IBM Client Security Implementierungshandbuch Version 5.4.0

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.

Vierte Ausgabe (November 2004)

Diese Veröffentlichung ist eine Übersetzung des Handbuchs
IBM Client Security Deployment Guide, Version 5.4.0,
herausgegeben von International Business Machines Corporation, USA

Herausgegeben von:
SW TSC Germany
Kst. 2877
November 2004

Vorwort

IT-Administratoren müssen bei der Implementierung von IBM Client Security zahlreiche Faktoren kennen und berücksichtigen. In diesem Handbuch wird die unternehmensweite Softwareimplementierung auf Computern mit integriertem IBM Security Chip behandelt, nicht jedoch die Verwendung des Chips von IBM Embedded Security Subsystem oder von Client Security.

Zielgruppe

Dieses Handbuch ist für IT-Administratoren vorgesehen oder für Personen, die für die Implementierung von IBM Client Security Version 5.4 (CSS) auf den Computern in ihrem Unternehmen verantwortlich sind. Dieses Handbuch enthält die erforderlichen Informationen zur Installation von IBM Client Security auf einem oder mehreren Computern. Bevor Sie dieses Handbuch lesen, sollten Sie sich mit dem *IBM Client Security Administrator- und Benutzerhandbuch Version 5.4* vertraut machen. Neben dem *IBM Client Security Administrator- und Benutzerhandbuch Version 5.4* stehen Ihnen Anwendungshilfen zur Verfügung, in denen Sie Informationen zur Verwendung der Anwendung finden können.

Produktveröffentlichungen

Die Bibliothek von Client Security Version 5.4 enthält folgende Dokumente:

- *IBM Client Security Administrator- und Benutzerhandbuch Version 5.4*:

  Dieses Handbuch enthält Informationen zur Konfiguration und zur Verwendung der Sicherheitsfunktionen von Client Security sowie zur Ausführung von Tasks mit Client Security, wie z. B. zum UVM-Anmeldeschutz, zum Einrichten des Client Security-Bildschirmschoners, zur Erstellung eines digitalen Zertifikats und zur Verwendung des Benutzerkonfigurationsdienstprogramms.
- *IBM Client Security Installationshandbuch Version 5.4*:

  Dieses Handbuch enthält Informationen zur Installation von Client Security auf IBM Netzwerkcomputern, auf denen der integrierte IBM Security Chip installiert ist.

Zusätzliche Informationen

Zusätzliche Informationen und Aktualisierungen für Sicherheitsprodukte werden auf IBM Website unter http://www.pc.ibm.com/us/security/index.html bereitgestellt.

Inhaltsverzeichnis

Vorwort iii
Zielgruppe iii
Produktveröffentlichungen iii
Zusätzliche Informationen iii

Kapitel 1. Hinweise zur Implementierung von IBM Client Security 1
Voraussetzungen und Spezifikationen für die Implementierung 1

Kapitel 2. Client Security installieren . . 3
Standardinstallation 3
Administrative Installation. 4
Befehlszeilenparameter 4
Angepasste öffentliche Eigenschaften in Client Security 6
Installationsfunktionen von Client Security 6
Beispiele unter Verwendung von Setup.exe . . . 7

Kapitel 3. Funktionsweise des integrierten IBM Security Chips 9
Schlüsselauslagerungshierarchie 12
Gründe für die Schlüsselauslagerung 12

Kapitel 4. Wichtige Hinweise zur Schlüsselarchivierung 13
Warum ist ein Administratorschlüsselpaar erforderlich? 17

Kapitel 5. IBM Client Security 27
Benutzer registrieren und Registrierung verwalten 27
Einen Verschlüsselungstext erfordern 28
Einen Verschlüsselungstext festlegen 28
Einen Verschlüsselungstext verwenden 29
TPM-Initialisierung 32
Bewährte Verfahren. 33
Benutzerinitialisierung. 35
Persönliche Initialisierung 36
Implementierungsszenarien 37
Informationen zur Konfigurationsdatei 41

Kapitel 6. Client Security-Komponente auf einem Tivoli Access Manager-Server installieren 47
Voraussetzungen 47
Client Security-Komponente herunterladen und installieren. 47
Client Security-Komponenten auf dem Tivoli Access Manager-Server hinzufügen 48
Sichere Verbindung zwischen dem IBM Client und dem Tivoli Access Manager-Server aufbauen . . . 49
IBM Clients konfigurieren 51
Voraussetzungen 51
Informationen zur Konfiguration von Tivoli Access Manager angeben 51
Lokalen Cache definieren und verwenden . . . 52
Tivoli Access Manager zur Steuerung von IBM Client-Objekten aktivieren 53
Fehlerbehebungstabellen 55
Fehlerbehebungsinformationen zu digitalen Zertifikaten 55
Fehlerbehebungsinformationen zu Tivoli Access Manager 55
Fehlerbehebungsinformationen zu Lotus Notes 56
Fehlerbehebungsinformationen zur Verschlüsselung 57

Kapitel 7. Treiber für Hardwareeinheiten von Fremdanbietern zur Ergänzung von IBM Client Security installieren . . 59

Kapitel 8. Neue oder überarbeitete Sicherheitspolicy-Dateien über Remotezugriff implementieren 61

Anhang. Bemerkungen 63
Websites anderer Anbieter 64
Marken 64

Kapitel 1. Hinweise zur Implementierung von IBM Client Security

Die zentrale Implementierung von IBM Client Security Version 5.4.0 erfolgt über den erweiterten Konfigurationsmodus im Installationsassistenten von IBM Client Security. Unter IBM Client Security Version 5.4 werden keine Original-Sicherheitschips (ohne TCPA) unterstützt. Benutzer solcher Systeme müssen Client Security Version 5.3 verwenden.

Die Software "IBM Client Security" (CSS), die die Hardware von IBM Embedded Security Subsystem auf IBM PCs verwendet, kann auf unterschiedliche Weise implementiert werden. In diesem Dokument wird erläutert, wie Sie ESS in Ihrer Umgebung implementieren können. Besonderes Augenmerk gilt der Implementierung von Computern in Ihrem Unternehmen von der Image-Erstellung bis zur Bereitstellung für den Endbenutzer. Dieser Prozess hat großen Einfluss auf den Einsatz von ESS in Ihrem Unternehmen. IBM ESS besteht im Wesentlichen aus zwei Komponenten, die in Abb. 1 dargestellt sind:

1. IBM Client Security
2. Integrierter IBM Security Chip

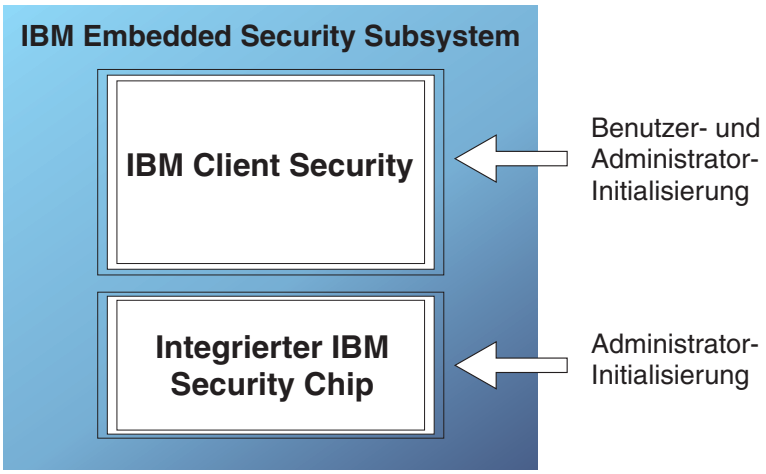

Abbildung 1. Komponenten des IBM Client Security-Systems

Voraussetzungen und Spezifikationen für die Implementierung

Für die Installation von IBM Client Security auf Computern mit integriertem IBM Security Chip gelten folgende Voraussetzungen und Spezifikationen:

1. IBM PC mit integriertem IBM Security Chip
2. Serverspeicherbedarf für installierbaren Code: ca. 12 MB
3. Durchschnittlicher Serverspeicherbedarf für wichtige Archivdaten pro Benutzer: 200 KB pro Benutzer als Archivierungsspeicher

Kapitel 2. Client Security installieren

In diesem Kapitel werden zwei unterschiedliche Möglichkeiten zur Installation von Client Security beschrieben: die Standardinstallation und die administrative Installation.

Standardinstallation

Bei der Datei "z046zis2018usaa.exe" handelt es sich um ein selbst extrahierendes Installationspaket, bei dem die Quellendateien für die Installation extrahiert werden und die Installation gestartet wird. Für diese Datei können eine Reihe von Befehlszeilenparametern angegeben werden, die weiter unten beschrieben werden. Die Befehlszeilenoptionen, für die ein Parameter erforderlich ist, müssen ohne Leerzeichen zwischen der Option und dem zugehörigen Parameter angegeben werden. Beispiel: `z046zis2018usaa.exe /s /v"/qn REBOOT="R""` ist zulässig, während `Setup.exe /s /v "/qn REBOOT="R""` nicht zulässig ist (**"/qn REBOOT="R""** ist ein Parameter zur Option **/v**). Anführungszeichen sind bei Optionsparametern nur erforderlich, wenn der Parameter Leerzeichen enthält.

Wenn Sie die Datei "Setup.exe" ohne Parameter ausführen, wird die Installation über eine Benutzeroberfläche durchgeführt. Dabei werden Sie am Ende des Installationsvorgangs standardmäßig zur Durchführung eines Neustarts aufgefordert. Bei einer Installation ohne Benutzeroberfläche wird am Ende des Installationsvorgangs standardmäßig ein Neustart durchgeführt. Mit der Eigenschaft REBOOT kann der Neustart allerdings auch später durchgeführt werden (Erläuterungen hierzu finden Sie oben und im Abschnitt mit den Beispielen).

/a Mit diesem Parameter führt die .exe-Datei eine administrative Installation durch. Bei einer administrativen Installation werden Ihre Datendateien in ein vom Benutzer festgelegtes Verzeichnis kopiert. Allerdings werden keine Verknüpfungen erstellt, keine COM-Server registriert und kein Deinstallationsprotokoll generiert.

/x Mit diesem Parameter deinstalliert die .exe-Datei ein zuvor installiertes Produkt.

/s Silent mode
Mit diesem Parameter wird die .exe-Datei im Befehlszeilenmodus als automatische Installation ausgeführt.

/v Der Parameter **/v** wird verwendet, um Befehlszeilenswitches und Werte öffentlicher Eigenschaften an die Datei "Msiexec.exe" zu übergeben.

/w Mit diesem Parameter wird die .exe-Datei gezwungen, vor dem Schließen auf den Abschluss des Installationsvorgangs zu warten. Wenn Sie diesen Parameter in einer Batchdatei verwenden, können Sie dem gesamten Befehlszeilenargument der .exe-Datei den Parameter `start /WAIT` voranstellen. Beispiel für eine ordnungsgemäße Verwendung:

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

Administrative Installation

Microsoft Windows Installer kann eine administrative Installation für eine Anwendung oder ein Produkt in einem Netzwerk zur Verwendung durch eine Arbeitsgruppe oder zur Anpassung durchführen. Bei dem Installationspaket für Client Security werden die Quellendateien bei einer administrativen Installation an einer angegebenen Speicherposition entpackt. Zur Durchführung einer administrativen Installation muss das Konfigurationspaket unter Verwendung des Parameters **/a** über die Befehlszeile ausgeführt werden:

```
z046zis2018usaa.exe /a
```

Sie können auch eine neue Speicherposition auswählen. Dabei können andere Laufwerke als Laufwerk C: angegeben werden, wie z. B. andere lokale Laufwerke, zugeordnete Netzlaufwerke usw. Bei diesem Schritt können auch neue Verzeichnisse erstellt werden.

Wenn eine administrative Installation automatisch ausgeführt wird, kann die öffentliche Eigenschaft TARGETDIR in der Befehlszeile so festgelegt werden, dass sie die Speicherposition für die extrahierten Daten angibt:

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

oder

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

Wenn Sie die entpackte Quellendatei nach der Durchführung von Anpassungen installieren möchten, müssen Sie die Datei ″msiexec.exe″ über die Befehlszeile aufrufen. Im Abschnitt „Befehlszeilenparameter″ werden die verfügbaren Befehlszeilenparameter beschrieben, die für die Datei ″msiexec.exe″ verwendet werden können. Außerdem wird ein Verwendungsbeispiel angegeben. Öffentliche Eigenschaften können auch direkt beim Aufrufen von ″msiexec″ über die Befehlszeile festgelegt werden.

Befehlszeilenparameter

/i *Paket* **oder** *Produkt*

Verwenden Sie zur Installation des Produkts folgendes Format:

```
msiexec /i "C:\WindowsOrdner\Profiles\Benutzername\Personal\MySetups\Othello
\TrialVersion\Release\DiskImages\Disk1\ProduktOthello Beta.msi"
```

Der Produktschlüssel bezieht sich auf die GUID, die in der Produktschlüsseleigenschaft in der Projektanzeige Ihres Produkts automatisch generiert wird. **Anmerkung:** Das oben angegebene Beispiel wurde auf zwei Zeilen aufgeteilt, damit es auf die Seite passt. Geben Sie den Befehl in eine Zeile ein.

/a *Paket*

Mit dem Parameter **/a** können Benutzer mit Administratorrechten ein Produkt im Netzwerk installieren.

/x *Paket* **oder** *Produktschlüssel*

Mit diesem Parameter wird ein Produkt deinstalliert.

/L [i|w|e|a|r|u|c|m|p|v|+] *Protokolldatei*

Mit diesem Parameter wird der Pfad zur Protokolldatei angegeben. Die folgenden Flags geben an, welche Informationen in der Protokolldatei erfasst werden:

- **i**

Protokolliert Statusnachrichten

- **w**
  Protokolliert unkritische Warnungen
- **e**
  Protokolliert alle Fehlernachrichten
- **a**
  Protokolliert den Anfang von Aktionssequenzen
- **r**
  Protokolliert aktionsspezifische Datensätze
- **u**
  Protokolliert Benutzeranforderungen
- **c**
  Protokolliert die Schnittstellenparameter von Erstbenutzern
- **m**
  Protokolliert Nachrichten bei fehlendem Arbeitsspeicher
- **p**
  Protokolliert Terminaleinstellungen
- **v**
  Protokolliert die Einstellung für ausführliche Ausgabe
- **+**
  Fügt Anhänge an eine vorhandene Datei an
- *
  Ist ein Platzhalterzeichen, mit dem Sie sämtliche Informationen außer der Einstellung für ausführliche Ausgabe protokollieren können

/? oder /h
Bei beiden Befehlen wird der Copyrightvermerk zu Windows Installer angezeigt

TRANSFORMS
Mit dem Befehlszeilenparameter TRANSFORMS können Sie beliebige Umwandlungen festlegen, die auf Ihr Basispaket angewendet werden sollen. Der Aufruf des Parameters TRANSFORMS über die Befehlszeile kann z. B. wie folgt aussehen:

```
msiexec /i "C:\WindowsOrdner\Profiles\Benutzername\Personal\MySetups\Projektname\
Testversion\Meine Version-1\DiskImages\Disk1\Produktname.msi"
TRANSFORMS="New Transform 1.mst"
```

Da mehrere Umwandlungen durch ein Semikolon voneinander getrennt werden können, ist es empfehlenswert, im Namen der Umwandlung keine Semikolons zu verwenden, weil sie von Windows Installer falsch interpretiert werden würden.

Anmerkung: Das oben angegebene Beispiel wurde auf drei Zeilen aufgeteilt, damit es auf die Seite passt. Geben Sie den Befehl in eine Zeile ein.

Eigenschaften
Sämtliche öffentlichen Eigenschaften können über die Befehlszeile festgelegt oder geändert werden. Öffentliche Eigenschaften unterscheiden sich von privaten Eigenschaften dadurch, dass sie nur aus Großbuchstaben bestehen. Beispielsweise ist COMPANYNAME eine öffentliche Eigenschaft.

Verwenden Sie folgende Syntax, um eine Eigenschaft über die Befehlszeile festzulegen: EIGENSCHAFT=WERT. Um den Wert der Eigenschaft *COMPANYNAME* zu ändern, müssten Sie Folgendes eingeben:

```
msiexec /i "C:\WindowsOrdner\Profiles\Benutzername\Personal\MySetups\Projektname\
Trial Version\Meine Version-1\DiskImages\Disk1\ProductName.msi"
COMPANYNAME="InstallShield"
```

Anmerkung: Das oben angegebene Beispiel wurde auf drei Zeilen aufgeteilt, damit es auf die Seite passt. Geben Sie den Befehl in eine Zeile ein.

Angepasste öffentliche Eigenschaften in Client Security

Das Installationspaket für Client Security enthält eine Reihe angepasster öffentlicher Eigenschaften, die beim Installationsvorgang über die Befehlszeile festgelegt werden können. Zu den derzeit verfügbaren angepassten öffentlichen Eigenschaften gehören:

INSTALLPWM
Mit dieser Eigenschaft können Sie steuern, ob Password Manager bei der Erstinstallation installiert wird. Wenn Sie den Wert 1 angeben, wird Password Manager installiert. Wenn Sie den Wert 0 angeben, wird Password Manager nicht installiert. Der Standardwert ist 1.

CFGFILE
Diese Eigenschaft kann bei einer automatischen Installation verwendet werden, um die Speicherposition einer Konfigurationsdatei anzugeben. Die Konfigurationsdatei kann den Wert des vorhandenen Kennworts für den Security Chip enthalten. Dadurch kann die Installation ohne Interaktion des Benutzers abgeschlossen werden, auch wenn bereits ein Kennwort im Chip gespeichert ist. Beispiel:

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

Installationsfunktionen von Client Security

Die Installation per Mausklick von Client Security beinhaltet zwei Hauptfunktionen: *Security* (IBM Client Security) und *PWManager* (IBM Password Manager). Standardmäßig werden beide Funktionen installiert. Allerdings können Sie bei der Installation mehrere Optionen auswählen, so dass nur die Security-Funktion installiert wird (die Security-Funktion ist obligatorisch, die PWManager-Funktion ist nicht obligatorisch). Wenn der Benutzer die Installation über eine Benutzeroberfläche ausführt und IBM Password Manager bis Version 1.3 noch nicht installiert ist, erscheint eine Anzeige, in der der Benutzer auswählen muss, ob nur IBM Client Security installiert werden soll oder IBM Client Security und IBM Password Manager. Wenn der Benutzer die Installation ohne Benutzeroberfläche (automatisch) ausführt, kann er mit Hilfe der Eigenschaft INSTALLPWM steuern, ob Password Manager installiert wird oder nicht (bei Angabe des Werts 0 wird Password Manager nicht installiert). Wenn der Benutzer bei der Erstinstallation nur IBM Client Security installiert und IBM Password Manager nachträglich installieren möchte, ist dies durch nochmaliges Ausführen des ursprünglichen Installationspakets möglich. Wenn die Installation erneut über eine Benutzeroberfläche ausgeführt wird, erscheint eine Anzeige, in der der Benutzer auf die Schaltfläche “Ändern” klicken kann, wenn Password Manager noch nicht installiert wurde. Daraufhin erscheint eine Anzeige, in der ausgewählt werden kann, ob wieder nur Client Security installiert werden soll, oder ob IBM Client Security und IBM Password Manager installiert werden sollen. Der Benutzer kann das Produkt auch ohne Benutzeroberfläche erneut installieren, um IBM Password Manager hinzuzufügen. Beispiele für diesbezügliche Befehle finden Sie im Folgenden.

Beispiele unter Verwendung von Setup.exe

Tabelle 1 enthält Beispiele für Installationen unter Verwendung der Datei "z046zis2018usaa.exe".

Tabelle 1. Beispiele für Installationen unter Verwendung der Datei "z046zis2018usaa.exe"

Typ	Beispiel
Automatische Installation mit Neustart am Ende des Installationsvorgangs	`z046zis2018usaa.exe /s /v/qn`
Automatische Installation ohne Neustart	`z046zis2018usaa.exe /s /v"/qn REBOOT="R""`
Automatische Installation ohne Neustart und ohne Installation von Password Manager	`z046zis2018usaa.exe /s /v"/qn REBOOT="R" INSTALLPWM=0"`
Automatische Installation ohne Neustart und mit Angabe des Installationsverzeichnisses	`z046zis2018usaa.exe /s /v"/qn REBOOT="R" INSTALLDIR=C:\ibmcss"`
Automatische Konfiguration ohne Neustart und mit Angabe der Konfigurationsdatei	`z046zis2018usaa.exe /s /v"/qn REBOOT="R" CFGFILE=C:\csec.ini"`
Automatische administrative Installation	`z046zis2018usaa.exe /a`
Automatische administrative Installation mit Angabe der Position für die extrahierten Daten	`z046zis2018usaa.exe /a /s /v"/qn TARGETDIR="F:\CSS""`
Installation ohne Neustart und mit Erstellung eines Installationsprotokolls im temporären Verzeichnis	`z046zis2018usaa.exe /v"REBOOT="R" /L*v %temp%\css.log"`
Automatische Neuinstallation des Produkts zum Hinzufügen von Password Manager	`z046zis2018usaa.exe /s /v"/qn ADDLOCAL=PWManager"`

Tabelle 2 enthält Beispiele für Installationen unter Verwendung der Datei "msiexec.exe".

