

Öffentlicher und privater Hardwareschlüssel

Grundsätzlich kann zum integrierten IBM Sicherheits-Subsystem gesagt werden, dass es als *Root of Trust* auf einem Clientsystem fungiert. Diese ″Root″ wird zum Sichern anderer Anwendungen und Funktionen verwendet. Zum Aufbauen einer ″Root of Trust″ ist das Erstellen eines öffentlichen Hardwareschlüssels und eines privaten Hardwareschlüssels erforderlich. Ein öffentlicher und ein privater Schlüssel, die als *Schlüsselpaar* bezeichnet werden, stehen in folgender mathematischer Beziehung zueinander:

- alle mit dem öffentlichen Schlüssel verschlüsselten Daten nur durch den entsprechenden privaten Schlüssel entschlüsselt werden können und
- alle mit dem privaten Schlüssel verschlüsselten Daten nur durch den entsprechenden öffentlichen Schlüssel entschlüsselt werden können.

Der private Hardwareschlüssel wird innerhalb der sicheren Hardware des Sicherheits-Subsystems erstellt, gespeichert und verwendet. Der öffentliche Hardwareschlüssel steht zu verschiedenen Zwecken zur Verfügung (daher die Bezeichnung ″öffentlicher Schlüssel″); er wird jedoch nie außerhalb der gesicherten Hardware des Sicherheits-Subsystems verwendet. Der öffentliche und der private Hardwareschlüssel sind ein kritischer Teil der IBM Schlüsselauslagerungshierarchie, die in einem der folgenden Abschnitte behandelt wird.

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

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

In Begriffen und in der Terminologie von TCG (Trusted Computing Group) ausgedrückt würden der öffentliche und der private Hardwareschlüssel als *Storage Root Key* (SRK) bezeichnet.

Öffentlicher und privater Administratorschlüssel

Der öffentliche und der private Administratorschlüssel sind integraler Bestandteil der IBM Schlüsselauslagerungshierarchie. Sie ermöglichen es, dass benutzerspezifische Daten bei einem Ausfall der Systemplatine oder des Festplattenlaufwerks gesichert und wiederhergestellt werden können.

Der öffentliche und der private Administratorschlüssel können entweder auf jedem System eindeutig oder für alle Systeme oder Systemgruppen gleich sein. Es ist wichtig zu beachten, dass diese Administratorschlüssel verwaltet werden müssen und dass das Vorhandensein einer Strategie der Verwendung eindeutiger bzw. bekannter Schlüssel entscheidend ist.

Öffentliche und private Schlüssel 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 von öffentlichen und privaten Administratorschlüsseln können benutzerspezifische Daten bei einem Ausfall der Systemplatine oder des Festplattenlaufwerks gesichert und wiederhergestellt werden.

Öffentliche und private Benutzerschlüssel

Das integrierte IBM Sicherheits-Subsystem erstellt öffentliche und private Benutzerschlüssel, um die benutzerspezifischen Daten zu sichern. Diese Schlüsselpaare werden bei der Registrierung eines Benutzers bei IBM Client Security erstellt. Diese Schlüssel werden transparent von der UVM-Komponente (User Verification Manager) von IBM Client Security erstellt und verwaltet. Die Schlüssel werden basierend darauf verwaltet, welcher Windows-Benutzer am Betriebssystem angemeldet ist.

IBM Schlüsselauslagerungshierarchie

Ein wesentlicher Bestandteil der Architektur des integrierten IBM Sicherheits-Subsystems ist die IBM Schlüsselauslagerungshierarchie. Die Basis (oder ″Root″) der IBM Schlüsselauslagerungshierarchie sind der öffentliche und der private Hardwareschlüssel. Der öffentliche und der private Hardwareschlüssel, als *Hardwareschlüsselpaar* bezeichnet, werden von IBM Client Security erstellt und sind auf jedem Client statistisch eindeutig.

Die nächste “Ebene” der Schlüsselhierarchie (über der Basis- oder Rootebene) sind der öffentliche und der private Administratorschlüssel bzw. das *Administratorschlüsselpaar*. Das Administratorschlüsselpaar kann auf jeder Maschine eindeutig sein, oder es kann auf allen Clients oder auf einer Untergruppe von Clients dasselbe sein. Die Verwaltung dieses Schlüsselpaares hängt davon ab, wie Sie Ihr Netzwerk verwalten möchten. Der private Administratorschlüssel ist insofern eindeutig, als er auf dem Clientsystem (durch den öffentlichen Hardwareschlüssel geschützt) an einer vom Administrator definierten Adresse gespeichert ist.

IBM Client Security registriert Windows-Benutzer in der Umgebung des integrierten IBM Sicherheits-Subsystems. Wird ein Benutzer registriert, werden öffentliche und private Benutzerschlüssel (das *Benutzerschlüsselpaar*) erstellt und eine neue "Schlüsselebene" wird erstellt. Der private Benutzerschlüssel wird mit dem öffentlichen Administratorschlüssel verschlüsselt. Der private Administratorschlüssel wird mit dem öffentlichen Hardwareschlüssel verschlüsselt. Daher muss zum Verwenden des privaten Benutzerschlüssels der private Administratorschlüssel (der mit dem öffentlichen Hardwareschlüssel verschlüsselt ist) in das Sicherheits-Subsystem geladen werden. Ist er in den Chip geladen, entschlüsselt der private Hardwareschlüssel den privaten Administratorschlüssel. Der private Administratorschlüssel ist nun für die Verwendung im Sicherheits-Subsystem bereit, so dass Daten, die mit dem entsprechenden öffentlichen Administatorschlüssel verschlüsselt wurden, in das Sicherheits-Subsystem ausgelagert, entschlüsselt und verwendet werden können. Der private (mit dem öffentlichen Administratorschlüssel verschlüsselte) Schlüssel des aktuellen Windows-Benutzers wird an das Sicherheits-Subsystem weitergeleitet. Alle von einer Anwendung benötigten Daten, die das integrierte Sicherheits-Subsystem einsetzt, werden ebenso an den Chip weitergeleitet, entschlüsselt und innerhalb der sicheren Umgebung des Sicherheits-Subsystems genutzt. Ein Beispiel hierfür ist ein privater Schlüssel, der zur Authentifizierung bei einem drahtlosen Netzwerk verwendet wird.

Wenn ein Schlüssel erforderlich ist, wird er in das Sicherheits-Subsystem ausgelagert. Die verschlüsselten privaten Schlüssel werden in das Sicherheits-Subsystem ausgelagert und können dann in der geschützten Umgebung des Chips verwendet werden. Die privaten Schlüssel werden niemals ungeschützt außerhalb dieser Hardwareumgebung verwendet. So kann eine beinahe unbegrenzte Datenmenge durch den integrierten IBM Security Chip geschützt werden.

Die privaten Schlüssel werden verschlüsselt, weil sie sehr gut geschützt werden müssen und im integrierten IBM Sicherheits-Subsystem der Speicherplatz begrenzt ist. Es können nur einige Schlüssel gleichzeitig im Sicherheits-Subsystem gespeichert werden. Der öffentliche und der private Hardwareschlüssel sind die einzigen Schlüssel, die bei jedem Booten im Sicherheits-Subsystem gespeichert bleiben. Damit mehrere Schlüssel und mehrere Benutzer zugelassen werden können, implementiert IBM Client Security die IBM Schlüsselauslagerungshierarchie. Wenn ein Schlüssel erforderlich ist, wird er in das integrierte IBM Sicherheits-Subsystem ausgelagert. Die zugehörigen verschlüsselten privaten Schlüssel werden in das Sicherheits-Subsystem ausgelagert und können dann in der geschützten Umgebung des Sicherheits-Subsystems verwendet werden. Die privaten Schlüssel werden niemals ungeschützt 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. Wenn der private Administratorschlüssel im Sicherheits-Subsystem entschlüsselt wird, kann ein privater Benutzerschlüssel (mit dem öffentlichen Administratorschlüssel verschlüsselt) in das Sicherheits-Subsystem weitergeleitet und mit dem privaten Administratorschlüssel entschlüsselt werden. Mit dem öffentlichen Administratorschlüssel können mehrere private Benutzerschlüssel verschlüsselt werden. Hierdurch kann eine fast unbegrenzte Anzahl an Benutzern auf einem System mit dem IBM ESS arbeiten; für eine optimale Leistung empfiehlt es sich jedoch, die Registrierung auf 25 Benutzer pro Computer zu beschränken.

IBM ESS verwendet eine Schlüsselauslagerungshierarchie, bei der der öffentliche und der private Hardwareschlüssel im Sicherheits-Subsystem zum Sichern weiterer Daten, die außerhalb des Chips gespeichert sind, verwendet werden können. Der

private Hardwareschlüssel wird im Sicherheits-Subsystem generiert und verlässt nie diese sichere Umgebung. Der öffentliche Hardwareschlüssel ist außerhalb des Sicherheits-Subsystems verfügbar und wird zum Verschlüsseln oder Sichern weiterer Daten, wie z. B. eines privaten Schlüssels, verwendet. Wenn diese Daten mit dem öffentlichen Hardwareschlüssel verschlüsselt sind, können sie nur durch den privaten Hardwareschlüssel entschlüsselt werden. Da der private Hardwareschlüssel nur in der sicheren Umgebung des Sicherheits-Subsystems verfügbar ist, können die Daten nur in dieser sicheren Umgebung entschlüsselt und verwendet werden. Jeder Computer verfügt über einen eindeutigen öffentlichen und privaten Hardwareschlüssel. Die Zufallszahlfunktion des integrierten IBM Sicherheits-Subsystems stellt sicher, dass jedes Hardwareschlüsselpaar statistisch eindeutig ist.

PKI-Funktionen (Public Key Infrastructure)

Client Security stellt alle erforderlichen Komponenten für die Erstellung einer PKI von öffentlichen Schlüsseln in Ihrem Unternehmen bereit. Zu diesen Komponenten gehören u. a.:

- **Steuerung der Client-Sicherheitspolicy über Administratoren.** Die Authentifizierung auf Clientebene ist ein wichtiger Gesichtspunkt der Sicherheitspolicy. Client Security stellt die Schnittstelle zur Verfügung, die für die Verwaltung der Sicherheitspolicy eines IBM Clients erforderlich ist. Diese Schnittstelle ist Bestandteil der Authentifizierungssoftware von User Verification Manager (UVM), der Hauptkomponente von Client Security.
- **Chiffrierschlüsselverwaltung für die Verschlüsselung öffentlicher Schlüssel:** Die Administratoren erstellen mit Hilfe von Client Security Chiffrierschlüssel für die Computerhardware und die Clientbenutzer. Beim Erstellen von Chiffrierschlüsseln sind sie über eine Schlüsselhierarchie an den integrierten IBM Security Chip gebunden. Hierbei werden über einen Hardwareschlüssel der Basisebene die höherrangigen Schlüssel sowie die Benutzerschlüssel für die einzelnen Clientbenutzer verschlüsselt. Das Verschlüsseln und Speichern der Schlüssel auf dem integrierten IBM Security Chip stellt eine wichtige Zusatzebene der Client-Sicherheit dar, da die Schlüssel fest an die Computerhardware gebunden sind.
- **Erstellung und Speicherung digitaler Zertifikate mit Schutz durch den integrierten IBM Security Chip.** Wenn Sie ein digitales Zertifikat anfordern, das zum digitalen Signieren oder Verschlüsseln einer E-Mail verwendet werden kann, können Sie über Client Security das integrierte IBM Sicherheits-Subsystem als CSP für Anwendungen, die Microsoft CryptoAPI verwenden, auswählen. Zu diesen Anwendungen gehören auch Internet Explorer und Microsoft Outlook Express. Hierdurch wird gewährleistet, dass der private Schlüssel des digitalen Zertifikats mit dem öffentlichen Benutzerschlüssel auf dem integrierten IBM Sicherheits-Subsystem verschlüsselt ist. Benutzer von Netscape können das integrierte IBM Sicherheits-Subsystem als Funktion zur Erstellung privater Schlüssel für digitale Zertifikate auswählen, die für die Sicherheit verwendet werden. Anwendungen, die das PKCS #11-Modul (Public-Key Cryptography Standard) verwenden, wie z. B. Netscape Messenger, können den vom integrierten IBM Sicherheits-Subsystem bereitgestellten Schutz in Anspruch nehmen.
- **Die Möglichkeit, digitale Zertifikate zum integrierten IBM Sicherheits-Subsystem zu übertragen.** Das Tool zur Übertragung von Zertifikaten von IBM Client Security ermöglicht das Übertragen von Zertifikaten, die mit dem Standard-Microsoft-CSP erstellt wurden, zum CSP des integrierten IBM Sicherheits-Subsystems. Dadurch wird der Schutz, den die privaten Schlüssel in Verbindung mit den Zertifikaten bieten, bedeutend erhöht, da diese nun sicher im integrierten IBM Sicherheits-Subsystem gespeichert werden, anstatt in anfälliger Software.

