IBM Client Security Version 5.30 Implementierungshandbuch

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.

Dritte Ausgabe (August 2004)

Diese Veröffentlichung ist eine Übersetzung des Handbuchs
IBM Client Security Software Version 5.30 Deployment Guide,
herausgegeben von International Business Machines Corporation, USA

Herausgegeben von:
SW TSC Germany
Kst. 2877
August 2004

Vorwort

IT-Administratoren müssen bei der Implementierung von IBM Client Security zahlreiche Faktoren kennen und berücksichtigen. Dieses Handbuch ist nicht dazu vorgesehen, die Verwendung des integrierten IBM Sicherheits-Subsystems, des Chips oder von Client Security zu erläutern; stattdessen wird die Implementierung der Software in Computern des gesamten Unternehmens, die mit dem integrierten IBM Security Chip ausgestattet sind, behandelt.

Zielgruppe

Dieses Handbuch ist für IT-Administratoren vorgesehen oder für Personen, die für die Implementierung von IBM Client Security, Version 5.3 (CSS) auf den Computern in ihrem Unternehmen verantwortlich sind. Dieses Handbuch soll Informationen bereitstellen, die für die Installation von IBM Client Security auf einen oder mehreren Computern erforderlich sind. Von IBM werden auch ein Benutzerhandbuch, ein Client Security Administratorhandbuch und Anwendungshilfen für Client Security zur Verfügung gestellt, in denen Sie Informationen zur Benutzung der Anwendung finden können.

Produktveröffentlichungen

Die folgenden Dokumente sind in der Bibliothek von Client Security, Version 5.3 verfügbar:

- *Client Security Version 5.3 Administratorhandbuch* :

  Enthält Informationen zur Konfiguration und zur Verwendung der Sicherheitsfunktionen von Client Security.

- *Client Security Version 5.3 Benutzerhandbuch*:

  Enthält Informationen zur Ausführung von Aufgaben mit Client Security, wie z. B. zum UVM-Anmeldeschutz, zum Einrichten des Client Security-Bildschirmschoners, zur Erstellung eines digitalen Zertifikats und zur Verwendung des Benutzerkonfigurationsprogramms.

- *Client Security Version 5.3 - Installationshandbuch*:

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

- *Client Security Version 5.3 mit Tivoli Access Manager verwenden*:

  Enthält nützliche Informationen zur Konfiguration von Client Security für die Verwendung mit Tivoli Access Manager.

Zusätzliche Informationen

Zusätzliche Informationen sowie Aktualisierungen für Sicherheitsprodukte können, falls verfügbar, von der IBM Website unter
http://www-132.ibm.com/content/search/security.html
heruntergeladen werden.

Inhaltsverzeichnis

Kapitel 1. Hinweise zur Implementierung von IBM Client Security

Die IBM Client Security-Software (CSS), die auf der im IBM Personal Computer integrierten Hardware "IBM Embedded Security Subsystem" (ESS) ausgeführt wird, 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

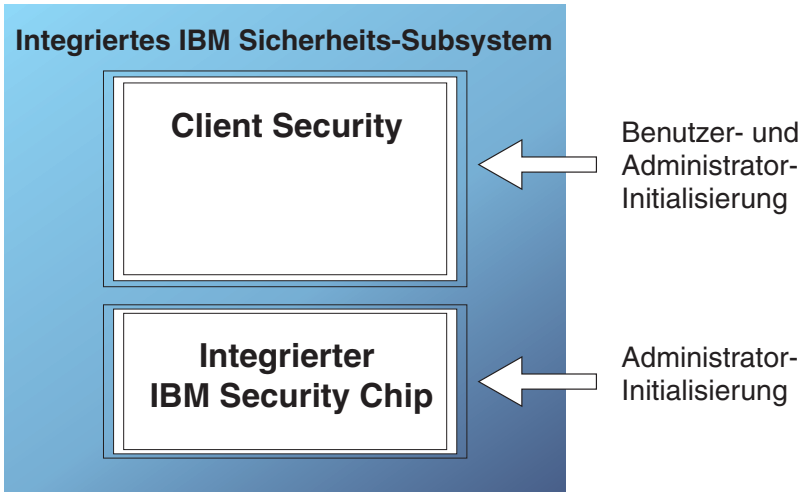

Abbildung 1. Komponenten des IBM Client Security-Systems

Voraussetzungen und Spezifikationen für die Implementierung

Wenn Sie IBM Client Security auf Computern installieren möchten, die mit dem integrierten IBM Security Chip ausgerüstet sind, müssen Sie die Voraussetzungen und Installationszeiten für Serverspeicher und Download planen:

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

Kapitel 2. Funktionen 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

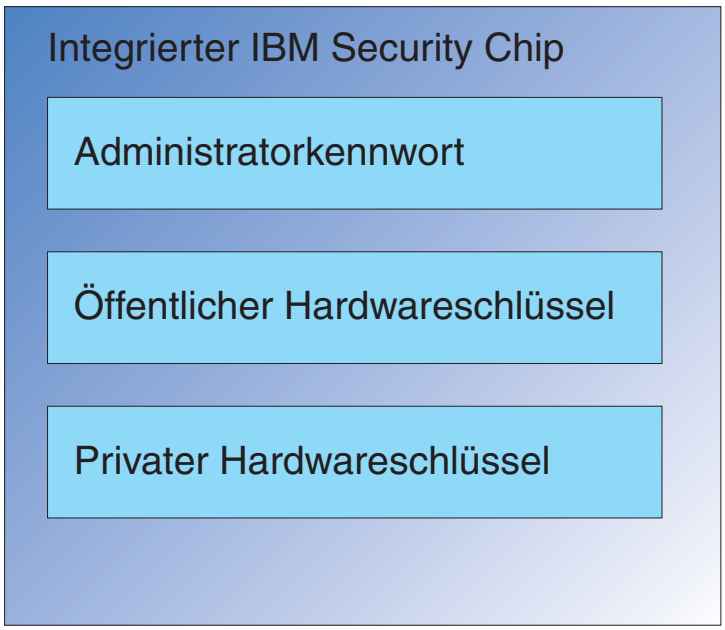

Abbildung 2. Im integrierten IBM Security Chip enthaltene Daten

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

- Über den Assistenten von 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 eingerichtet. Das Verfahren und der Zeitpunkt des Einrichtens des Administratorkennworts werden später in diesem Dokument ausführlich behandelt.

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

Die anderen Komponenten des integrierten IBM Security Chips bestehen aus dem öffentlichen und dem 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 5 werden zwei weitere Komponenten des integrierten IBM Security Chips beschrieben. Die Funktionsweise dieser zwei Komponenten zu kennen, ist für eine effektive Verwaltung der Infrastruktur des integrierten IBM Sicherheits-Subsystems von entscheidender Bedeutung. In Abb. 3 auf Seite 5 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:

- Öffentliche und private Schlüssel werden als "Schlüsselpaar" bezeichnet.
- Die privaten und öffentlichen Schlüssel stehen wie folgt in einer mathematischen Beziehung:
  - 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.

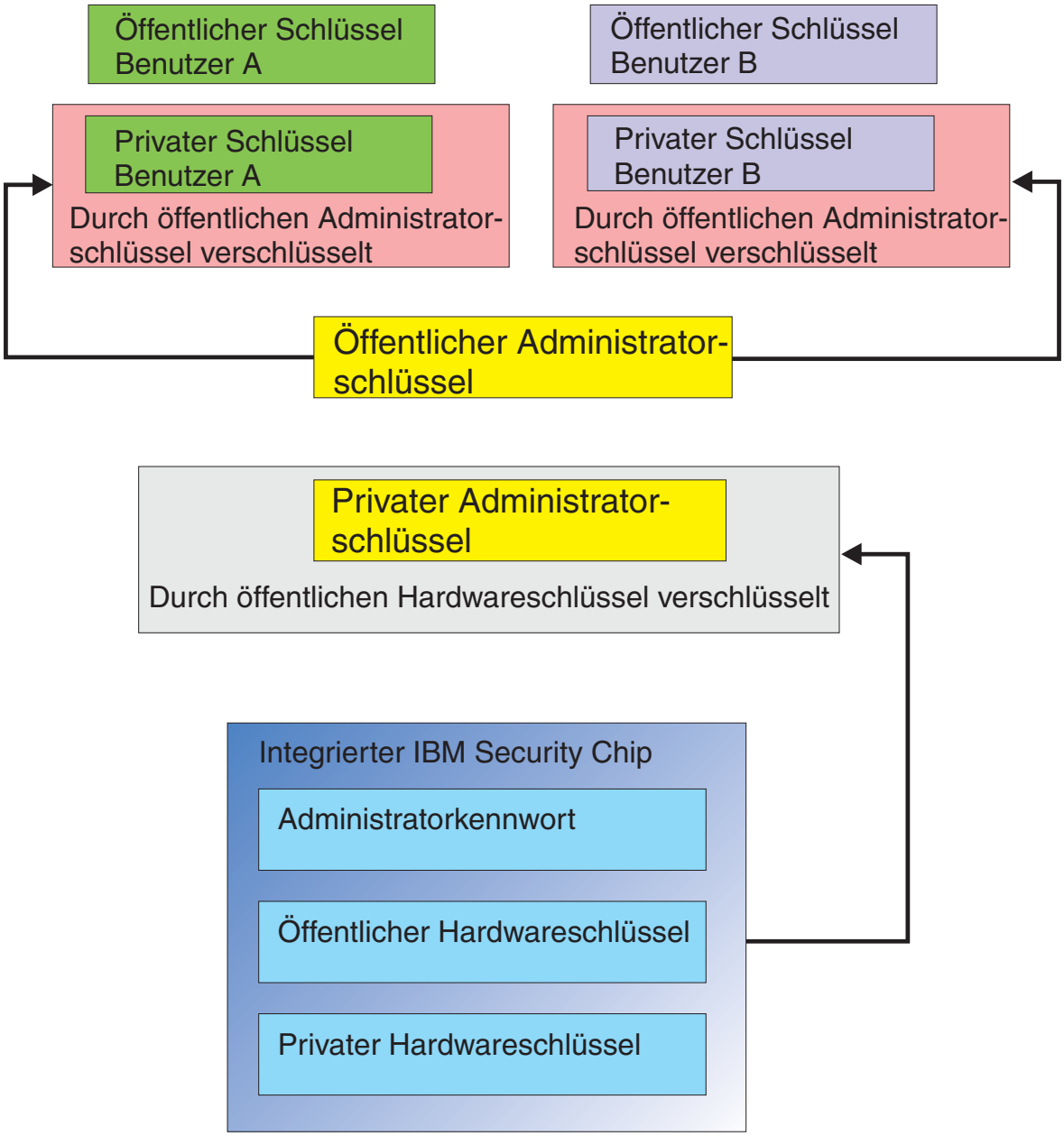

Abbildung 3. Mehrere Verschlüsselungsebenen bieten große Sicherheit

Schlüsselauslagerungshierarchie

Teil der IBM ESS-Architektur ist eine Schlüsselauslagerungshierarchie. Ihre Funktionen werden ausführlich im *Administratorhandbuch* behandelt. Wir möchten hier jedoch etwas darauf eingehen, da dieses Konzept in der Massenkonfiguration, Implementierung und Verwaltung Anwendung findet. In Abbildung 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 sind das öffentliche und das private Administratorschlüsselpaar abgebildet. Das öffentliche und das private Administratorschlüsselpaar können auf allen Computern eindeutig oder für alle Clients bzw. für ein Subset von Clients gleich sein. Die Vor- und Nachteile werden später in diesem Dokument behandelt. Das öffentliche und das private Administratorschlüsselpaar ermöglichen Folgendes:

- Schutz der öffentlichen und privaten Benutzerschlüssel
- Archivierung und Wiederherstellung der Benutzerberechtigungen
- Standortunabhängiger Zugriff auf die Benutzerberechtigungen. Dies wird im *Administratorhandbuch* 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 5 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 an Schlüsseln enthalten sein. Die öffentlichen und privaten Hardwareschlüssel sind die einzigen Schlüssel in diesem Szenario, die ständig (bei jedem Booten) im Chip enthalten sind. Damit mehrere Schlüssel und mehrere Benutzer aktiviert werden können, wird im 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 Hardwareschlüssel 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 der private 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 5 ist ersichtlich, dass mehrere private Benutzerschlüssel mit dem öffentlichen Administratorschlüssel verschlüsselt werden können. Dadurch können alle erforderlichen Benutzer auf einem Computer mit IBM ESS konfiguriert werden.

Kapitel 3. Wichtige Hinweise zur Archivierung

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 Client Security dargestellt. Das Dialogfeld zur Anmeldung in Windows fordert Benutzer A zur Anmeldung auf, und Benutzer A meldet sich an. Das IBM Client Security-System ermittelt durch die vom Betriebssystem bereitgestellten Informationen, wer der aktuelle Benutzer ist. Der private Administratorschlüssel, der mit dem öffentlichen Hardwareschlüssel verschlüsselt ist, wird in den integrierten IBM Security Chip geladen.