Tabelle 2. Installation unter Verwendung der Datei "msiexec.exe"

Typ	Beispiel
Installation mit Protokolldatei	`msiexec /i "C:\IBM Client Security Software.msi" /L*v %temp%\css.log`
Automatische Installation ohne Neustart	`msiexec /i "C:\IBM Client Security Software.msi" /qn REBOOT="R"`
Automatische Installation ohne Neustart und ohne Installation von Password Manager	`msiexec /i "C:\IBM Client Security Software.msi" /qn REBOOT="R" INSTALLPWM=0`
Automatische Neuinstallation des Produkts zum Hinzufügen von Password Manager	`msiexec /i "C:\IBM Client Security Software.msi" /qn ADDLOCAL=PWManager`

Kapitel 3. Funktionsweise des integrierten IBM Security Chips

Der integrierte IBM Security Chip ist in Abb. 2 grafisch dargestellt. Er beinhaltet drei Hauptkomponenten:

1. Administratorkennwort
2. Öffentlicher Hardwareschlüssel
3. Privater Hardwareschlüssel

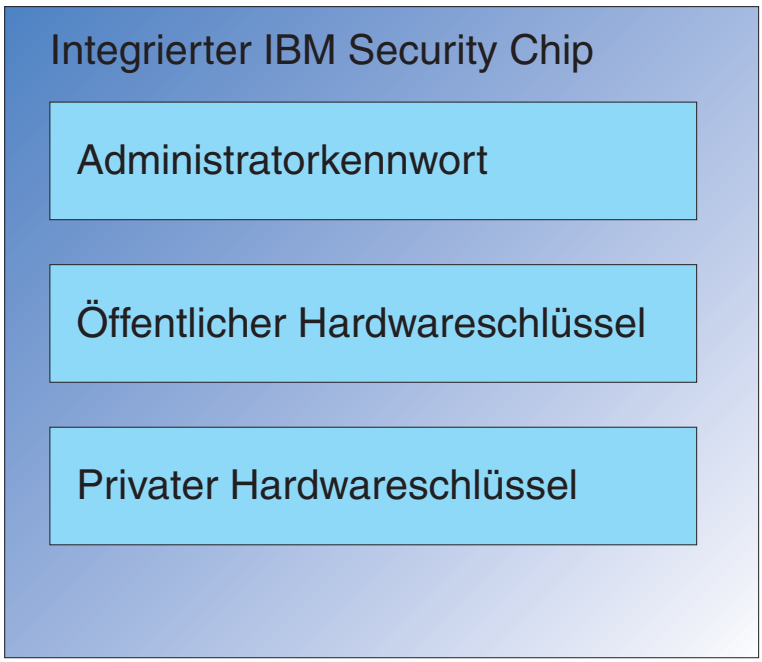

Abbildung 2. Im integrierten IBM Security Chip enthaltene Daten

Der öffentliche und der private Hardwareschlüssel sind auf jedem Computer eindeutig festgelegt. Der private Hardwareschlüssel kann niemals vom Chip extrahiert werden. Neue Schlüsselpaare können wie folgt generiert werden:

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

Beachten Sie, dass die Hardwareschlüssel nicht vom Chip extrahiert werden können.

Der Administrator greift mit Hilfe des Administratorkennworts auf folgende Funktionen zu:

- Hinzufügen von Benutzern
- Festlegen der Sicherheitspolicy
- Festlegen der Verschlüsselungstextpolicy
- Registrieren von Smart-Cards
- Registrieren biometrischer Sicherheitseinrichtungen

Ein Administrator muss beispielsweise einen weiteren Benutzer einrichten, damit dieser die Funktionen des integrierten IBM Security Chips nutzen kann. Das Administratorkennwort wird bei der Installation von Client Security festgelegt. Das Verfahren und der Zeitpunkt für das Festlegen des Administratorkennworts werden später in diesem Dokument ausführlich behandelt.

Wichtig: Sie müssen eine Strategie zur Verwaltung der Administratorkennwörter entwickeln, die während der ersten Konfiguration von ESS festgelegt werden muss. Es ist möglich, dass jeder Computer mit einem integrierten Security Chip über dasselbe Administratorkennwort verfügt, wenn dies vom IT-Administrator oder vom Sicherheitsadministrator festgelegt wird. Jeder Abteilung oder jedem Gebäude können jedoch auch unterschiedliche Administratorkennwörter zugewiesen werden.

Bei den anderen Komponenten des integrierten IBM Security Chips handelt es sich um den öffentlichen und den privaten Hardwareschlüssel. Dieses RSA-Schlüsselpaar wird bei der Konfiguration von Client Security generiert.

Jeder Computer verfügt über einen eindeutigen öffentlichen und einen eindeutigen privaten Hardwareschlüssel. Durch die Verwendung von Zufallszahlen im integrierten IBM Security Chip wird gewährleistet, dass jedes Hardwareschlüsselpaar statistisch eindeutig ist.

In Abb. 3 auf Seite 11 werden zwei weitere Komponenten des integrierten IBM Security Chips beschrieben. Die Funktionsweise dieser zwei Komponenten zu kennen, ist für eine effektive Verwaltung der Infrastruktur von IBM Embedded Security Subsystem von entscheidender Bedeutung. In Abb. 3 auf Seite 11 werden der öffentliche und der private Administratorschlüssel sowie die öffentlichen und privaten Benutzerschlüssel dargestellt. Im Folgenden erhalten Sie eine Zusammenfassung der Informationen zu öffentlichen und privaten Schlüsseln:

- Die Kombination aus einem öffentlichen und einem privaten Schlüssel wird als "Schlüsselpaar" bezeichnet.
- Zwischen einem privaten und einem öffentlichen Schlüssel bestehen die folgenden mathematischen Beziehungen:
  - Alle mit dem öffentlichen Schlüssel verschlüsselten Daten können nur mit dem privaten Schlüssel entschlüsselt werden.
  - Alle mit dem privaten Schlüssel verschlüsselten Daten können nur mit dem öffentlichen Schlüssel entschlüsselt werden.
  - Selbst wenn Sie den privaten Schlüssel kennen, können Sie daraus nicht den öffentlichen Schlüssel ableiten.
  - Selbst wenn Sie den öffentlichen Schlüssel kennen, können Sie daraus nicht den privaten Schlüssel ableiten.
  - Der öffentliche Schlüssel wird im Allgemeinen jedem Benutzer zur Verfügung gestellt.
- Der private Schlüssel muss unbedingt geschützt werden.
- Öffentliche und private Schlüssel stellen die Grundlage für eine PKI-Infrastruktur (Public Key Infrastructure) dar.

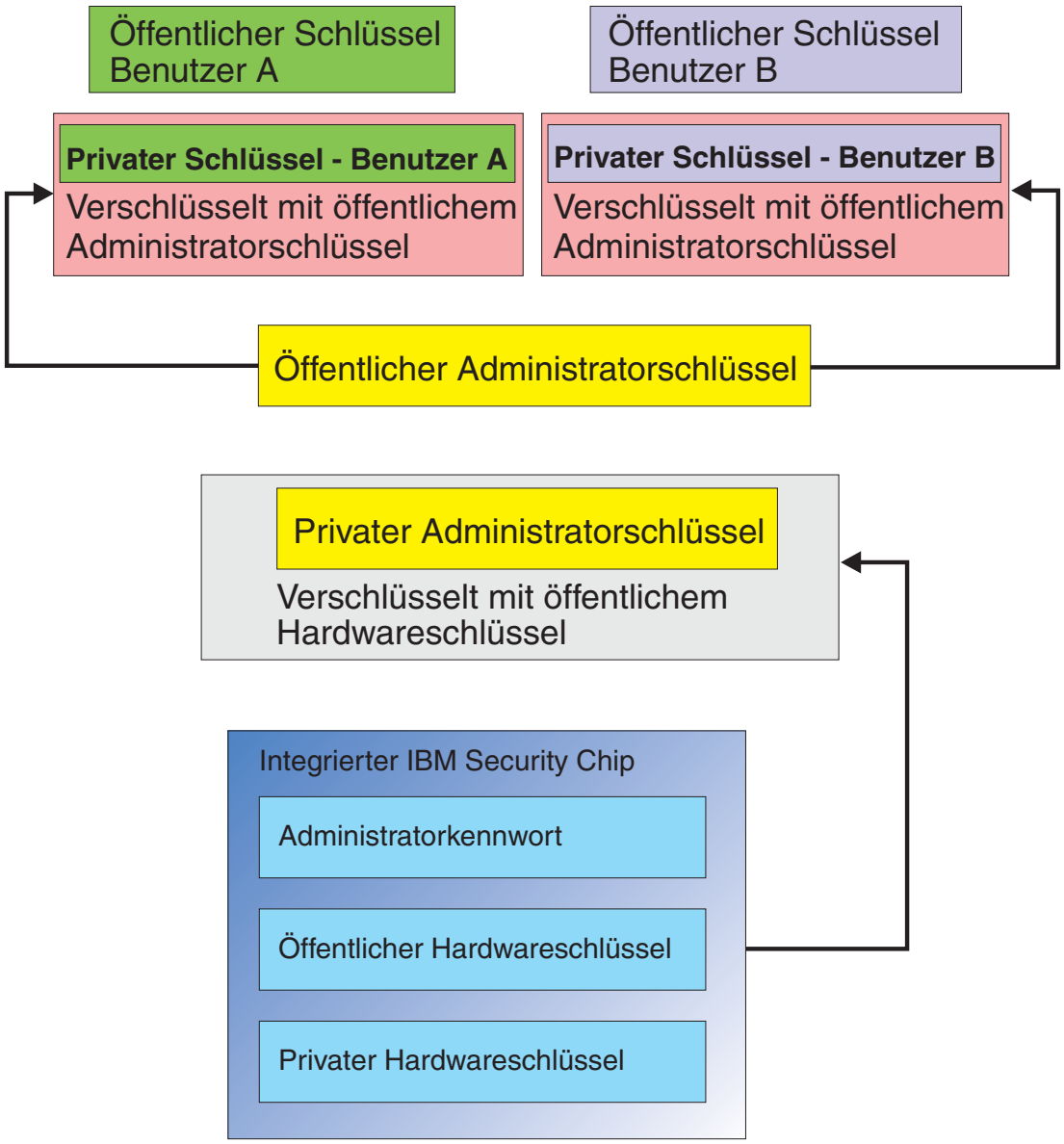

Abbildung 3. Mehrere Verschlüsselungsebenen bieten große Sicherheit

Schlüsselauslagerungshierarchie

Bestandteil der IBM ESS-Architektur ist eine Schlüsselauslagerungshierarchie. Ihre Funktionen werden ausführlich im *IBM Client Security Administrator- und Benutzerhandbuch* behandelt. Wir möchten hier jedoch ansatzweise darauf eingehen, da dieses Konzept in der Massenkonfiguration, Implementierung und Verwaltung Anwendung findet. In Abb. 3 werden der öffentliche und der private Hardwareschlüssel dargestellt. Wie bereits erwähnt, werden diese Schlüssel von Client Security erstellt und sind auf den einzelnen Clients statistisch eindeutig. Über dem integrierten IBM Security Chip ist das Schlüsselpaar aus öffentlichem und privatem Administratorschlüssel abgebildet. Das Schlüsselpaar aus öffentlichem und privatem Administratorschlüssel kann auf allen Computern eindeutig oder für alle Clients bzw. für eine Gruppe von Clients gleich sein. Die Vor- und Nachteile werden später in diesem Dokument behandelt. Der öffentliche und der private Administratorschlüssel ermöglichen Folgendes:

- Schutz des öffentlichen und des privaten Benutzerschlüssels
- Archivierung und Wiederherstellung der Benutzerberechtigungen
- Standortunabhängiger Zugriff auf die Benutzerberechtigungen. Dies wird im *IBM Client Security Administrator- und Benutzerhandbuch* beschrieben.

Gründe für die Schlüsselauslagerung

In den folgenden Abschnitten wird auf Benutzer in der IBM ESS-Umgebung eingegangen. Dort wird auch die Konfiguration von IBM Client Security und von ESS, um diese Benutzer aufzunehmen, ausführlich behandelt. An dieser Stelle wird nur darauf eingegangen, dass jeder Benutzer über einen öffentlichen und einen privaten Schlüssel verfügt. Der private Schlüssel des Benutzers wird mit dem öffentlichen Administratorschlüssel verschlüsselt. Aus Abb. 3 auf Seite 11 können Sie ersehen, dass der private Administratorschlüssel mit dem öffentlichen Hardwareschlüssel verschlüsselt ist. Warum müssen die verschiedenen privaten Schlüssel verschlüsselt werden?

Der Grund dafür geht auf die bereits erwähnte Hierarchie zurück. Aufgrund des begrenzten Speicherplatzes im integrierten IBM Security Chip kann im Chip jeweils nur eine begrenzte Anzahl von Schlüsseln enthalten sein. Der öffentliche und der private Hardwareschlüssel sind die einzigen Schlüssel in diesem Szenario, die ständig (von einem Bootvorgang zum nächsten) im Chip enthalten sind. Damit mehrere Schlüssel und mehrere Benutzer aktiviert werden können, wird über IBM ESS eine Schlüsselauslagerungshierarchie implementiert. Wenn ein Schlüssel benötigt wird, wird er im integrierten IBM Security Chip ausgelagert. Durch das Auslagern des verschlüsselten privaten Schlüssels im Chip kann der private Schlüssel entschlüsselt und nur in der geschützten Umgebung des Chips verwendet werden.

Der private Administratorschlüssel wird mit dem öffentlichen Hardware schlüssel verschlüsselt. Der private Hardwareschlüssel, der nur im Chip verfügbar ist, wird zum Entschlüsseln des privaten Administratorschlüssels verwendet. Nach dem Entschlüsseln des privaten Administratorschlüssels im Chip kann ein privater Benutzerschlüssel (der mit dem öffentlichen Administratorschlüssel verschlüsselt ist) von der Festplatte in den Chip übergeben und mit dem privaten Administratorschlüssel entschlüsselt werden. Aus Abb. 3 auf Seite 11 ist ersichtlich, dass mehrere private Benutzerschlüssel mit dem öffentlichen Administratorschlüssel verschlüsselt werden können. Dadurch können so viele Benutzer wie erforderlich auf einem Computer mit IBM ESS konfiguriert werden.

Kapitel 4. Wichtige Hinweise zur Schlüsselarchivierung

Kennwörter und Schlüssel dienen neben anderen optionalen Authentifizierungsgeräten dazu, die Identität von Systembenutzern zu überprüfen.

In Abb. 4 wird die Interaktion von IBM Embedded Security Subsystem und IBM Client Security dargestellt. Im Dialogfeld zur Anmeldung in Windows wird Benutzer A zur Anmeldung aufgefordert, und Benutzer A meldet sich an. Anhand der vom Betriebssystem bereitgestellten Informationen ermittelt das IBM Client Security-System den aktuellen Benutzer. Der private Administratorschlüssel, der mit dem öffentlichen Hardwareschlüssel verschlüsselt ist, wird in den integrierten IBM Security Chip geladen.

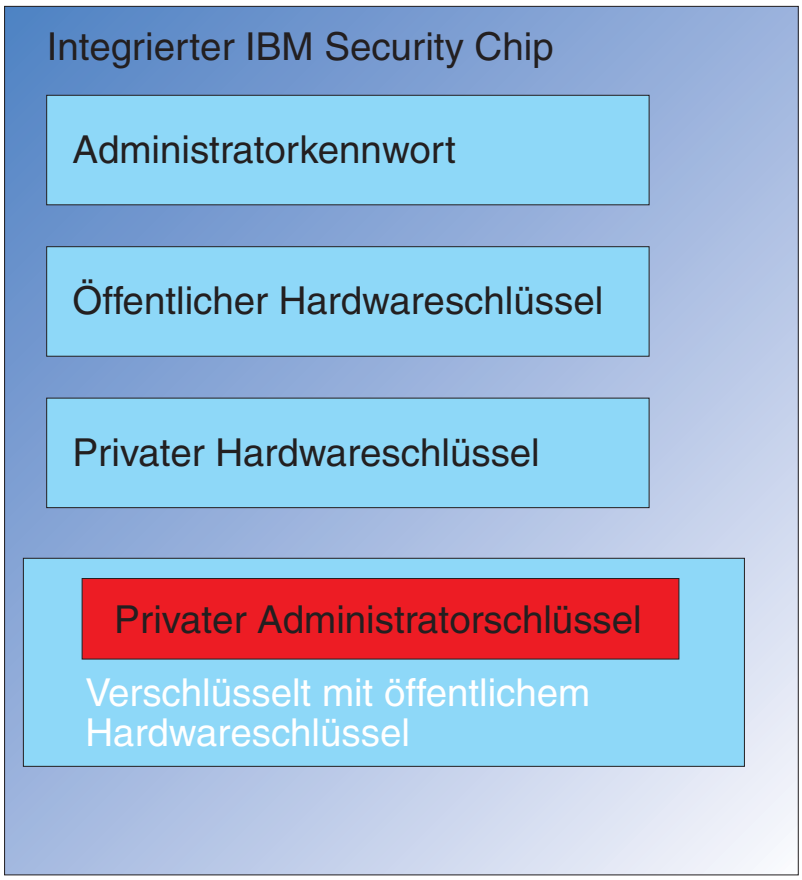

Abbildung 4. Der private Administratorschlüssel, der mit dem öffentlichen Hardwareschlüssel verschlüsselt ist, wird in den integrierten IBM Security Chip geladen

Der private Administratorschlüssel wird mit dem privaten Hardwareschlüssel (der nur im Chip verfügbar ist) entschlüsselt. Nun kann der private Administratorschlüssel im Chip verwendet werden (siehe Abb. 5).

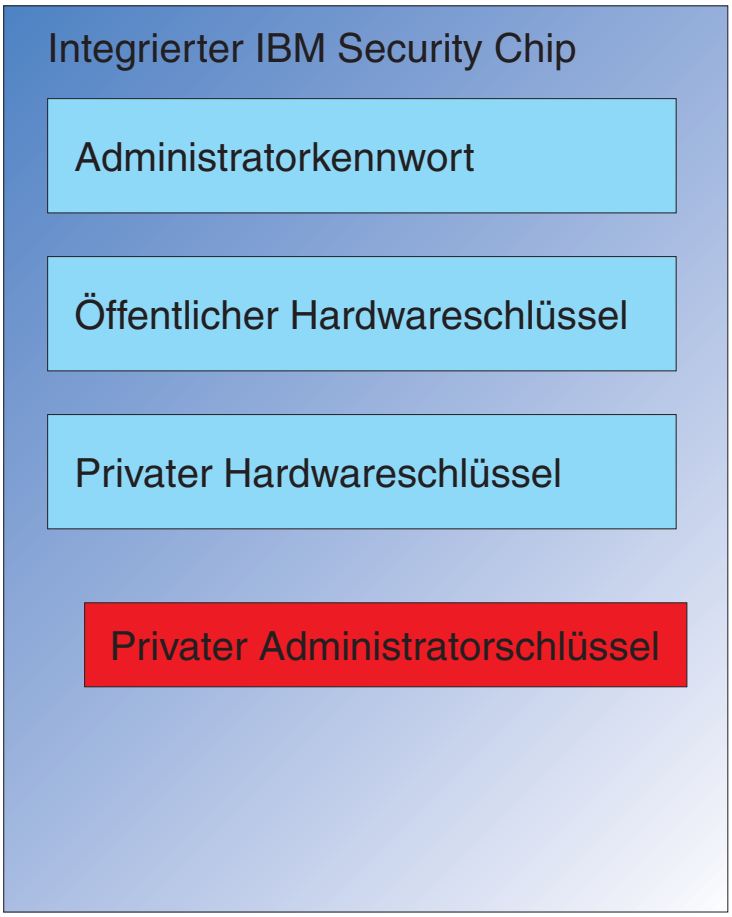

Abbildung 5. Der private Administratorschlüssel kann im Security Chip verwendet werden

Da Benutzer A beim Computer angemeldet ist, wird der private Schlüssel von Benutzer A (der mit dem öffentlichen Administratorschlüssel verschlüsselt ist) an den Chip übergeben (siehe Abb. 6).

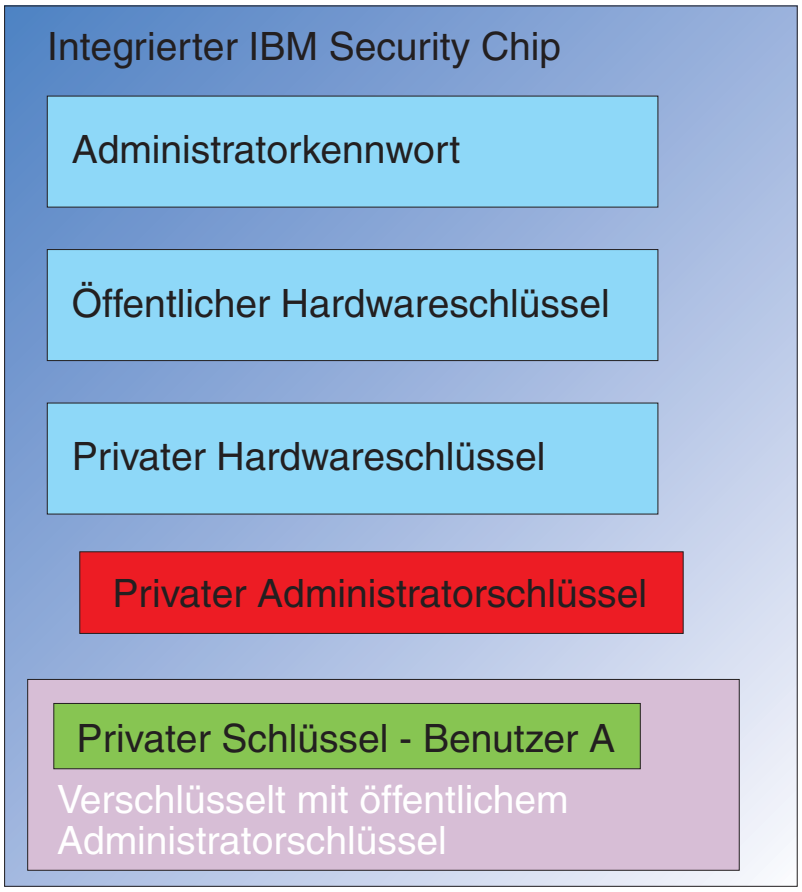

Abbildung 6. Der private Schlüssel von Benutzer A, der mit dem öffentlichen Administratorschlüssel verschlüsselt ist, wird an den Security Chip übergeben

Der private Administratorschlüssel wird verwendet, um den privaten Schlüssel von Benutzer A zu entschlüsseln. Nun kann der private Schlüssel von Benutzer A verwendet werden (siehe Abb. 7).