Anmerkung: Digitale Zertifikate, die durch den CSP des integrierten IBM Sicherheits-Subsystems geschützt wurden, können nicht in einen anderen CSP exportiert werden.

- **Funktion zur Schlüsselarchivierung und -wiederherstellung.** Eine wichtige PKI-Funktion ist das Erstellen eines Schlüsselarchivs, in dem die Schlüssel wiederhergestellt werden können, wenn die Originalschlüssel verloren gegangen sind oder beschädigt wurden. IBM Client Security stellt eine Schnittstelle zur Verfügung, über die Sie ein Archiv für Schlüssel und digitale Zertifikate, die mit dem integrierten IBM Sicherheits-Subsystems erstellt wurden, einrichten können. Außerdem können Sie darüber bei Bedarf die entsprechenden Schlüssel und Zertifikate wiederherstellen.
- **FFE (File and Folder Encryption, Verschlüsselung von Dateien und Ordnern).** Die Verschlüsselung von Dateien und Ordnern ermöglicht es Clientbenutzern, Dateien oder Ordner zu verschlüsseln oder zu entschlüsseln. So steht ein höheres Maß an Datensicherheit an erster Stelle der Maßnahmen zur Systemsicherheit von CSS.
- **Authentifizierung über Fingerabdrücke.** IBM Client Security unterstützt das Lesegerät für Fingerabdrücke von Targus als PC-Karte oder über USB für die Authentifizierung. Client Security 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, sollte die Systemsicherheit erhöht werden, da diese Karte mit einem Kennwort geliefert werden muss, das möglicherweise ausspioniert werden kann.
- **Standortunabhängiger Zugriff mit Berechtigungsnachweis.** Der standortunabhängige Zugriff mit Berechtigungsnachweis ermöglicht es einem für das Netzwerk autorisierten Benutzer, jedes System im Netzwerk genau wie die eigene Workstation zu verwenden. Wenn ein Benutzer berechtigt ist, UVM auf irgendeinem bei Client Security registrierten Client zu verwenden, kann er seine persönlichen Daten in alle anderen registrierten Clients im Netzwerk für standortunabhängigen Zugriff mit Berechtigungsnachweis importieren. Die persönlichen Daten werden im CSS-Archiv und auf jedem System, in das sie importiert wurden, automatisch aktualisiert und gewartet. Aktualisierungen der persönlichen Daten, wie z. B. neue Zertifikate oder Änderungen am Verschlüsselungstext, sind sofort auf allen Systemen verfügbar.
- **FIPS 140-1-Zertifizierung.** Client Security unterstützt FIPS 140-1-zertifizierte, verschlüsselte Bibliotheken.
- **Ablauf des Verschlüsselungstexts.** Client Security legt bei jedem Hinzufügen eines Benutzers einen benutzerspezifischen Verschlüsselungstext und eine Policy für das Ablaufen des Verschlüsselungstexts fest.

Kapitel 2. Erste Schritte

In diesem Kapitel werden die Hard- und Softwarevoraussetzungen zur Verwendung von IBM Client Security beschrieben. Außerdem werden Ihnen Informationen zum Herunterladen von IBM Client Security bereitgestellt.

Hardwarevoraussetzungen

Bevor Sie die Software herunterladen und installieren, vergewissern Sie sich, dass Ihre Computerhardware mit IBM Client Security kompatibel ist.

Die neusten Informationen zu den Hard- und Softwarevoraussetzungen finden Sie auf der IBM Website unter http://www.pc.ibm.com/us/security/index.html.

Integriertes IBM Sicherheits-Subsystem

Das integrierte IBM Sicherheits-Subsystem (IBM Embedded Security Subsystem) ist ein verschlüsselter Mikroprozessor, der in der Systemplatine des IBM Clients integriert ist. Diese grundlegende Komponente von IBM Client Security wandelt die Funktionen der Sicherheitspolicy von ungeschützter Software in sichere Hardware um und trägt so dazu bei, die Sicherheit des lokalen Client wesentlich zu erhöhen.

Nur die IBM Computer und Workstations, die das integrierte IBM Sicherheits-Subsystem enthalten, unterstützen auch IBM Client Security. Wenn Sie versuchen, die Software herunterzuladen und auf einem Computer zu installieren, der über kein integriertes IBM Sicherheits-Subsystem verfügt, hat dies zur Folge, dass die Software nicht ordnungsgemäß installiert und demzufolge auch nicht fehlerfrei ausgeführt wird.

Unterstützte IBM Modelle

Client Security ist für eine Vielzahl von IBM Desktopcomputern und Notebooks lizenziert, die es auch unterstützt. Eine vollständige Liste der unterstützten Modelle finden Sie auf der Webseite http://www.pc.ibm.com/us/security/index.html.

Softwarevoraussetzungen

Bevor Sie die Software herunterladen und installieren, vergewissern Sie sich, dass Ihre Computersoftware sowie das von Ihnen verwendete Betriebssystem mit IBM Client Security kompatibel sind.

Betriebssysteme

Für die Ausführung von IBM Client Security ist eines der folgenden Betriebssysteme erforderlich:

- Windows XP
- Windows 2000 Professional

UVM-sensitive Produkte

IBM Client Security wird mit der Software "User Verification Manager" (UVM) geliefert. Mit dieser Software können Sie die Authentifizierung für Ihren Desktopcomputer anpassen. Diese erste Stufe der Policy-basierten Steuerung erhöht den Investitionsschutz und die Effizienz der Kennwortverwaltung. UVM ist mit den unternehmensübergreifenden Sicherheitspolicy-Programmen kompatibel und ermöglicht es Ihnen, UVM-sensitive Produkte zu verwenden. Zu diesen Produkten gehören u. a. folgende:

- **Biometrische Geräte, wie z. B. Lesegeräte für Fingerabdrücke**

  UVM bietet eine Plug-and-Play-Schnittstelle für biometrische Geräte. Sie müssen IBM Client Security *vor* der Installation eines UVM-Sensors installieren.

  Um einen UVM-Sensor zu verwenden, der bereits auf einem IBM Client installiert wurde, müssen Sie zuerst den UVM-Sensor wieder deinstallieren, anschließend IBM Client Security installieren und dann den UVM-Sensor erneut installieren.

- **Tivoli Access Manager Version 5.1**

  UVM erleichtert und verbessert die Policy-Verwaltung durch eine reibungslose Integration in eine zentralisierte, Policy-basierte Zugriffssteuerungslösung, wie z. B. Tivoli Access Manager.

  UVM erzwingt eine lokale Policy, unabhängig davon, ob es sich bei dem System um ein in ein Netzwerk integriertes System (Desktop) oder ein Standalone-System handelt, und stellt somit ein einziges, einheitliches Policy-Modell bereit.

- **Lotus Notes ab Version 4.5**

  UVM erhöht zusammen mit IBM Client Security die Sicherheit Ihrer Lotus Notes-Anmeldung (Lotus Notes ab Version 4.5).

- **Entrust Desktop Solutions 5.1, 6.0 oder 6.1**

  Die Unterstützung durch Entrust Desktop Solutions verbessert das Leistungsspektrum für die Internet-Sicherheit, so dass kritische Unternehmensprozesse über das Internet abgewickelt werden können. Entrust Entelligence stellt einen Single Security Layer zur Verfügung, der die gesamten Anforderungen eines Unternehmens hinsichtlich der erweiterten Sicherheitseinrichtungen (einschließlich Identifikation, Vertraulichkeit, Prüfung und Sicherheitsverwaltung) erfüllt.

- **RSA SecurID Software Token**

  Mit RSA SecurID Software Token kann der gleiche Datensatz für den Generierungswert für Zufallszahlen, der auch in herkömmlichen RSA Hardware Tokens verwendet wird, in bereits vorhandene Benutzerplattformen integriert werden. Demzufolge haben Benutzer die Möglichkeit, sich auf geschützten Ressourcen zu authentifizieren, indem sie auf die integrierte Software zugreifen, statt dedizierte Authentifizierungseinheiten verwenden zu müssen.

- **Gemplus GemPC400-Smartcard-Leseeinheit**

  Die Gemplus GemPC400-Smartcard-Leseeinheit aktiviert die Sicherheitspolicy für die Smartcard-Authentifizierung und fügt so dem Standardschutz durch Verschlüsselungstext eine weitere Sicherheitsebene hinzu.

Web-Browser

Folgende Web-Browser werden von IBM Client Security bei der Anforderung digitaler Zertifikate unterstützt:

- Internet Explorer ab Version 5.0
- Netscape 4.8 und Netscape 7.1

Informationen zum Browser-Verschlüsselungsgrad

Wenn eine Unterstützung für hochgradige Verschlüsselung installiert ist, verwenden Sie die 128-Bit-Version Ihres Web-Browsers. Weitere Informationen zur Feststellung des Verschlüsselungsgrades erhalten Sie über die Hilfefunktion des Browsers.

Verschlüsselungsdienste

IBM Client Security unterstützt folgende Verschlüsselungsdienste:

- **Microsoft CryptoAPI:** CryptoAPI ist der Standardverschlüsselungsdienst für Betriebssysteme und Anwendungen von Microsoft. Mit der integrierten Unterstützung von CryptoAPI können Sie über IBM Client Security die Verschlüsselungsvorgänge des integrierten IBM Sicherheits-Subsystems beim Erstellen von digitalen Zertifikaten für Microsoft-Anwendungen verwenden.
- **PKCS #11-Modul:** Beim PKCS #11-Modul handelt es sich um den Verschlüsselungsstandard für Netscape, Entrust, RSA und andere Produkte. Wenn Sie das PKCS #11-Modul für das integrierte IBM Sicherheits-Subsystem installiert haben, können Sie mit dem integrierten IBM Sicherheits-Subsystem digitale Zertifikate für Netscape, Entrust, RSA und andere Anwendungen, die das PKCS #11-Modul verwenden, erstellen.

E-Mail-Anwendungen

IBM Client Security unterstützt folgende Anwendungstypen über gesicherte E-Mail:

- E-Mail-Anwendungen, die Microsoft CryptoAPI für Verschlüsselungsvorgänge verwenden, wie z. B. Outlook Express und Outlook (sofern eine unterstützte Version von Internet Explorer verwendet wird).
- E-Mail-Anwendungen, die das PKCS #11-Modul (Public Key Cryptographic Standard) für Verschlüsselungsvorgänge verwenden, wie z. B. Netscape Messenger (sofern eine unterstützte Version von Netscape verwendet wird).
- Unterstützung von Lotus Notes über einen erweiterten Anmeldungsauthentifizierungsprozess.