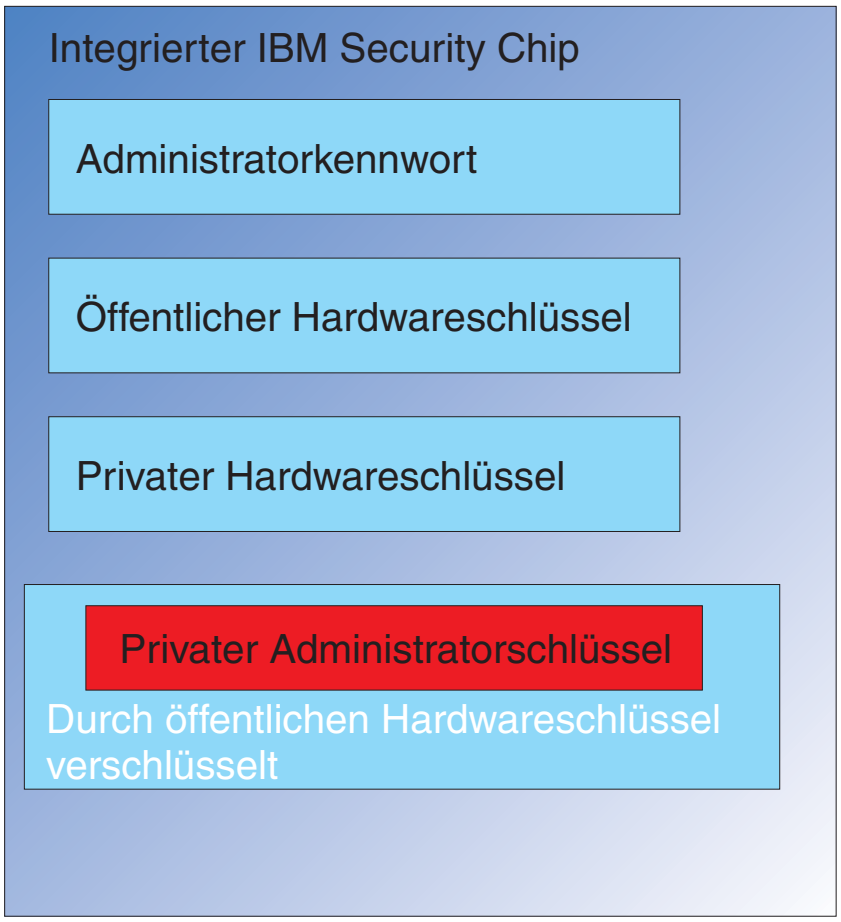

Abbildung 4. Der private Administratorschlüssel, der mit dem öffentlichen Hardwareschlüssel verschlüsselt ist, wird in den integrierten IBM Security Chip geladen.

In Abb. 5 wird das Entschlüsseln des privaten Administratorschlüssels durch den privaten Hardwareschlüssel (der nur im Chip verfügbar ist) dargestellt. Nun kann der private Administratorschlüssel im Chip verwendet werden.

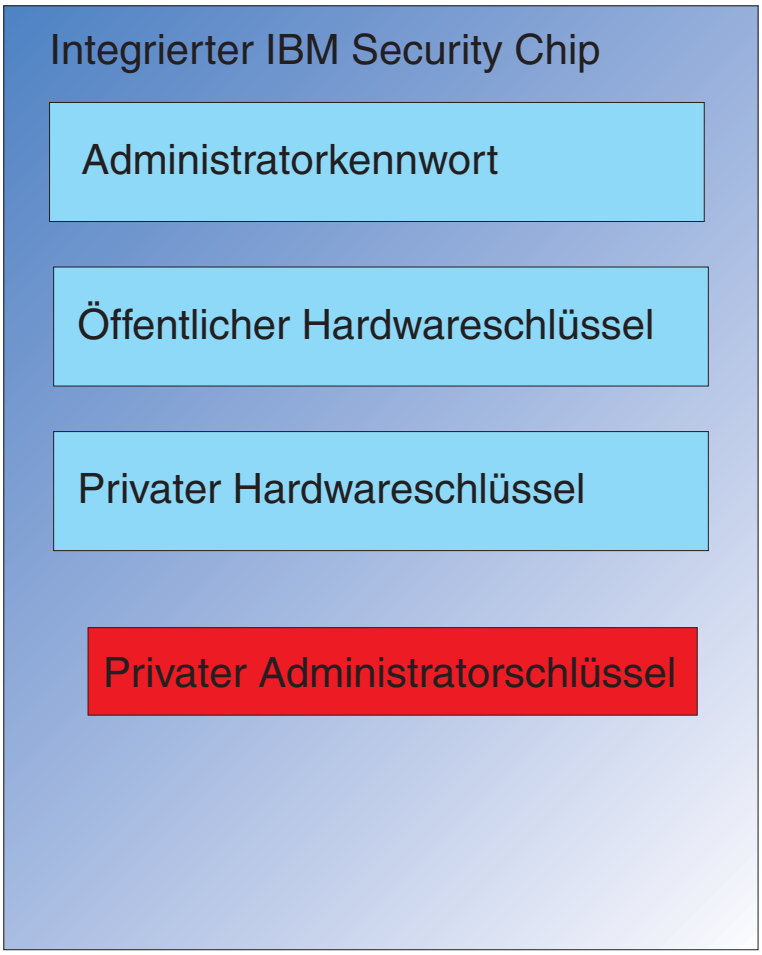

Abbildung 5. Der private Administratorschlüssel ist zur Nutzung im Security Chip verfügbar.

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

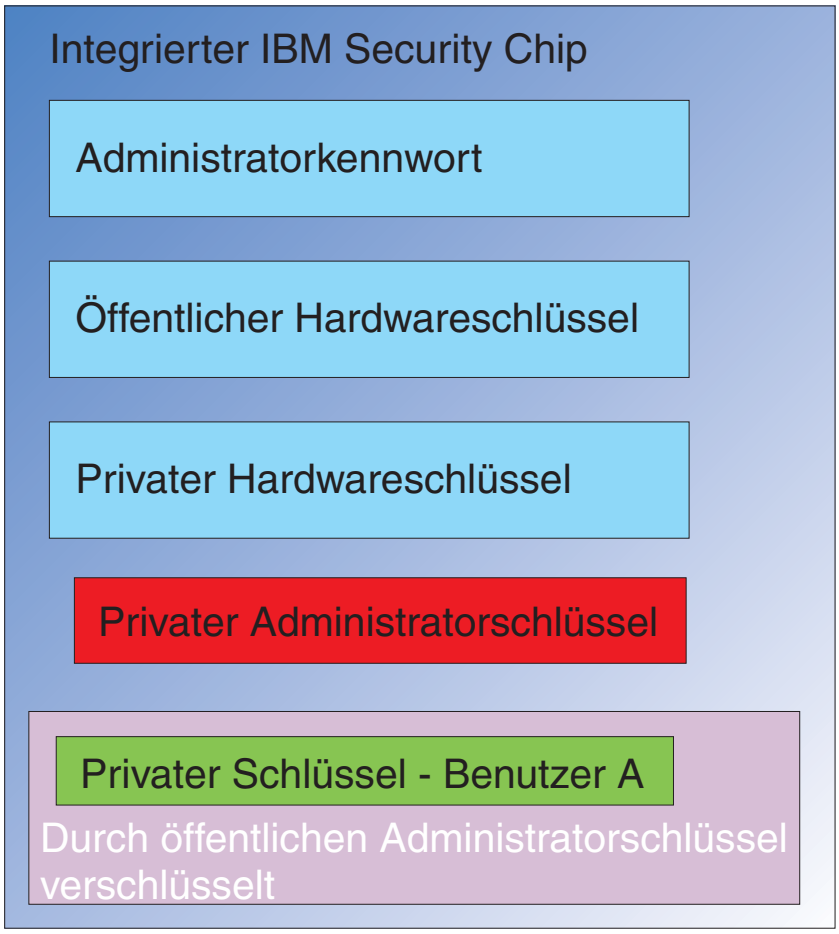

Abbildung 6. Der private Schlüssel von Benutzer A, der mit dem öffentlichen Administratorschlüssel verschlüsselt ist, wird an den Security Chip übergeben.

Mit Hilfe des privaten Administratorschlüssels wird der private Schlüssel von Benutzer A entschlüsselt. Nun ist der private Schlüssel von Benutzer A, wie in Abb. 7 dargestellt, zur Verwendung bereit.

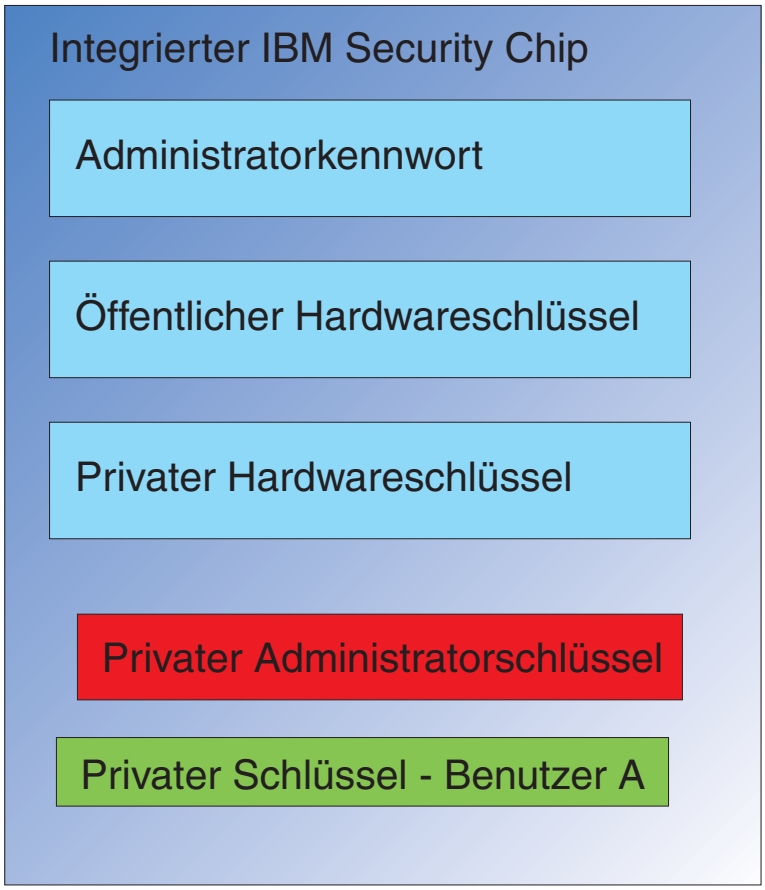

Abbildung 7. Der private Schlüssel von Benutzer A ist zur Verwendung bereit.

Mit dem öffentlichen Schlüssel von Benutzer A können eine Reihe weiterer 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 zur Verfügung und kann die gewünschte Operation ausführen, 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 am Computer anmeldet.

Warum ist ein Administratorschlüsselpaar erforderlich?

Der Hauptgrund für ein Administratorschlüsselpaar liegt in der Archivierung und Wiederherstellung. Das Administratorschlüsselpaar dient als eine abstrakte Ebene zwischen dem Chip und den Benutzerberechtigungen. Die benutzerspezifischen privaten Schlüsselinformationen werden, wie in Abb. 8 dargestellt, mit dem öffentlichen Administratorschlüssel verschlüsselt.

Wichtig: Entwickeln Sie eine Strategie zur Verwaltung der Administratorschlüsselpaare. 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 und jedem Gebäude können jedoch auch unterschiedliche Administratorschlüsselpaare zugewiesen werden.

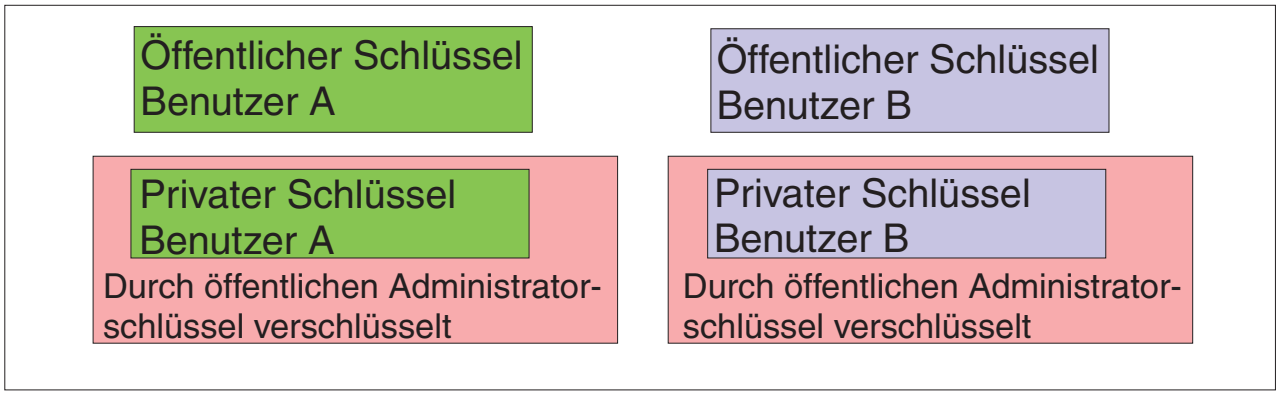

Abbildung 8. Die benutzerspezifischen privaten Schlüsselinformationen werden mit dem öffentlichen Administratorschlüssel verschlüsselt.