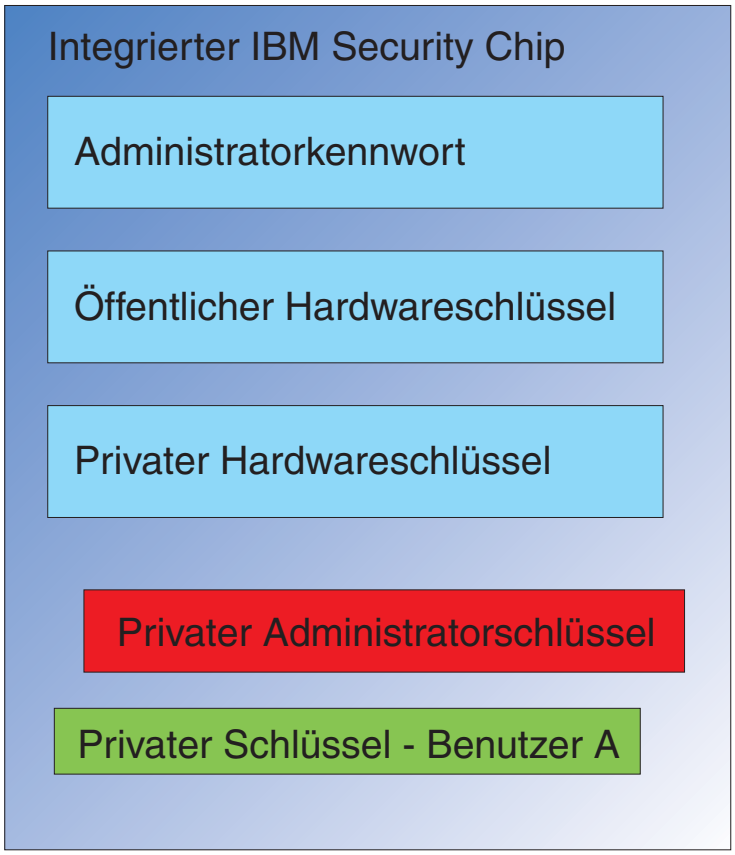

Abbildung 7. Der private Schlüssel von Benutzer A kann verwendet werden

Mit dem öffentlichen Schlüssel von Benutzer A können auch andere Schlüssel verschlüsselt werden, wie z. B. ein privater Schlüssel zum Signieren von E-Mails. Wenn Benutzer A eine signierte E-Mail senden möchte, wird der private Schlüssel für die Signatur (der mit dem öffentlichen Schlüssel von Benutzer A verschlüsselt ist) an den Chip übergeben. Mit dem privaten Schlüssel von Benutzer A, der bereits im Chip enthalten ist, wird der private Signierschlüssel von Benutzer A dann entschlüsselt. Nun steht der private Signierschlüssel von Benutzer A im Chip für die gewünschte Operation zur Verfügung, wie in diesem Fall das Erstellen einer digitalen Signatur (das Verschlüsseln eines Hash). Das Verschieben der Schlüssel in den und aus dem Chip findet genauso statt, wenn Benutzer B sich beim Computer anmeldet.

Warum ist ein Administratorschlüsselpaar erforderlich?

Der Hauptgrund für die Verwendung eines Administratorschlüsselpaars liegt in der Archivierung und Wiederherstellung. Das Administratorschlüsselpaar dient als eine abstrakte Ebene zwischen dem Chip und der Benutzerberechtigung. Die benutzerspezifischen privaten Schlüsselinformationen werden mit dem öffentlichen Administratorschlüssel verschlüsselt (siehe Abb. 8).

Wichtig: Sie müssen eine Strategie zur Verwaltung der Administratorschlüsselpaare entwickeln. Es ist möglich, dass jeder Computer mit einem integrierten Security Chip über dasselbe Administratorschlüsselpaar verfügt, wenn dies vom IT-Administrator oder vom Sicherheitsadministrator festgelegt wird. Jeder Abteilung oder jedem Gebäude können jedoch auch unterschiedliche Administratorschlüsselpaare zugewiesen werden.

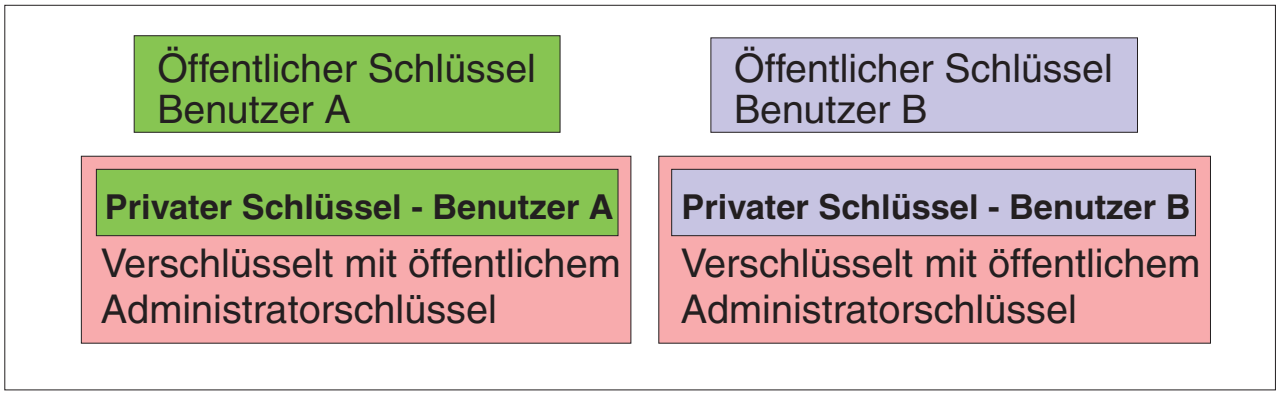

Abbildung 8. Die benutzerspezifischen privaten Schlüsselinformationen werden mit dem öffentlichen Administratorschlüssel verschlüsselt

Ein weiterer Grund für die Verwendung eines Administratorschlüsselpaars liegt im Signieren der Policy-Datei von Client Security. Dadurch wird gewährleistet, dass nur der Administrator Änderungen an der Sicherheitspolicy vornehmen kann.

Damit eine hohe Sicherheit für die Policy-Datei von Client Security erreicht werden kann, können Sie den privaten Administratorschlüssel auf bis zu fünf einzelne Benutzer aufteilen. In diesem Fall müssen alle fünf Benutzer, die über einen Teil des privaten Schlüssels verfügen, beim Signieren oder Verschlüsseln von Dateien, wie z. B. der Policy-Datei von Client Security, anwesend sein. Dadurch wird verhindert, dass ein einzelner Benutzer Administratorfunktionen ausführt. Informationen zum Aufteilen des privaten Administratorschlüssels finden Sie in Tabelle 6 auf Seite 41 unter der Einstellung "keysplit=1".

Während der Initialisierung von IBM Client Security können die Administratorschlüsselpaare von der Software erstellt oder von einer externen Datei importiert werden. Wenn Sie ein einheitliches Administratorschlüsselpaar einsetzen möchten, geben Sie die Speicherposition der erforderlichen Dateien während der Clientinstallation an.

Eine Sicherungskopie dieser benutzerspezifischen Informationen wird an einer durch den Administrator definierten Archivposition gespeichert (siehe Abb. 8 auf Seite 17). Bei der Archivposition kann es sich um jede Art von Datenträger handeln, der physisch oder logisch mit dem Client verbunden ist. Im Abschnitt zur Installation von IBM Client Security werden bewährte Verfahren für die Archivposition erläutert.

Der öffentliche und der private Administratorschlüssel sind nicht archiviert. Die Benutzerdaten in der Archivposition werden mit dem öffentlichen Administratorschlüssel verschlüsselt. Zum Entschlüsseln der Archivdaten des Benutzers benötigen Sie den privaten Administratorschlüssel. Der öffentliche und der private Administratorschlüssel werden in der Dokumentation zu IBM Client Security häufig als "Archivschlüsselpaar" bezeichnet. Beachten Sie, dass der private Archivschlüssel nicht verschlüsselt ist. Gehen Sie deshalb beim Speichern und Schützen des Archivschlüsselpaars mit besonderer Sorgfalt vor.

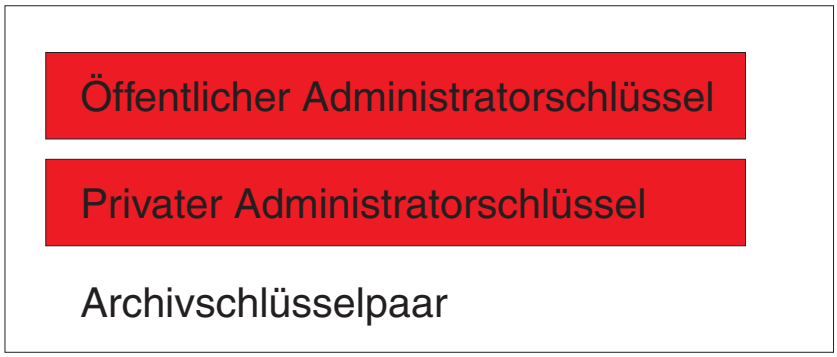

Abbildung 9. Der öffentliche und der private Administratorschlüssel bilden das Archivschlüsselpaar

Wie bereits erwähnt, liegt eine der wichtigsten Funktionen des öffentlichen und privaten Administratorschlüssels in der Sicherung und Wiederherstellung der Inhalte von Datenträgern.

Diese Funktion ist in den Schritten 10 bis 15 beschrieben. Die Schritte sind wie folgt:

1. Aus irgendeinem Grund kann Benutzer A Client A nicht mehr nutzen. In diesem Beispiel wurde Client A von einem Blitzeinschlag getroffen (siehe Abb. 10).

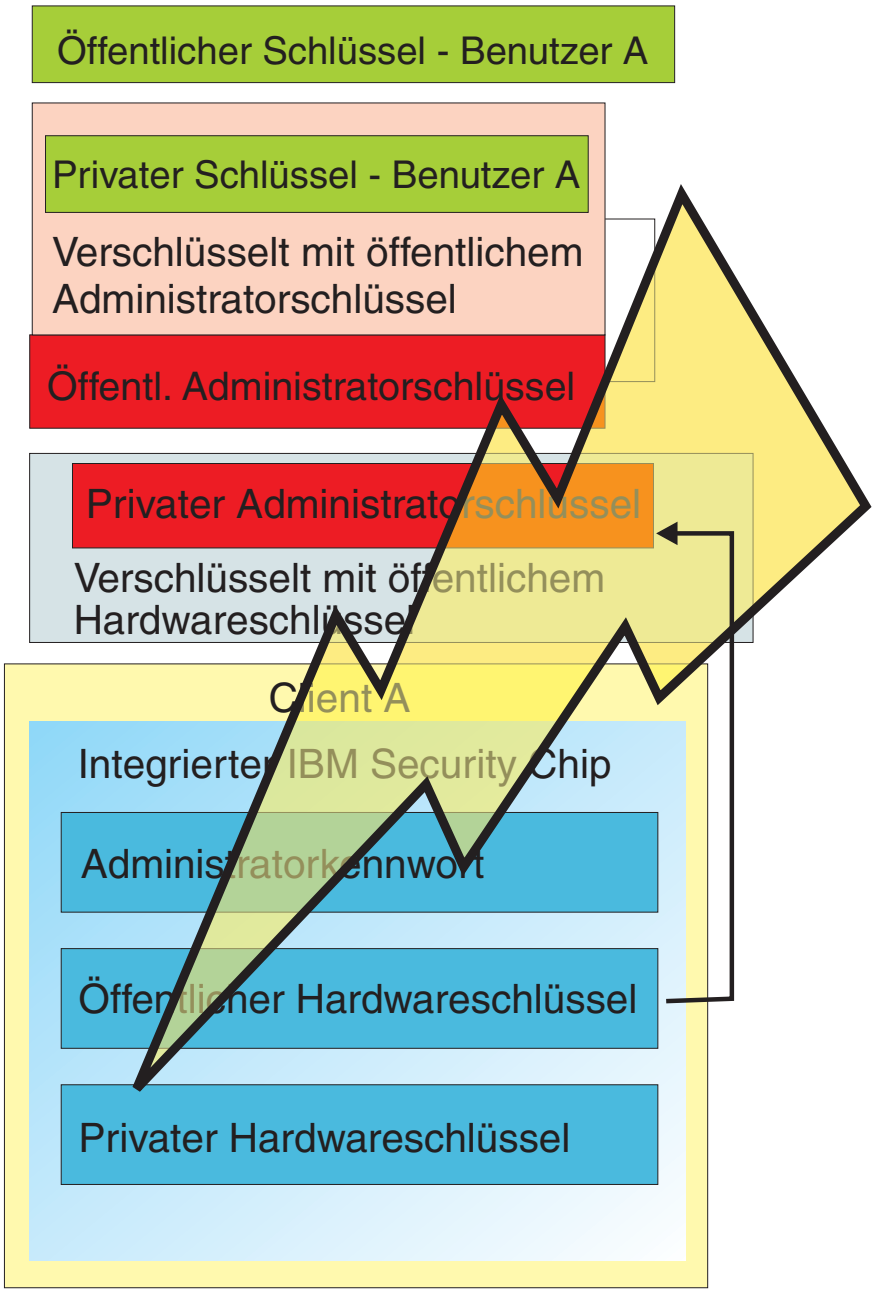

Abbildung 10. Der Computer von Benutzer A ist aufgrund eines Blitzeinschlags nicht mehr funktionsfähig

2. Benutzer A erhält einen neuen und verbesserten IBM Computer, der als Client B bezeichnet wird (siehe Abb. 11). In Client B werden ein anderer öffentlicher und ein anderer privater Hardwareschlüssel als in Client A eingesetzt. Dieser Unterschied wird grafisch durch die graue Farbe der Schlüssel für Client B und durch die grüne Farbe der Schlüssel für Client A dargestellt. Beachten Sie jedoch, dass das Administratorkennwort für Client A und Client B gleich ist.

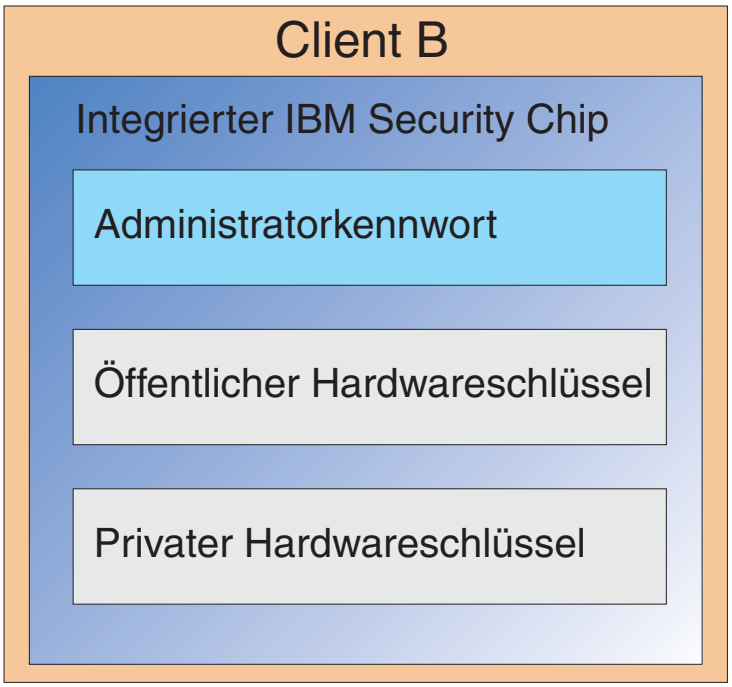

Abbildung 11. Benutzer A erhält einen neuen Computer, Client B, mit einem neuen integrierten IBM Security Chip

3. Für Client B ist nun die gleiche Benutzerberechtigung erforderlich wie für Client A. Diese Informationen wurden von Client A archiviert. Wenn Sie sich noch einmal Abb. 8 auf Seite 17 ansehen, werden Sie sich daran erinnern, dass die Benutzerschlüssel mit dem öffentlichen Administratorschlüssel verschlüsselt wurden und in der Archivposition gespeichert sind. Damit die Benutzerberechtigung nun auf Client B verfügbar ist, müssen der öffentliche und der private Administratorschlüssel auf diesen Rechner übertragen werden. In Abbildung 12 ist dargestellt, wie Client B den öffentlichen und den privaten Administratorschlüssel abruft, um die Benutzerdaten aus der Archivposition wiederherzustellen.

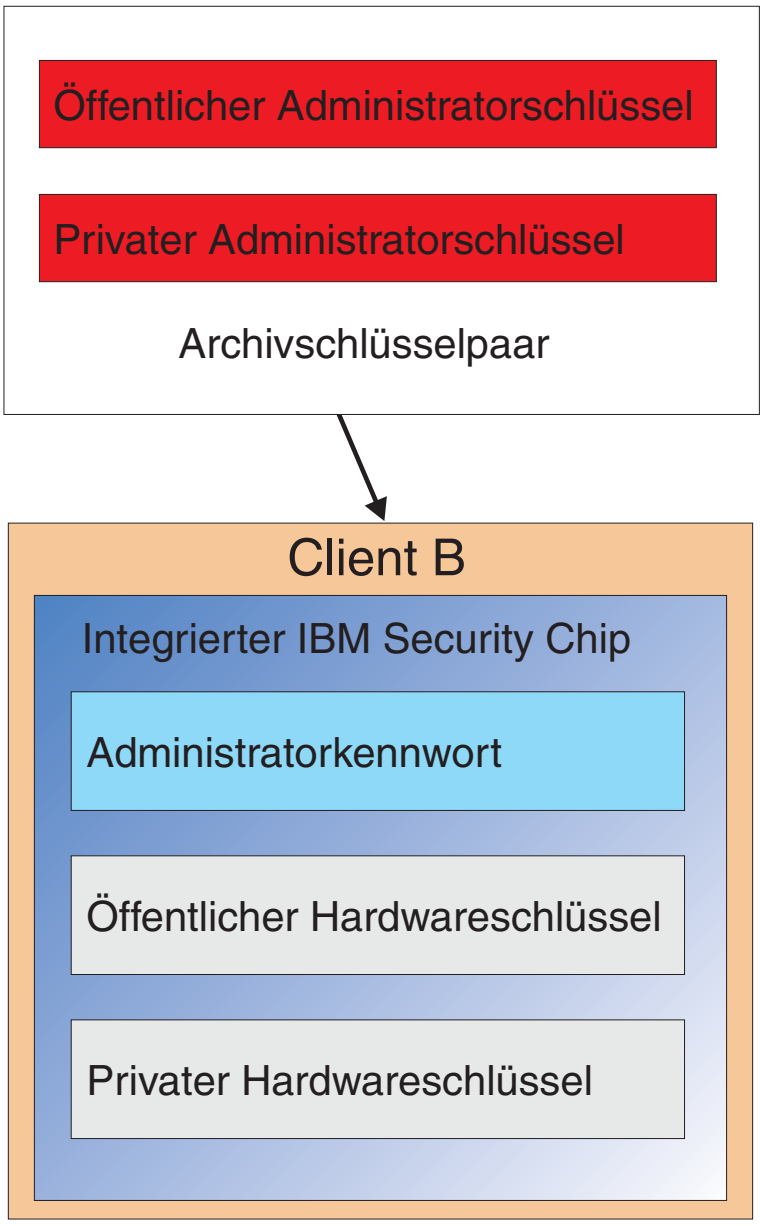

Abbildung 12. Client B ruft den öffentlichen und den privaten Administratorschlüssel aus der Archivposition ab

4. In Abb. 13 ist dargestellt, wie der private Administratorschlüssel mit dem öffentlichen Hardwareschlüssel von Client B verschlüsselt wird.

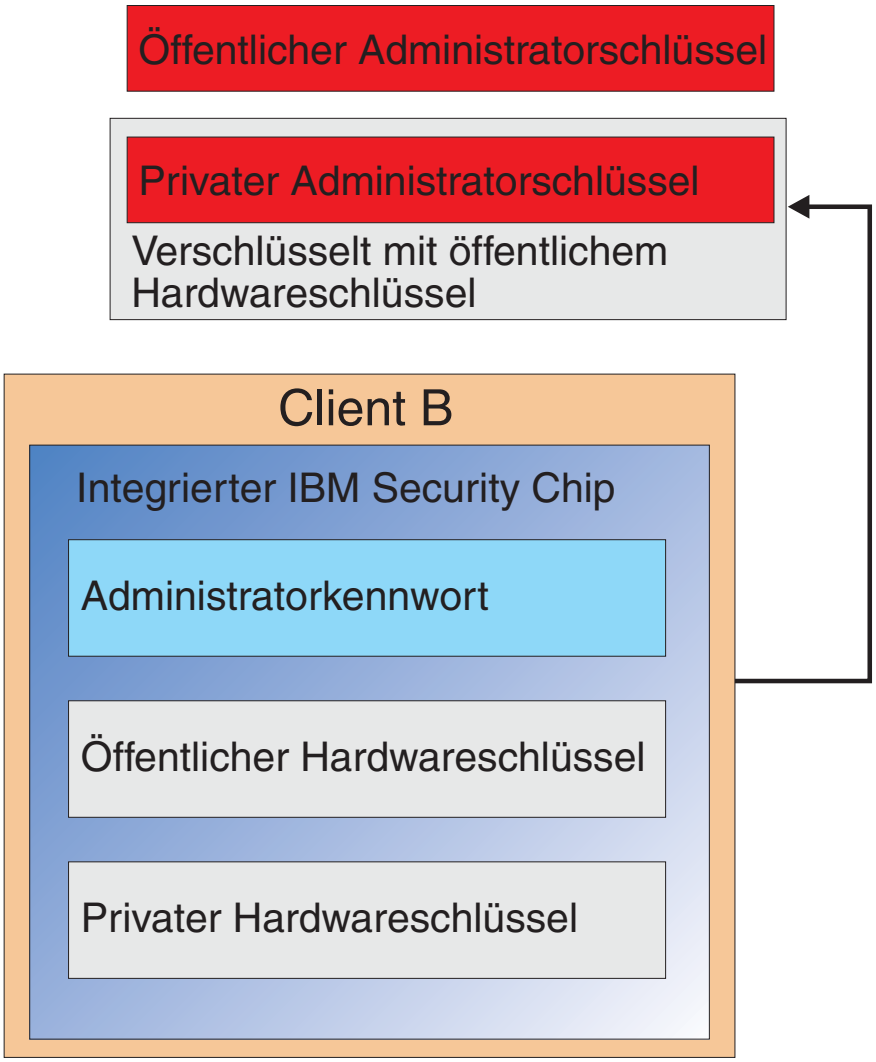

Abbildung 13. Der private Administratorschlüssel wird mit dem Hardwareschlüssel von Client B verschlüsselt

Da der private Administratorschlüssel nun mit dem öffentlichen Hardwareschlüssel verschlüsselt ist, kann die Benutzerberechtigung für Benutzer A auf Client B geladen werden (siehe Abb. 14).