Kapitel 3. Vorbereitung der Softwareinstallation

Dieses Kapitel enthält alle Vorbereitungen zum Ausführen des Installationsprogramms und zum Konfigurieren von IBM Client Security auf IBM Clients.

Alle für die Installation von Client Security erforderlichen Dateien finden Sie auf der IBM Website http://www.pc.ibm.com/us/security/index.html. Auf der Website finden Sie Informationen, mit deren Hilfe Sie sicherstellen können, dass Sie über das integrierte IBM Sicherheits-Subsystem (IBM Embedded Security Subsystem) verfügen und die Ihnen die Auswahl des passenden IBM Client Security-Angebots für Ihr System ermöglichen.

Softwareinstallation einleiten

Das Installationsprogramm installiert IBM Client Security auf dem IBM Client und aktiviert das integrierte IBM Sicherheits-Subsystem. Die einzelnen Installationsschritte können in Abhängigkeit von verschiedenen Faktoren unterschiedlich ausfallen.

Zum Installieren des Programms "IBM Client Security" müssen die entsprechenden Benutzer mit Administratorrechten angemeldet sein.

Für die Verwendung mit Tivoli Access Manager installieren

Wenn Sie Tivoli Access Manager zur Steuerung der Authentifizierungsbestimmungen für Ihren Computer verwenden möchten, müssen Sie *vor* der Installation von IBM Client Security zuerst bestimmte Komponenten von Tivoli Access Manager installieren. Weitere Informationen hierzu finden Sie im Handbuch *Client Security mit Tivoli Access Manager verwenden*.

Wichtige Hinweise zu den Funktionen beim Systemstart

Es gibt zwei IBM Funktionen beim Systemstart, die die Art und Weise, in der Sie das integrierte IBM Sicherheits-Subsystem (IBM Embedded Security Subsystem) aktivieren und Chiffrierschlüssel erstellen, beeinflussen können. Diese Funktionen bestehen aus dem BIOS-Administratorkennwort und den erweiterten Sicherheitseinrichtungen (BIOS-Menüpunkt "Enhanced Security"). Der Zugriff auf diese Funktionen erfolgt auf IBM Computern über das Programm "Configuration/Setup Utility". IBM Client Security verfügt über ein eigenes Administratorkennwort. Um Verwechslungen zu vermeiden, wird das Administratorkennwort, das im Programm "Configuration/Setup Utility" festgelegt wird, in den Handbüchern zu Client Security als das *BIOS-Administratorkennwort* bezeichnet.

BIOS-Administratorkennwort

Ein BIOS-Administratorkennwort verhindert, dass nicht autorisierte Personen die Konfigurationseinstellungen eines IBM Computers ändern. Diese Art von Kennwörtern wird über das Programm "Configuration/Setup Utility" auf einem NetVista- oder ThinkCentre-Computer oder über das Programm "IBM BIOS Setup Utility" auf einem ThinkPad festgelegt. Sie können das jeweilige Programm aufrufen, indem Sie beim Systemstart des Computers die Eingabetaste oder die Taste F1 drücken. Ein solches Kennwort wird im ThinkCentre-Programm "Configuration/Setup Utility" als *Administratorkennwort* und im ThinkPad-Programm "BIOS Setup Utility" als *Administratorkennwort (Supervisor Password)* bezeichnet.

Erweiterte Sicherheitseinrichtungen

Die erweiterten Sicherheitseinrichtungen bieten einen zusätzlichen Schutz für das BIOS-Administratorkennwort und die Einstellungen während des Systemstarts. Im Programm "Configuration/Setup Utility" können Sie feststellen, ob die erweiterten Sicherheitseinrichtungen aktiviert sind oder nicht. Dieses Programm können Sie während des Computerstarts mit F1 aufrufen.

Weitere Informationen zu Kennwörtern und erweiterten Sicherheitseinrichtungen finden Sie in der Dokumentation zu Ihrem Computer.

Erweiterte Sicherheitseinrichtungen auf den NetVista-Modellen 6059, 6569, 6579, 6649 und auf allen NetVista Q1x-Modellen: Wenn auf den NetVista-Modellen 6059, 6569, 6579, 6649, 6646 und allen Q1x-Modellen ein Administratorkennwort festgelegt wurde, müssen Sie das integrierte IBM Sicherheits-Subsystem im Administratordienstprogramm aktivieren und die Chiffrierschlüssel erstellen.

Wenn auf diesen Modellen die erweiterten Sicherheitseinrichtungen aktiviert wurden, müssen Sie nach der Installation von Client Security im Administratordienstprogramm das integrierte IBM Sicherheits-Subsystem aktivieren und die Chiffrierschlüssel erstellen, *nachdem* Sie IBM Client Security installiert haben. Wenn das Installationsprogramm feststellt, dass die erweiterten Sicherheitseinrichtungen aktiviert sind, erhalten Sie am Ende des Installationsprozesses eine entsprechende Nachricht. Starten Sie den Computer erneut, und öffnen Sie das Administratordienstprogramm, um das integrierte IBM Sicherheits-Subsystem zu aktivieren und die Chiffrierschlüssel zu erstellen.

Erweiterte Sicherheitseinrichtungen auf allen anderen NetVista-Modellen (mit Ausnahme von 6059, 6569, 6579, 6649 und allen NetVista Q1x-Modellen): Wenn für ein anderes Modell ein Administratorkennwort festgelegt wurde, müssen Sie während des Installationsprozesses *kein* Administratorkennwort eingeben.

Wenn auf diesen NetVista-Modellen die erweiterten Sicherheitseinrichtungen aktiviert wurden, können Sie die Software mit Hilfe des Installationsprogramms installieren, müssen jedoch das integrierte IBM Sicherheits-Subsystem über das Programm "Configuration/Setup Utility" aktivieren. *Nachdem* Sie das integrierte IBM Sicherheits-Subsystem aktiviert haben, können Sie im Administratordienstprogramm die Chiffrierschlüssel erstellen.

Informationen zur BIOS-Aktualisierung

Bevor Sie die Software installieren, müssen Sie möglicherweise den neuesten BIOS-Code (Basic Input/Output System) für Ihren Computer herunterladen. Um die auf Ihrem Computer verwendete BIOS-Stufe festzustellen, müssen Sie den Computer erneut starten und mit F1 das Programm "Configuration/Setup Utility" aufrufen. Wenn das Hauptmenü des Programms "Configuration/Setup Utility" angezeigt wird, wählen Sie "Product Data" aus, um weitere Informationen zum BIOS-Code zu erhalten. Die BIOS-Codestufe wird auch als EEPROM-Änderungsstufe bezeichnet.

Um IBM Client Security ab Version 2.1 auf den NetVista-Modellen 6059, 6569, 6579, 6649 auszuführen, müssen Sie ein BIOS ab Stufe xxxx22axx verwenden. Um IBM Client Security ab Version 2.1 auf den NetVista-Modellen 6790, 6792, 6274, 2283 auszuführen, müssen Sie ein BIOS ab Stufe xxxx20axx verwenden. Weitere Informationen hierzu finden Sie in der README-Datei, die im Software-Download enthalten ist.

Die neusten BIOS-Code-Aktualisierungen für Ihren Computer finden Sie auf der IBM Website unter http://www.pc.ibm.com/support, indem Sie dort in das Suchfeld BIOS eingeben, die entsprechenden Downloads aus der Dropdown-Liste auswählen und die Eingabetaste drücken. Daraufhin Ihnen wird eine Liste mit allen BIOS-Code-Aktualisierungen angezeigt. Klicken Sie auf die zutreffende Modellnummer, und befolgen Sie die auf der Webseite angezeigten Anweisungen.

Administratorschlüsselpaar zur Schlüsselarchivierung verwenden

Das Archivschlüsselpaar ist eine Kopie des Administratorschlüsselpaars, das Sie zur Wiederherstellung auf einem externen Datenträger speichern können. Da das Administratordienstprogramm zur Erstellung des Archivschlüsselpaars verwendet wird, müssen Sie IBM Client Security auf einem ersten IBM Client installieren, bevor Sie das Administratorschlüsselpaar erstellen können.

Kapitel 4. Software herunterladen, installieren und konfigurieren

Dieses Kapitel enthält Anweisungen zum Herunterladen, Installieren und Konfigurieren von IBM Client Security auf IBM Clients. Außerdem enthält dieses Kapitel Anweisungen zum Deinstallieren der Software. Installieren Sie IBM Client Security, bevor Sie eines der Dienstprogramme für Client Security installieren.

Wichtig: Wenn Sie von einer Version von IBM Client Security aufrüsten, die älter als Version 5.0 ist, *müssen* Sie alle verschlüsselten Dateien entschlüsseln, *bevor* Sie Client Security ab Version 5.1 installieren. IBM Client Security ab Version 5.1 kann aufgrund von Änderungen bei der Dateiverschlüsselungsimplementierung keine Dateien entschlüsseln, die mit älteren Versionen von IBM Client Security als Version 5.0 verschlüsselt wurden.

Software herunterladen

Alle für die Installation von Client Security erforderlichen Dateien finden Sie auf der IBM Website http://www.pc.ibm.com/us/security/index.html. Auf der Website finden Sie Informationen, mit deren Hilfe Sie sicherstellen können, dass Sie über das integrierte IBM Sicherheits-Subsystem (IBM Embedded Security Subsystem) verfügen und die Ihnen die Auswahl des passenden IBM Client Security-Angebots für Ihr System ermöglichen.

Gehen Sie wie folgt vor, um die entsprechenden Dateien für Ihr System herunterzuladen:

1. Rufen Sie in einem Web-Browser folgende IBM Website auf: http://www.pc.ibm.com/us/security/index.html.
2. Klicken Sie im Feld ″Resources″ auf **Support and downloads**.
3. Klicken Sie im Abschnitt zum integrierten IBM Sicherheits-Subsystem und IBM Client Security auf der Webseite auf **Software download**.
4. Klicken Sie im Feld ″Select a system″ auf **Detect my system & continue**, oder geben Sie die siebenstellige Maschinentyp-/Modellnummer in das vorgesehene Feld ein.
5. Geben Sie Ihre E-Mail-Adresse in dem entsprechenden Feld ein, und wählen Sie das gewünschte Land bzw. die Region im Dropdown-Menü aus.
6. Wählen Sie mit dem entsprechenden Markierungsfeld aus, ob Sie in Zukunft Informationen zu anderen Angeboten erhalten möchten.
7. Lesen Sie die Lizenzvereinbarung. Klicken Sie dazu auf **View Licence**, und klicken Sie anschließend auf **Accept Licence**, um die Bedingungen der Lizenzvereinbarung zu akzeptieren.

   Sie werden danach automatisch zur Download-Seite für IBM Client Security weitergeleitet.
8. Klicken Sie neben dem Link für ″Client Security 5.4″ auf **Download Now**, um die Software herunterzuladen.

   Anmerkung: Informationen zu Upgrades und Einschränkungen finden Sie in der Datei `css54readme.html`.
9. Klicken Sie auf **Save**, um die ausführbare Installationsdatei auf Ihrem Festplattenlaufwerk zu speichern.

10. Geben Sie die Position an, in der die Datei gespeichert werden soll, und klicken Sie auf **Save**. Um die Installation der Software zu starten, können Sie auf **Öffnen** klicken, wenn das Herunterladen der Datei abgeschlossen ist; oder klicken Sie doppelt auf das Symbol für die ausführbare Datei.

    Das Begrüßungsfenster des InstallShield-Assistenten von IBM Client Security wird angezeigt.