Ein weiterer Grund für ein Administratorschlüsselpaar 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 einziger Benutzer Administratorfunktionen ausführt. Weitere Informationen zum Aufteilen des privaten Administratorschlüssels finden Sie in Tabelle 4 auf Seite 39 unter der Einstellung ″keysplit=1″.

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

Diese benutzerspezifischen Informationen werden, wie in Abb. 8 auf Seite 11 dargestellt, an einer durch den Administrator definierten Archivposition gesichert. 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 des IBM Client Security-Systems werden die bewährten Verfahren für die Archivposition erläutert.

Der öffentliche und der private Administratorschlüssel werden nicht archiviert. Die Benutzerdaten in der Archivposition werden mit dem öffentlichen Administratorschlüssel verschlüsselt. Die archivierten Benutzerdaten nützen Ihnen nichts, wenn Sie nicht über den privaten Administratorschlüssel verfügen, um sie zu entschlüsseln. Der öffentliche und der private Administratorschlüssel werden in der Dokumentation von 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.

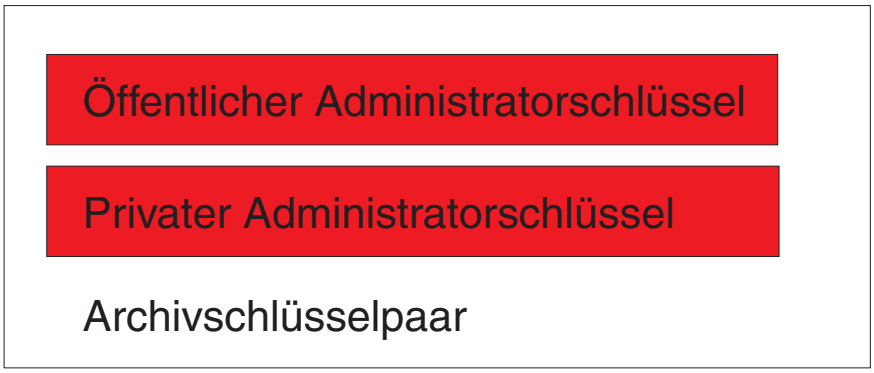

Abbildung 9. Das Archivschlüsselpaar setzt sich aus dem öffentlichen und dem privaten Administratorschlüssel zusammen.

Wie bereits erwähnt, liegt eine der wichtigsten Funktionen der öffentlichen und privaten Administratorschlüssel in der Sicherung und Wiederherstellung der Inhalte eines Datenträgers. 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 war Client A von einem Blitzeinschlag betroffen. Dies ist in Abb. 10 auf Seite 13 dargestellt.

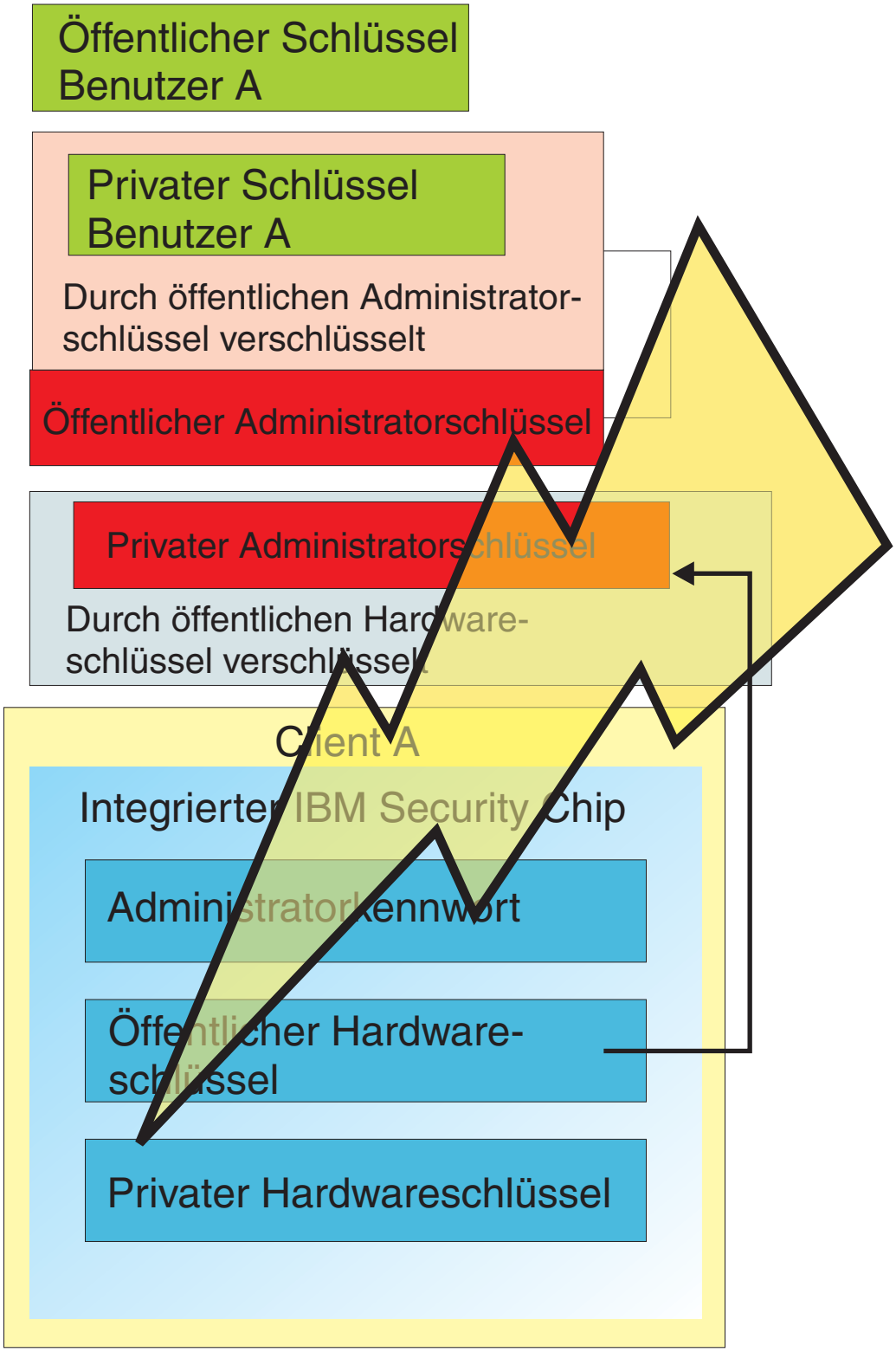

Abbildung 10. Der Computer von Benutzer A ist aufgrund eines Blitzeinschlags nicht mehr funktionsfähig.

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

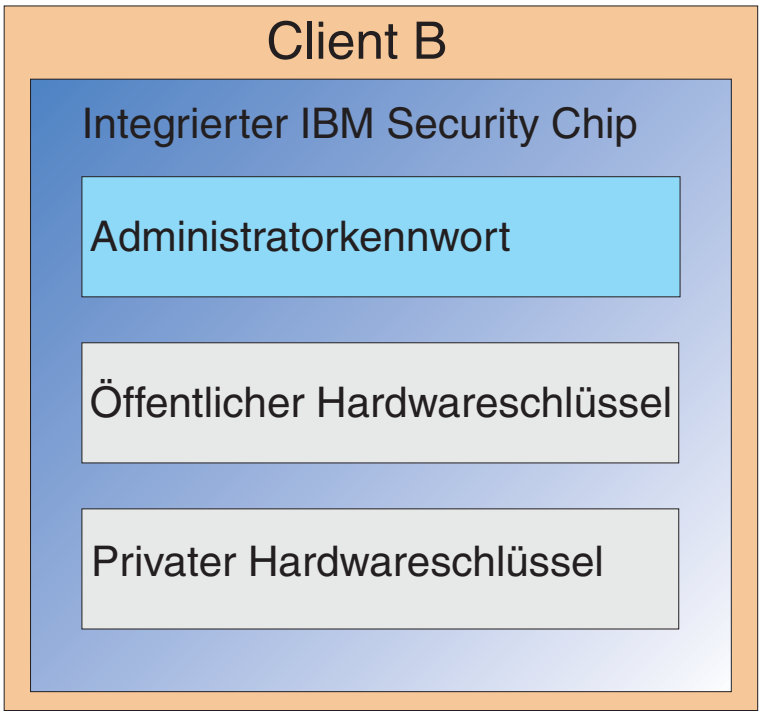

Abbildung 11. Benutzer A erhält einen neuen Computer, Client B, mit einem neuen integrierten Security Chip.

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 11 ansehen, werden Sie sich daran erinnern, dass die Benutzerschlüssel mit dem öffentlichen Administratorschlüssel verschlüsselt wurden und in der Archivposition gespeichert sind. Damit die Benutzerberechtigungen nun auf Client B verfügbar sind, 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.

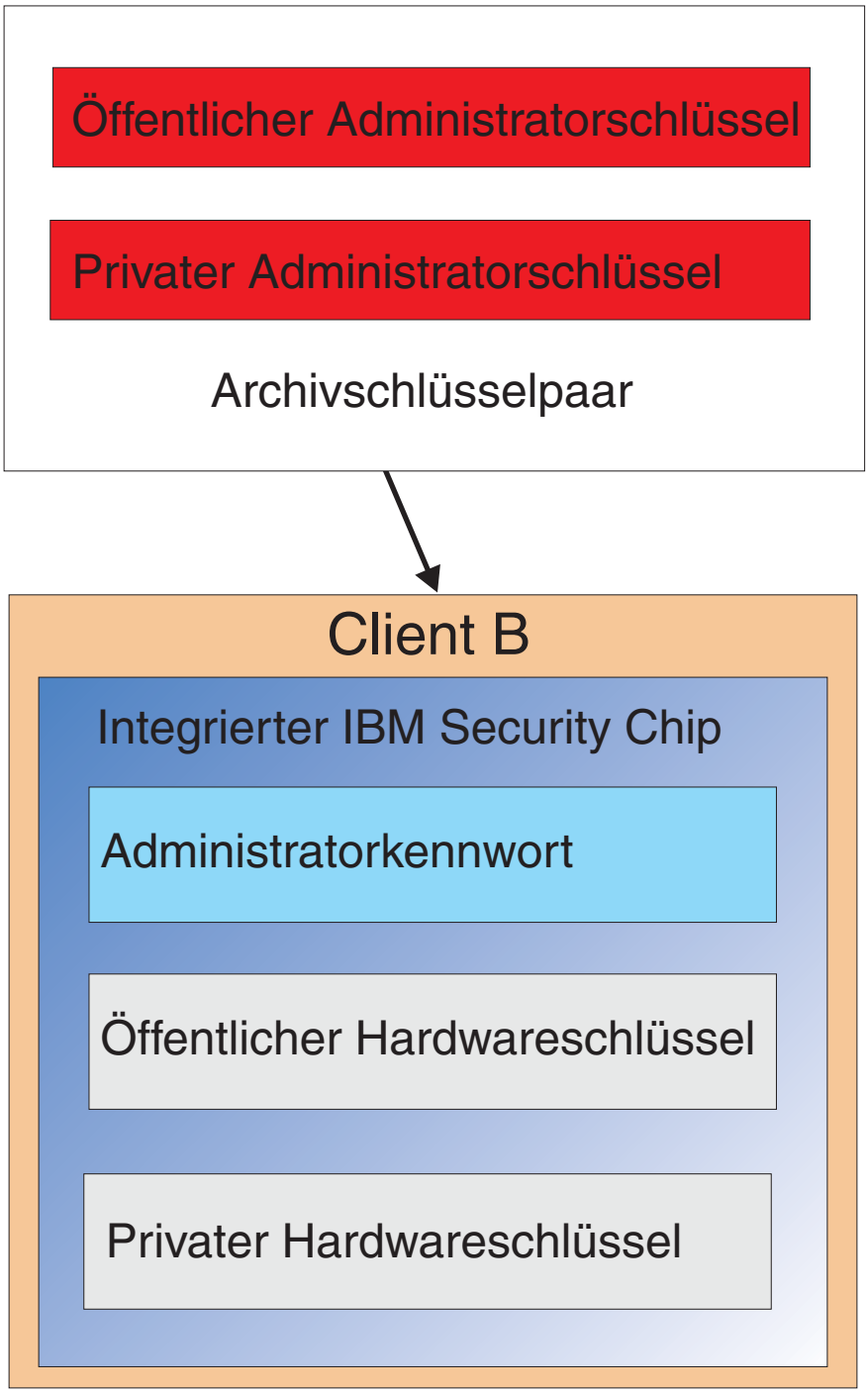

Abbildung 12. Client B ruft den öffentlichen und den privaten Administratorschlüssel aus der Archivposition ab.