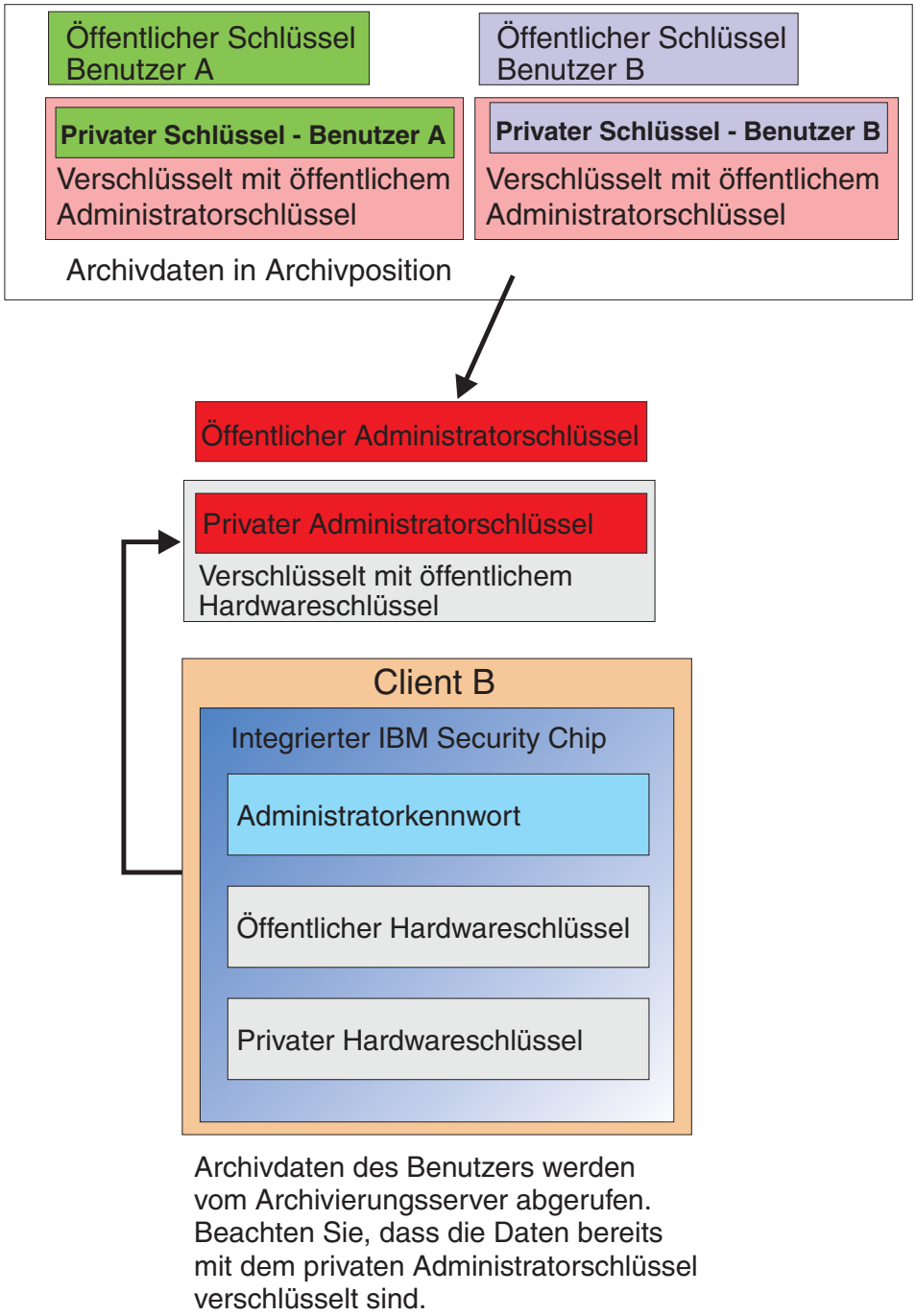

Abbildung 14. Die Benutzerberechtigung von Benutzer A kann nach der Verschlüsselung des privaten Administratorschlüssels auf Client B geladen werden

In Abb. 15 ist die vollständige Wiederherstellung von Benutzer A auf Client B dargestellt. Beachten Sie, dass der private Schlüssel von Benutzer A auf dem Archivierungsserver mit dem öffentlichen Administratorschlüssel verschlüsselt war. Der öffentliche Administratorschlüssel besteht aus einem RSA-Schlüssel mit 2048 Bit. Es ist nahezu unmöglich, dass dieser Schlüssel von Unbefugten entschlüsselt werden kann. Dadurch muss die Archivposition nicht unbedingt geschützt werden oder über eine strenge Zugriffskontrolle verfügen. Solange das Archivschlüsselpaar (der öffentliche und der private Administratorschlüssel), insbesondere der private Administratorschlüssel, sicher aufbewahrt werden, kann sich die Archivposition für die Benutzerberechtigung an einer beliebigen Speicherposition befinden.

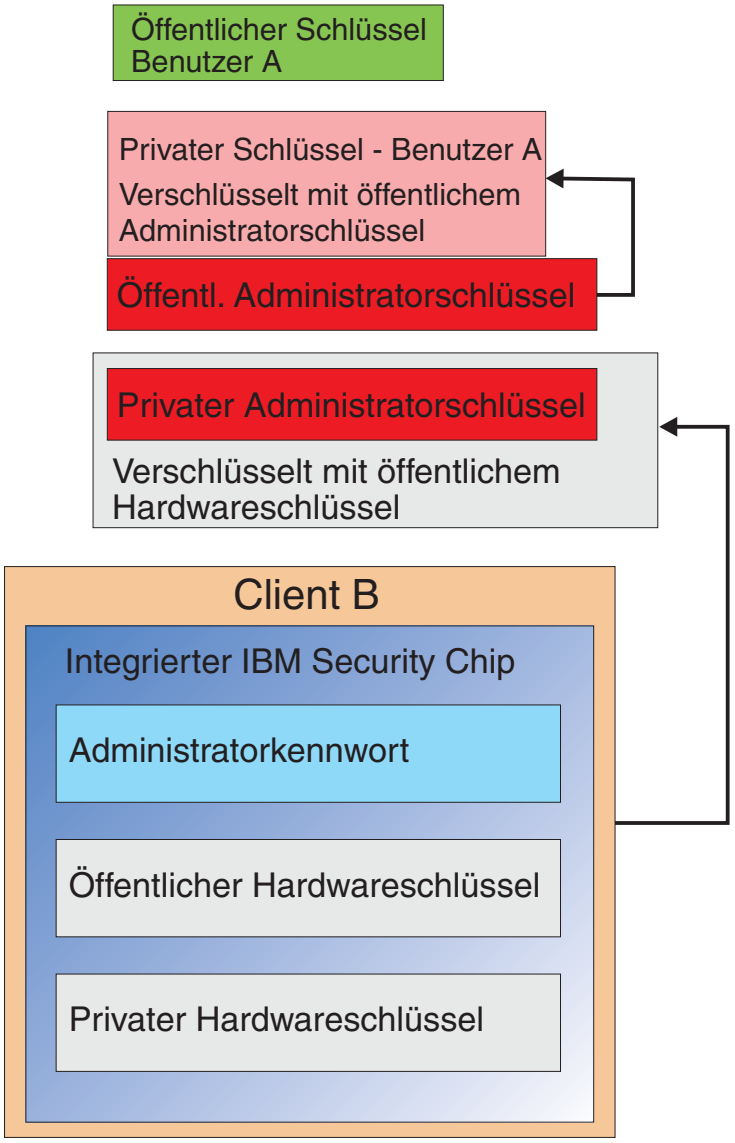

Abbildung 15. Benutzer A ist auf Client B vollständig wiederhergestellt

Einzelheiten zum Festlegen des Administratorkennworts, empfehlenswerte Archivpositionen usw. werden im Abschnitt zur Softwareinstallation behandelt. Abb. 16 enthält eine Übersicht über die Komponenten in einer ESS-Umgebung. Der entscheidende Punkt dabei ist, dass alle Clients zwar einen eindeutigen öffentlichen und einen eindeutigen privaten Hardwareschlüssel aufweisen, sie jedoch über denselben öffentlichen und denselben privaten Administratorschlüssel verfügen. Die Clients verfügen zwar über eine gemeinsame Archivposition, doch diese Archivposition gilt möglicherweise nur für für ein Segment oder eine Benutzergruppe.

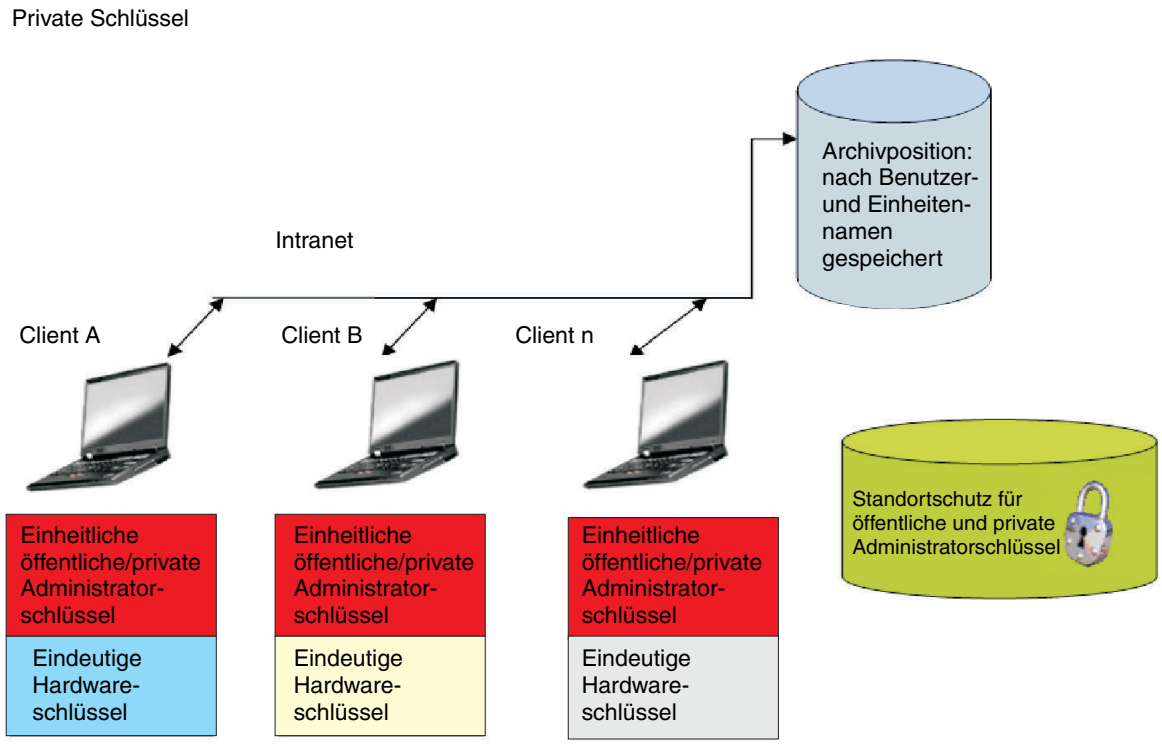

Abbildung 16. Hauptkomponenten des IBM Client Security-Systems

Beispiel: Die Personalabteilung verfügt über eine andere Archivposition als die Entwicklungsabteilung. Die Archivierung erfolgt anhand der Benutzer- und Computernamen. IBM Client Security archiviert die Benutzer eines Systems in einer definierten Archivposition anhand der Benutzer- und Computernamen, wie es bereits für Benutzer A und Benutzer B beschrieben wurde. Beachten Sie auch den Standortschutz für öffentliche und private Administratorschlüssel.

Anmerkung: Die Computer- und Benutzernamen, die in der gleichen Archivposition archiviert werden sollen, müssen eindeutig sein. Durch einen doppelten Computer- oder Benutzernamen wird der vorherige Archiveintrag des gleichen Namens überschrieben.

Kapitel 5. IBM Client Security

IBM Client Security stellt die Verbindung zwischen Anwendungen und dem integrierten IBM Security Chip sowie die Schnittstelle zum Registrieren von Benutzern, Festlegen der Policy und Ausführen grundlegender Administrationsfunktionen dar. IBM Client Security besteht hauptsächlich aus den folgenden Komponenten:

- Administratordienstprogramm
- Benutzerkonfigurationsdienstprogramm
- Administratorkonsole
- Installationsassistent
- User Verification Manager (UVM)
- Verschlüsselungsserviceanbieter
- PKCS#11-Modul

Mit IBM Client Security können Sie verschiedene Schlüsselfunktionen ausführen:

- Benutzer registrieren
- Policy festlegen
- Verschlüsselungstextpolicy festlegen
- Vergessene Verschlüsselungstexte neu festlegen
- Benutzerberechtigungen wiederherstellen

Wenn Benutzer A sich beispielsweise beim Betriebssystem anmeldet, basieren alle Entscheidungen von IBM Client Security auf der Annahme, dass Benutzer A angemeldet ist. (**Anmerkung:** Die Sicherheitspolicy ist rechnergestützt und nicht benutzergestützt; die Policy gilt für alle Benutzer auf einem Computer.) Wenn Benutzer A IBM Embedded Security Subsystem nutzen möchte, erzwingt IBM Client Security die Sicherheitspolicies, die für Benutzer A auf diesem Computer konfiguriert wurden, wie z. B. Verschlüsselungstext oder Authentifizierung über Fingerabdrücke. Wenn die als Benutzer A angemeldete Person nicht den korrekten Verschlüsselungstext oder den richtigen Fingerabdruck für die Authentifizierung bereitstellen kann, untersagt IBM ESS dem Benutzer das Ausführen der angeforderten Aktion.

Benutzer registrieren und Registrierung verwalten

Benutzer von IBM ESS sind ganz einfach Benutzer von Windows, die in der IBM ESS-Umgebung registriert sind. Benutzer können mit unterschiedlichen Methoden registriert werden. Dies wird später in diesem Dokument ausführlicher behandelt. In diesem Abschnitt wird beschrieben, was bei der Registrierung eines Benutzers geschieht. Wenn Ihnen dieser Prozess bekannt ist, können Sie besser nachvollziehen, wie IBM ESS funktioniert und wie Sie es dann erfolgreich in Ihrer Umgebung verwalten können.

Client Security verwaltet mit Hilfe von User Verification Manager (UVM) Verschlüsselungstexte und andere Elemente zur Authentifizierung von Systembenutzern. UVM unterstützt die folgenden Funktionen:

- UVM-Client-Policy-Schutz
- UVM-Schutz bei der Systemanmeldung
- UVM-Schutz über Client Security-Bildschirmschoner

Jeder Benutzer in der IBM ESS-Umgebung verfügt über mindestens ein Personalisierungsobjekt, das ihm zugeordnet ist und für Authentifizierungszwecke verwendet wird. Die Mindestvoraussetzung ist ein Verschlüsselungstext. Jeder Benutzer in der UVM-Komponente der ESS-Umgebung muss über einen Verschlüsselungstext verfügen, und dieser Verschlüsselungstext muss mindestens ein Mal beim Start des Computers eingegeben werden (aus der Perspektive des Benutzers verwaltet UVM die Authentifizierung und setzt die Sicherheitspolicy um). In den folgenden Abschnitten wird erläutert, warum ein Verschlüsselungstext verwendet wird, wie er festgelegt und wie er verwendet wird.

Einen Verschlüsselungstext erfordern

Einfach ausgedrückt ist ein Verschlüsselungstext für Sicherheitszwecke erforderlich. Eine Hardwarekomponente wie IBM Embedded Security Subsystem bietet einen enormen Vorteil, da sie eine sichere, autonome Speicherposition für den Berechtigungsnachweis eines Benutzers zur Verfügung stellt. Der Schutz, den ein Hardware-Chip bietet, bringt jedoch wenig Nutzen, wenn die erforderliche Authentifizierung zum Zugriff auf den Chip schwach ist. Sie verfügen beispielsweise über einen Hardware-Chip, der Sicherheitsfunktionen ausführt. Die erforderliche Authentifizierung zum Aufrufen einer Aktion besteht jedoch aus einer einzigen Ziffer. Dadurch braucht ein potenzieller Hacker nur eine einzige Ziffer (von 0 bis 9) zu erraten, um Aktionen mit Ihrem Berechtigungsnachweis aufzurufen. Die Authentifizierung mit einer einzigen Ziffer schwächt die Sicherheit des Chips so, dass sie kaum oder sogar keine Vorteile gegenüber der softwarebasierten Lösung bietet. Wenn Sie über keine starke Authentifizierung in Verbindung mit dem Hardwareschutz verfügen, erzielen Sie unter Umständen gar keine Sicherheitsvorteile. Mit dem von IBM ESS erforderlichen Verschlüsselungstext wird ein Benutzer authentifiziert, bevor Aktionen mit dem Berechtigungsnachweis des Benutzers in der Hardware ausgeführt werden. Der UVM-Verschlüsselungstext kann nur über das Administratorschlüsselpaar wiederhergestellt werden. Er kann also nicht von einem gestohlenen System abgerufen werden.

Einen Verschlüsselungstext festlegen

Jeder Benutzer wählt einen Verschlüsselungstext aus, um seinen Berechtigungsnachweis zu schützen. In Kapitel 3, „Funktionsweise des integrierten IBM Security Chips", auf Seite 9 wurde erläutert, dass ein privater Benutzerschlüssel mit dem öffentlichen Administratorschlüssel verschlüsselt ist. Der private Benutzerschlüssel verfügt ebenfalls über einen zugeordneten Verschlüsselungstext. Mit Hilfe dieses Verschlüsselungstexts wird der Benutzer mit seinem Berechtigungsnachweis authentifiziert. In Abb. 17 ist dargestellt, dass der Verschlüsselungstext sowie die private Schlüsselkomponente mit dem öffentlichen Administratorschlüssel verschlüsselt werden.

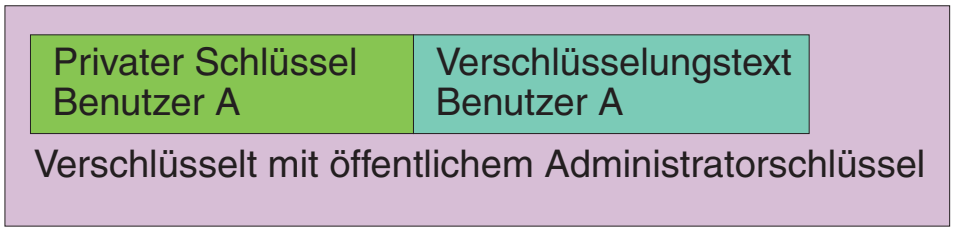

Abbildung 17. Benutzer A muss den Verschlüsselungstext angeben, um Funktionen ausführen zu können, für die der private Schlüssel von Benutzer A erforderlich ist

Der in Abb. 17 auf Seite 28 dargestellte Verschlüsselungstext wird vom Benutzer gemäß der bestehenden Policy ausgewählt, d. h. nach den konfigurierten Regeln, die die Kennworterstellung (z. B. Anzahl der Zeichen und Anzahl der Tage, die das Kennwort gültig ist) steuern. Der Verschlüsselungstext wird erstellt, wenn ein Benutzer bei UVM registriert wird. Informationen zu diesem Vorgang bei der Einführung von IBM Client Security finden Sie später in diesem Dokument.

Der private Schlüssel von Benutzer A wird mit dem öffentlichen Administratorschlüssel verschlüsselt, weil für die Entschlüsselung des privaten Schlüssels der private Administratorschlüssel erforderlich ist. Wenn der Verschlüsselungstext von Benutzer A vergessen wurde, kann der Administrator einen neuen Verschlüsselungstext festlegen.

Einen Verschlüsselungstext verwenden

In Abb. 18 bis Abb. 20 auf Seite 31 ist dargestellt, wie der Verschlüsselungstext des Benutzers im Chip verarbeitet wird. Ein Verschlüsselungstext muss immer als Erstes und mindestens ein Mal pro Sitzung angegeben werden. Ein Verschlüsselungstext ist immer erforderlich. Sie können zusätzliche Authentifizierungsgeräte hinzufügen, doch kann keines dieser Geräte den ersten erforderlichen Verschlüsselungstext des Benutzers ersetzen. Kurz ausgedrückt werden die biometrischen oder anderen Authentifizierungsdaten mit dem öffentlichen Benutzerschlüssel verschlüsselt. Zum Entschlüsseln dieser zusätzlichen Sicherheitsdaten ist ein Zugriff auf den privaten Schlüssel erforderlich.