Software installieren

Gehen Sie wie folgt vor, um die entsprechenden Dateien auf Ihrem System zu installieren:

1. Klicken Sie doppelt auf die ausführbare Datei.

    Das Begrüßungsfenster des InstallShield-Assistenten von IBM Client Security wird angezeigt.
2. Klicken Sie auf **Weiter**.

    Die Lizenzvereinbarung für IBM Client Security wird angezeigt.
3. Lesen Sie die Bedingungen der Lizenzvereinbarung, wählen Sie den Radioknopf **Ich akzeptiere die Lizenzvereinbarung** aus, und klicken Sie auf **Weiter**.

    Die Anzeige für die Produktauswahl erscheint.
4. Wählen Sie einen der folgenden Radioknöpfe aus, und klicken Sie auf **Weiter**.
    - **IBM Client Security und IBM Password Manager.** Wenn Sie diese Option auswählen, werden IBM Client Security, IBM Password Manager und alle erforderlichen Einheitentreiber installiert oder aktualisiert.
    - **Nur IBM Client Security.** Wenn Sie diese Option auswählen, werden IBM Client Security und alle erforderlichen Einheitentreiber installiert oder aktualisiert.

    Die Anzeige für den Zielordner erscheint.
5. Klicken Sie auf **Weiter**, um die Standardposition für die Installation zu akzeptieren, oder klicken Sie auf **Ändern**, um den gewünschten Zielordner selbst auszuwählen.

    Eine Anzeige, dass die Installation nun beginnen kann, erscheint.
6. Klicken Sie auf **Installieren**, um die Installation zu starten, oder klicken Sie auf **Zurück**, um die von Ihnen ausgewählten Installationseinstellungen zu überprüfen oder zu ändern.

    Eine Fortschrittsanzeige gibt den Verlauf der Installation an. Anschließend erscheint eine Anzeige des InstallShield-Assistenten, die angibt, dass die Installation abgeschlossen ist.
7. Klicken Sie auf **Fertig stellen**, um den Assistenten zu verlassen.

Damit die durch die Installation vorgenommenen Änderungen auf Ihrem Computer wirksam werden, müssen Sie den Computer erneut starten.

Konfigurationsoptionen auswählen

In der ersten Anzeige des Konfigurationsassistenten von IBM Client Security können Sie eine Konfigurationsoption auswählen. Die Auswahl einer geeigneten Konfigurationsoption ist sehr wichtig. Lesen Sie die folgenden Informationen sorgfältig durch, bevor Sie sich für eine Konfigurationsoption entscheiden. Benutzer mit wenig Vorkenntnissen zu IBM Client Security sollten die Option *Standardkonfiguration* auswählen.

Standardkonfiguration

Wenn Sie die Standardkonfiguration von IBM Client Security mit dem Konfigurationsassistenten von Client Security auswählen, werden folgende Funktionen von Client Security konfiguriert:

- IBM Password Manager (falls bei der Installation ausgewählt)
- Dateiverschlüsselung durch Klicken mit der rechten Maustaste
- Authentifizierung über Verschlüsselungstexte und Fingerabdrücke
- Unterstützung für digitale Signaturen

Wenn Sie die empfohlene Option *Standardkonfiguration* im Konfigurationsassistenten von Client Security auswählen, ist der Konfigurationsprozess einfach. Wenn Sie diese Konfiguration auswählen, sind jedoch einige erweiterte Funktionen von Client Security inaktiviert. Diese CSS-Funktionen sind nach der Konfiguration nicht verfügbar.

Standardeinstellungen für eine Standardkonfiguration

Folgende fest codierte Standardeinstellungen werden für eine Standardkonfiguration verwendet:

- **Archivposition:** C:\Dokumente und Einstellungen\All Users\Anwendungsdaten\ibm\security\archive
- **Position des Administratorschlüsselpaars:** C:\Dokumente und Einstellungen\All Users\Anwendungsdaten\ibm\security\keys

  Der private Administratorschlüssel wird nicht geteilt und wird mit dem CSS-Administratorverschlüsselungstext verschlüsselt.

Außerdem werden folgende Einstellungen verwendet:

- Unterstützung für IBM Password Manager ist aktiviert.
- Als Sicherheitspolicy wird die mittlere Stufe verwendet: Alle verfügbaren Authentifizierungsmethoden sind nur bei der ersten Verwendung einer CSS-Funktion erforderlich.
- Authentifizierung über Verschlüsselungstext ist immer erforderlich.
- Authentifizierung über Fingerabdruck ist erforderlich, wenn ein integriertes Lesegerät für Fingerabdrücke während der Konfiguration festgestellt wird.
- Der UVM-Verschlüsselungstext des Benutzers, der CSS konfiguriert hat, wird auch als *CSS-Administratorkennwort* verwendet. Wenn dieser UVM-Verschlüsselungstext geändert wird, wird das CSS-Administratorkennwort ebenfalls geändert. Für das CSS-Administratorkennwort gilt kein Ablaufdatum, das Kennwort ist unbegrenzt gültig.

Einschränkungen für Komponenten bei einer Standardkonfiguration

Einige Funktionen von Client Security, die durch eine erweiterte Konfiguration aktiviert werden, sind inaktiviert, wenn Sie die Standardkonfiguration auswählen. Diese Funktionen können bei einer Standardkonfiguration von CSS nicht verwendet werden. Um diese Funktionen verwenden zu können, müssen Sie Ihre Standardkonfiguration in eine erweiterte Konfiguration konvertieren. Folgende funktionale Unterschiede gelten nach einer Standardkonfiguration:

- **Administratordienstprogramm**

  Folgende Aktionen sind nach einer Standardkonfiguration nicht zulässig:

  – Benutzer zurücksetzen

  – Benutzer entfernen

– Ändern des Administratorkennworts über die Schaltfläche ″Chipeinstellungen″
– Funktionen für die Schlüsselkonfiguration

Wenn ein Benutzer versucht, eine der oben beschriebenen Operationen auszuführen, wird er aufgefordert, eine Konvertierung zur erweiterten CSS-Konfiguration durchzuführen. Durch den Konvertierungsprozess wird der private Administratorschlüssel entschlüsselt und das Administratorschlüsselpaar in eine Position verschoben, die der Benutzer angibt.

- **Administratorkonsole**

  Folgende Unterschiede in der Verwendung gelten bei einer Standardkonfiguration:

  – Das Archivverzeichnis und die Positionen des privaten und des öffentlichen Schlüssels sind fest codiert und können nicht geändert werden. Das Archiv kann nur auf dem lokalen Computer bearbeitet werden.
  – Bei einer Standardkonfiguration ist die Option zum Konfigurieren von standortunabhängigem Zugriff mit Berechtigungsnachweis nicht verfügbar. Wenn Sie eine Standardkonfiguration auswählen und anschließend ein Netzwerk mit standortunabhängigem Zugriff mit Berechtigungsnachweis konfigurieren möchten, müssen Sie zuerst die Standardkonfiguration in eine erweiterte Konfiguration konvertieren.
  – Für den CSS-Administrator kann keine Umgehungsoperation für den UVM-Verschlüsselungstext durchgeführt werden.

- **Benutzerkonfigurationsdienstprogramm**

  Folgende Unterschiede in der Verwendung gelten bei einer Standardkonfiguration:

  – Der UVM-Verschlüsselungstext des Benutzers, der CSS konfiguriert hat, wird auch als Administratorkennwort verwendet. Wenn dieser UVM-Verschlüsselungstext geändert wird, wird das Administratorkennwort ebenfalls geändert.
  – Der Benutzer mit CSS-Administratorberechtigung kann nicht zurückgesetzt werden.
  – Bei einer Standardkonfiguration ist die Option zum Konfigurieren von standortunabhängigem Zugriff mit Berechtigungsnachweis nicht verfügbar.

Standardkonfiguration in eine erweiterte Konfiguration konvertieren

Gehen Sie wie folgt vor, um eine Standardkonfiguration von Client Security in eine erweiterte Konfiguration zu konvertieren:

1. Starten Sie das Administratordienstprogramm.
2. Geben Sie das CSS-Administratorkennwort ein.
3. Klicken Sie auf die Schaltfläche **Schlüsselkonfiguration**.
4. Klicken Sie auf **OK**, um fortzufahren.
5. Geben Sie die Position an, in der Sie das entschlüsselte Administratorschlüsselpaar speichern möchten. Das entschlüsselte Schlüsselpaar sollte nicht auf dem lokalen Festplattenlaufwerk gespeichert werden. Der Konvertierungsprozess ist damit abgeschlossen.
6. Ändern Sie die Archivposition. Das Archiv sollte nicht auf dem lokalen Festplattenlaufwerk gespeichert werden.

Nach der Konvertierung von IBM Client Security in eine erweiterte Konfiguration ist es nicht mehr möglich, eine erneute Konvertierung zurück zu einer Standardkonfiguration durchzuführen.

Erweiterte Konfiguration

Mit der *erweiterten Konfiguration* von IBM Client Security werden folgende *zusätzliche* Funktionen von Client Security konfiguriert:

- **UVM-Anmeldeschutz**
- **Auswahl der Schlüsselspeicherposition**
- **Anwendungsunterstützung:** für Entrust, für Verschlüsselung von Dateien und Ordnern sowie für Lotus Notes

Konfigurationsassistenten von IBM Client Security verwenden

Der Konfigurationsassistent von IBM Client Security stellt eine Schnittstelle zur Verfügung, die Sie beim Installieren von Client Security und beim Aktivieren des integrierten IBM Security Chips unterstützt. Führen Sie die folgenden Schritte aus, damit der Konfigurationsassistent von IBM Client Security Sie durch die erforderlichen Tasks zum Konfigurieren einer Sicherheitspolicy auf einem IBM Client führt. Die wichtigsten Konfigurationsschritte, durch die Sie der Konfigurationsassistent von IBM Client Security führt, werden im Folgenden beschrieben. Die genauen Schritte können von den hier beschriebenen abweichen und richten sich nach der von Ihnen ausgewählten Konfigurationsoption.

- **Kennwort des Sicherheitsadministrators festlegen**

  Das Sicherheitsadministratorkennwort, das in diesen Handbüchern als Administratorkennwort bezeichnet wird, wird zur Steuerung des Zugriffs auf das Administratordienstprogramm von IBM Client Security verwendet, das zur Änderung der Sicherheitseinstellungen für diesen Computer dient.

- **Sicherheitsschlüssel für Administratoren erstellen**

  Bei Sicherheitsschlüsseln für Administratoren handelt es sich um eine Gruppe digitaler Schlüssel, die in einer Computerdatei gespeichert sind. Diese Schlüsseldateien werden auch als Administratorschlüssel, Administratorschlüsselpaar oder als Archivschlüsselpaar bezeichnet. Es empfiehlt sich, diese wichtigen Sicherheitsschlüssel auf einem austauschbaren Datenträger oder Laufwerk zu speichern. Wenn im Administratordienstprogramm eine Änderung an der Sicherheitspolicy vorgenommen wird, erfolgt eine Systemanfrage nach einem Administratorschlüssel als Nachweis dafür, dass die Berechtigung zur Änderung der Sicherheitspolicy vorliegt.

  Eine Backup-Version der Sicherheitsdaten wird auch für den Fall gespeichert, dass die Systemplatine oder ein Festplattenlaufwerk des Computers ausgetauscht werden muss. Speichern Sie diese Sicherheitsdaten außerhalb des lokalen Systems.

- **Anwendungen mit IBM Client Security schützen**

  Wählen Sie die Anwendungen aus, die mit IBM Client Security gegen unzulässige Zugriffe geschützt werden sollen. Einige Optionen sind nur verfügbar, wenn hierfür erforderliche Anwendungen installiert sind.