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

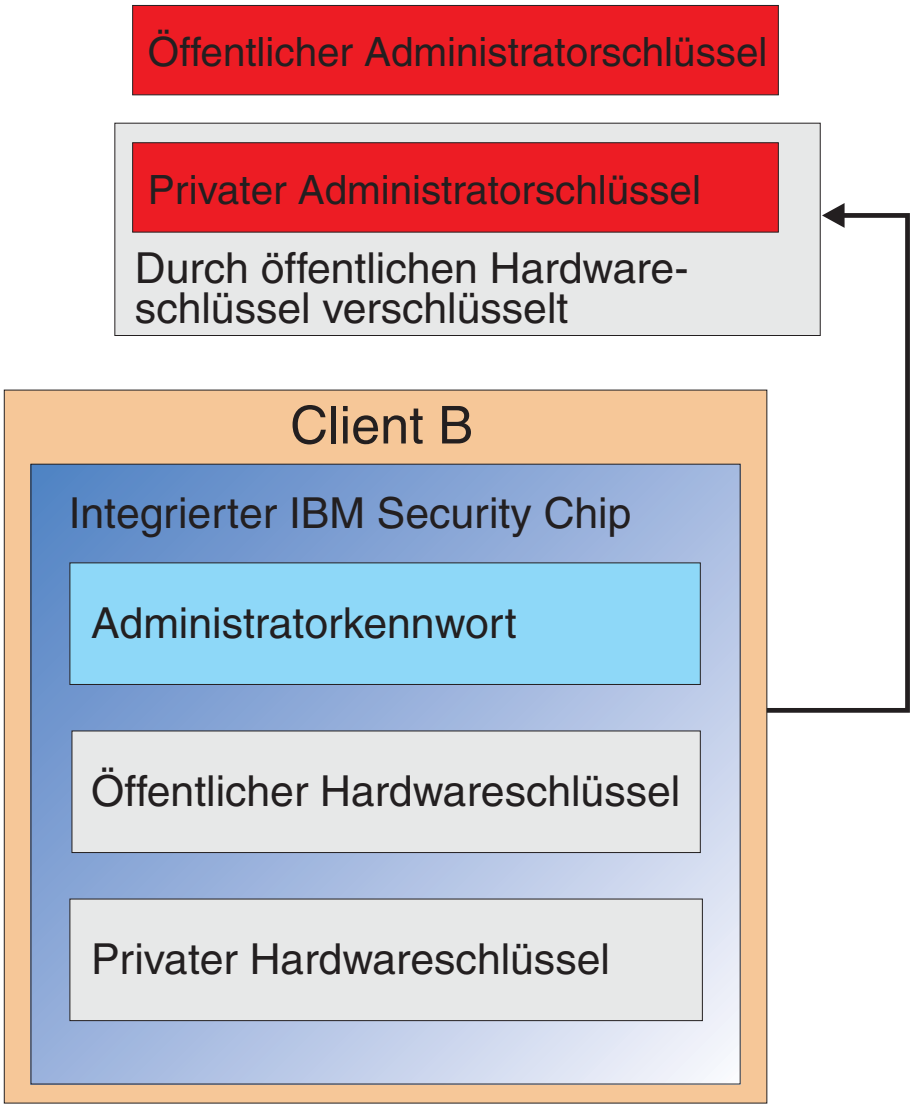

Abbildung 13. Der private Administratorschlüssel wird mit dem Hardwareschlüssel von Client B verschlüsselt.

   schlüssel verschlüsselt ist, können die Benutzerberechtigungen für Benutzer A auf Client B geladen werden. Dies ist in Abb. 14 auf Seite 17 dargestellt.

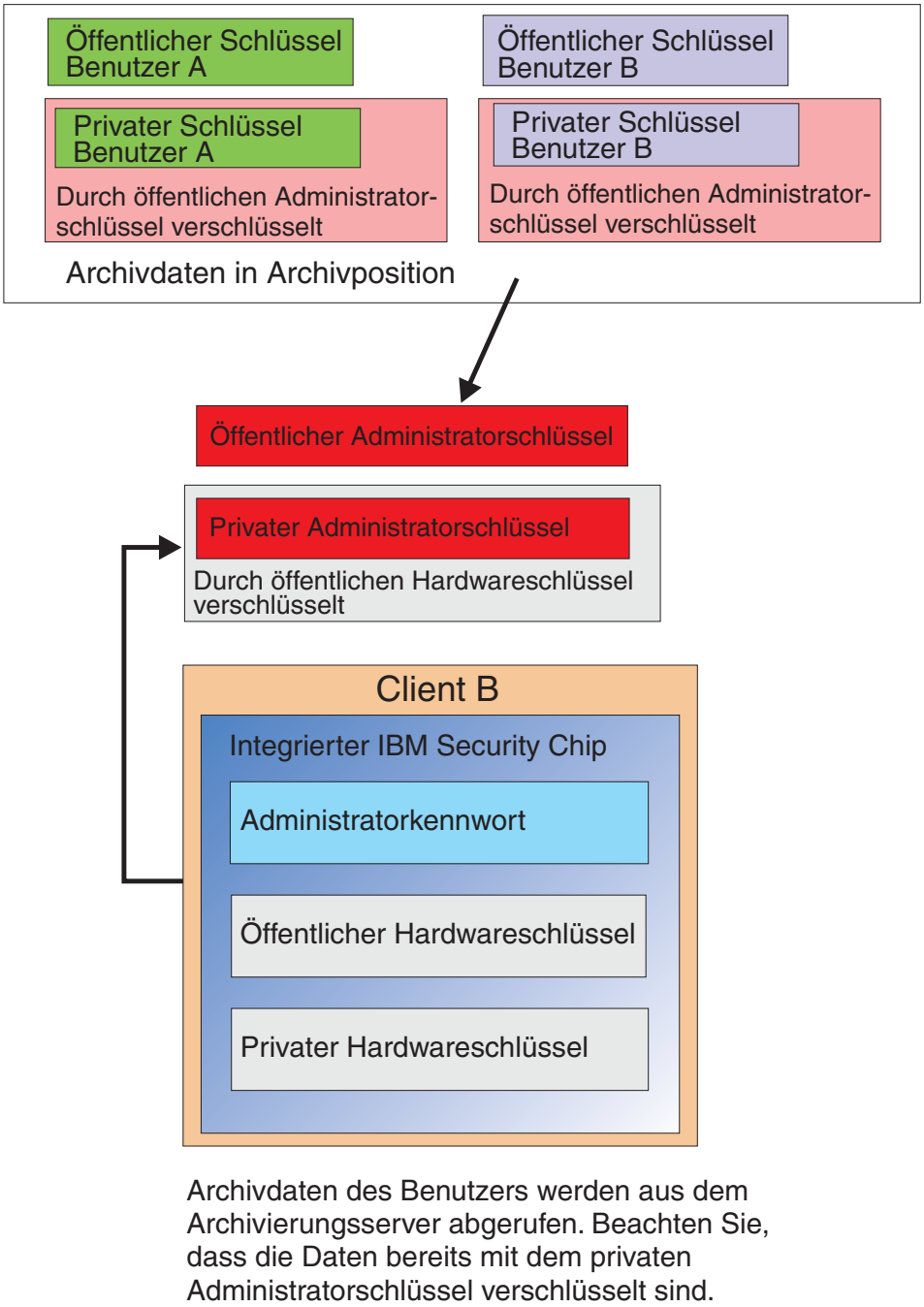

Abbildung 14. Der Berechtigungsnachweis von Benutzer A kann nach der Verschlüsselung des privaten Administratorschlüssels in Client B geladen werden.

In Abb. 15 wird angezeigt, dass Benutzer A wieder vollständig auf Client B hergestellt wurde. 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, diesen Schlüssel zu entschlüsseln. Dies bedeutet, dass die Archivposition nicht unbedingt geschützt sein oder über eine strenge Zugriffskontrolle verfügen muss. Solange das Archivschlüsselpaar (der öffentliche und der private Administratorschlüssel), insbesondere der private Administratorschlüssel, sicher aufbewahrt werden, kann sich die Archivposition für die Berechtigungsnachweise der Benutzer an einem beliebigen Speicherort befinden.

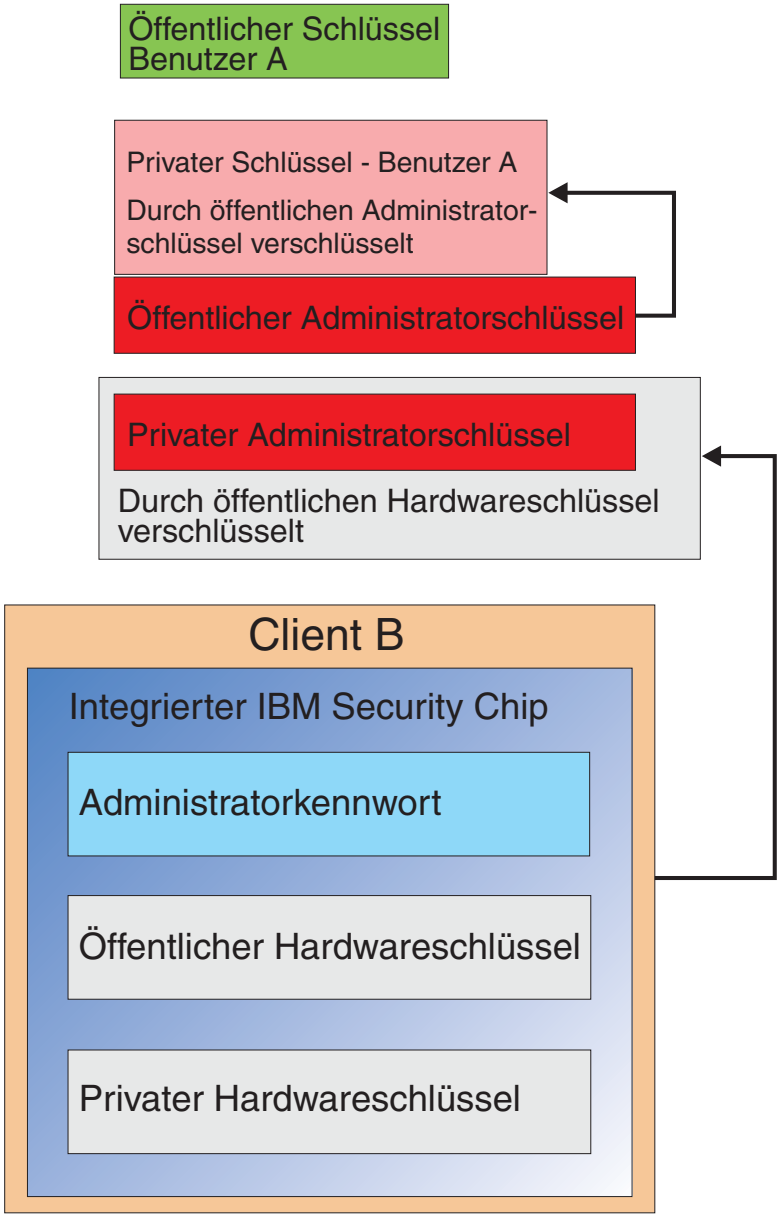

Abbildung 15. Benutzer A ist wieder vollständig auf Client B hergestellt.

Die Einzelheiten zum Einrichten des Administratorkennworts, zu empfehlenswerten Archivpositionen usw. werden im Abschnitt zur Softwareinstallation ausführlicher behandelt. In Abbildung 16 wird eine Übersicht über die Komponenten in einer ESS-Umgebung geboten. Der entscheidende Punkt dabei ist, dass alle Clients zwar einen eindeutigen öffentlichen und privaten Hardwareschlüssel aufweisen, sie jedoch über einen gemeinsamen öffentlichen und privaten Administratorschlüssel verfügen. Die Clients verfügen zwar über eine gemeinsame Archivposition, doch diese Archivposition kann für ein Segment oder eine Benutzergruppe gelten.