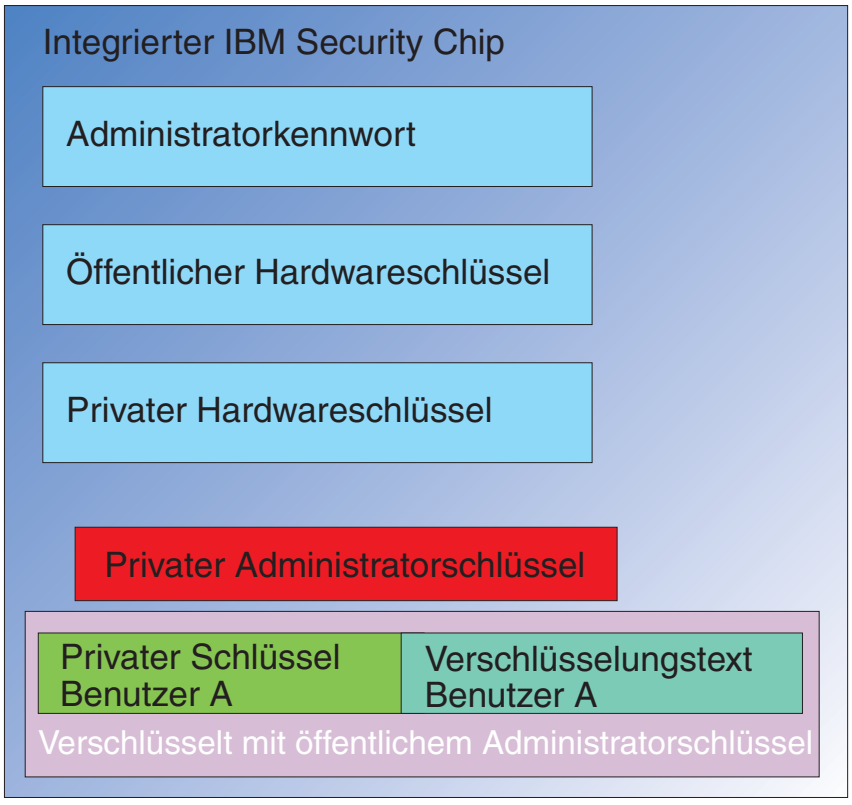

Abbildung 18. Der private Administratorschlüssel wird im Chip entschlüsselt

Daher muss der Verschlüsselungstext mindestens ein Mal pro Sitzung angegeben werden, um die zusätzlichen Daten zu entschlüsseln. Der Berechtigungsnachweis, der den mit dem öffentlichen Administratorschlüssel verschlüsselten privaten Schlüssel und den Verschlüsselungstext von Benutzer A ausmacht, wird an den integrierten IBM Security Chip übergeben. Der private Administratorschlüssel wird, wie zuvor beschrieben, bereits im Chip entschlüsselt. Der Berechtigungsnachweis wird, wie in Abb. 19 dargestellt, übergeben.

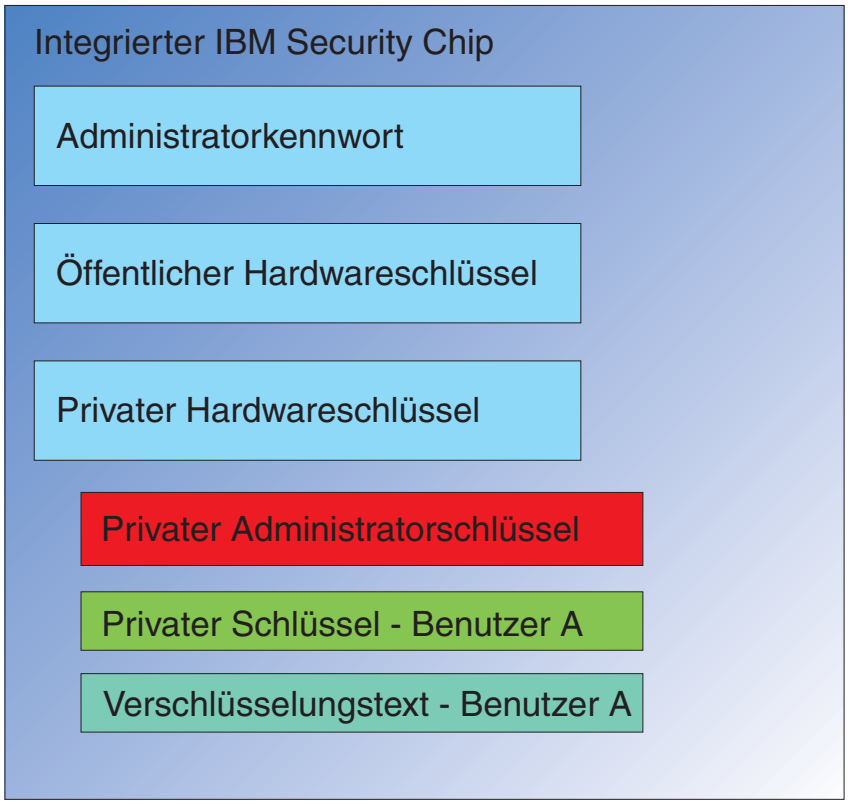

Abbildung 19. Der private Schlüssel sowie der Verschlüsselungstext von Benutzer A sind im Chip verfügbar

Der Berechtigungsnachweis wird entschlüsselt, und somit werden der private Schlüssel sowie der Verschlüsselungstext von Benutzer A im Chip verfügbar. Wenn der derzeit angemeldete Benutzer, der von IBM Client Security als Benutzer A erkannt wird, den Berechtigungsnachweis von Benutzer A verwenden möchte, wird ein Dialog zum Verschlüsselungstext eröffnet (siehe Abb. 20 auf Seite 31).

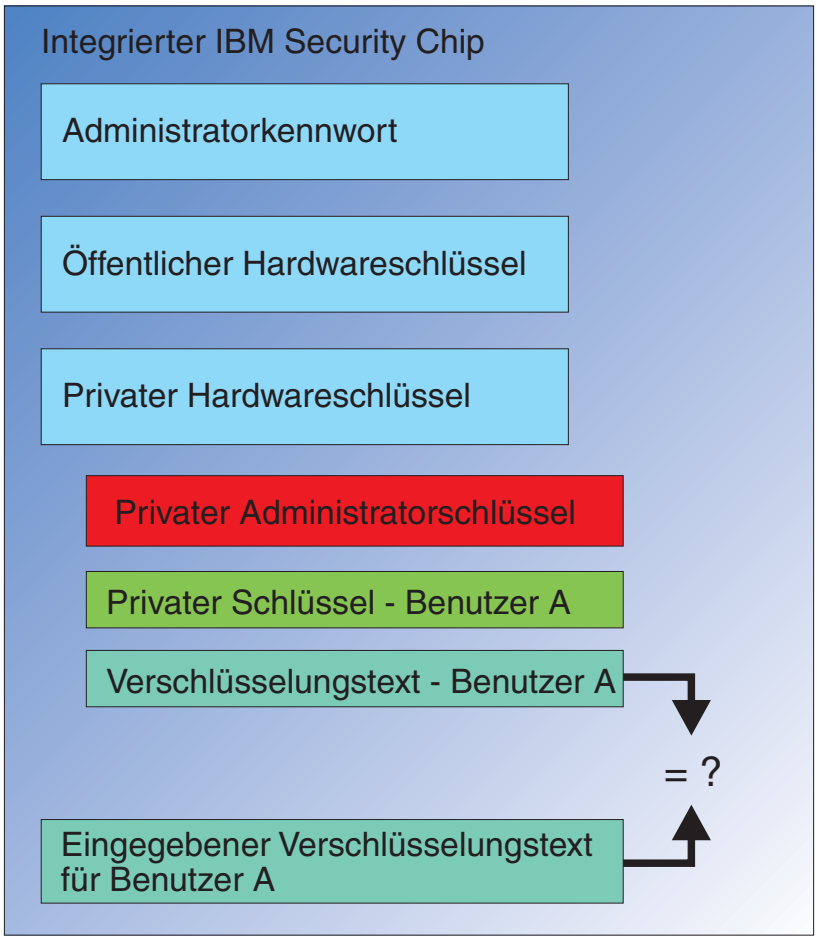

Abbildung 20. Wenn Benutzer A den Berechtigungsnachweis von Benutzer A verwenden möchte, wird ein Dialog zum Verschlüsselungstext geöffnet

Der eingegebene Verschlüsselungstext wird an den Chip übermittelt und mit dem entschlüsselten Wert des Verschlüsselungstexts verglichen. Bei einer Übereinstimmung kann der Berechtigungsnachweis von Benutzer A dann für verschiedene Funktionen, wie z. B. für digitale Signaturen oder für das Entschlüsseln von E-Mails, verwendet werden. Beachten Sie, dass der Vergleich des Verschlüsselungstexts in der sicheren Umgebung des Chips stattfindet. Der Chip verfügt über eine Anti-Hammering-Funktion, mit der wiederholt fehlgeschlagene Zugriffsversuche erkannt werden. Beachten Sie außerdem, dass der registrierte Verschlüsselungstext von Benutzer A niemals außerhalb des Chips offen gelegt wird. Teil der Installation von IBM Client Security ist die Registrierung von Benutzern, und Teil dieser Registrierung wiederum ist die Erstellung von Verschlüsselungstexten der Benutzer. In diesem Handbuch wird detailliert beschrieben, wie dieser Verschlüsselungstext festgelegt wird und wie Verschlüsselungstextregeln erzwungen werden können.

In Abb. 1 auf Seite 1 sind der integrierte IBM Security Chip sowie IBM Client Security dargestellt. In Abb. 1 auf Seite 1 ist außerdem die Initialisierung des Unternehmens und der Benutzer abgebildet. Die Unternehmensinitialisierung ist IBM Embedded Security Subsystem zugeordnet, und die Benutzerinitialisierung ist mit IBM Client Security verknüpft. In den vorherigen Abschnitten wurde die Initialisierung beschrieben, um das allgemeine Konzept zu erklären. Die folgenden Abschnitte enthalten ausführlichere Informationen zum Prozess der Initialisierung.

TPM-Initialisierung

Die TPM-Initialisierung dient im Wesentlichen zum Hinzufügen des öffentlichen und des privaten Hardwareschlüssels sowie eines Administratorkennworts. Bei diesem Prozess wird ein von IBM ausgelieferter generischer Computer eindeutig für Ihr Unternehmen konfiguriert. In der folgenden Tabelle werden die Methoden für die Initialisierung von öffentlichen und privaten Schlüsseln sowie von Administratorkennwörtern dargestellt.

Tabelle 3. Methoden zur Hardwareinitialisierung

Maßnahme	**Kann im BIOS erstellt werden**	**Kann vom Administrator manuell in CSS erstellt werden**	**Kann in einem Script erstellt werden**
Erstellung von öffentlichen/privaten Hardwareschlüsseln	Nein	Ja	Ja
Erstellung von Administratorkennwörtern	Ja, auf einigen mit TCPA kompatiblen Clients. Prüfen Sie den BIOS-Eintrag.	Ja	Ja

In Tabelle 3 wird veranschaulicht, dass der öffentliche und der private Hardwareschlüssel nicht automatisch bei der Installation der Software erstellt werden. Die Erstellung des öffentlichen und des privaten Hardwareschlüssels muss manuell in der Software oder über ein Script veranlasst werden. Das Administratorkennwort kann im BIOS, in IBM Client Security oder durch ein Script erstellt werden. Der Chip steuert die für den öffentlichen und den privaten Hardwareschlüssel festgelegten Werte. Sie können diese Werte nicht selbst konfigurieren. Mit der Zufallszahlenfunktion im Chip werden statistisch willkürliche Paare aus einem öffentlichen und einem privaten Schlüssel erstellt. Das Administratorkennwort wird allerdings von Ihnen festgelegt.

Das Administratorkennwort ist jedoch anders, da der Administrator diesen Wert bestimmen muss. Bezüglich des Administratorkennworts müssen verschiedene Punkte beachtet werden:

- Welchen Wert legen Sie als Administratorkennwort bzw. -kennwörter fest?
- Legen Sie mehrere Kennwörter für verschiedene Gruppen fest? Wenn ja, wie treffen Sie die logische Entscheidung, welcher Computer über welches Kennwort verfügt?
- Welcher Administrator hat Zugriff auf das Kennwort? Wer hat Zugriff auf welches Kennwort, wenn Sie mehrere Kennwörter für separate Benutzergruppen anlegen?
- Können Endbenutzer, die sich selbst verwalten, auf das Administratorkennwort zugreifen?

Damit Sie eine effektive Entscheidung zu den oben aufgeführten Punkten treffen können, müssen Sie die Funktionen des Administratorkennworts kennen:
- Zugriff auf Administratordienstprogramme
- Hinzufügen/Entfernen von Benutzern
- Festlegen, welche Anwendungen bzw. Funktionen von IBM Client Security verwendet werden können

In den folgenden Abschnitten wird der Zusammenhang zwischen der Policy-Datei und dem privaten Administratorschlüssel erläutert. Im Augenblick genügt es zu wissen, dass der private Administratorschlüssel zum Ändern der Policy erforderlich ist. In Tabelle 4 sind die Funktionen des Administratorkennworts und/oder des privaten Administratorschlüssels zusammengefasst.

Tabelle 4. Administratoraktionen mit Kennwort und privatem Schlüssel

Maßnahme	**Administratorkennwort**	**Privater Administratorschlüssel**
Zugriff auf das Administratordienstprogramm	Ja	Nein
Hinzufügen/Entfernen /Wiederherstellen von Benutzern	Ja	Nein
Festlegen, welche CSS-Anwendungen/-funktionen verwendet werden können	Ja	Nein
Festlegen/Ändern der Policy	Ja	Ja
Erstellen der Datei zum Zurücksetzen des Verschlüsselungstexts eines Benutzers	Ja	Ja

Die TPM-Initialisierung bezieht sich auch auf den öffentlichen und den privaten Administratorschlüssel. Aus der Tabelle oben können Sie die Funktionen dieser Schlüssel ersehen. Überlegen Sie sich, wie Sie den öffentlichen und den privaten Administratorschlüssel festlegen möchten. Dieses Schlüsselpaar kann auf jedem Computer eindeutig oder auf allen Rechnern identisch sein. Bei der Initialisierung von IBM Client Security hat der Administrator die Möglichkeit, ein vorhandenes Schlüsselpaar zu verwenden oder ein neues Schlüsselpaar für den Client zu erstellen. Auch hier bestimmt das Verwendungsmodell das beste Verfahren für Ihr Unternehmen.

Bewährte Verfahren

Große Unternehmen können einen eindeutigen Schlüssel auf jedem Computer oder einen eindeutigen Schlüssel für jede Abteilung verwenden. So können Sie beispielsweise ein Administratorkennwort bzw. einen privaten Administratorschlüssel für alle Computer in der Personalabteilung festlegen, einen anderen für die Entwicklungsabteilung usw. Sie können auch eine Trennung auf physischer Ebene vornehmen, wie z. B. nach Gebäuden oder Standorten. Wenn Sie bestimmen, welcher private Administratorschlüssel verwendet werden soll, um eine Datei zum Zurücksetzen von Verschlüsselungstexten zu erstellen, sollten Sie berücksichtigen, wer das Zurücksetzen anfordert. Wie in Tabelle 3 auf Seite 32 und in Tabelle 5 auf Seite 36 angegeben, muss auch die Initialisierung von Benutzern und Unternehmen bzw. Hardware stattfinden.

Sicherheitspolicy vor der Implementierung von CSS festlegen

Sicherheits- und Authentifizierungsbestimmungen gehen aus den Anforderungen verschiedener Beteiligter in Ihrem Unternehmen hervor. Einzelne Benutzer mit Administratorzugriff können zwar Änderungen an der Policy vornehmen und diese auf Clients "durchsetzen" (siehe Kapitel 8, „Neue oder überarbeitete Sicherheitspolicy-Dateien über Remotezugriff implementieren", auf Seite 61), doch führt das Konfigurieren von Policy-Einstellungen vor der Implementierung zum besten Ergebnis. Weitere Informationen zum Konfigurieren der Policy finden Sie im *Client Security Administratorhandbuch* unter "Mit der UVM-Policy arbeiten".

Vorbereitungen für vergessene Verschlüsselungstexte oder fehlerhafte Authentifizierungsgeräte treffen

Benutzer vergessen zwangsläufig einmal einen Verschlüsselungstext; und Authentifizierungsgeräte, wie z. B. biometrische Sicherheitseinrichtungen für elektronische Fingerabdrücke oder Smart-Cards, können fehlerhaft sein.

Vergessener Verschlüsselungstext: Der Verschlüsselungstext des Benutzers wird nirgends auf der Festplatte des Clients oder im integrierten IBM Security Chip in einem vom Menschen lesbaren Format gespeichert. Er wird sicher im Gedächtnis des Benutzers aufbewahrt – und auch an einer weiteren Stelle: im Archiv, das mit dem Administratorschlüsselpaar geschützt ist. Der Administrator muss die im Archiv gesicherten Benutzerdaten mit Hilfe des privaten Administratorschlüssels entschlüsseln. Danach kann der Administrator dem Benutzer einen neuen Verschlüsselungstext zur Verfügung stellen.

Wenn der Benutzer den Verschlüsselungstext ändert, werden die neuen Daten in der angegebenen Archivposition archiviert.

Wenn einmal ein Authentifizierungsgerät ausfällt, können Sie IBM Client Security so konfigurieren, dass eine Schaltfläche zum Umgehen des Geräts angezeigt wird. Durch das Klicken auf die Schaltfläche zum Umgehen wird der Benutzer lediglich dazu aufgefordert, den Verschlüsselungstext korrekt einzugeben. Anschließend kann der Benutzer geschützte Tasks ausführen.

Gehen Sie wie folgt vor, um CSS so zu konfigurieren, dass die Schaltfläche zum Umgehen angezeigt wird:

1. Suchen Sie in der Datei CSEC.INI, die sich im Stammverzeichnis befindet, den Eintrag `AllowBypass= 0`. Durch den Standardwert `0` ist die Schaltfläche zum Umgehen ausgeblendet.
2. Geben Sie für `AllowBypass` den Wert 1 an. Die Schaltfläche zum Umgehen wird angezeigt, wenn der Benutzer im CSS-Fenster aufgefordert wird, zusätzlich zum Verschlüsselungstext eine Authentifizierung anzugeben.
3. Speichern Sie die Datei CSEC.INI.

Anmerkungen:

1. Damit diese Informationen archiviert werden, muss die Archivposition in der Datei CSEC.INI mit `kal=c:\jgk\archive` angegeben werden. Wenn es sich bei c:\jgk\archive um ein Netzlaufwerk handelt, muss dieses Laufwerk außerdem dem Client zugeordnet sein, damit der Verschlüsselungstext archiviert wird.
2. Wenn Sie keine Archivposition angeben oder die Position nicht dem Client zugeordnet ist, können Verschlüsselungstexte nicht wiederhergestellt werden.

Benutzerinitialisierung

Mit IBM ESS können mehrere Benutzer voneinander unabhängige und sichere Transaktionen auf einem einzigen Computer ausführen. Diesen Benutzern muss ein Verschlüsselungstext zugeordnet sein und möglicherweise andere Authentifizierungselemente, wie z. B. elektronische Fingerabdrücke und/oder Smart-Cards. Dies wird als *Berechtigung über mehrere Faktoren* bezeichnet. Die Benutzerinitialisierung stellt einen wichtigen Schritt bei der Konfiguration von Clients für die Verwendung von IBM ESS dar. Die Benutzerinitialisierung besteht aus zwei Teilen:

1. Registrierung
2. Personalisierung

Registrierung

Registrierung bedeutet, dass ein Benutzer zu IBM Client Security hinzugefügt, also registriert, wird. In Abb. 21 ist die Komponente "User Verification Manager" (UVM) von IBM Client Security dargestellt. Über UVM werden die Berechtigungsnachweise der einzelnen Benutzer gesteuert und die Policy erzwungen.

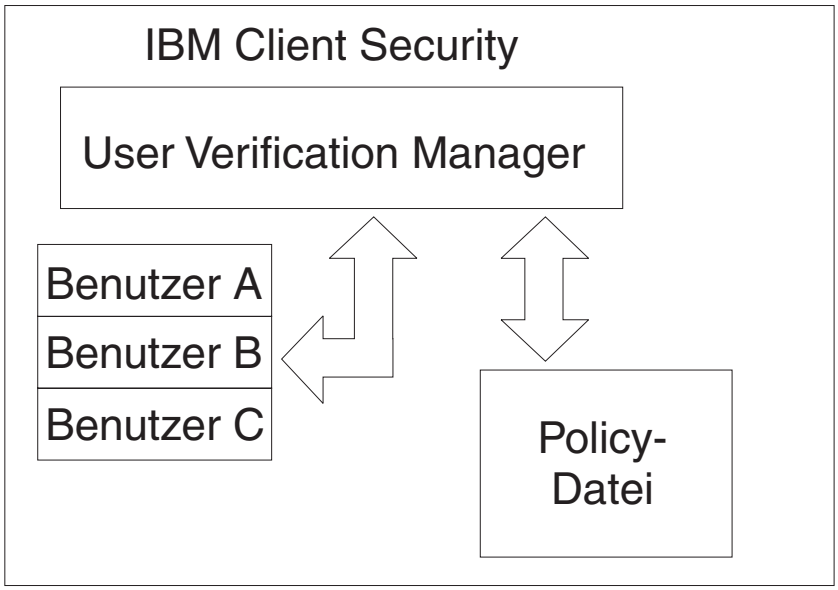

Abbildung 21. Über User Verification Manager werden die Berechtigungsnachweise der einzelnen Benutzer gesteuert und die Sicherheitspolicies erzwungen

Eine Policy-Datei, wie z. B. in Abb. 21 dargestellt, enthält die Authentifizierungsbestimmungen für jeden Benutzer, der von UVM verwaltet wird. Beachten Sie, dass UVM-Benutzer ganz einfach Windows-Benutzer (lokal oder auf einer Domäne) sind. In UVM wird der Berechtigungsnachweis (an anderer Stelle auch als Berechtigung bezeichnet) auf Grundlage des derzeit am Computer und Betriebssystem angemeldeten Benutzers verwaltet. Wenn sich Benutzer A beispielsweise bei Windows anmeldet und Benutzer A auch bei UVM registriert ist, wird die Policy erzwungen, wenn Benutzer A Operationen ausführen möchte, für die ein Berechtigungsnachweis erforderlich ist. Ein weiteres Beispiel: Benutzer A meldet sich am Computer an. Benutzer A öffnet dann Microsoft Outlook und sendet eine digital signierte E-Mail. Der private Schlüssel, mit dessen Hilfe die digital signierte E-Mail gesendet wird, ist im IBM Embedded Security Subsystem geschützt.

Bevor UVM das Senden zulässt, wird die Policy, wie in der Policy-Datei festgelegt, erzwungen. In diesem Beispiel muss der Verschlüsselungstext authentifiziert werden, bevor die Operation ausgeführt werden kann. UVM fordert den Benutzer zur Eingabe des Verschlüsselungstexts auf. Wenn dieser als korrekt bestätigt wird, wird die Operation mit dem privaten Schlüssel im Chip ausgeführt.