- **Benutzer autorisieren**

  Benutzer müssen, bevor Sie auf den Computer zugreifen können, für den Zugriff autorisiert werden. Beim Autorisieren eines Benutzers müssen Sie den Verschlüsselungstext des betreffenden Benutzers angeben. Nicht autorisierte Benutzer haben keinen Zugriff auf den Computer.

- **Sicherheitsstufe des Systems auswählen**

  Durch Auswahl einer Systemsicherheitsstufe können Sie auf schnelle und einfache Weise eine grundlegende Sicherheitspolicy einrichten. Sie können zu einem späteren Zeitpunkt im Administratordienstprogramm von IBM Client Security eine angepasste Sicherheitspolicy definieren.

Konfigurationsassistenten zum Abschließen einer Standardkonfiguration verwenden

Gehen Sie wie folgt vor, um den Konfigurationsassistenten zum Abschließen einer Standardkonfiguration zu verwenden:

1. Klicken Sie auf **Start > Programme > Access IBM > IBM Client Security > Konfigurationsassistent von IBM Client Security**.

   In der Begrüßungsanzeige des Konfigurationsassistenten von IBM Client Security können Sie eine Konfigurationsoption auswählen.

2. Wählen Sie den Radioknopf ″Standardkonfiguration (empfohlene Einstellung)″ aus, und klicken Sie auf **Weiter**.

   Diese Auswahl aktiviert IBM Password Manager. Sie müssen dafür nur einige Parameter eingeben. Wenn Sie die Standardkonfiguration auswählen, speichert CSS die Sicherungsdaten und Sicherheitsschlüssel auf Ihrem Festplattenlaufwerk. Benutzer mit wenig Vorkenntnissen sollten die Option für die Standardkonfiguration auswählen. Dies ist die Standardeinstellung.

   Die Anzeige für die Eingabe des Verschlüsselungstexts erscheint.

3. Gehen Sie wie folgt vor:

   a. Geben Sie einen Verschlüsselungstext in das Feld ″Verschlüsselungstext eingeben″ ein. Klicken Sie, falls erforderlich, auf die Schaltfläche **Anforderungen für Verschlüsselungstext anzeigen**, um mit Hilfe dieser Informationen einen gültigen Verschlüsselungstextes festzulegen.

      Anmerkung: Bei der Erstinstallation oder nach dem Löschen des Inhalts des integrierten IBM Security Chips müssen Sie Ihren Verschlüsselungstext im Feld ″Verschlüsselungstext bestätigen″ bestätigen. Gegebenenfalls müssen Sie auch Ihr Administratorkennwort eingeben.

   b. Geben Sie ein Wort oder einen Satz in das Feld mit dem Hinweis für den Verschlüsselungstext ein.

   c. Klicken Sie auf **Weiter**.

   Wenn ein Lesegerät für Fingerabdrücke in Ihrem Computer festgestellt wird, wird die Anzeige ″Speicherung der Fingerabdrücke″ angezeigt. Das Markierungsfeld **Ja, ich möchte meine Fingerabdrücke jetzt speichern** ist standardmäßig ausgewählt.

4. Führen Sie einen der folgenden Schritte aus:

   - Heben Sie die Auswahl des Markierungsfelds **Ja, ich möchte meine Fingerabdrücke jetzt speichern** auf, und klicken Sie auf **Weiter**.
   - Klicken Sie auf **Weiter**, und befolgen Sie die angezeigten Anweisungen zur sofortigen Registrierung Ihres Fingerabdrucks.

   Die Anzeige ″Weitere Benutzer autorisieren″ erscheint.

5. Führen Sie einen der folgenden Schritte aus:

   - Wählen Sie das Markierungsfeld **Weitere Benutzer auswählen, die jetzt autorisiert werden sollen (optional)** aus, und klicken Sie auf **Weiter**.
   - Klicken Sie auf **Überspringen**, um diesen Schritt zu überspringen.

   Die Anzeige ″Zusammenfassung der Sicherheitseinstellungen und -funktionen″ erscheint.

6. Klicken Sie auf **Fertig stellen**, um die ausgewählten Sicherheitseinstellungen zu implementieren. Dieser Prozess dauert möglicherweise einige Minuten. Es wird eine Nachricht angezeigt, dass Ihr Computer jetzt durch IBM Client Security geschützt ist.
7. Klicken Sie auf **OK**.

Konfigurationsassistenten zum Abschließen einer erweiterten Konfiguration verwenden

Gehen Sie wie folgt vor, um den Konfigurationsassistenten zum Abschließen einer erweiterten Konfiguration zu verwenden:

1. Klicken Sie auf **Start > Programme > Access IBM > IBM Client Security > Konfigurationsassistent von IBM Client Security**.

   In der Begrüßungsanzeige des Konfigurationsassistenten von IBM Client Security können Sie eine Konfigurationsoption auswählen.
2. Wählen Sie den Radioknopf **Erweiterte Konfiguration** aus, und klicken Sie auf **Weiter**.

   Diese Auswahl erfordert die Angabe von Konfigurationsdaten, wie z. B. einer Schlüsselspeicherposition und einer Sicherheitsstufe. Sie ermöglicht es Ihnen, einen CSS-Anmeldeschutz, Schutzfunktionen für Lotus Notes und IBM Password Manager zu aktivieren.

   Die Anzeige ″Sicherheitsadministratorkennwort angeben″ erscheint.
3. Geben Sie in das Feld ″Geben Sie das Administratorkennwort ein″ das Kennwort des Sicherheitsadministrators ein, und klicken Sie auf **Weiter**.

   Anmerkung: Bei der Erstinstallation oder nach dem Löschen des Inhalts des integrierten IBM Security Chip müssen Sie das Kennwort des Sicherheitsadministrators im Feld ″Bestätigen Sie das Administratorkennwort″ bestätigen. Gegebenenfalls müssen Sie auch Ihr Administratorkennwort eingeben.

   Die Anzeige ″Sicherheitsschlüssel für Administratoren erstellen″ erscheint.
4. Führen Sie einen der folgenden Schritte aus:
   - **Neue Sicherheitsschlüssel erstellen**

     Gehen Sie wie folgt vor, um neue Sicherheitsschlüssel zu erstellen:
     a. Klicken Sie auf den Radioknopf **Neue Schlüssel erstellen**.
     b. Geben Sie die Speicherposition für die Sicherheitsschlüssel der Administratoren an, indem Sie entweder den Pfadnamen in das dafür dafür vorgesehene Feld eingeben oder auf **Durchsuchen** klicken und den entsprechenden Ordner auswählen.
     c. Wenn Sie den Sicherheitsschlüssel für einen erhöhten Schutz teilen möchten, klicken Sie auf das Markierungsfeld **Archivschlüssel für erhöhte Sicherheit teilen**, so dass ein Haken in dem Feld angezeigt wird. Mit Hilfe der Pfeiltasten können Sie anschließend im Auswahlfeld **Anzahl der Teilungen** die gewünschte Anzahl auswählen.
   - **Einen vorhandenen Sicherheitsschlüssel verwenden**

     Gehen Sie wie folgt vor, um einen vorhandenen Sicherheitsschlüssel zu verwenden:
     a. Klicken Sie auf den Radioknopf **Einen vorhandenen Sicherheitsschlüssel verwenden**.

b. Geben Sie entweder durch Eingabe des Pfadnamens in das entsprechende Feld oder durch Klicken auf **Durchsuchen** und Auswählen des entsprechenden Ordners die Speicherposition des öffentlichen Schlüssels an.

c. Geben Sie entweder durch Eingabe des Pfadnamens in das entsprechende Feld oder durch Klicken auf **Durchsuchen** und Auswählen des entsprechenden Ordners die Speicherposition des privaten Schlüssels an.

5. Geben Sie die Schlüsselarchivposition an, in der Sie die Sicherungskopie der Sicherheitsdaten speichern möchten, indem Sie entweder den Pfadnamen in das dafür dafür vorgesehene Feld eingeben oder auf **Durchsuchen** klicken und den entsprechenden Ordner auswählen.
6. Klicken Sie auf **Weiter**.

   Die Anzeige ″Anwendungen mit IBM Client Security schützen″ erscheint.
7. Aktivieren Sie den Schutz für IBM Client Security, indem Sie die entsprechenden Markierungsfelder auswählen, so dass darin ein Haken angezeigt wird, und auf **Weiter** klicken. Folgende Auswahlmöglichkeiten von Client Security stehen Ihnen jetzt zur Verfügung:
   - **Sicherer Zugriff auf das System durch Ersetzen der normalen Windows-Anmeldung durch die gesicherte Client Security-Anmeldung**

     Wählen Sie dieses Feld aus, um die normale Windows-Anmeldung durch die sichere Client-Security-Anmeldung zu ersetzen. Dadurch wird die Systemsicherheit erhöht. Bei der Anmeldung ist dann jeweils eine Authentifizierung mit dem integrierten IBM Sicherheitschip und optionalen Einheiten, wie z. B. Lesegeräten für Fingerabdrücke oder Smartcards, erforderlich.
   - **Datei- und Ordnerverschlüsselung aktivieren**

     Wählen Sie dieses Feld aus, wenn Sie Dateien auf Ihrem Festplattenlaufwerk mit dem integrierten IBM Security Chip sichern möchten. (Hierzu muss das Dienstprogramm zur Verschlüsselung von Dateien und Ordnern von IBM Client Security heruntergeladen werden.)
   - **Unterstützung für IBM Client Security Password Manager aktivieren**

     Wählen Sie dieses Feld aus, wenn Sie IBM Passwort Manager verwenden möchten, um die Kennwörter für Ihre Website-Anmeldungen und -Anwendungen zweckmäßig und sicher zu speichern.
   - **Lotus Notes-Anmeldung durch IBM Client Security-Anmeldung ersetzen**

     Wählen Sie dieses Feld aus, wenn Benutzer von Lotus Notes in Client Security über den integrierten IBM Security Chip automatisch authentifiziert werden sollen.
   - **Unterstützung für Entrust aktivieren**

     Wählen Sie dieses Feld aus, wenn Sie die Integration in Entrust-Sicherheitssoftwareprodukte aktivieren möchten.
   - **Microsoft Internet Explorer schützen**

     Mit diesem Schutz können Sie Ihre E-Mail-Kommunikation und die Suche im Web mit Microsoft Internet Explorer (erfordert ein digitales Zertifikat) schützen. Standardmäßig ist die Unterstützung für Microsoft Internet Explorer aktiviert.

   Nach Auswahl der entsprechenden Markierungsfelder wird das Fenster ″Benutzer autorisieren″ angezeigt.
8. Geben Sie die erforderlichen Angaben in die Anzeige ″Benutzer autorisieren″ ein. Verwenden Sie dafür eine der folgenden Prozeduren:

- Gehen Sie wie folgt vor, um Benutzer zum Ausführen der Funktionen von IBM Client Security zu autorisieren:
  a. Wählen Sie im Bereich ″Nicht autorisierte Benutzer″ einen Benutzer aus.
  b. Klicken Sie auf **Benutzer autorisieren**.
  c. Geben Sie den Verschlüsselungstext für IBM Client Security in die dafür vorgesehenen Felder ein, bestätigen Sie diese Eingaben, und klicken Sie auf **Weiter**.

     Das Fenster für das Ablaufen des UVM-Verschlüsselungstexts wird angezeigt.
  d. Legen Sie die Regel für den Ablauf des Verschlüsselungstextes für den Benutzer fest, und klicken Sie auf **Fertig stellen**.
  e. Klicken Sie auf **Weiter**.
- Gehen Sie wie folgt vor, um die Autorisierung von Benutzern zur Ausführung der Funktionen von IBM Client Security aufzuheben:
  a. Wählen Sie im Bereich ″Autorisierte Benutzer″ einen Benutzer aus.
  b. Klicken Sie auf **Benutzerberechtigung widerrufen**.