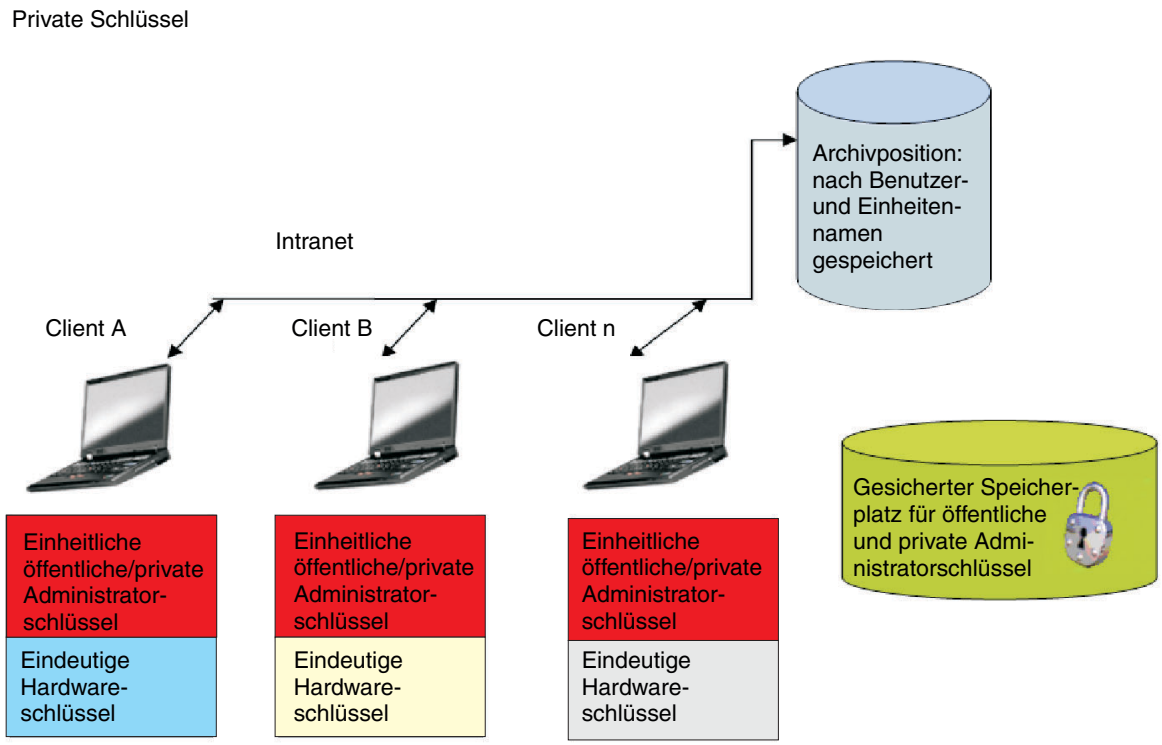

Abbildung 16. Hauptkomponenten des IBM Client Security-Systems.

Nehmen wir folgendes Beispiel an: Die Personalabteilung verfügt über eine separate Archivposition zu der der 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 sicheren Speicherort für den öffentlichen und den privaten Administratorschlüssel.

Anmerkung: Jeder Computer- und Benutzername, der in der gleichen Archivposition archiviert werden soll, muss eindeutig sein. Durch einen doppelten Computer- oder Benutzernamen wird der vorherige Archiveintrag des gleichen Namens überschrieben.

Kapitel 4. IBM Client Security

IBM Client Security stellt die Verbindung zwischen Anwendungen und dem integrierten IBM Security Chip sowie die Schnittstelle zum Registrieren von Benutzern, Implementieren 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 konfigurieren
- Policy für Verschlüsselungstext konfigurieren
- Vergessenen Verschlüsselungstext zurücksetzen
- Benutzerberechtigungen wiederherstellen

Wenn Benutzer A sich beispielsweise beim Betriebssystem anmeldet, basiert IBM Client Security alle Entscheidungen auf die 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 das integrierte IBM Sicherheits-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 Fingerabdruck für die Authentifizierung bereitstellen kann, untersagt IBM ESS dem Benutzer das Ausführen der Aktionsanforderung.

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 ausführlich 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) Verschlüsselungstext 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 konfiguriert und wie er verwendet wird.

Einen Verschlüsselungstext erfordern

Einfach ausgedrückt ist ein Verschlüsselungstext für Sicherheitszwecke erforderlich. Eine Hardwarekomponente wie das integrierte IBM Sicherheits-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. Nehmen wir beispielsweise an, dass Sie über einen Hardware-Chip verfügen, der Sicherheitsfunktionen ausführt. Die erforderliche Authentifizierung zum Aufrufen einer Aktion besteht jedoch aus einer einzigen Ziffer. Dadurch braucht ein potenzieller Hacker nur eine einzige Zahl (von 0 bis 9) zu raten, 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 u. U. 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 konfigurieren

Jeder Benutzer wählt einen Verschlüsselungstext aus, um seinen Berechtigungsnachweis zu schützen. In Kapitel 2, „Funktionen des integrierten IBM Security Chips", auf Seite 3 ist ersichtlich, dass der private Schlüssel eines Benutzers 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.

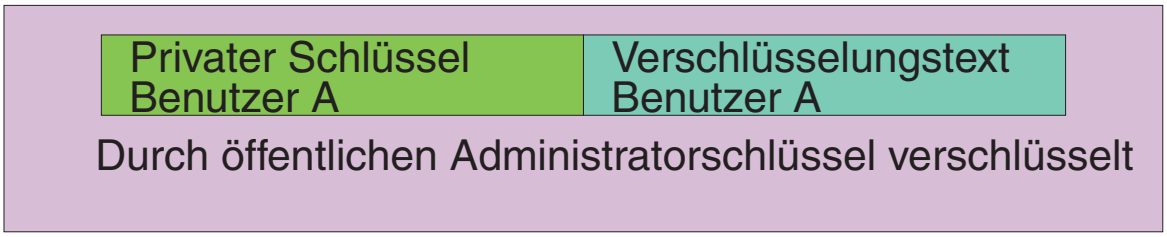

Abbildung 17. Benutzer A muss den Verschlüsselungstext angeben, um Funktionen ausführen zu können, für die der private Schlüssel von Benutzer A erforderlich ist.

Der in Abb. 17 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. Wie dies vor sich geht, wenn IBM Client Security eingeführt wird, wird später in diesem Dokument behandelt.

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 konfigurieren.

Einen Verschlüsselungstext verwenden

In Abb. 18 bis Abb. 20 auf Seite 26 ist dargestellt, wie der Verschlüsselungstext des Benutzers im Chip verarbeitet wird. Ein Verschlüsselungstext muss immer als Erstes und mindestens einmal 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. Zugriff auf den privaten Schlüssel ist erforderlich, um diese zusätzlichen Sicherheitsdaten zu entschlüsseln.

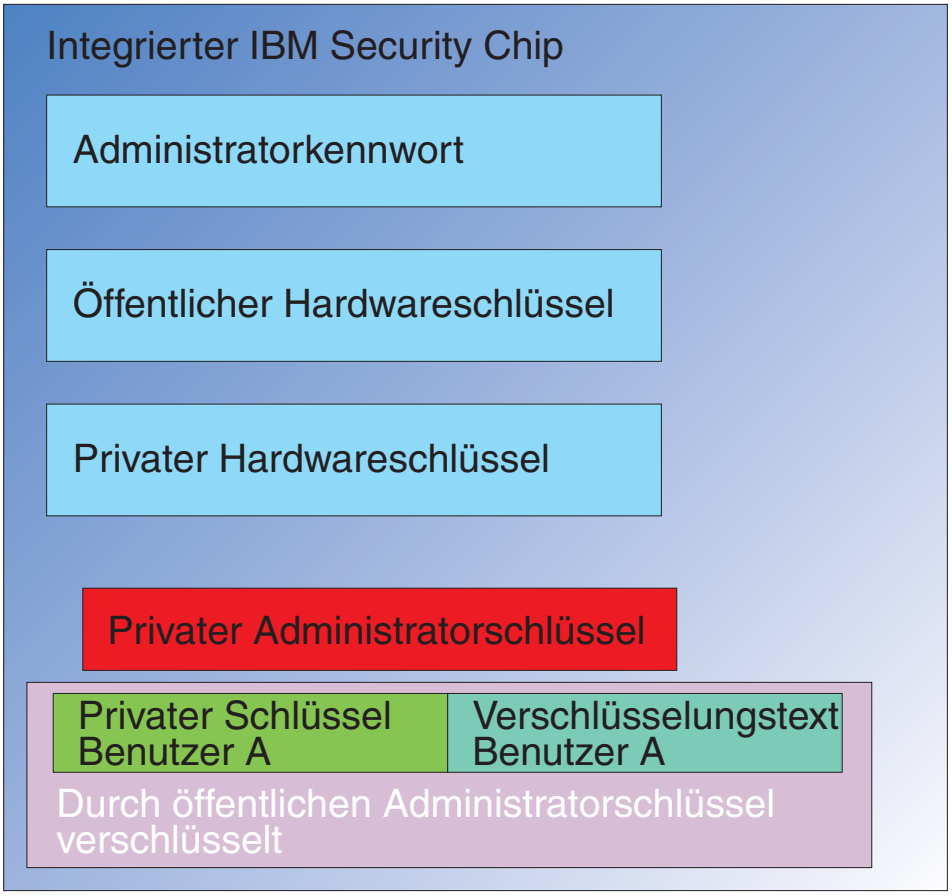

Abbildung 18. Der private Administratorschlüssel wird im Chip entschlüsselt.

Daher muss der Verschlüsselungstext mindestens einmal 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 ist, wie zuvor beschrieben, bereits im Chip entschlüsselt. Der Berechtigungsnachweis wird, wie in Abb. 19 beschrieben, übergeben.

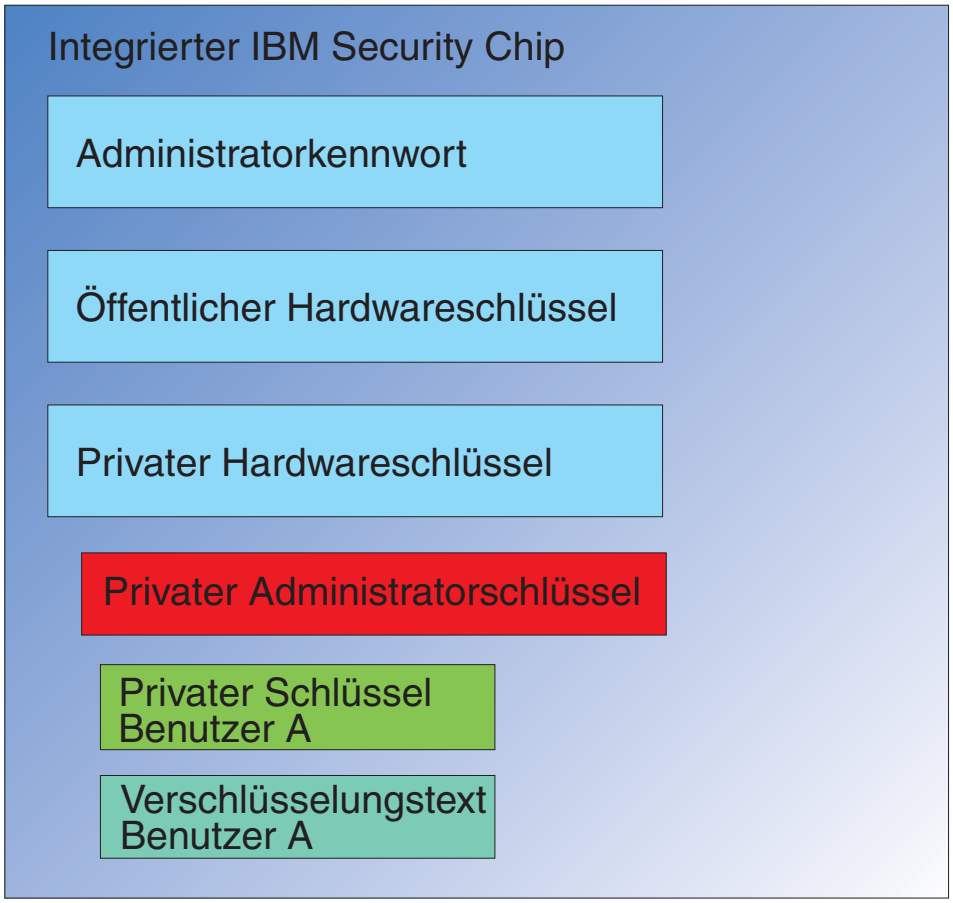

Abbildung 19. Der private Schlüssel sowie der Verschlüsselungstext von Benutzer A sind im Chip verfügbar.

Der Berechtigungsnachweis wird entschlüsselt, und somit wird 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 geöffnet, wie in Abb. 20 dargestellt.