Persönliche Initialisierung

Die persönliche Initialisierung bedeutet lediglich das Festlegen eines persönlichen UVM-Verschlüsselungstexts für einen Benutzer. Unterschiedliche Personen können die verschiedenen Teile des Prozesses ausführen. Der persönliche UVM-Verschlüsselungstext sollte nur dem jeweiligen Benutzer bekannt sein. Wenn ein Benutzer den Initialisierungsprozess nicht selbst ausführt, muss dieser Benutzer unter Umständen einen weiteren Schritt ausführen. UVM kann auch so konfiguriert werden, dass der Benutzer den Verschlüsselungstext beim ersten Anmelden ändern muss.

Beispiel: Benutzer A wird vom IT-Administrator initialisiert. Der IT-Administrator wählt Benutzer A aus einer Windows-Benutzerliste aus (z. B. von einer Domäne). UVM gibt eine Aufforderung zur Zuordnung des UVM-Verschlüsselungstexts zu Benutzer A aus. Der IT-Administrator gibt einen "Standardwert" des "IT-Administratorverschlüsselungstexts" ein. Damit die Sicherheit des Systems gewährleistet ist, muss Benutzer A nach Erhalt des Systems den Verschlüsselungstext anpassen, so dass sichere Transaktionen nicht mit dem Standardverschlüsselungstext ausgeführt werden können.

Tabelle 5. Methoden zur Benutzerinitialisierung

Methode	Befehlsverarbeitung	Verarbeitungsbestimmungen
Manuell	Der Administrator kann CSS über das Administratordienstprogramm manuell für den Benutzer personalisieren.	Der Administrator muss bei der Konfiguration der einzelnen Computer anwesend sein.
Administratorkonfigurationsdatei	Der Administrator kann eine Konfigurationsdatei erstellen, die eine verschlüsselte Version des Administratorkennworts enthält. Diese Datei wird an den Benutzer gesendet, der sich dann ohne Eingreifen oder Anwesenheit des Administrators registrieren kann.	Der Benutzer führt die Konfiguration aus.
*.ini	Der Administrator erstellt ein Script, das die .ini-Datei ausführt und ein Standard- oder personalisiertes Kennwort einfügt.	Die Anwesenheit des Administrators oder Benutzers ist optional.

Implementierungsszenarien

Sie implementieren 1.000 Clients für 1.000 Endbenutzer. Eines der folgenden Szenarien könnte Ihren Implementierungsansatz beschreiben:

- Sie wissen genau, welcher Rechner für welchen Endbenutzer bestimmt ist. Zum Beispiel ist Rechner 1 für Robert bestimmt, so dass Sie Robert auf Rechner 1 registrieren. Robert muss seinen Computer personalisieren (seinen persönlichen Verschlüsselungstext konfigurieren), wenn er seinen Computer erhält. Robert erhält den Computer, startet IBM Client Security und legt seinen Verschlüsselungstext fest.
- Sie wissen nicht, welcher Rechner für welchen Benutzer bestimmt ist. Sie vergeben Client 1 an Endbenutzer X.

Durch diese zwei variablen Faktoren unterscheidet sich die Implementierung von IBM ESS von der Implementierung einer normalen Anwendung. Es gibt jedoch mehrere Implementierungsoptionen, die Flexibilität bei der Implementierung von IBM ESS ermöglichen.

Ein typisches Flussdiagramm für die Bereitstellung von PCs in Ihrem Unternehmen kann wie folgt aussehen:

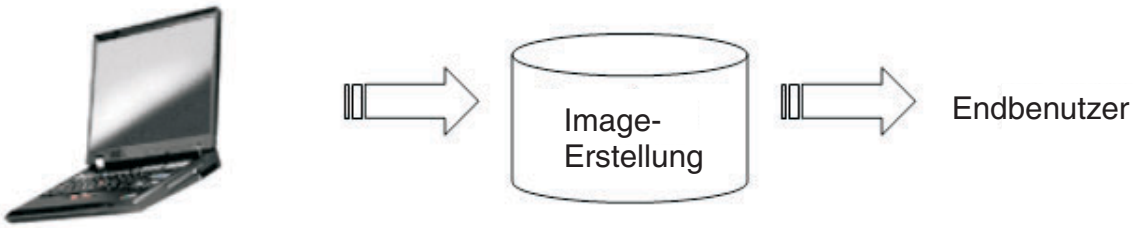

Abbildung 22. Typisches Flussdiagramm für die Implementierung von PCs

Sechs Implementierungsszenarien

Es gibt sechs Implementierungsmethoden für IBM Client Security:

1. **Hinzugefügte Komponente:** Der IBM Client Security-Code ist kein Bestandteil des Plattenimages. Er wird nach der Implementierung der Computer installiert, initialisiert und personalisiert.
2. **Image-Komponente:** Der IBM Client Security-Code ist Bestandteil des Images, ist jedoch nicht installiert. Die Unternehmenspersonalisierung sowie die Benutzerpersonalisierung wurden nicht initialisiert. (Siehe Abb. 23 auf Seite 38.)
3. **Einfache Installation:** IBM Client Security wurde installiert und für das Unternehmen oder den Endbenutzer personalisiert. (Siehe Abb. 24 auf Seite 39.)
4. **Teilweise Personalisierung:** IBM Client Security wurde installiert und für das Unternehmen personalisiert. Eine Personalisierung für den Endbenutzer ist jedoch nicht erfolgt. (Siehe Abb. 24 auf Seite 39.)
5. **Temporäre Personalisierung:** IBM Client Security wurde installiert und eine Personalisierung für Unternehmen sowie Endbenutzer durchgeführt. Der Benutzer muss den Verschlüsselungstext zurücksetzen und bei Bedarf weitere Authentifizierungsinformationen, wie z. B. gescannten Fingerabdruck oder Smart-Card-Zuordnung, angeben. (Siehe Abb. 25 auf Seite 40.)

6. **Vollständige Personalisierung:** IBM Client Security wurde installiert und eine Personalisierung für Unternehmen sowie Endbenutzer durchgeführt. Der Administrator legt den Verschlüsselungstext des Benutzers fest. Wenn ein gescannter Fingerabdruck oder eine andere Authentifizierung erforderlich ist, muss der Benutzer sie personalisieren. (Siehe Abb. 25 auf Seite 40.)

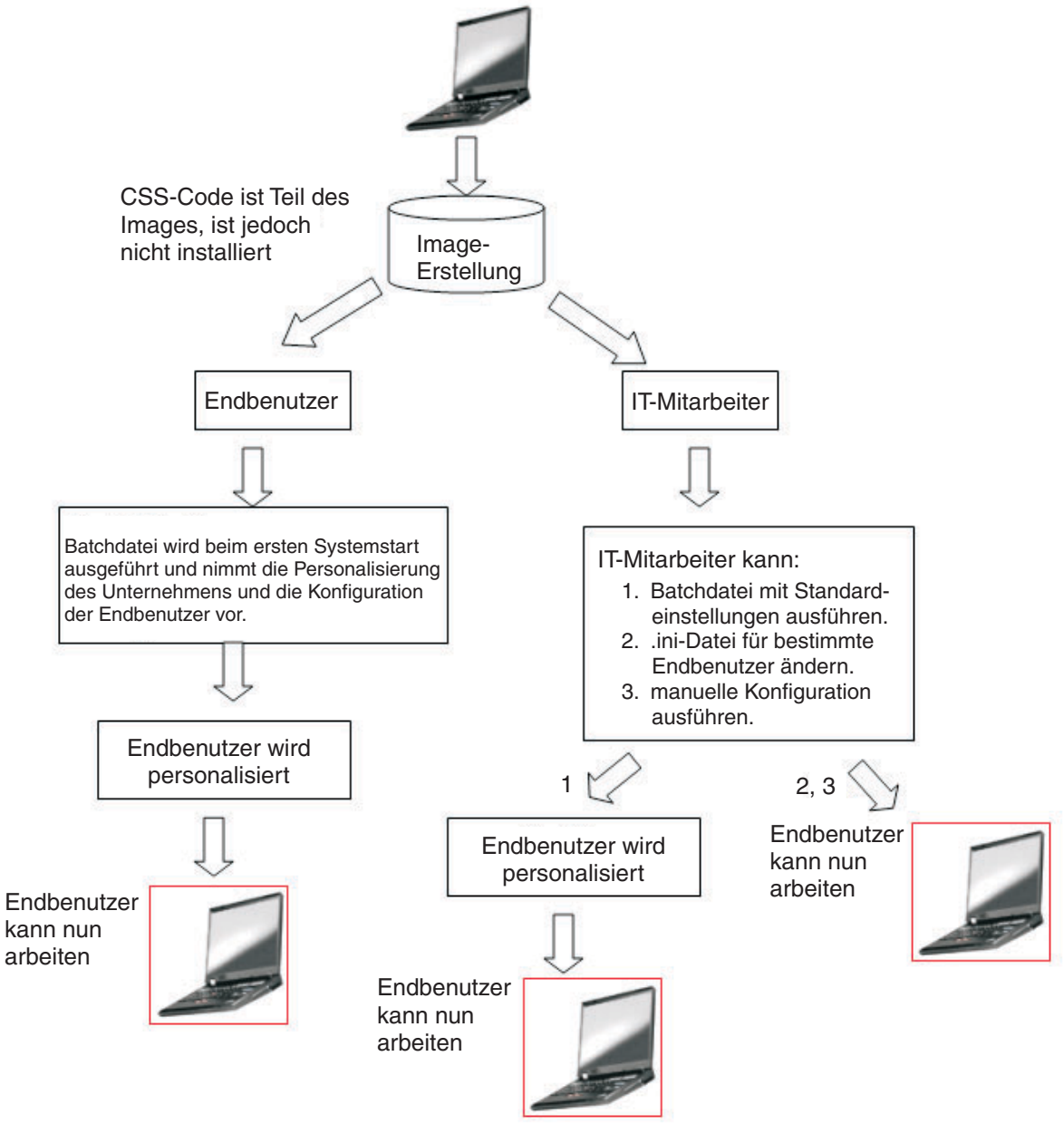

Abbildung 23. Der IBM Client Security-Code ist Bestandteil des Images, ist jedoch nicht installiert

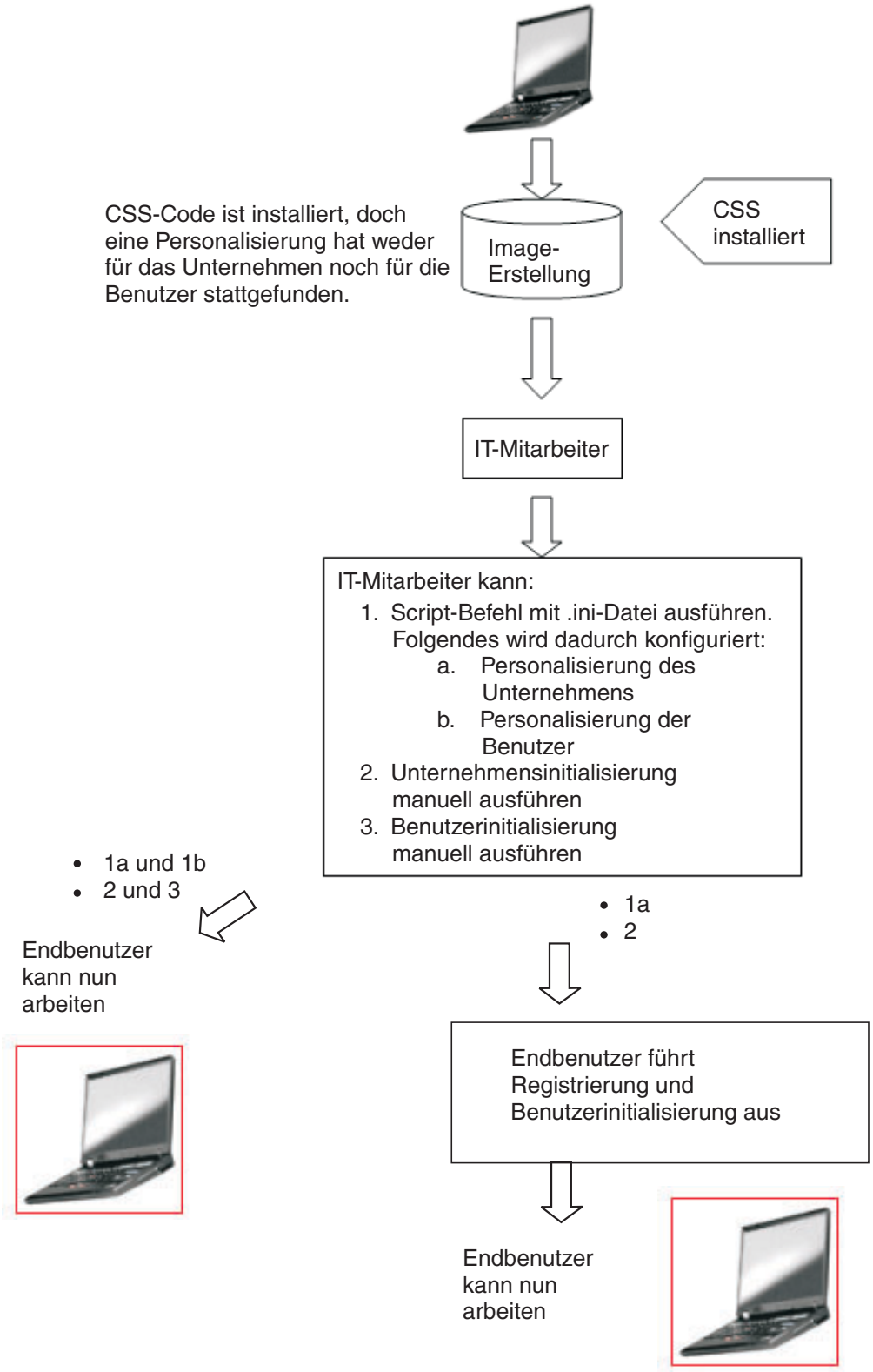

Abbildung 24. Der IBM Client Security-Code ist installiert, doch die Personalisierung des Unternehmens oder des Benutzers hat nicht stattgefunden

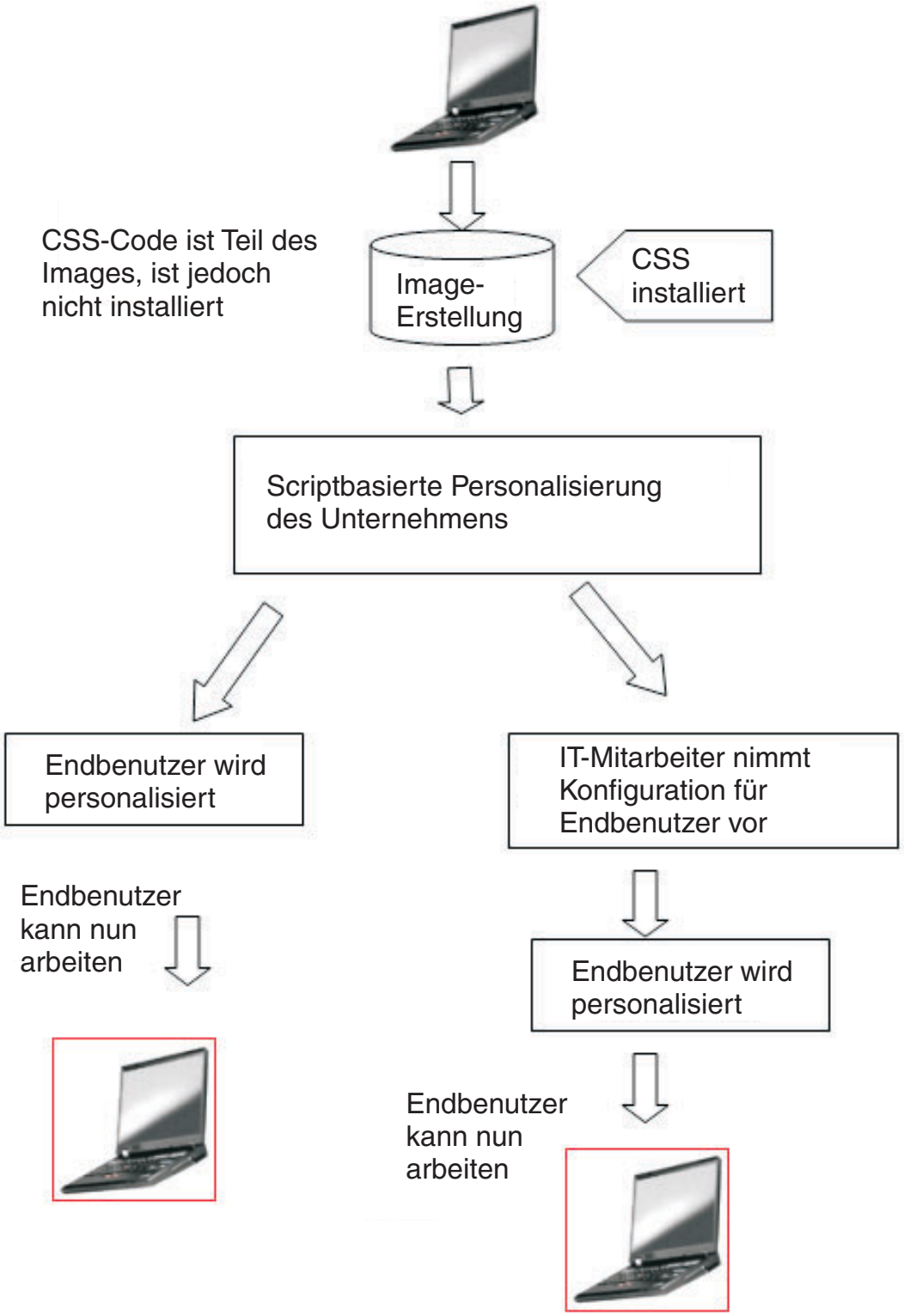

Abbildung 25. IBM Client Security wurde installiert und eine Personalisierung für Unternehmen sowie Benutzer durchgeführt

In Szenario 1 wird IBM Client Security implementiert, nachdem das Plattenimage auf den Computer geladen wurde. IBM Client Security wird installiert sowie konfiguriert, und der integrierte IBM Security Chip wird konfiguriert, nachdem das Plattenimage installiert wurde.

Die Szenarien 2 bis 6 stellen verschiedene Optionen der Softwareimplementierung und -konfiguration sowie der Chipkonfiguration dar. Je nach Ihren Anforderungen und Ihrer Umgebung können Sie das für Sie beste Szenario und die Installationsmethode auswählen.

Informationen zur Konfigurationsdatei

Sie können die Datei CSEC.INI mit Hilfe des Assistenten von Client Security erstellen: CSECWIZ.EXE im Sicherheitsverzeichnis. Aktivieren Sie nach Abschluss des Assistenten das Markierungsfeld neben **Einstellungen speichern, jedoch nicht Subsystem konfigurieren. (Einstellungen werden in C:\CSEC.INI gespeichert.)**

Konfigurationsvorgang

Die Datei CSCC.INI ist bei der Initialisierung einer Massenkonfiguration erforderlich. Der Name der Datei kann beliebig ausgewählt werden, nur die Erweiterung ″.ini″ ist obligatorisch. In der folgenden Tabelle werden die Einstellungen sowie Erläuterungen zu diesen Einstellungen für die von Ihnen zu erstellende .ini-Datei aufgeführt. Bevor Sie die Datei CSEC.INI öffnen und überarbeiten können, müssen Sie sie zuerst mit Hilfe von CONSOLE.EXE im Sicherheitsverzeichnis entschlüsseln.

Tabelle 6. Konfigurationseinstellungen von Client Security

[CSSSetup]	Abschnittsüberschrift für CSS-Konfiguration.
suppw=bootup	BIOS-Administratorkennwort. Lassen Sie es leer, wenn es nicht erforderlich ist.
hwpw=11111111	CSS-Hardwarekennwort. Muss aus 8 Zeichen bestehen. Ist immer erforderlich. Muss richtig eingegeben werden, wenn das Hardwarekennwort bereits festgelegt wurde.
newkp=1	1: Neues Administratorschlüsselpaar generieren, 0: Vorhandenes Administratorschlüsselpaar verwenden.
keysplit=1	Wenn ″newkp″ den Wert 1 aufweist, wird mit dieser Einstellung die Anzahl der privaten Schlüsselkomponenten festgelegt. **Anmerkung:** Enthält das vorhandene Schlüsselpaar mehrere private Schlüsselkomponenten, müssen alle privaten Schlüsselkomponenten in demselben Verzeichnis gespeichert werden.
kpl=c:\jgk	Position des Administratorschlüsselpaars, wenn ″newkp″ = 1. Handelt es sich hierbei um ein Netzlaufwerk, muss das Laufwerk zugeordnet sein.
kal=c:\jgk\archive	Position des Benutzerschlüsselarchivs. Handelt es sich hierbei um ein Netzlaufwerk, muss das Laufwerk zugeordnet sein.
pub=c:\jk\admin.key	Position des öffentlichen Administratorschlüssels, wenn ein vorhandenes Administratorschlüsselpaar verwendet wird. Handelt es sich hierbei um ein Netzlaufwerk, muss das Laufwerk zugeordnet sein.