     Die Nachricht mit dem Inhalt ″Sind Sie sicher, dass Sie die Autorisierung aufheben möchten?″ wird angezeigt.
  c. Klicken Sie auf **Ja**.
  d. Klicken Sie auf **Weiter**.

Das Fenster ″Sicherheitsstufe des Systems auswählen″ wird angezeigt.

9. Wählen Sie die gewünschten Authentifizierungsbestimmungen aus, indem Sie auf die entsprechenden Markierungsfelder klicken. Sie können mehrere Anforderungen für die Authentifizierung auswählen.
   - Das Markierungsfeld **UVM-Verschlüsselungstext verwenden** ist standardmäßig ausgewählt.
   - Die Einheitentreiber für das Lesegerät für Fingerabdrücke und für die Smartcard müssen installiert werden, bevor der Konfigurationsassistent von IBM Client Security gestartet wird, damit diese Einheiten für den Konfigurationsassistenten verfügbar sind.
   - Wählen Sie eine Systemsicherheitsstufe aus, indem Sie die Auswahlleiste auf die gewünschte Sicherheitsstufe ziehen und auf **Weiter** klicken.

     Anmerkung: Sie können zu einem späteren Zeitpunkt eine angepasste Sicherheitspolicy definieren, indem Sie den Policy-Editor des Administratordienstprogramms verwenden.

   Die Anzeige ″Konfiguration ist abgeschlossen - Sicherheitseinstellungen prüfen″ erscheint.
10. Überprüfen Sie die Sicherheitseinstellungen, und wählen Sie einen der folgenden Schritte aus:
    - Klicken Sie auf **Fertig stellen**, um die Einstellungen zu akzeptieren.
    - Gehen Sie zum Ändern der Einstellungen wie folgt vor: Klicken Sie auf **Zurück**, nehmen Sie gewünschten Änderungen vor, und kehren Sie zu dieser Anzeige zurück. Klicken Sie dann auf **Fertig stellen**.

    Ihre Einstellungen werden über den integrierten IBM Security Chip in IBM Client Security konfiguriert. Es wird eine Nachricht angezeigt, die bestätigt, dass Ihr Computer jetzt durch IBM Client Security geschützt ist.
11. Klicken Sie auf **OK**.

IBM Sicherheits-Subsystem aktivieren

Zur Verwendung von IBM Client Security muss das IBM Sicherheits-Subsystem aktiviert sein. Falls der Chip nicht aktiviert ist, können Sie ihn mit Hilfe des Administratordienstprogramms aktivieren. Anweisungen zur Verwendung des Konfigurationsassistenten finden Sie im vorhergehenden Abschnitt.

Gehen Sie wie folgt vor, um das IBM Sicherheits-Subsystem mit dem Administratordienstprogramm zu aktivieren:

1. Klicken Sie auf **Start > Einstellungen > Systemsteuerung > Integriertes IBM Sicherheits-Subsystem**.

   Es erscheint eine Anzeige mit der Mitteilung, dass das IBM Sicherheits-Subsystem nicht aktiviert ist, und der Frage, ob es jetzt aktiviert werden soll.
2. Klicken Sie auf **Ja**.

   Es wird eine Nachricht angezeigt, die darauf hinweist, dass vor dem Fortfahren das Administratorkennwort oder ein BIOS-Administratorkennwort über das Programm "IBM BIOS Setup Utility" inaktiviert werden muss, falls ein entsprechendes definiert ist.
3. Führen Sie einen der folgenden Schritte aus:
   - Wenn ein Administratorkennwort definiert ist, klicken Sie auf **Abbrechen**, inaktivieren Sie das Kennwort, und führen Sie dann diese Prozedur aus.
   - Ist kein Administratorkennwort definiert, klicken Sie auf **OK**, um fortzufahren.
4. Schließen Sie alle geöffneten Anwendungen, und klicken Sie auf **OK**, um einen Neustart des Computers durchzuführen.
5. Klicken Sie nach dem Neustart zum Öffnen des Administratordienstprogramms auf **Start > Einstellungen > Systemsteuerung > Integriertes IBM Sicherheits-Subsystem**.

   Es wird eine Nachricht angezeigt, die darauf hinweist, dass das IBM Sicherheits-Subsystem nicht konfiguriert wurde oder sein Inhalt gelöscht wurde. An dieser Stelle muss ein neues Kennwort eingegeben werden.
6. Geben Sie in das entsprechende Feld ein neues Administratorkennwort ein, und bestätigen Sie das Kennwort. Klicken Sie anschließend auf **OK**.

   Daraufhin kehrt das Programme zur Hauptanzeige des Administratordienstprogramms zurück.

Softwareversion von Client Security aktualisieren

Bei Clients, auf denen frühere Versionen von Client Security installiert sind, sollten Sie die Software auf diese Version aktualisieren, um die neuen Client Security-Funktionen nutzen zu können.

Wichtig: Bei Systemen, auf denen IBM Client Security Version 4.0x installiert war, muss Version 4.0x der Software deinstalliert und der Inhalt des Chips gelöscht werden, um diese Version von IBM Client Security zu installieren. Andernfalls besteht die Möglichkeit, dass die Installation fehlschlägt oder die Software nicht reagiert.

Upgrade mit neuen Sicherheitsdaten durchführen

Gehen Sie wie folgt vor, um Client Security vollständig zu entfernen und eine Neuinstallation durchzuführen:

1. Deinstallieren Sie die vorhandene Version von Client Security (Systemsteuerung -> Software).

2. Führen Sie einen Neustart des Systems durch.
3. Löschen Sie den Inhalt des integrierten IBM Security Chips über das Programm "IBM BIOS Setup Utility".
4. Führen Sie einen Neustart des Systems durch.
5. Installieren Sie die aktuellste Version von IBM Client Security, und konfigurieren Sie die Software mit dem Konfigurationsassistenten von IBM Client Security.

Upgrade von CSS ab Version 5.0 mit vorhandenen Sicherheitsdaten durchführen

Gehen Sie wie folgt vor, um ein Upgrade von Client Security ab Version 5.0 unter Verwendung Ihrer vorhandenen Sicherheitsdaten durchzuführen:

1. Gehen Sie wie folgt vor, um Ihr Archiv zu aktualisieren:
   a. Klicken Sie auf **Start > Programme > Access IBM > IBM Client Security > Sicherheitseinstellungen ändern**.
   b. Klicken Sie auf die Schaltfläche **Schlüsselarchiv aktualisieren**, um Ihre Backup-Daten zu aktualisieren.

      Notieren Sie sich das Archivverzeichnis.
   c. Beenden Sie das Benutzerkonfigurationsprogramm von IBM Client Security.
2. Gehen Sie wie folgt vor, um für die vorhandene Version von IBM Client Security ein Upgrade durchzuführen:
   a. Klicken Sie auf dem Windows-Desktop auf **Start > Ausführen**.
   b. Geben Sie im Feld "Ausführen" `d:\Verzeichnis\csec5xxus_00yy.exe` ein, wobei `d:\Verzeichnis\` für den Laufwerkbuchstaben und das Verzeichnis steht, in dem sich die ausführbare Datei befindet. `xx` und `yy` bestehen aus alphanumerischen Zeichen.
   c. Wählen Sie die Option **Upgrade** aus.
   d. Führen Sie einen Neustart des Systems durch.

Client Security deinstallieren

Stellen Sie sicher, dass die verschiedenen Dienstprogramme (IBM Client Security Password Manager, Dienstprogramm zur Verschlüsselung von Dateien und Ordnern von IBM Client Security, FFE), die die Funktionalität von Client Security verbessern, deinstalliert wurden, bevor Sie IBM Client Security deinstallieren. Zum Deinstallieren von Client Security müssen Benutzer mit Administratorbenutzerrechten angemeldet sein.

Anmerkung: Vor dem Deinstallieren von IBM Client Security müssen Sie alle Dienstprogramme von IBM Client Security und die gesamte UVM-Sensorsoftware deinstallieren. Das Administratorkennwort ist zum Deinstallieren von Client Security erforderlich.

Gehen Sie wie folgt vor, um Client Security zu deinstallieren:

1. Schließen Sie alle Windows-Programme.
2. Klicken Sie auf dem Windows-Desktop auf **Start > Einstellungen > Systemsteuerung**.
3. Klicken Sie auf das Symbol **Software**.
4. Wählen Sie in der Liste der Software, die automatisch entfernt werden kann, den Eintrag **IBM Client Security** aus.
5. Klicken Sie auf **Ändern/Entfernen**.

6. Wählen Sie den Radioknopf **Entfernen** aus.
7. Klicken Sie auf **Weiter**, um die Software zu deinstallieren.
8. Klicken Sie auf **OK**, um diese Aktion zu bestätigen.
9. Geben Sie das Administratorkennwort in die vorgesehene Schnittstelle ein, und klicken Sie auf **OK**.
10. Führen Sie einen der folgenden Schritte aus:
    - Wenn Sie das PKCS #11-Modul des integrierten IBM Security Chips für Netscape installiert haben, wird eine Nachricht angezeigt, die Sie zum Starten des Inaktivierungsprozesses des PKCS #11-Moduls des integrierten IBM Security Chips auffordert. Klicken Sie auf **Ja**, um fortzufahren.

      Daraufhin wird Ihnen eine Reihe von Nachrichten angezeigt. Klicken Sie bei jeder einzelnen Nachricht so lange immer wieder auf **OK**, bis das PKCS #11-Modul des integrierten IBM Security Chips entfernt ist.
    - Wenn Sie das PKCS #11-Modul des integrierten IBM Security Chips für Netscape nicht installiert haben, wird eine Nachricht angezeigt, in der Sie gefragt werden, ob Sie die gemeinsam benutzten DLL-Dateien, die mit Client Security installiert wurden, löschen möchten.

      Klicken Sie auf **Ja**, um diese Dateien zu deinstallieren, oder klicken Sie auf **Nein**, wenn die installierten Dateien weiterhin installiert bleiben sollen. Wenn Sie die installierten Dateien beibehalten möchten, hat dies keinen Einfluss auf die normale Funktion des Computers.

    Die Nachricht mit dem Inhalt "Sollen die Daten zu diesem System aus dem Archiv gelöscht werden?" wird angezeigt. Wenn Sie **Nein** auswählen, können Sie diese Daten wiederherstellen, wenn Sie die aktuellere Version von IBM Client Security installieren.
11. Klicken Sie nach dem Entfernen der Software auf **Fertig stellen**.

    Nach dem Deinstallieren von Client Security müssen Sie den Computer erneut starten.

Beim Deinstallieren von Client Security werden alle installierten Softwarekomponenten von Client Security mit allen Benutzerschlüsseln, digitalen Zertifikaten, registrierten Fingerabdrücken und gespeicherten Kennwörtern entfernt.

Kapitel 5. Fehlerbehebung

Dieses Kapitel enthält nützliche Informationen zum Verhindern oder Erkennen und Beheben möglicher Fehler beim Installieren oder Konfigurieren von Client Security.

Administratorfunktionen

Benutzer autorisieren

Bevor Sie die Clientbenutzerinformationen schützen können, **muss** IBM Client Security auf dem Client installiert werden und die Benutzer **müssen** für diese Software berechtigt werden. Ein benutzerfreundlicher Konfigurationsassistent führt Sie durch den gesamten Installationsprozess.

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

Wenn Sie den Konfigurationsassistenten abgeschlossen haben, ohne Benutzer zu berechtigen, führen Sie einen Neustart Ihres Computers durch; führen Sie dann den Konfigurationsassistenten von Client Security vom Windows-Startmenü aus, und berechtigen Sie einen Windows-Benutzer für die Verwendung von UVM. Hierdurch übernimmt IBM Client Security Ihre Sicherheitseinstellungen und schützt Ihre schutzwürdigen Daten.