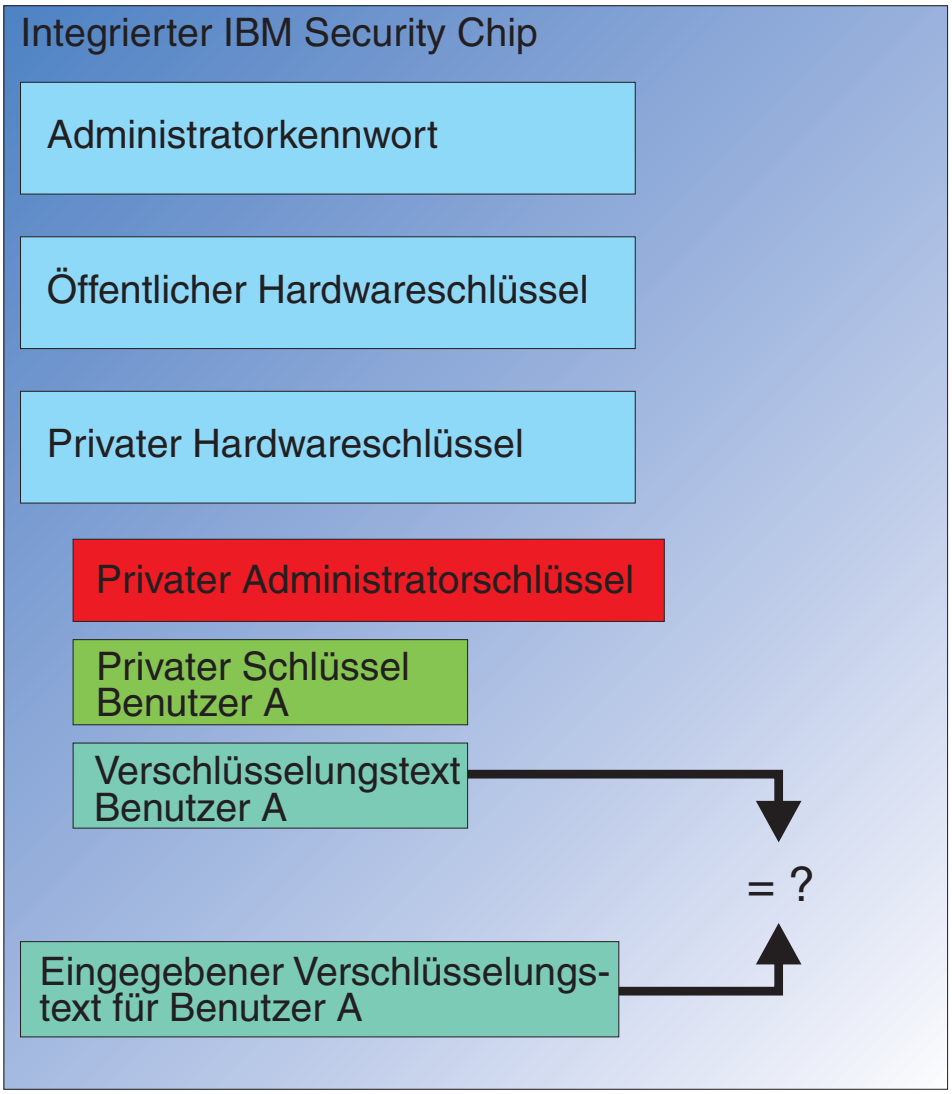

Abbildung 20. Wenn Benutzer A den Berechtigungsnachweis von Benutzer A verwenden möchte, wird ein Dialog zum Verschlüsselungstext geöffnet.

Der eingegebene Verschlüsselungstext wird an den Chip übermittelt und mit dem verschlüsselten 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 bloßgelegt wird. Teil der Installation von IBM Client Security ist die Registrierung von Benutzern. Und Teil dieser Registrierung wiederum ist die Erstellung des Verschlüsselungstexts der Benutzer. In dieser Veröffentlichung wird detailliert beschrieben, wie dieser Verschlüsselungstext konfiguriert 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 dem integrierten IBM Sicherheits-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 der öffentlichen und privaten Hardwareschlüssel sowie eines Administratorkennworts. Mit diesem Prozess wird ein von IBM ausgelieferter generischer Computer eindeutig für Ihr Unternehmen konfiguriert. In der folgenden Abbildung werden die Methoden für die Initialisierung der öffentlichen und privaten Schlüssel sowie des Administratorkennworts dargestellt.

Tabelle 1. Methoden zur Hardwareinitialisierung

Maßnahme	**kann im BIOS erstellt werden**	**kann vom Administrator manuell in CSS erstellt werden**	**kann in einem Script erstellt werden**
Erstellung der öffentlichen und privaten Hardwareschlüssel	Nein	Ja	Ja
Erstellung des Administratorkennworts	Ja, auf einigen mit TCPA kompatiblen Clients. Prüfen Sie den BIOS-Eintrag.	Ja	Ja

In Tabelle 1 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 eingeleitet 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 öffentliche und private Schlüsselpaare 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 an? Wenn ja, wie treffen Sie die logische Entscheidung, welcher Computer über welches Kennwort verfügt?
- Welcher Administrator verfügt über Zugriff auf das Kennwort? Wer verfügt über den 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 zu den Administratordienstprogrammen
- Hinzufügen/Entfernen von Benutzern
- Festlegen, welche Anwendung bzw. Funktionen von IBM Client Security verwendet werden können

In den folgenden Abschnitten wird die Beziehung 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 2 sind die Funktionen des Administratorkennworts und/oder des privaten Administratorschlüssels zusammengefasst.

Tabelle 2. Administratoraktionen mit Kennwort und privatem Schlüssel

Aktion	**Administratorkennwort**	**privater Administrator-schlüssel**
Zugriff auf das Administratordienst-programm	Ja	Nein
Hinzufügen/Entfernen /Wiederherstellen von Benutzern	Ja	Nein
Festlegen, welche CSS-Anwendung/-funktionen verwendet werden können	Ja	Nein
Festlegen/Ändern der Policy	Ja	Ja
Erstellen der Datei zum Zurücksetzen des Verschlüsselungstexts des 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 konfigurieren möchten. Dieses Schlüsselpaar kann auf jedem Computer eindeutig oder auf allen Maschinen dasselbe sein. Wenn IBM Client Security initialisiert wird, hat der Administrator die Möglichkeit, ein vorhandenes Schlüsselpaar zu verwenden oder ein neues Schlüsselpaar auf dem Client zu erstellen. Wie bereits erwähnt, 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 konfigurieren, einen anderen für die Entwicklungsabteilung usw. Sie können Ihre Entscheidung auch auf physischer Basis, wie z. B. nach Gebäude oder Standort, treffen. Wenn Sie eine Datei zum Zurücksetzen des Verschlüsselungstexts erstellen, sollte aufgrund dessen, wer das Zurücksetzen anfordert, die Wahl des privaten Administratorschlüssels relativ einfach sein. Wie in Tabelle 1 auf Seite 27 und Tabelle 3 auf Seite 32 angedeutet, muss auch die Initialisierung von Benutzer 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 Client-Computern "durchsetzen" (siehe Kapitel 7, „Neue oder überarbeitete Sicherheitspolicy-Dateien über Remotezugriff implementieren", auf Seite 57), 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".

Sich auf vergessene Verschlüsselungstexte oder fehlerhafte Authentifizierungsgeräte vorbereiten

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 der Benutzer 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 den entschlüsselten 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 hier klicken** 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 Aufgaben ausführen.

Wenn Sie CSS so konfigurieren möchten, dass die Schaltfläche zum Umgehen angezeigt wird, gehen Sie wie folgt vor:

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, ist es erforderlich, dass die Archivposition in der Datei CSEC.INI mit `kal=c:\jgk\archive` angegeben wird. Des Weiteren muss das Laufwerk, wenn es sich bei c:\jgk\archive um ein Netzlaufwerk handelt, dem Client-Computer zugeordnet sein, damit der Verschlüsselungstext archiviert wird.
2. Wenn Sie keine Archivposition angeben oder die Position nicht dem Client-Computer zugeordnet ist, kann der Verschlüsselungstext 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 kritischen Schritt in der Konfiguration von Client-Computern mit IBM ESS dar. Beachten Sie, dass die Benutzerinitialisierung ein zweiteiliger Prozess ist:

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. In UVM werden die Berechtigungsnachweise der einzelnen Benutzer gesteuert, und die Policy wird erzwungen.

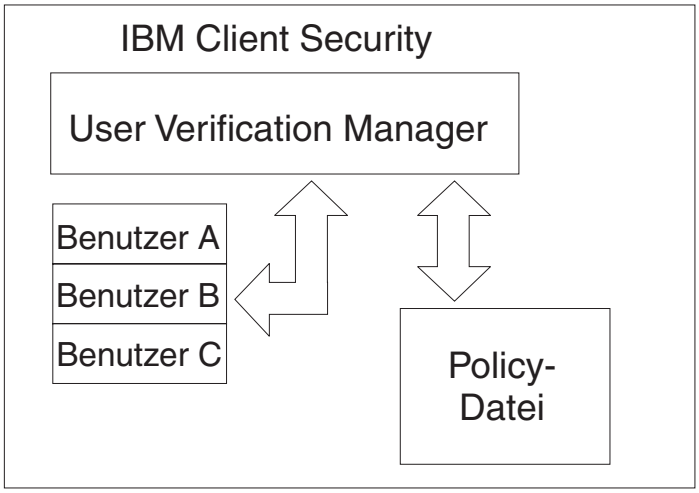

Abbildung 21. In User Verification Manager werden die Berechtigungsnachweise der einzelnen Benutzer gesteuert, und die Sicherheitspolicies werden erzwungen.

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 Domäne) sind. In UVM wird der Berechtigungsnachweis auf Grundlage des derzeit am Computer und Betriebssystem angemeldeten Benutzers verwaltet. Wenn sich Benutzer A beispielsweise bei Windows anmeldet und Benutzer A auch Teil von UVM ist, wird die Policy erzwungen, wenn Benutzer A Aufgaben ausführen möchte, für die ein Berechtigungsnachweis erforderlich ist. Ein anderes 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 Hilfe dessen die digital signierte E-Mail gesendet wird, ist im integrierten IBM Sicherheits-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 Verarbeitung ausgeführt werden kann. UVM fordert den Benutzer zur Eingabe des Verschlüsselungstexts auf. Wenn dieser als korrekt bestätigt wird, wird die Verarbeitung mit dem privaten Schlüssel im Chip ausgeführt.

Persönliche Initialisierung

Die persönliche Initialisierung bedeutet, dass der persönliche Verschlüsselungstext in UVM eingerichtet wird. 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 u. U. einen weiteren Schritt ausführen. UVM kann auch so konfiguriert werden, dass der Benutzer beim ersten Anmelden den Verschlüsselungstext ändern muss.

Beispiel: Benutzer A wird vom IT-Administrator initialisiert. Der IT-Administrator wählt Benutzer A aus einer Windows-Liste von Benutzern 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, sodass sichere Transaktionen nicht mit dem Standardverschlüsselungstext ausgeführt werden können.

Tabelle 3. Methoden zur Benutzerinitialisierung

Methode	Befehlsverarbeitung	Verarbeitungsbestimmungen
Manuell	Der Administrator kann über das Administratordienstprogramm CSS 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 des Administrators oder ohne seiner Anwesenheit 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, welche Maschine für welchen Endbenutzer bestimmt ist. Zum Beispiel ist Maschine 1 für Robert bestimmt. 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, welche Maschine für welchen Benutzer bestimmt ist. Sie vergeben Client 1 an Endbenutzer X.

Durch diese zwei variablen Faktoren sieht die Implementierung von IBM ESS anders aus als die Implementierung einer regulären 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:

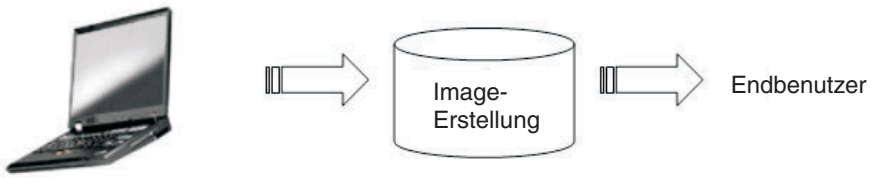

Abbildung 22. Typisches Flussdiagramm für die Bereitstellung von PCs

Sechs Implementierungsszenarien

Es gibt sechs Implementierungsmethoden für IBM Client Security:

1. **Hinzugefügte Komponente:** Der Code von IBM Client Security ist kein Bestandteil des Plattenimages. Er wird installiert, initialisiert und personalisiert, nachdem der Computer eingerichtet ist.
2. **Image-Komponente:** Der Code von IBM Client Security ist Bestandteil des Images, ist jedoch nicht installiert. Die Unternehmenspersonalisierung sowie die Benutzerpersonalisierung wurden nicht eingeleitet. (Siehe Abb. 23 auf Seite 34.)
3. **Einfache Installation:** IBM Client Security wurde installiert und für das Unternehmen oder den Endbenutzer personalisiert. (Siehe Abb. 24 auf Seite 35.)
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 35.)
5. **Vorläufige Personalisierung:** IBM Client Security wurde installiert und eine Personalisierung für Unternehmen sowie Endbenutzer eingerichtet. Der Benutzer muss seinen Verschlüsselungstext zurücksetzen und bei Bedarf andere Authentifizierungsinformationen, wie z. B. gescannten Fingerabdruck oder Smart-Card-Zuordnung, angeben. (Siehe Abb. 25 auf Seite 36.)
6. **Vollständige Personalisierung:** IBM Client Security wurde installiert und eine Personalisierung für Unternehmen sowie Endbenutzer eingerichtet. 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 36.)