Tabelle 6. Konfigurationseinstellungen von Client Security (Forts.)

pri=c:\jk\private1.key	Position des privaten Administratorschlüssels, wenn ein vorhandenes Administratorschlüsselpaar verwendet wird. Handelt es sich hierbei um ein Netzlaufwerk, muss das Laufwerk zugeordnet sein.
wiz=0	Gibt an, ob diese Datei mit dem CSS-Installationsassistenten generiert wurde. Dieser Eintrag ist nicht erforderlich. Wenn Sie ihn in die Datei aufnehmen, muss er den Wert 0 aufweisen.
clean=0	1: .ini-Datei nach Initialisierung löschen, 0: .ini-Datei nach Initialisierung nicht löschen.
enableroaming=1	1: Standortunabhängigen Zugriff für den Client aktivieren, 0: Standortunabhängigen Zugriff für den Client inaktivieren.
username= [promptcurrent]	[promptcurrent]: Der derzeitige Benutzer wird zur Eingabe des Systemregistrierungskennworts aufgefordert. [current]: Wenn das Systemregistrierungskennwort für den derzeitigen Benutzer über den Eintrag ″sysregpwd″ bereitgestellt wird und der derzeitige Benutzer zur Systemregistrierung über den Roaming-Server berechtigt ist. [<bestimmter_Benutzeraccount>]: Wenn der designierte Benutzer zur Systemregistrierung über den Roaming-Server berechtigt ist und das Systemregistrierungskennwort für diesen Benutzer über den Eintrag ″sysregpwd″ bereitgestellt wird. Verwenden Sie diesen Eintrag nicht, wenn der Wert für ″enableroaming″ 0 ist oder wenn der Eintrag ″enableroaming″ nicht vorhanden ist.
sysregpwd=12345678	Systemregistrierungskennwort. Definieren Sie für diesen Wert das richtige Kennwort, um für das System eine Registrierung über den Roaming-Server zu ermöglichen. Nehmen Sie diesen Eintrag nicht auf, wenn der Wert für ″username″ als [promptcurrent] definiert ist oder wenn der Eintrag ″username″ nicht vorhanden ist.
[UVMEnrollment]	Abschnittsüberschrift für die Benutzerregistrierung.
enrollall=0	1: Alle lokalen Benutzeraccounts in UVM registrieren, 0: Bestimmte Benutzeraccounts in UVM registrieren.
defaultuvmpw=top	Wenn ″enrollall″ den Wert 1 aufweist, ist dies der UVM-Verschlüsselungstext für alle Benutzer.
defaultwinpw=down	Wenn ″enrollall″ den Wert 1 aufweist, ist dies das bei UVM registrierte Windows-Kennwort für alle Benutzer.
defaultppchange=0	Wenn ″enrollall″ den Wert 1 aufweist, gibt dieser Wert die Policy für das Ändern des UVM-Verschlüsselungstexts für alle Benutzer an. 1: Der Benutzer muss den UVM-Verschlüsselungstext bei der nächsten Anmeldung ändern, 0: Der Benutzer muss den UVM-Verschlüsselungstext bei der nächsten Anmeldung nicht ändern.
defaultppexppolicy=1	Wenn ″enrollall″ den Wert 1 aufweist, gibt dieser Wert die Policy für das Ablaufen des UVM-Verschlüsselungstexts für alle Benutzer an. 0: Der UVM-Verschlüsselungstext läuft ab, 1: Der UVM-Verschlüsselungstext läuft nicht ab.

Tabelle 6. Konfigurationseinstellungen von Client Security (Forts.)

defaultppexpdays=0	Wenn "enrollall" den Wert 1 aufweist, wird mit diesem Wert die Anzahl von Tagen bis zum Ablaufen des UVM-Verschlüsselungstexts für alle Benutzer festgelegt. Wenn "ppexppoliall" den Wert 0 aufweist, legen Sie mit diesem Wert die Anzahl von Tagen bis zum Ablaufen des UVM-Verschlüsselungstexts fest.
enrollusers=*x*, hierbei ist x die Gesamtanzahl der Benutzer, die Sie auf dem Computer registrieren.	Der Wert in dieser Anweisung gibt die Gesamtanzahl der Benutzer an, die Sie registrieren. Wenn "enrollall" den Wert 0 aufweist, ist dies die Anzahl der Benutzer, die bei UVM registriert sind.
user1=jknox	Geben Sie die Informationen für jeden zu registrierenden Benutzer ab Benutzer 1 an. (Es gibt keinen Benutzer 0.) Als Benutzernamen müssen die Accountnamen verwendet werden. Gehen Sie wie folgt vor, um den Accountnamen unter Windows XP abzurufen: 1. Starten Sie die Computerverwaltung (Geräte-Manager). 2. Erweitern Sie den Knoten der lokalen Benutzer und Gruppen. 3. Öffnen Sie den Benutzerordner. Bei den in der Namensspalte enthaltenen Einträgen handelt es sich um die Accountnamen.
user1uvmpw=chrome	Geben Sie den UVM-Verschlüsselungstext für Benutzer 1 in UVM an.
user1winpw=spinning	Geben Sie den Windows-Verschlüsselungstext für Benutzer 1 an, der bei UVM registriert werden soll.
user1domain=0	Geben Sie an, ob es sich bei dem Account für Benutzer 1 um einen lokalen oder einen Domänenaccount handelt. 0: Es handelt sich um einen lokalen Account, 1: Es handelt sich um einen Domänenaccount.
user1ppchange=0	Geben Sie an, ob Benutzer 1 bei der nächsten Anmeldung den UVM-Verschlüsselungstext ändern muss. 1: Der Benutzer muss den UVM-Verschlüsselungstext bei der nächsten Anmeldung ändern, 0: Der Benutzer muss den UVM-Verschlüsselungstext bei der nächsten Anmeldung nicht ändern.
user1ppexppolicy=1	Geben Sie an, ob der UVM-Verschlüsselungstext für Benutzer 1 abläuft. 0: Der UVM-Verschlüsselungstext läuft ab, 1: Der UVM-Verschlüsselungstext läuft nicht ab.
user1ppexpdays=0	Wenn "user1ppexppolicy" den Wert 0 aufweist, legen Sie mit diesem Wert die Anzahl von Tagen bis zum Ablaufen des UVM-Verschlüsselungstexts fest.
Geben Sie für jeden Benutzer die vollständigen Konfigurationseinstellungen in der im grauen Bereich der Tabelle angegebenen Reihenfolge an. Geben Sie zuerst alle Parameter für einen Benutzer und dann die Parameter für den nächsten Benutzer an. Wenn "enrollusers" beispielsweise den Wert 2 aufweist, fügen Sie die folgende Gruppe von Konfigurationseinstellungen hinzu.	
user2=chrome	
user2uvmpw=left	
user2winpw=right	
user2domain=0	
user2ppchange=1	

Tabelle 6. Konfigurationseinstellungen von Client Security (Forts.)

user2ppexppolicy=0	
user2ppexpdays=90	
[UVMAppConfig]	Abschnittsüberschrift für die Einrichtung von UVM-sensitiven Anwendungen und Modulen.
uvmlogon=0	1: UVM-Anmeldeschutz verwenden, 0: Windows-Anmeldung verwenden.
entrust=0	1: UVM für Entrust-Authentifizierung verwenden, 0: Entrust-Authentifizierung verwenden.
notes=1	1: UVM-Anmeldeschutz für Lotus Notes verwenden, 0: Notes-Kennwortschutz verwenden.
netscape=0	1: E-Mails mit dem IBM PKCS#11-Modul signieren und verschlüsseln, 0: E-Mails nicht mit dem IBM PKCS#11-Modul signieren und verschlüsseln.
passman=0	1: Password Manager verwenden, 0: Password Manager nicht verwenden.
folderprotect=0	1: Verschlüsselung von Dateien und Ordnern verwenden, 0: Verschlüsselung von Dateien und Ordnern nicht verwenden.

Anmerkungen:

1. Bei einer Erweiterung und Aktualisierung von IBM Client Security können sich die Parameter der *.ini-Datei unter Umständen ändern.
2. Wenn sich Dateien oder Pfade auf einem Netzlaufwerk befinden, muss dem Netzlaufwerk ein Laufwerkbuchstabe zugeordnet sein.
3. Die Datei CSEC.ini muss verschlüsselt werden, damit die Software den Inhalt laden kann. Sie muss über CONSOLE.EXE im Sicherheitsverzeichnis verschlüsselt werden. Mit dem folgenden Befehl kann eine INI-Datei ebenfalls über ein Script verschlüsselt werden. (Bei langen Pfadnamen sind Anführungszeichen erforderlich): *CSS-Installationsordner*\console.exe /q /ini: *vollständiger Pfad zu einer unverschlüsselten INI-Datei*
4. Durch den folgenden Befehl wird die .ini-Datei von der Befehlszeile aus ausgeführt, wenn die Massenkonfiguration nicht in Verbindung mit einer Masseninstallation durchgeführt wird:

   CSS-Installationsordner\acamucli /ccf:c:\csec.ini
5. Die INI-Datei unterstützt das Hinzufügen neuer Benutzer, nachdem das Subsystem konfiguriert wurde, was für die Benutzerregistrierung praktisch ist. Führen Sie eine INI-Datei, wie zuvor beschrieben, aus, jedoch ohne die Werte ″pub=″ und ″pri=″. Der Code übernimmt lediglich die Benutzerregistrierung und führt keine Reinitialisierung des Subsystems aus.

IBM Client Security ermöglicht es Ihnen, die Datei CSEC.INI ein zweites Mal auszuführen, ohne dass sich dies auf die Installation von Client Security auswirkt. Sie können diese Datei beispielsweise ein zweites Mal ausführen, um weitere Benutzer zu registrieren.

Tabelle 7. Konfigurationseinstellungen von Client Security, wenn die Datei ein zweites Mal ausgeführt wird

[CSSSetup]	Abschnittsüberschrift für CSS-Konfiguration.
suppw=	BIOS-Administratorkennwort. Lassen Sie es leer, wenn es nicht erforderlich ist.
hwpw=11111111	CSS-Hardwarekennwort. Muss aus 8 Zeichen bestehen. Ist immer erforderlich. Muss richtig eingegeben werden, wenn das Hardwarekennwort bereits festgelegt wurde.
newkp=0	Geben Sie 0 ein, um ein vorhandenes Administratorschlüsselpaar zu verwenden.
keysplit=1	Wenn "newkp" den Wert 1 aufweist, wird mit dieser Einstellung die Anzahl der privaten Schlüsselkomponenten festgelegt. **Anmerkung:** Enthält das vorhandene Schlüsselpaar mehrere private Schlüsselkomponenten, müssen alle privaten Schlüsselkomponenten in demselben Verzeichnis gespeichert werden.
pub=	Keine Angabe
pri=	Keine Angabe
kal=c:\archive	Position des Benutzerschlüsselarchivs. Handelt es sich hierbei um ein Netzlaufwerk, muss das Laufwerk zugeordnet sein.
wiz=0	Gibt an, ob diese Datei mit dem CSS-Installationsassistenten generiert wurde. Dieser Eintrag ist nicht erforderlich. Wenn Sie ihn in die Datei aufnehmen, muss er den Wert 0 aufweisen.
clean=0	Geben Sie 0 ein, um die .ini-Datei nach der Initialisierung nicht zu löschen.
enableroaming=0	Geben Sie 0 ein, um den standortunabhängigen Zugriff für den Client zu inaktivieren.
[UVMEnrollment]	Abschnittsüberschrift für die Benutzerregistrierung.
enrollall=0	1: Alle lokalen Benutzeraccounts in UVM registrieren, 0: Bestimmte Benutzeraccounts in UVM registrieren.
enrollusers=1	Der Wert in dieser Anweisung gibt die Gesamtanzahl der Benutzer an, die Sie registrieren.
user1=*eddy*	Hierbei handelt es sich um den Namen des neuen Benutzers, der registriert wird.
user1uvmpw=pass1word	Geben Sie den UVM-Verschlüsselungstext für Benutzer 1 in UVM an.
user1winpw=	Geben Sie den Windows-Verschlüsselungstext für Benutzer 1 an, der bei UVM registriert werden soll.
user1domain=0	Geben Sie an, ob es sich bei dem Account für Benutzer 1 um einen lokalen oder einen Domänenaccount handelt. 0: Es handelt sich um einen lokalen Account, 1: Es handelt sich um einen Domänenaccount.
user1ppchange=0	Geben Sie an, ob Benutzer 1 bei der nächsten Anmeldung den UVM-Verschlüsselungstext ändern muss. 1: Der Benutzer muss den UVM-Verschlüsselungstext bei der nächsten Anmeldung ändern, 0: Der Benutzer muss den UVM-Verschlüsselungstext bei der nächsten Anmeldung nicht ändern.

Tabelle 7. Konfigurationseinstellungen von Client Security, wenn die Datei ein zweites Mal ausgeführt wird (Forts.)

user1ppexppolicy=1	Geben Sie an, ob der UVM-Verschlüsselungstext für Benutzer 1 abläuft. 0: Der UVM-Verschlüsselungstext läuft ab, 1: Der UVM-Verschlüsselungstext läuft nicht ab.
user1ppexpdays=0	Wenn "user1ppexppolicy" den Wert 0 aufweist, legen Sie mit diesem Wert die Anzahl von Tagen bis zum Ablaufen des UVM-Verschlüsselungstexts fest.

Kapitel 6. Client Security-Komponente auf einem Tivoli Access Manager-Server installieren

Die Authentifizierung von Endbenutzern auf der Clientebene ist ein wichtiger Sicherheitsaspekt. Client Security stellt die Schnittstelle zur Verfügung, die für die Verwaltung der Sicherheitspolicy eines IBM Clients erforderlich ist. Diese Schnittstelle ist Teil der Authentifizierungssoftware "User Verification Manager" (UVM), die die Hauptkomponente von Client Security darstellt.

Für die Verwaltung der UVM-Sicherheitspolicy für einen IBM Client stehen zwei Methoden zur Verfügung:

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

Damit Client Security mit Tivoli Access Manager verwendet werden kann, muss die Client Security-Komponente von Tivoli Access Manager installiert werden. Diese Komponente kann von der IBM Website http://www.pc.ibm.com/us/security/index.html heruntergeladen werden.

Voraussetzungen

Damit eine sichere Verbindung zwischen dem IBM Client und dem Tivoli Access Manager-Server hergestellt werden kann, müssen die folgenden Komponenten auf dem IBM Client installiert werden:

- IBM Global Security Toolkit
- IBM SecureWay Directory Client
- Tivoli Access Manager Runtime Environment

Ausführliche Informationen zur Installation und Verwendung von Tivoli Access Manager finden Sie in der Dokumentation auf der Website unter http://www.tivoli.com/products/index/secureway_policy_dir/index.htm.

Client Security-Komponente herunterladen und installieren

Die Client Security-Komponente kann gebührenfrei von der IBM Website heruntergeladen werden.

Gehen Sie wie folgt vor, um die Client Security-Komponente herunterzuladen und auf dem Tivoli Access Manager-Server und dem IBM Client zu installieren:

1. Vergewissern Sie sich anhand der Informationen auf der Website, dass Ihr System über den integrierten IBM Security Chip verfügt, indem Sie Ihre Modellnummer mit den Angaben in der Tabelle mit den Systemvoraussetzungen vergleichen. Klicken Sie anschließend auf **Continue**.
2. Wählen Sie den Radioknopf für Ihren Maschinentyp aus, und klicken Sie auf **Continue**.
3. Erstellen Sie eine Benutzer-ID, füllen Sie das Onlineformular zur Registrierung bei IBM aus, und lesen Sie die Lizenzvereinbarung. Klicken Sie dann auf **Accept Licence**.

Daraufhin wird automatisch die Download-Seite für Client Security aufgerufen.

4. Befolgen Sie die angezeigten Anweisungen, um die erforderlichen Einheitentreiber, Readme-Dateien, Softwareprogramme, Referenzdokumente und zusätzlichen Dienstprogramme zu installieren.
5. Gehen Sie wie folgt vor, um Client Security zu installieren:
   a. Klicken Sie auf dem Windows-Desktop auf **Start > Ausführen**.
   b. Geben Sie im Fenster "Ausführen" `d:\verzeichnis\csec53.exe` ein. Dabei steht d:\verzeichnis\ für den Laufwerkbuchstaben und das Verzeichnis, in dem die Datei gespeichert ist.
   c. Klicken Sie auf **OK**.

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

      Der Assistent extrahiert die Dateien und installiert die Software. Nach Abschluss der Installation werden Sie gefragt, ob der erforderliche Neustart sofort oder zu einem späteren Zeitpunkt durchgeführt werden soll.
   e. Wählen Sie den entsprechenden Radioknopf aus, und klicken Sie auf **OK**.
6. Klicken Sie nach dem Neustart auf dem Windows-Desktop auf **Start > Ausführen**.
7. Geben Sie im Fenster "Ausführen" *d:*`\`*verzeichnis*`\TAMCSS.exe` ein. Dabei steht *d:*`\`*verzeichnis*`\` für den Laufwerkbuchstaben und das Verzeichnis, in dem die Datei gespeichert ist. Oder klicken Sie auf **Durchsuchen**, um nach der Datei zu suchen.
8. Klicken Sie auf **OK**.
9. Geben Sie einen Zielordner an, und klicken Sie auf die Option zum Dekomprimieren.

   Der Assistent extrahiert die Dateien in den angegebenen Ordner. Sie werden in einer Nachricht darüber informiert, dass die Dateien erfolgreich dekomprimiert wurden.
10. Klicken Sie auf **OK**.

Client Security-Komponenten auf dem Tivoli Access Manager-Server hinzufügen

Beim Dienstprogramm "pdadmin" handelt es sich um ein Befehlszeilentool, mit dem der Administrator die meisten Tivoli Access Manager-Verwaltungstasks durchführen kann. Die Funktion zur Ausführung mehrerer Befehle ermöglicht es dem Administrator, über eine Datei, die mehrere pdadmin-Befehle enthält, eine vollständige Task oder eine Reihe von Tasks auszuführen. Die Kommunikation zwischen dem Dienstprogramm "pdadmin" und dem Verwaltungsserver (pdmgrd) wird über SSL gesichert. Das Dienstprogramm "pdadmin" wird als Teil des Runtime Environment-Pakets von Tivoli Access Manager installiert.

Das Dienstprogramm "pdadmin" akzeptiert ein Argument für einen Dateinamen, das die Position einer solchen Datei angibt, z. B.:

```
MSDOS>pdadmin [-a Admin-Benutzer][-p Kennwort ]Datei-Pfadname
```

Der folgende Befehl ist ein Beispiel dafür, wie auf dem Tivoli Access Manager-Server der Objektbereich für IBM Solutions, Client Security Actions und einzelne ACL-Einträge erstellt werden können:

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

Weitere Informationen zum Dienstprogramm ″pdadmin″ und zur Befehlssyntax finden Sie im *Tivoli Access Manager Base Administrator Guide*.

Sichere Verbindung zwischen dem IBM Client und dem Tivoli Access Manager-Server aufbauen

Für den IBM Client muss innerhalb der gesicherten Tivoli Access Manager-Domäne eine eigene authentifizierte Identität aufgebaut werden, um vom Tivoli Access Manager Authorization Service Autorisierungsentscheidungen anfordern zu können.

In der gesicherten Tivoli Access Manager-Domäne muss für die Anwendung eine eindeutige Identität erstellt werden. Damit für die authentifizierte Identität Authentifizierungsüberprüfungen durchgeführt werden können, muss die Anwendung zur Gruppe der fernen ACL-Benutzer gehören. Wenn die Anwendung auf einen der Services der gesicherten Domäne zugreifen möchte, muss sie sich zuerst bei der gesicherten Domäne anmelden.

Mit Hilfe des Dienstprogramms ″svrsslcfg″ können IBM Client Security-Anwendungen mit dem Verwaltungsserver und dem Autorisierungsserver von Tivoli Access Manager kommunizieren.

Das Dienstprogramm ″svrsslcfg″ führt die folgenden Tasks aus:
- Erstellt für die Anwendung eine Benutzeridentität. Beispiel: DemoBenutzer/HOSTNAME
- Erstellt eine SSL-Schlüsseldatei für diesen Benutzer. Beispiel: DemoBenutzer.kdb und DemoBenutzer.sth
- Fügt den Benutzer der Gruppe der fernen ACL-Benutzer hinzu

Die folgenden Parameter werden benötigt:
- **-f cfg_file** Pfad und Name der Konfigurationsdatei. Verwenden Sie TAMCSS-.conf.
- **-d kdb_dir** Das Verzeichnis, das die Schlüsselringdatenbankdateien für den Server enthalten soll.
- **-n server_name** Der tatsächliche Windows-Benutzername/UVM-Benutzername des gewünschten IBM Client-Benutzers.
- **-P admin_pwd** Das Tivoli Access Manager-Administratorkennwort.
- **-s server_type** Es muss ″fern/remote″ angegeben werden.
- **-S server_pwd** Das Kennwort für den neu erstellten Benutzer. Hierbei handelt es sich um einen erforderlichen Parameter.
- **-r port_num** Definition der Nummer des Empfangsports für den IBM Client. Dabei handelt es sich um den in der Tivoli Access Manager Runtime-Variablen ″SSL Server Port for PD Management Server″ (SSL-Serverport für PD-Verwaltungsserver) angegebenen Parameter.
- **-e pwd_life** Definition der Zeitdauer bis zum Ablaufen des Kennworts in Anzahl von Tagen.

Gehen Sie wie folgt vor, um eine sichere Verbindung zwischen dem IBM Client und dem Tivoli Access Manager-Server aufzubauen:

1. Erstellen Sie ein Verzeichnis, und verschieben Sie die Datei TAMCSS.conf in das neue Verzeichnis.

   Beispiel: `MSDOS> mkdir C:\TAMCSS MSDOS> move C:\TAMCSS.conf C:\TAMCSS\`

2. Führen Sie ″svrsslcfg″ aus, um den Benutzer zu erstellen.

   MSDOS> svrsslcfg -config -f C:\TAMCSS\TAMCSS.conf -d C:\TAMCSS\ -n <Servername> - s remote -S <Serverkennwort> -P <Administratorkennwort> -e 365 -r 199

   Anmerkung: Geben Sie für <Servername> den gewünschten UVM-Benutzernamen und den Hostnamen des IBM Clients an. Beispiel: –n DemoBenutzer /NameMeinesHosts. Den Hostnamen des IBM Clients können Sie herausfinden, indem Sie an der MSDOS-Eingabeaufforderung “hostname” eingeben. Das Dienstprogramm ″svrsslcfg″ erstellt auf dem Tivoli Access Manager-Server einen gültigen Eintrag und stellt eine eindeutige SSL-Schlüsseldatei für verschlüsselte Übertragung zur Verfügung.