BIOS-Administratorkennwort festlegen (ThinkCentre)

Mit den im Programm "Configuration/Setup Utility" verfügbaren Sicherheitseinstellungen können die Administratoren folgende Vorgänge durchführen:

- Integriertes IBM Sicherheits-Subsystem aktivieren oder inaktivieren
- Inhalt des integrierten IBM Sicherheits-Subsystems löschen

Achtung:

- Wenn der Inhalt des integrierten IBM Sicherheits-Subsystems gelöscht wird, gehen alle auf dem Sicherheits-Subsystem gespeicherten Chiffrierschlüssel und Zertifikate verloren.

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. Schalten Sie den Computer aus, und starten Sie ihn erneut.
2. Wenn die Eingabeaufforderung für das Programm "Configuration/Setup Utility" am Bildschirm angezeigt wird, drücken Sie **F1**.

   Das Hauptmenü des Programms "Configuration/Setup Utility" wird geöffnet.
3. Wählen Sie **System Security** aus.
4. Wählen Sie **Administrator Password** aus.

5. Geben Sie Ihr Kennwort ein, und drücken Sie den Abwärtspfeil auf der Tastatur.
6. Geben Sie Ihr Kennwort erneut ein, und drücken Sie den Abwärtspfeil.
7. Wählen Sie **Change Administrator password** aus, und drücken Sie die Eingabetaste. Drücken Sie anschließend erneut die Eingabetaste.
8. Drücken Sie **Esc**, um die Einstellungen zu speichern und das Menü zu verlassen.

Wenn Sie ein BIOS-Administratorkennwort festgelegt haben, wird bei jedem Zugriff auf das Programm ″Configuration/Setup Utility″ eine Eingabeaufforderung angezeigt.

Wichtig: Notieren Sie sich das BIOS-Administratorkennwort, und bewahren Sie es an einem sicheren Platz auf. Wenn Sie das BIOS-Administratorkennwort verlieren oder vergessen, können Sie auf das Programm ″Configuration/Setup Utility″ nicht mehr zugreifen und das Kennwort nicht mehr ändern oder löschen, ohne die Abdeckung des Computers zu entfernen und eine Brücke auf die Systemplatine zu versetzen. Weitere Informationen hierzu finden Sie in der Hardwaredokumentation zu Ihrem Computer.

Administratorkennwort festlegen (ThinkPad)

Mit den im Programm ″IBM BIOS Setup Utility″ verfügbaren Sicherheitseinstellungen können die Administratoren folgende Tasks durchführen:

- Integriertes IBM Sicherheits-Subsystem aktivieren oder inaktivieren
- Inhalt des integrierten IBM Sicherheits-Subsystems löschen

Achtung:

- Auf einigen ThinkPad-Modellen müssen Sie das Administratorkennwort vorübergehend inaktivieren, bevor Sie Client Security installieren oder aktualisieren können.

Wenn Sie Client Security konfiguriert haben, legen Sie ein Administratorkennwort fest, um zu verhindern, dass diese Einstellungen durch nicht autorisierte Benutzer geändert werden.

Gehen Sie nach einer der beiden folgenden Prozeduren vor, um ein Administratorkennwort festzulegen:

Beispiel 1

1. Schalten Sie den Computer aus, und starten Sie ihn erneut.
2. Wenn die Eingabeaufforderung für das Konfigurationsdienstprogramm am Bildschirm angezeigt wird, drücken Sie die Taste F1.

   Das Hauptmenü des Konfigurationsdienstprogramms wird geöffnet.
3. Wählen Sie **Password** aus.
4. Wählen Sie **Supervisor Password** aus.
5. Geben Sie Ihr Kennwort ein, und drücken Sie die Eingabetaste.
6. Geben Sie Ihr Kennwort erneut ein, und drücken Sie die Eingabetaste.
7. Klicken Sie auf **Continue**.
8. Drücken Sie die Taste F10, um die Eingaben zu speichern und das Menü zu verlassen.

Beispiel 2

1. Schalten Sie den Computer aus, und starten Sie ihn erneut.
2. Wenn die Nachricht ″To interrupt normal startup, press the blue Access IBM button″ angezeigt wird, drücken Sie die blaue Taste ″Access IBM″.
   Access IBM Predesktop Area wird geöffnet.
3. Klicken Sie doppelt auf **Start setup utility**.
4. Navigieren Sie mit Hilfe der Cursortasten im Menü, und wählen Sie die Option **Security** aus.
5. Wählen Sie **Password** aus.
6. Wählen Sie **Supervisor Password** aus.
7. Geben Sie Ihr Kennwort ein, und drücken Sie die Eingabetaste.
8. Geben Sie Ihr Kennwort erneut ein, und drücken Sie die Eingabetaste.
9. Klicken Sie auf **Continue**.
10. Drücken Sie die Taste F10, um die Eingaben zu speichern und das Menü zu verlassen.

Wenn Sie ein Administratorkennwort festgelegt haben, wird bei jedem Zugriff auf das Programm ″IBM BIOS Setup Utility″ eine Eingabeaufforderung angezeigt.

Wichtig: Notieren Sie sich das Administratorkennwort, und bewahren Sie es an einem sicheren Platz auf. Wenn Sie das Administratorkennwort verlieren oder vergessen, können Sie auf das Programm ″IBM BIOS Setup Utility″ nicht mehr zugreifen und das Kennwort nicht mehr ändern oder löschen. Weitere Informationen hierzu finden Sie in der Hardwaredokumentation zu Ihrem Computer.

Inhalt des integrierten IBM Sicherheits-Subsystems löschen (ThinkCentre)

Wenn Sie alle Chiffrierschlüssel für Benutzer aus dem integrierten IBM Sicherheits-Subsystem entfernen und das Administratorkennwort für das Sicherheits-Subsystem löschen möchten, müssen Sie den Inhalt des Chips löschen. Lesen Sie die folgenden Hinweise, bevor Sie den Inhalt des integrierten IBM Sicherheits-Subsystems löschen.

Achtung:

- Wenn der Inhalt des integrierten IBM Sicherheits-Subsystems gelöscht wird, gehen alle auf dem Sicherheits-Subsystem gespeicherten Chiffrierschlüssel und Zertifikate verloren.

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

1. Schalten Sie den Computer aus, und starten Sie ihn erneut.
2. Wenn die Eingabeaufforderung für das Konfigurationsdienstprogramm am Bildschirm angezeigt wird, drücken Sie die Taste F1.
   Das Hauptmenü des Konfigurationsdienstprogramms wird geöffnet.
3. Wählen Sie **Security** aus.
4. Wählen Sie **IBM TCPA Security Feature** aus, und drücken Sie die Eingabetaste.
5. Klicken Sie auf **Yes**.
6. Drücken Sie die Eingabetaste, um die Auswahl zu bestätigen.
7. Drücken Sie die Taste F10, um Ihre Änderungen zu speichern und das Programm ″Setup Utility″ zu verlassen.
8. Wählen Sie **Yes** aus, und drücken Sie die Eingabetaste. Der Computer wird erneut gestartet.

Inhalt des integrierten IBM Sicherheits-Subsystems löschen (ThinkPad)

Wenn Sie alle Chiffrierschlüssel für Benutzer aus dem integrierten IBM Sicherheits-Subsystem entfernen und das Administratorkennwort löschen möchten, müssen Sie den Inhalt des Sicherheits-Subsystems löschen. Lesen Sie die folgenden Hinweise, bevor Sie den Inhalt des integrierten IBM Sicherheits-Subsystems löschen.

Achtung:

- Wenn der Inhalt des integrierten IBM Sicherheits-Subsystems gelöscht wird, gehen alle auf dem Sicherheits-Subsystem gespeicherten Chiffrierschlüssel und Zertifikate verloren.

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

1. Schalten Sie den Computer aus, und starten Sie ihn erneut.
2. Wenn die Eingabeaufforderung für das Konfigurationsdienstprogramm am Bildschirm angezeigt wird, drücken Sie die Taste F1.

   Das Hauptmenü des Konfigurationsdienstprogramms wird geöffnet.
3. Wählen Sie **Security** aus.
4. Wählen Sie **IBM Security Chip** aus, und drücken Sie die Eingabetaste.
5. Drücken Sie die Eingabetaste, und wählen Sie **Disabled** aus.
6. Drücken Sie die Eingabetaste, um die Auswahl zu bestätigen.
7. Drücken Sie die Eingabetaste, um fortzufahren.
8. Drücken Sie die Taste F10, um Ihre Änderungen zu speichern und das Programm "Setup Utility" zu verlassen.
9. Wählen Sie **Yes** aus, und drücken Sie die Eingabetaste. Der Computer wird erneut gestartet.

Bekannte Probleme und Einschränkungen bei CSS Version 5.4

Die folgenden Informationen sind möglicherweise beim Installieren und Konfigurieren von Client Security Version 5.4 hilfreich.

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 dem Register 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 5.4 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.

Einschränkungen bei Smartcards

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 ein Benutzeraccount registriert werden.

Fehlerbehebungstabellen

Der folgende Abschnitt enthält Fehlerbehebungstabellen, die sich beim Auftreten von Fehlern in Client Security Fehler als hilfreich erweisen können.

Fehlerbehebungsinformationen zur Installation

Die folgenden Informationen zur Fehlerbehebung können hilfreich sein, wenn bei der Installation von Client Security Fehler auftreten.

Fehlersymptom	**Mögliche Lösung**
Während der Softwareinstallation wird eine Fehlernachricht angezeigt	**Maßnahme**
Während der Softwareinstallation wird eine Nachricht angezeigt, in der Sie gefragt werden, ob Sie die ausgewählte Anwendung und alle zugehörigen Komponenten entfernen möchten.	Klicken Sie auf **OK**, um das Fenster zu schließen. Starten Sie den Installationsprozess noch ein Mal, um die neue Softwareversion von Client Security zu installieren.
Bei der Installation wird eine Nachricht angezeigt, dass Sie einen Programm-Upgrade durchführen oder dieses Programm entfernen müssen.	Führen Sie einen der folgenden Schritte aus: • Wenn eine ältere Client Security-Version als 5.0 installiert ist, wählen Sie **Entfernen** aus, und entfernen Sie das Programm. Starten Sie anschließend den Computer erneut, und löschen Sie den Inhalt des Sicherheits-Subsystems mit Hilfe des Programms "IBM BIOS Setup Utility". • Wählen Sie andernfalls **Upgrade** aus, und fahren Sie mit der Installation fort.
Unbekanntes Administratorkennwort. Installationszugriff wird nicht zugelassen	**Maßnahme**
Wenn Sie die Software auf einem IBM-Client mit einem aktivierten integrierten IBM Sicherheits-Subsystem installieren, ist das Administratorkennwort für das integrierte IBM Sicherheits-Subsystem unbekannt.	Löschen Sie den Inhalt des Sicherheits-Subsystems, um mit der Installation fortzufahren.

Fehlersymptom	Mögliche Lösung
Beim Versuch, bestimmte Administrator-funktionen von Client Security aufzurufen, wird eine Fehlernachricht angezeigt.	**Maßnahme**
Nach dem Versuch, eine Client Security-Administratorfunktion auszuführen, wird eine Fehlermeldung angezeigt.	Das ThinkPad-Administratorkennwort bzw. das ThinkCentre-BIOS-Administrator-kennwort muss inaktiviert sein, damit das Hardwareschlüsselpaar auf einem Crypto-1-System (kein TCG-System) generiert werden kann. Der CSS-Installationsprozess kann das integrierte IBM Sicherheits-Subsystem erst aktivieren, wenn das entsprechende Kenn-wort inaktiviert ist.