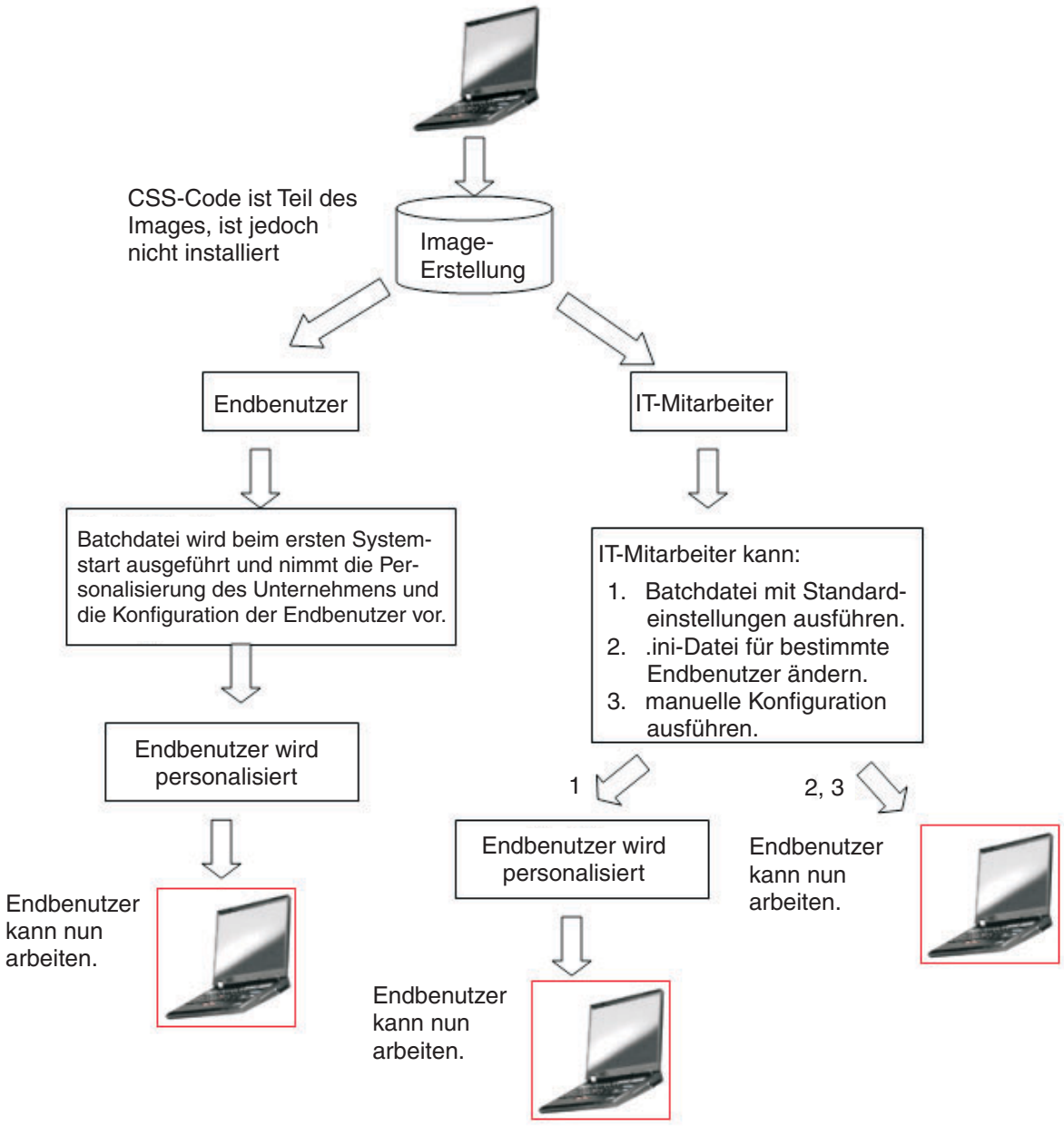

Abbildung 23. Der Code von IBM Client Security ist Bestandteil des Images, ist jedoch nicht installiert.

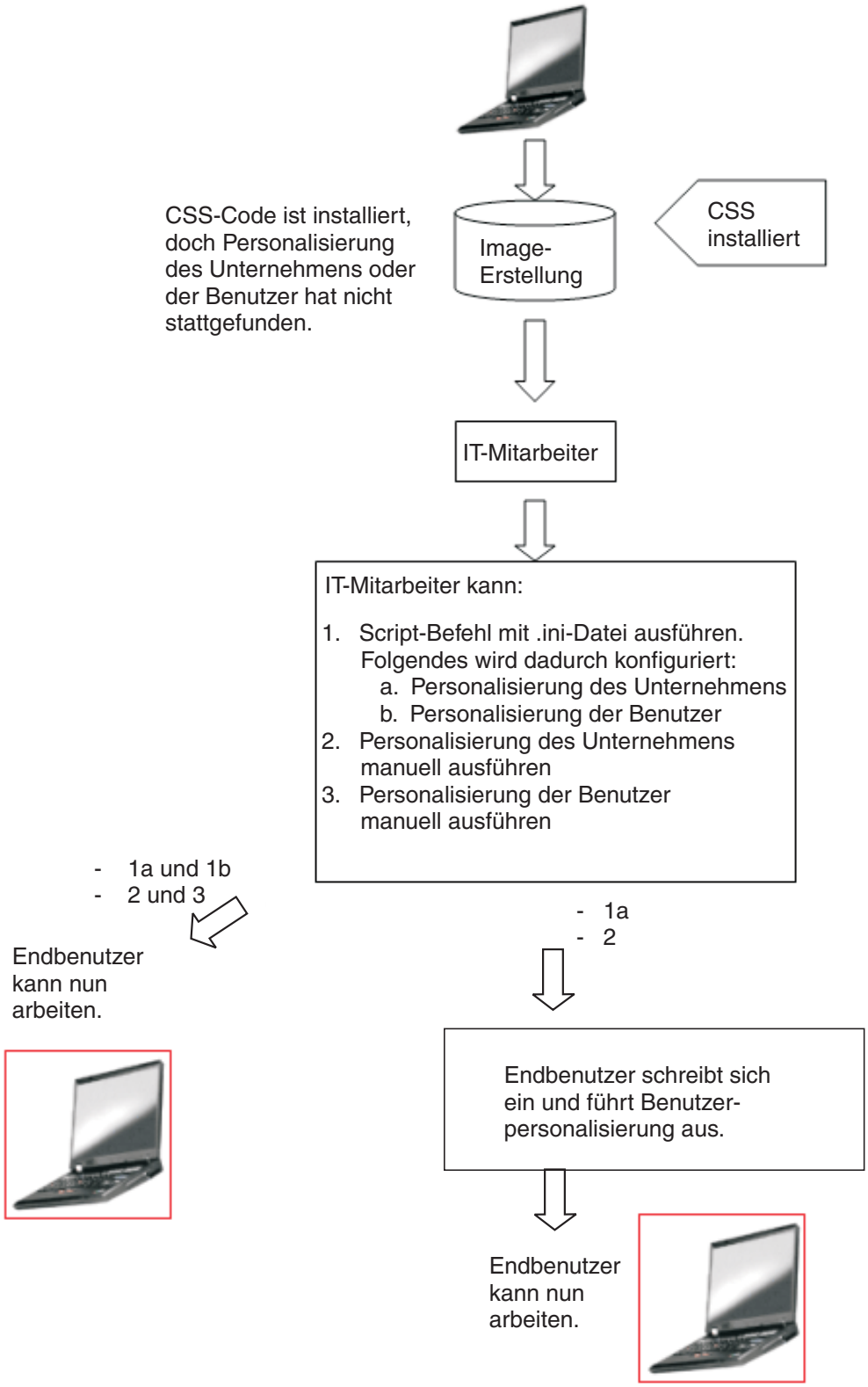

Abbildung 24. Der Code von IBM Client Security ist installiert, doch die Personalisierung des Unternehmens oder des Benutzers hat nicht stattgefunden.

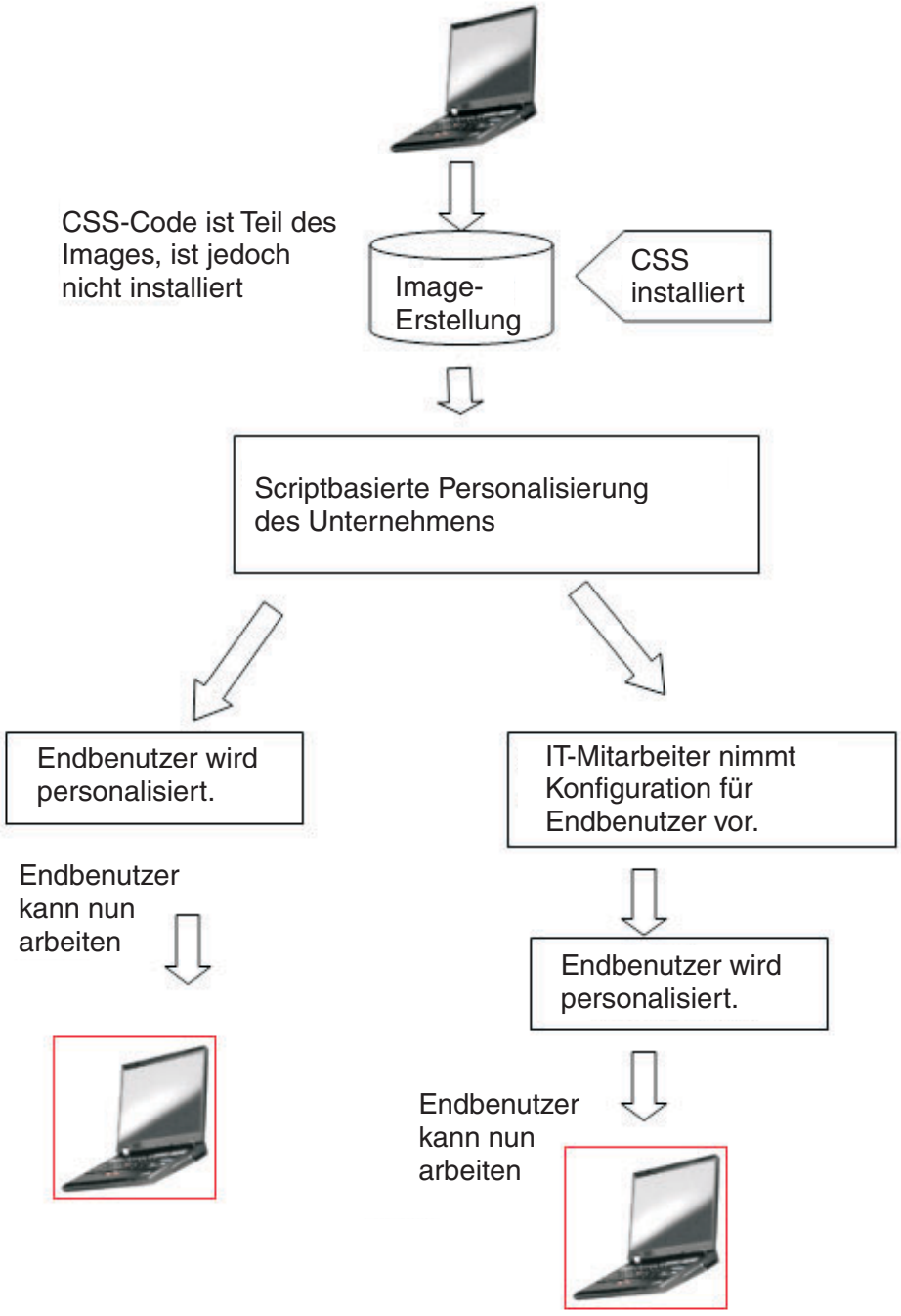

Abbildung 25. IBM Client Security ist installiert und eine Personalisierung für Unternehmen sowie Benutzer wurde eingerichtet.

In Szenario 1 wird IBM Client Security implementiert, nachdem das Plattenimage auf den Computer geladen wird. 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 wählen. Weitere Informationen zu Installationsmethoden finden Sie unter ″Installation und Initialisierung″.

Installation und Initialisierung

Die Installation von IBM Client Security kann in zwei Prozesse unterteilt werden: die Installation und die Initialisierung. Der Installationsprozess läuft ähnlich ab wie bei der Installation gewöhnlicher Software. Die Installation kann durch zwei Methoden erfolgen:

1. Client Security wird bereits eingerichteten Computern hinzugefügt. (Siehe Szenario 1 auf Seite 33.)
2. Client Security ist Bestandteil des Basisimages. (Siehe Szenario 2 auf Seite 33 bis 6 auf Seite 33.)

Installation

In Methode 1 wird IBM Client Security einem Image hinzugefügt, das durch Programme, wie z. B. ImageUltra Builder von IBM, auf jeden Computer geladen wird.

In Methode 2 wird IBM Client Security dem PC eines Endbenutzers hinzugefügt, nachdem der Computer mit dem Basisimage eingerichtet wurde. Für Methode 2 gibt es zwei Möglichkeiten:

1. **Benutzergesteuert:** Der Benutzer startet die Installation und schließt sie ab, indem er auf Dialoge klickt und alle erforderlichen Benutzereingaben angibt.
2. **Automatische Installation:** Der Installationsprozess kann über Remotezugriff gestartet und automatisch ohne Eingreifen des Benutzers abgeschlossen werden.

Initialisierung

Es gibt zwei Arten der Initialisierung:

1. Masseninitialisierung
2. Einzelinitialisierung

Für die Masseninitialisierung muss eine Datei mit Namen CSS.ini verwendet werden. Diese Datei stellt Parameter für Optionen, wie z. B. das Registrieren aller Benutzer auf einem System und das Vergeben eines bestimmten Verschlüsselungstexts für alle Benutzer, zur Verfügung. Bei der Einzelinitialisierung kann dem Endbenutzer eine Datei gegeben werden, die die Selbstregistrierung und benutzerdefinierte Kennwörter ermöglicht.