3. Führen Sie ″svrsslcfg″ aus, um die Position von ″ivacld″ zur Datei TAMCSS-.conf hinzuzufügen.

   Standardmäßig ist beim PD-Autorisierungsserver der Port 7136 empfangsbereit. Sie können das über den Parameter ″tcp_req_port″ in der Zeilengruppe ″ivacld″ der Datei ″ivacld.conf″ auf dem Tivoli Access Manager-Server überprüfen. Es ist wichtig, dass Sie den richtigen ivacld-Hostnamen eingeben. Diese Information können Sie über den Befehl ″pdadmin server list″ anfordern. Die Server werden wie folgt benannt: **Servername-Hostname**. Beispiel für den Befehl ″pdadmin server list″:

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

Mit dem folgenden Befehl wird anschließend ein Replikatseintrag für den oben angezeigten ivacld-Server hinzugefügt. Es wird davon ausgegangen, dass für ″ivacld″ der Standardport 7136 empfangsbereit ist.

```
svrsslcfg -add_replica  -f Pfad_zur_Konfigurationsdatei -h Hostname
MSDOS>svrsslcfg -add_replica  -f C:\TAMCSS\TAMCSS.conf -h MyHost.ibm.com
```

IBM Clients konfigurieren

Sie müssen zunächst jeden Client mit dem Administratordienstprogramm, einer Komponente von Client Security, konfigurieren, damit Sie dann über den Tivoli Access Manager die Authentifizierungsobjekte für IBM Clients steuern können. Der folgende Abschnitt beschreibt die Voraussetzungen und enthält die Anweisungen für die Konfiguration von IBM Clients.

Voraussetzungen

Stellen Sie sicher, dass die folgende Software in der angegebenen Reihenfolge auf dem IBM Client installiert ist:

1. **Von Microsoft Windows unterstütztes Betriebssystem.** Bei IBM Clients unter Windows XP, Windows 2000 oder Windows NT Workstation 4.0 können Sie über den Tivoli Access Manager die Authentifizierungsbestimmungen steuern.
2. **Client Security ab Version 3.0.** Nach dem Installieren der Software und dem Aktivieren des integrierten IBM Security Chips können Sie mit dem Administratordienstprogramm von Client Security die Benutzerauthentifizierung konfigurieren und die UVM-Sicherheitspolicy bearbeiten. Ausführliche Anweisungen zur Installation und Verwendung von Client Security finden Sie im *Client Security Installationshandbuch* und im *Client Security Administratorhandbuch*.

Informationen zur Konfiguration von Tivoli Access Manager angeben

Nach dem Installieren von Tivoli Access Manager auf dem lokalen Client können Sie die Informationen zur Konfiguration von Tivoli Access Manager mit dem Administratordienstprogramm, einer Komponente von Client Security, angeben. Die Informationen zur Konfiguration von Tivoli Access Manager umfassen die folgenden Angaben:

- Vollständigen Pfad für die Konfigurationsdatei auswählen
- Aktualisierungsintervall für lokalen Cache auswählen

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

1. Klicken Sie auf **Start > Einstellungen > Systemsteuerung** und anschließend auf den Eintrag für IBM Embedded Security Subsystem.
2. Geben Sie das Administratorkennwort ein, und klicken Sie auf **OK**.

   Wenn Sie das Kennwort eingegeben haben, wird das Hauptfenster des Administratordienstprogramms geöffnet.
3. Klicken Sie auf die Schaltfläche **Anwendungsunterstützung und Policies konfigurieren**.

   Die Anzeige "Konfiguration der UVM-Anwendungen und -Policies" wird angezeigt.
4. Aktivieren Sie das Markierungsfeld **Die Windows-Standardanmeldung durch eine gesicherte UVM-Anmeldung ersetzen**.
5. Klicken Sie auf die Schaltfläche **Anwendungspolicy...**.

6. Wählen Sie im Bereich mit den Informationen zur Konfiguration von Tivoli Access Manager den vollständigen Pfad zur Konfigurationsdatei TAMCSS.conf aus. Beispiel: `C:\TAMCSS\TAMCSS.conf`

   Dieser Bereich ist nur verfügbar, wenn Tivoli Access Manager auf dem Client installiert ist.
7. Klicken Sie auf die Schaltfläche **Policy bearbeiten**.

   Die Anzeige "Administratorkennwort eingeben" wird geöffnet.
8. Geben Sie das Administratorkennwort in das entsprechende Feld ein, und klicken Sie auf **OK**.

   Die Anzeige mit der IBM UVM-Policy wird angezeigt.
9. Wählen Sie im Dropdown-Menü "Aktionen" die Aktionen aus, die über Tivoli Access Manager gesteuert werden sollen.
10. Aktivieren Sie das Markierungsfeld "Access Manager steuert ausgewähltes Objekt".
11. Klicken Sie auf die Schaltfläche **Übernehmen**.

    Die Änderungen werden bei der nächsten Aktualisierung des Caches wirksam. Wenn Sie möchten, dass die Änderungen sofort wirksam werden, klicken Sie auf die Schaltfläche **Lokalen Cache aktualisieren**.

Lokalen Cache definieren und verwenden

Nach Auswahl der Tivoli Access Manager-Konfigurationsdatei kann das Aktualisierungsintervall für den lokalen Cache festgelegt werden. Auf dem IBM Client wird ein lokales Replikat der von Tivoli Access Manager verwalteten Sicherheitspolicy-Informationen verwaltet. Sie können festlegen, dass der lokale Cache automatisch in einem Intervall von Monaten (0 - 12) oder Tagen (0 - 30) aktualisiert wird.

Gehen Sie wie folgt vor, um den lokalen Cache zu definieren oder zu aktualisieren:

1. Klicken Sie auf **Start > Einstellungen > Systemsteuerung** und anschließend auf den Eintrag für IBM Embedded Security Subsystem.
2. Geben Sie das Administratorkennwort ein, und klicken Sie auf **OK**.

   Das Fenster "Administratordienstprogramm" wird angezeigt. Ausführliche Informationen zur Verwendung des Administratordienstprogramms finden Sie im *Client Security Administratorhandbuch*.
3. Klicken Sie im Administratordienstprogramm auf die Schaltfläche **Anwendungsunterstützung und Policies konfigurieren** und anschließend auf die Schaltfläche **Anwendungspolicy**.

   Die Anzeige "Policy-Konfiguration von Client Security ändern" wird angezeigt.
4. Führen Sie eine der folgenden Aktionen aus:
   - Klicken Sie auf **Lokalen Cache aktualisieren**, um den lokalen Cache jetzt zu aktualisieren.
   - Geben Sie den Wert für Monat (0 - 12) und Tag (0 - 30) in die entsprechenden Felder ein, und klicken Sie auf **Lokalen Cache aktualisieren**, um die Häufigkeit automatischer Aktualisierungen anzugeben. Der lokale Cache wird aktualisiert und das Ablaufdatum für Dateien im lokalen Cache wird aktualisiert, damit ersichtlich ist, wann die nächste automatische Aktualisierung durchgeführt wird.

Tivoli Access Manager zur Steuerung von IBM Client-Objekten aktivieren

Die UVM-Policy wird durch eine globale Policy-Datei gesteuert. Die globale Policy-Datei, die sogenannte UVM-Policy-Datei, enthält Authentifizierungsbestimmungen für Aktionen, die auf dem IBM Client-System ausgeführt werden, wie z. B. am System anmelden, Bildschirmschoner aufheben oder E-Mails signieren.

Bearbeiten Sie zunächst mit dem UVM-Policy-Editor die UVM-Policy-Datei, damit Sie den Tivoli Access Manager zur Steuerung der Authentifizierungsobjekte für einen IBM Client verwenden können. Der UVM-Policy-Editor gehört zum Administratordienstprogramm.

Wichtig: Wenn Sie den Tivoli Access Manager zur Steuerung eines Objekts verwenden, wird die Objektsteuerung dem Tivoli Access Manager-Objektbereich übergeben. Wenn das Objekt dann wieder lokal gesteuert werden soll, müssen Sie Client Security erneut installieren.

Lokale UVM-Policy bearbeiten

Bevor Sie versuchen, die UVM-Policy für den lokalen Client zu bearbeiten, muss mindestens ein Benutzer in UVM registriert sein. Ist dies nicht der Fall, wird eine Fehlernachricht angezeigt, wenn der Policy-Editor versucht, die lokale Policy-Datei zu öffnen.

Sie bearbeiten eine lokale UVM-Policy und verwenden sie nur auf dem Client, für den sie bearbeitet wurde. Wurde Client Security im Standardverzeichnis installiert, wird die lokale UVM-Policy mit dem folgenden Verzeichnispfad \Program Files\IBM\Security\UVM_Policy\globalpolicy.gvm gespeichert. Nur ein Benutzer, der zu UVM hinzugefügt wurde, kann den UVM-Policy-Editor verwenden.

Anmerkung: Wird für UVM-Policy angegeben, dass für ein Authentifizierungsobjekt (wie z. B. die Anmeldung am Betriebssystem) ein Fingerabdruck erforderlich ist, müssen Benutzer, die zu UVM hinzugefügt sind, ihren Fingerabdruck registrieren, um dieses Objekt verwenden zu können.

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

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

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

   Die Anzeige ″Administratorkennwort eingeben″ wird geöffnet.
3. Geben Sie das Administratorkennwort in das entsprechende Feld ein, und klicken Sie auf **OK**.

   Die Anzeige mit der IBM UVM-Policy wird angezeigt.

4. Klicken Sie in der Registerkarte ″Objektauswahl″ auf **Aktion** oder **Objekttyp**, und wählen Sie das Objekt aus, dem Authentifizierungsbestimmungen zugeordnet werden sollen.

   Zu den Beispielen für zulässige Aktionen gehören Systemanmeldung, Entsperren des Systems und E-Mail-Entschlüsselung. Ein Beispiel für einen Objekttyp ist ″Digitales Zertifikat anfordern″.
5. Wählen Sie für jedes ausgewählte Objekt **Tivoli Access Manager steuert ausgewähltes Objekt** aus, um den Tivoli Access Manager für das entsprechende Objekt zu aktivieren.

   Wichtig: Wenn Sie den Tivoli Access Manager zur Steuerung eines Objekts verwenden, wird die Objektsteuerung dem Tivoli Access Manager-Objektbereich übergeben. Wenn dieses Objekt zu einem späteren Zeitpunkt wieder lokal gesteuert werden soll, müssen Sie Client Security erneut installieren.

   Anmerkung: Beim Bearbeiten der UVM-Policy können Sie eine Zusammenfassung der Informationen zur Policy aufrufen, indem Sie auf **Policy-Zusammenfassung** klicken.
6. Klicken Sie auf **Übernehmen**, um Ihre Änderungen zu speichern.
7. Klicken Sie auf **OK**, um den Vorgang zu beenden.

UVM-Policy für ferne Clients bearbeiten und verwenden

Damit die UVM-Policy auf mehreren IBM Clients verwendet werden kann, bearbeiten und speichern Sie die UVM-Policy für einen fernen Client. Anschließend kopieren Sie die UVM-Policy-Datei auf andere IBM Clients. Wenn Sie Client Security im Standardverzeichnis installieren, wird die UVM-Policy-Datei im Verzeichnis \Program Files\IBM\Security\UVM_Policy\remote\globalpolicy.gvm gespeichert.

Kopieren Sie die folgenden Dateien auf die anderen fernen IBM Clients, auf denen diese UVM-Policy verwendet werden soll:

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

Wurde Client Security im Standardverzeichnis installiert, ist das Stammverzeichnis der oben genannten Pfade \Program Files. Kopieren Sie die beiden Dateien auf den fernen Clients in den Verzeichnispfad \IBM\Security\UVM_Policy\.

Fehlerbehebungstabellen

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

Fehlerbehebungsinformationen zu digitalen Zertifikaten

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

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

Fehlerbehebungsinformationen zu Tivoli Access Manager

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

Fehlersymptom	Mögliche Lösung
Die lokalen Policy-Einstellungen entsprechen nicht denen auf dem Server.	**Maßnahme**
Tivoli Access Manager lässt bestimmte Bit-Konfigurationen zu, die von UVM nicht unterstützt werden. Folglich können lokale Policy-Anforderungen Einstellungen überschreiben, die ein Administrator bei der Konfiguration des PD-Servers vorgenommen hat.	Diese Einschränkung ist bekannt.

Fehlersymptom	Mögliche Lösung
Ein Zugriff auf die Konfigurationseinstellungen von Tivoli Access Manager ist nicht möglich.	**Maßnahme**
Im Administratordienstprogramm kann auf der Seite zur Policy-Installation weder auf die Konfigurationseinstellungen von Tivoli Access Manager noch auf die entsprechenden Einstellungen zur lokalen Cache-Einrichtung zugegriffen werden.	Installieren Sie Tivoli Access Manager Runtime Environment. Wenn die Laufzeitumgebung (Runtime Environment) auf dem IBM Client nicht installiert ist, sind auf der Seite zur Policy-Installation auch keine Einstellungen für Tivoli Access Manager verfügbar.
Eine Benutzersteuerung gilt sowohl für den Benutzer als auch für die Gruppe.	**Maßnahme**
Wenn Sie beim Konfigurieren des Tivoli Access Manager-Servers einen Benutzer für eine Gruppe definieren, gilt die Benutzersteuerung sowohl für den Benutzer als auch für die Gruppe, wenn die Option **Traverse-bit** aktiviert wurde.	Es ist keine Maßnahme erforderlich.

Fehlerbehebungsinformationen zu Lotus Notes

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

Fehlersymptom	Mögliche Lösung
Nach dem Aktivieren des UVM-Schutzes für Lotus Notes kann die Konfiguration von Lotus Notes nicht abgeschlossen werden.	**Maßnahme**
Lotus Notes kann nach dem Aktivieren des UVM-Schutzes mit dem Administratordienstprogramm die Konfiguration nicht fertig stellen.	Diese Einschränkung ist bekannt. Lotus Notes muss konfiguriert und aktiv sein, bevor die Lotus Notes-Unterstützung im Administratordienstprogramm aktiviert werden kann.
Beim Versuch, das Notes-Kennwort zu ändern, wird eine Fehlernachricht angezeigt.	**Maßnahme**
Wenn Sie während der Verwendung von Client Security das Notes-Kennwort ändern, kann dies zur Anzeige einer Fehlernachricht führen.	Wiederholen Sie die Kennwortänderung. Wurde der Fehler dadurch nicht behoben, starten Sie den Client erneut.

Fehlersymptom	Mögliche Lösung
Nachdem Sie ein Kennwort per Zufallsgenerator festgelegt haben, wird eine Fehlernachricht angezeigt.	**Maßnahme**
Möglicherweise wird eine Fehlernachricht angezeigt, wenn Sie folgende Schritte ausführen: • Über das Tool zur Lotus Notes-Konfiguration UVM-Schutz für eine Notes-ID festlegen • Notes aufrufen und über die entsprechende Notes-Funktion das Kennwort für die Datei mit der Notes-ID ändern • Notes sofort nach dem Ändern des Kennworts schließen	Klicken Sie auf **OK**, um die Fehlernachricht zu schließen. Es ist keine weitere Maßnahme erforderlich. Entgegen der Fehlernachricht wurde das Kennwort geändert. Das neue Kennwort wurde von Client Security per Zufallsgenerator festgelegt. Die Datei mit der Notes-ID wird nun mit dem per Zufallsgenerator festgelegten Kennwort verschlüsselt, und der Benutzer benötigt keine neue Benutzer-ID-Datei. Wenn der Endbenutzer das Kennwort erneut ändert, wird in UVM ein neues, per Zufallsgenerator festgelegtes, Kennwort für die Notes-ID erstellt.

Fehlerbehebungsinformationen zur Verschlüsselung

Die folgenden Informationen zur Fehlerbehebung können hilfreich sein, wenn beim Verschlüsseln von Dateien mit Hilfe von Client Security ab Version 3.0 Fehler auftreten.

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

Kapitel 7. Treiber für Hardwareeinheiten von Fremdanbietern zur Ergänzung von IBM Client Security installieren

Mit Client Security und den Lösungen von Fremdanbietern können Sie Ihre gesamte Infrastruktur schützen, indem Sie zusätzliche Angebote integrieren und somit den Schutzumfang für Ihre Systemumgebung an Ihre Bedürfnisse anpassen können.

IBM Embedded Security Subsystem wurde auf Kompatibilität mit bestimmten Hardwareangeboten zur Sicherheitsauthentifizierung von folgenden Organisationen geprüft:

- Targus für Lesegeräte für Fingerabdrücke
- Gemplus für Smart-Card-Lösungen
- Ensure Technologies für berührungslose Ausweise (Proximity Badges)

Auf der Website http://www.pc.ibm.com/us/security/index.html finden Sie Links zu diesen Organisationen und weitere Informationen zu ihren Angeboten.

Wie bei vielen Komponenten, die Teil eines Plattenimages sind, ist die Installationsreihenfolge von sehr großer Bedeutung. Wenn Sie die oben aufgeführten Authentifizierungsgeräte und die dazugehörigen Treiber sowie andere Software implementieren möchten, muss zuerst IBM Client Security installiert werden. Die Treiber und Software für diese Geräte werden nicht ordnungsgemäß installiert, wenn die Einheitentreiberdateien vor CSS auf der Festplatte installiert werden.

Gezielte und aktuelle Informationen zur Installation der Software und Treiber für die Authentifizierungshardware finden Sie in der Dokumentation zum entsprechenden Gerät.

Kapitel 8. Neue oder überarbeitete Sicherheitspolicy-Dateien über Remotezugriff implementieren

Ob Sie nun Sicherheitspolicies aktualisieren oder verschiedene Policies für unterschiedliche Computer erstellen, als IT-Administrator mit Signierberechtigung können Sie Policy-Dateien überarbeiten und implementieren. Bearbeiten Sie die Policy-Datei mit Hilfe von ACAMUCLI.EXE. (Sie können die Policy auch bearbeiten, indem Sie in der Systemsteuerung doppelt auf das Symbol für IBM Embedded Security Subsystem klicken.)

Signieren Sie die Policy-Datei gemäß den angezeigten Anweisungen, nachdem Sie auf ″Übernehmen″ geklickt haben. (**Anmerkung:** Wenn der private Administratorschlüssel aufgeteilt wurde, müssen alle Komponenten eingegeben werden, um die Policy-Datei zu signieren.) Die von Ihnen bearbeiteten Dateien heißen GLOBALPOLICY.GVM und GLOBPOLICY.GVM.SIG. Geben Sie diese Dateien an die entsprechenden Benutzer weiter. Die Dateien müssen im Ordner ″Security\UVM_Policy″ gespeichert werden.

Sie können Verschlüsselungstextpolicies nach der Implementierung über Remotezugriff aktualisieren. Durch das Aktualisieren der Policy-Datei des Verschlüsselungstexts können Sie die Verschlüsselungstextanforderungen ändern, wenn (oder falls) ein Benutzer seinen Verschlüsselungstext ändert. Der Administrator kann einen Zeitraum festlegen, nach dem der Benutzer den Verschlüsselungstext ändern muss. Dieser Zeitraum wird während der Benutzerregistrierung festgelegt. Beispiel: Der Administrator registriert einen Benutzer, Simone. In der anfänglichen Policy wird festgelegt, dass das Kennwort von Benutzer Simone acht Zeichen umfassen muss und nach 30 Tagen abläuft. Der Administrator kann die Policy-Datei aktualisieren und bestimmen, dass der neue Verschlüsselungstext von Simone bei der nächsten Änderung zwölf Zeichen umfassen muss. Der Administrator kann auch den Ablaufzeitraum ändern. Anstatt den Verschlüsselungstext alle 30 Tage zu ändern, kann der Administrator festlegen, dass er beispielsweise alle 15 Tage geändert werden muss. Was geschieht im folgenden Szenario? Der 10. Tag der ″Lebensdauer″ des 30-tägigen Verschlüsselungstexts ist erreicht. Eine neue Policy-Datei für den Verschlüsselungstext wird an den Client gesendet. Laut dieser muss der Verschlüsselungstext alle 15 Tage geändert werden. Läuft der Verschlüsselungstext nun nach 5 oder nach 20 Tagen ab? Der Verschlüsselungstext läuft, wie in der ursprünglichen Policy angegeben, nach 20 Tagen ab. Die Ablaufpolicy des Verschlüsselungstexts tritt beim Festlegen des Verschlüsselungstexts in Kraft. Die Policy mit der Änderung nach 15 Tagen beginnt, wenn Simone ihren Verschlüsselungstext nach 20 Tagen ändert.

Wenn Sie die Eigenschaften des Verschlüsselungstexts ändern möchten, folgen Sie den oben aufgeführten Anweisungen. Verteilen Sie dann die folgenden Dateien aus dem Ordner SECURITY\UVM_POLICY: UVM_PP_POLICY.DAT und UVM_PP-_POLICY.DAT.SIG.

Anhang. Bemerkungen

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

Für in diesem Dokument 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.

Die in diesem Dokument beschriebenen Produkte sind nicht zur Verwendung bei Implantationen oder anderen lebenserhaltenden Anwendungen, bei denen ein Nichtfunktionieren zu Verletzungen oder zum Tod führen könnte, vorgesehen. IBM Produktspezifikationen oder Gewährleistungen werden durch die in dieser Dokumentation enthaltenen Informationen nicht beeinflusst oder geändert. Keine Passagen dieses Dokuments sollen als explizite oder implizite Lizenz oder Schadensersatzerklärung unter den gewerblichen Schutzrechten der IBM oder anderer Firmen dienen. Alle Informationen in diesem Dokument wurden in bestimmten Umgebungen erfasst und werden zur Veranschaulichung präsentiert. In anderen Betriebsumgebungen werden möglicherweise andere Ergebnisse erfasst.

Werden an IBM Informationen eingesandt, können diese beliebig verwendet werden, ohne dass eine Verpflichtung gegenüber dem Einsender entsteht.

Websites anderer Anbieter

Verweise in diesen Informationen auf Websites anderer Anbieter dienen lediglich als Benutzerinformationen und stellen keinerlei Billigung des Inhalts dieser Websites dar. Das über diese Websites verfügbare Material ist nicht Bestandteil des Materials für dieses IBM Produkt. Die Verwendung dieser Websites geschieht auf eigene Verantwortung.

Marken

Folgende Namen sind in gewissen Ländern Marken der International Business Machines Corporation:

IBM
ThinkPad
ThinkCentre
Tivoli

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

Andere Namen von Unternehmen, Produkten oder Services können Marken oder Servicemarken anderer Unternehmen sein.