Anhang A. Informationen zu Kennwörtern und Verschlüsselungstexten

Dieser Anhang enthält Informationen zu Kennwörtern und Verschlüsselungstexten.

Regeln für Kennwörter und Verschlüsselungstexte

In einem sicheren System gibt es viele verschiedene Kennwörter und Verschlüsselungstexte. Für die verschiedenen Kennwörter gelten unterschiedliche Regeln. Dieser Abschnitt enthält Informationen zum Administratorkennwort sowie zum UVM-Verschlüsselungstext.

Regeln für Administratorkennwörter

Eine Schnittstelle im Administratordienstprogramm bietet für Sicherheitsadministratoren eine einfache Möglichkeit zur Steuerung von Kriterien für Administratorkennwörter. Diese Schnittstelle ermöglicht es einem Administrator, folgende Regeln für Administratorkennwörter festzulegen:

Anmerkung: Die Standardeinstellungen für die einzelnen Kennwortkriterien sind im Folgenden in Klammern angegeben. Für das Administratorkennwort gilt kein Verfallsdatum, das Kennwort ist unbegrenzt gültig.

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

  Wenn z. B. ″6″ erlaubte Zeichen definiert sind, ist `1234567xxx` ein ungültiges Kennwort.
- ob eine Mindestanzahl an Ziffern festgelegt werden soll (ja, 1)

  Wenn hierfür ″1″ festgelegt ist, ist `thisismypassword` ein ungültiges Kennwort.
- ob eine Mindestanzahl an Leerzeichen festgelegt werden soll (keine Mindestanzahl)

  Wenn hierfür ″2″ festgelegt ist, ist `i am not here` ein ungültiges Kennwort.
- ob der Verschlüsselungstext mit einer Ziffer beginnen darf (nein)

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

  Standardmäßig ist z. B. `password8` ein ungültiges Kennwort.

Für Administratorkennwörter gelten folgende allgemeine Regeln:

Länge Das Kennwort kann bis zu 256 Zeichen lang sein.

Zeichen
Das Kennwort kann sich aus jeder beliebigen Kombination von Zeichen zusammensetzen, die auf der Tastatur enthalten sind. Dazu gehören auch Leerzeichen und nicht-alphanumerische Zeichen.

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

Fehlversuche

Wenn das Administratorkennwort mehrere Male während einer Sitzung falsch eingegeben wird, führt der Computer eine Reihe entsprechender Verzögerungsaktionen (eine so genannte Anti-Hammering-Verzögerung) durch.

Regeln für UVM-Verschlüsselungstexte

In IBM Client Security können Administratoren Regeln für UVM-Verschlüsselungstexte der Benutzer festlegen. Zur Erhöhung der Sicherheit kann der UVM-Verschlüsselungstext länger und eindeutiger abgefasst sein 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 in Klammern angegeben.

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

  Wenn z. B. ″6″ erlaubte Zeichen definiert sind, ist `1234567xxx` ein ungültiges Kennwort.
- ob eine Mindestanzahl an Ziffern festgelegt werden soll (ja, 1)

  Wenn hierfür ″1″ festgelegt ist, ist `thisismypassword` ein ungültiges Kennwort.
- ob eine Mindestanzahl an Leerzeichen festgelegt werden soll (keine Mindestanzahl)

  Wenn hierfür ″2″ festgelegt ist, ist `i am not here` ein ungültiges Kennwort.
- ob der Verschlüsselungstext mit einer Ziffer beginnen darf (nein)

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

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

  Standardmäßig ist z. B. `Benutzername` ein ungültiges Kennwort, 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. `mypassword` ein ungültiges Kennwort, wenn eines der drei vorherigen Kennwörter `mypassword` war.
- ob der Verschlüsselungstext mehr als drei identische aufeinanderfolgende Zeichen des letzten Kennworts enthalten darf (nein)

  Standardmäßig ist z. B. `paswor` ein ungültiges Kennwort, wenn das vorherige Kennwort `pass` oder `word` lautete.

Das Fenster ″Policy für UVM-Verschlüsselungstext″ des Administratordienstprogramms stellt Sicherheitsadministratoren eine einfache Schnittstelle zur Steuerung des Ablaufs von Verschlüsselungstexten bereit. Über das Fenster ″Policy für UVM-Verschlüsselungstext″ kann der Administrator zwischen den folgenden Regeln für Verschlüsselungstexte auswählen:

- Entscheiden, ob der Verschlüsselungstext nach einer bestimmten Anzahl von Tagen ablaufen soll (ja, 184).

  Standardmäßig läuft der Verschlüsselungstext z. B. nach 184 Tagen ab. Der neue Verschlüsselungstext muss mit der festgelegten Policy für Verschlüsselungstexte übereinstimmen.
- Entscheiden, ob der Verschlüsselungstext ablaufen soll (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 umfassen.

Zeichen
Der Verschlüsselungstext kann sich aus jeder beliebigen Kombination von Zeichen zusammensetzen, die auf der Tastatur enthalten sind. Dazu gehören auch Leerzeichen und nicht alphanumerische Zeichen.

Merkmale
Der UVM-Verschlüsselungstext weicht von einem Kennwort, das Sie für die Anmeldung an einem Betriebssystem verwenden können, ab. Der UVM-Verschlüsselungstext kann zusammen mit anderen Authentifizierungseinheiten, wie z. B. einem UVM-Sensor für Fingerabdrücke, verwendet werden.

Fehlversuche
Wenn Sie den UVM-Verschlüsselungstext während einer Sitzung mehrmals falsch eingeben, führt der Computer eine Reihe von Anti-Hammering-Verzögerungen aus. Diese Verzögerungen werden im folgenden Abschnitt näher beschrieben.

Anzahl der Fehlversuche für Systeme mit National TPM

In der folgenden Tabelle sind die Einstellungen für die Verzögerungsaktionen in Systemen mit National TPM dargestellt:

Versuche	Verzögerung beim nächsten Fehlversuch
7 - 13	jeweils 4 Sekunden
14 - 20	jeweils 8 Sekunden
21 - 27	jeweils 16 Sekunden
28 - 34	jeweils 32 Sekunden
35 - 41	jeweils 64 Sekunden (jeweils 1,07 Minuten)
42 - 48	jeweils 128 Sekunden (jeweils 2,13 Minuten)
49 - 55	jeweils 256 Sekunden (jeweils 4,27 Minuten)
56 - 62	jeweils 512 Sekunden (jeweils 8,53 Minuten)
63 - 69	jeweils 1.024 Sekunden (jeweils 17,07 Minuten)
70 - 76	jeweils 2.048 Sekunden (jeweils 34,13 Minuten)
77 - 83	jeweils 68,26 Minuten (jeweils 1,14 Stunden)

Versuche	Verzögerung beim nächsten Fehlversuch
84 - 90	jeweils 136,52 Minuten (jeweils 2,28 Stunden)
91 - 97	jeweils 273,04 Minuten (jeweils 4,55 Stunden)
98 - 104	jeweils 546,08 Minuten (jeweils 9,1 Stunden)
105 - 111	jeweils 1.092,16 Minuten (jeweils 18,2 Stunden)
112 - 118	jeweils 2.184,32 Minuten (jeweils 36,4 Stunden)

Auf Systemen mit National TPM findet keine Unterscheidung zwischen Benutzerverschlüsselungstexten und Administratorkennwort statt. Jede Authentifizierung über den integrierten IBM Security Chip unterliegt der gleichen Policy. Es gibt keinen Maximalwert für eine Zeitlimitüberschreitung. Jeder fehlgeschlagene Anmeldeversuch aktiviert eine Verzögerungaktion, wie in der Tabelle angegeben. Die Anti-Hammering-Verzögerungen enden nicht mit dem 118. Versuch. Sie werden nach den in der Tabelle angegebenen Regeln unendlich weitergeführt.

Anzahl der Fehlversuche für Systeme mit Atmel TPM

In der folgenden Tabelle sind die Einstellungen für die Verzögerungsaktionen in Systemen mit Atmel TPM dargestellt:

Versuche	Verzögerung beim nächsten Fehlschlagen
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 Systemen mit Atmel TPM findet keine Unterscheidung zwischen Benutzerverschlüsselungstexten und Administratorkennwort statt. Jede Authentifizierung über den integrierten IBM Security Chip unterliegt der gleichen Policy. Das maximale Zeitlimit liegt bei 4,7 Stunden. Systeme mit Atmel TPM führen keine Verzögerungsaktionen durch, die länger als 4,7 Stunden dauern.

Verschlüsselungstext zurücksetzen

Wenn ein Benutzer seinen Verschlüsselungstext vergisst, kann der Administrator den Benutzer diesen Verschlüsselungstext wiederherstellen lassen.

Verschlüsselungstext über Remotezugriff zurücksetzen

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

- **Administratoren**

  Ein ferner Administrator muss wie folgt vorgehen:

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

     Die Datendatei kann dem Benutzer per E-Mail gesendet werden, auf einen austauschbaren Datenträger wie z. B. eine Diskette kopiert werden oder direkt in die Archivdatei des Benutzers geschrieben werden (vorausgesetzt, dass der Benutzer auf dieses System zugreifen kann). Diese verschlüsselte Datei wird zum Abgleich mit dem neuen Kennwort für den einmaligen Gebrauch verwendet.

- **Benutzer**

  Der Benutzer muss wie folgt vorgehen:

  1. Melden Sie sich am Computer an.
  2. Wenn Sie zum Eingeben des Verschlüsselungstextes aufgefordert werden, wählen Sie das Markierungsfeld ″Verschlüsselungstext vergessen″ aus.
  3. Geben Sie das Kennwort für den einmaligen Gebrauch, das der ferne Administrator Ihnen mitgeteilt hat, ein, und geben Sie die Position der vom Administrator gesendeten Datei an.

     Nachdem UVM überprüft hat, ob die Informationen in der Datei mit dem angegebenen Verschlüsselungstext übereinstimmen, wird dem Benutzer Zugriff gewährt. Der Benutzer wird dann unverzüglich aufgefordert, den Verschlüsselungstext zu ändern.

Dies ist die empfohlene Vorgehensweise, um einen vergessenen Verschlüsselungstext wiederherzustellen.

Verschlüsselungstext manuell zurücksetzen

Wenn der Administrator direkt auf das System des Benutzers, der seinen Verschlüsselungstext vergessen hat, zugreifen kann, kann er sich am System des Benutzers als Administrator anmelden, im Administratordienstprogramm den privaten Administratorschlüssel angeben und manuell den Verschlüsselungstext des Benutzers ändern. Der Administrator muss zum Ändern des Verschlüsselungstextes den alten Verschlüsselungstext des Benutzers nicht kennen.

Anhang B. Bemerkungen und Marken

Dieser Anhang enthält rechtliche Hinweise auf IBM Produkte sowie Informationen zu den 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 IBM Produkte, Programme oder Dienstleistungen können auch andere ihnen äquivalente Produkte, Programme oder Dienstleistungen verwendet werden, solange diese keine gewerblichen oder anderen Schutzrechte der IBM verletzen. Die Verantwortung für den Betrieb von Fremdprodukten, Fremdprogrammen und Fremddienstleistungen liegt beim Kunden.

Für in diesem Handbuch beschriebene Erzeugnisse und Verfahren kann es IBM Patente oder 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 Handbuch aufgeführten Lizenzprogramms sowie des zugehörigen Lizenzmaterials erfolgt im Rahmen der Allgemeinen Geschäftsbedingungen der IBM, der ICA-Lizenzbedingungen (IBM Customer Agreement), der IPLA-Lizenzbedingungen (International Program License Agreement) oder einer äquivalenten Vereinbarung.

Marken

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

Tivoli ist in gewissen Ländern eine Marke der 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.