IBM Client Security zu eingerichteten Computern mit dem IBM Security Chip hinzufügen

Der Administrator kann lediglich IBM Client Security (auf dem Basisimage) implementieren (ohne Personalisierung oder Konfiguration) und die Software dann auf den Clients konfigurieren. Der Administrator kann auch eine Masseninstallation von IBM Client Security und eine anschließende automatische Massenkonfiguration vornehmen. In jedem Fall wird die Software zuerst installiert und anschließend konfiguriert.

IBM Client Security installieren: Damit IBM Client Security dem Basisimage hinzugefügt werden kann, müssen die folgenden Komponenten enthalten sein:

1. Treiber: LPC (für TCPA-Systeme) und SMBus

   Anmerkungen:

   a. SMBus verfügt zwar über Code für eine automatische Installation, doch wurde dieser Treiber noch nicht von Microsoft signiert. Daher muss während der Installation dieses Treibers ein Benutzer anwesend sein. Zurzeit wird daran gearbeitet, diese Einschränkung aufzuheben.

   b. Wenn Sie ein Sysprep-Donator-Image für die Implementierung erstellen, muss bei der Installation des Treibers ein Benutzer lediglich während der Erstellung des Donator-Images anwesend sein.

   c. Wenn Sie IBM ImageUltra Builder verwenden, müssen Sie ein Portable Sysprep-Image vorbereiten. SMBus muss Bestandteil des Basisimages sein. Wenn SMBus nicht auf jedem Computer Teil des Basisimages sein soll, müssen Sie zwei Basisimages erstellen.

2. Code von IBM Client Security
3. Administratorkennwort und privates Schlüsselpaar definiert
4. Installierte Applets von IBM Client Security (Verschlüsselung von Dateien und Ordnern sowie Password Manager müssen installiert sein, wenn ihre Verwendung in der Policy-Datei vorgeschrieben ist. Informationen zum automatischen Installieren dieser Applets finden Sie im *IBM Client Security Installationshandbuch*).

Nachdem die drei oben aufgeführten Komponenten dem Donatorsystem hinzugefügt wurden, muss die Hardware des integrierten Sicherheits-Subsystems (der Security Chip) initialisiert werden. Gehen Sie zum Einleiten einer Massenimplementierung wie folgt vor:

1. Erstellen Sie die Datei CSEC.INI. (Sie können die Datei CSEC.INI mit Hilfe des Assistenten von Client Security erstellen: CSECWIZ.EXE im Sicherheitsverzeichnis. Markieren Sie nach Abschluss des Assistenten das Markierungsfeld neben **Einstellungen speichern, konfigurieren Sie jedoch nicht das Subsystem. (Die Einstellungen werden unter C:\CSEC.INI gespeichert)**.
2. Extrahieren Sie mit Winzip unter Verwendung von Ordnernamen den Inhalt des Installationspakets (csecxxxxx_00xx.exe) von IBM Client Security.
3. Bearbeiten Sie in der Datei SETUP.ISS die für eine Massenkonfiguration erforderlichen Einträge ″szIniPath″ und ″szDir″. Der Parameter ″szIniPath″ ist für eine Massenkonfiguration erforderlich. (Siehe weiter unten die vollständige Datei SETUP.ISS.)
4. Kopieren Sie die Dateien auf das Zielsystem.
5. Erstellen Sie die Befehlszeilenanweisung ″\setup -s″. Führen Sie die Befehlszeilenanweisung vom Desktop eines Benutzers mit Administratorberechtigung aus. Ein geeigneter Ort hierfür ist die Programmgruppe ″Autostart″ oder das Fenster ″Ausführen″.
6. Entfernen Sie nach dem nächsten Systemstart die Befehlszeilenanweisung.

Der vollständige Inhalt der Datei ″setup.iss″ ist im Folgenden mit einigen Beschreibungen aufgeführt:

```
[InstallShield Silent] Version=v6.00.000 File=Response File szIniPath=d:\csec.ini
```

(Der obige Parameter enthält den Namen und die Position der .ini-Datei, die für die Massenkonfiguration erforderlich ist. Wenn sich die .ini-Datei auf einem Netzlaufwerk befindet, muss das Laufwerk verbunden sein. Wenn Sie eine unbeaufsichtigte Installation

ausführen, die nicht zu einer Massenkonfiguration gehört, entfernen Sie diesen Eintrag. Wenn Sie lediglich IBM Client Security installieren möchten, löschen Sie "szIniPath=d:\csec.ini" aus der oben aufgeführten Codezeile. Wenn Sie IBM Client Security installieren und auch konfigurieren möchten, lassen Sie den Befehl stehen und prüfen Sie den Pfad.)

```
[FileTransfer] OverwrittenReadOnly=NoToAll [{7BD2CFF6-B037-47D6-A76BD941EE13AD96}-
DlgOrder] Dlg0={7BD2CFF6-B037-47D6-A76B-D941EE13AD96}-
SdLicense-0 Count=4 Dlg1={7BD2CFF6-B037-47D6-A76B-D941EE13AD96}-
SdAskDestPath-0 Dlg2={7BD2CFF6-B037-47D6-A76B-D941EE13AD96}-
SdSelectFolder-0 Dlg3={7BD2CFF6-B037-47D6-A76B-D941EE13AD96}-
SdFinishReboot-0 [{7BD2CFF6-B037-47D6-A76B-D941EE13AD96}-SdLicense-0]
Result=1 [{7BD2CFF6-B037-47D6-A76B-D941EE13AD96}-SdAskDestPath-0]
szDir=C:\Program Files\IBM\Security
```

(Beim obigen Parameter handelt es sich um das Verzeichnis zum Installieren von Client Security. Es muss sich auf einem lokalen Laufwerk des Computers befinden.)

```
Result=1
[{7BD2CFF6-B037-47D6-A76B-D941EE13AD96}-SdSelectFolder-0] szFolder=IBM Client
Security Software
```

(Beim obigen Parameter handelt es sich um die Programmgruppe für Client Security.)

```
Result=1 [Application] Name=Client Security Version=5.00.002f
Company=IBM Lang=0009 [{7BD2CFF6-B037-47D6-A76B-D941EE13AD96}-
SdFinishReboot-0] Result=6 BootOption=3
```

Konfiguration: Die folgende Datei wird ebenfalls zum Einleiten einer Massenkonfiguration benötigt. Diese Datei kann beliebig benannt werden, nur die Erweiterung ".ini" ist erforderlich. In der folgenden Liste 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 Sicherheitsordner entschlüsseln. 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
```

Tabelle 4. 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 8 Zeichen aufweisen. Ist immer erforderlich. Muss richtig eingegeben werden, wenn das Hardwarekennwort bereits definiert wurde.
newkp=1	1: Generieren eines neuen Administratorschlüsselpaars, 0: Verwenden eines vorhandenen Administratorschlüsselpaars.
keysplit=1	Wenn "newkp" den Wert 1 aufweist, wird dadurch die Anzahl der privaten Schlüsselkomponenten festgelegt. **Anmerkung:** Enthält das vorhandene Schlüsselpaar mehrere private Schlüsselkomponenten, müssen alle privaten Schlüsselkomponenten im selben Verzeichnis gespeichert werden.
kpl=c:\jgk	Speicherposition des Administratorschlüsselpaars, wenn "newkp" = 1. Falls es sich um ein Netzlaufwerk handelt, muss dieses verbunden sein.

Tabelle 4. Konfigurationseinstellungen von Client Security (Forts.)

kal=c:\jgk\archive	Position des Benutzerschlüsselarchivs. Handelt es sich hierbei um ein Netzlaufwerk, muss das Laufwerk verbunden 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 verbunden sein.
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 verbunden sein.
wiz=0	Gibt an, ob diese Datei vom Installationsassistenten von CSS generiert wurde. Dieser Eintrag ist nicht erforderlich. Wenn Sie ihn in die Datei aufnehmen, sollte er den Wert 0 aufweisen.
clean=0	1: .ini-Datei nach Initialisierung löschen, 0: .ini-Datei nach Initialisierung nicht löschen.
enableroaming=1	1: Aktivierung von standortunabhängigem Zugriff für den Client, 0: Inaktivierung von standortunabhängigem Zugriff für den Client.
username= [promptcurrent]	[promptcurrent]: der derzeitige Benutzer wird zur Eingabe des Registrierungskennworts für das System aufgefordert. [current]: wenn das Registrierungskennwort für das System für den derzeitigen Benutzer durch den Eintrag ″sysregpwd″ geliefert wird und der derzeitige Benutzer zum Registrieren des Systems über den Roaming-Server berechtigt ist. [<bestimmter_Benutzeraccount>]: wenn der designierte Benutzer zum Registrieren des Systems über den Roaming-Server berechtigt ist und wenn das Systemregistrierungskennwort für diesen Benutzer durch den Eintrag ″sysregpwd″ geliefert wird. Verwenden Sie diesen Eintrag nicht, wenn der Wert für ″enableroaming″ 0 ist oder wenn der Eintrag nicht vorhanden ist.
sysregpwd=12345678	Systemregistrierungskennwort. Definieren Sie für diesen Wert das richtige Kennwort, um das System für die Registrierung über den Roaming-Server zu aktivieren. Nehmen Sie diesen Eintrag nicht auf, wenn der Wert des Benutzernamens als [promptcurrent] definiert ist oder wenn der Eintrag für den Benutzernamen nicht vorhanden ist.
[UVMEnrollment]	Abschnittsüberschrift für 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, gilt die Policy für das Ändern des UVM-Verschlüsselungstexts für alle Benutzer. 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 4. Konfigurationseinstellungen von Client Security (Forts.)

defaultppexppolicy=1	Wenn "enrollall" den Wert 1 aufweist, gilt die Policy für das Ablaufen des UVM-Verschlüsselungstexts für alle Benutzer. 0: Der UVM-Verschlüsselungstext läuft ab. 1: Der UVM-Verschlüsselungstext läuft nicht ab.
defaultppexpdays=0	Wenn "enrollall" den Wert 1 aufweist, wird die Anzahl von Tagen bis zum Ablaufen des UVM-Verschlüsselungstextes für alle Benutzer festgelegt. Wenn "ppexppoliall" den Wert 0 aufweist, definieren Sie diesen Wert, um die Anzahl von Tagen bis zum Ablaufen des UVM-Verschlüsselungstextes festzulegen.
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 in 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. Rufen Sie das Fenster "Computerverwaltung" auf. 2. Klicken Sie auf den Eintrag "Lokale Benutzer und Gruppen". 3. Öffnen Sie den Ordner "Benutzer". Bei den in der Spalte "Name" 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 in UVM registriert werden soll.
user1domain=0	Geben Sie an, ob es sich um einen lokalen oder einen Domänenaccount für Benutzer 1 handelt. 0: Angabe, dass es sich hierbei um einen lokalen Account handelt, 1: Angabe, dass es sich hierbei um einen Domänenaccount handelt.
user1ppchange=0	Geben Sie an, ob Benutzer 1 beim nächsten Anmelden den UVM-Verschlüsselungstext ändern soll. 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, definieren Sie diesen Wert, um die Anzahl von Tagen bis zum Ablaufen des UVM-Verschlüsselungstextes anzugeben.
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.	

Tabelle 4. Konfigurationseinstellungen von Client Security (Forts.)

user2=chrome	
user2uvmpw=left	
user2winpw=right	
user2domain=0	
user2ppchange=1	
user2ppexppolicy=0	
user2ppexpdays=90	
[UVMAppConfig]	Abschnittsüberschrift für Installation von UVM-sensitiven Anwendungen und Modulen.
uvmlogon=0	1: Verwendung von UVM-Anmeldeschutz, 0: Verwendung der Windows-Anmeldung.
entrust=0	1: Verwendung von UVM für Entrust-Authentifizierung, 0: Verwendung der Entrust-Authentifizierung.
notes=1	1: Verwendung des UVM-Anmeldeschutzes für Lotus Notes. 0: Verwendung des Notes-Kennwortschutzes.
netscape=0	1: Signieren und Verschlüsseln von E-Mails mit dem IBM PKCS#11-Modul, 0: kein Signieren und Verschlüsseln von E-Mails mit dem IBM PKCS#11-Modul.
passman=0	1: Verwendung von Password Manager, 0: keine Verwendung von Password Manager
folderprotect=0	1: Verwendung der Verschlüsselung von Dateien und Ordnern, 0: keine Verwendung der Verschlüsselung von Dateien und Ordnern.

Anmerkungen:

1. Wenn sich Dateien oder Pfade auf einem Netzlaufwerk befinden, muss dem Netzlaufwerk ein Laufwerkbuchstabe zugeordnet sein.
2. 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.
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. (Anführungszeichen sind für lange Pfadnamen erforderlich): `<CSS-Installationsordner>\console.exe /q /ini:` *`vollständiger Pfad zu einer unverschlüsselten INI-Datei`*
4. Wenn IBM Client Security erweitert und aktualisiert wird, ändern sich u. U. die Parameter für *.ini.

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 5. 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 8 Zeichen aufweisen. Ist immer erforderlich. Muss richtig eingegeben werden, wenn das Hardwarekennwort bereits definiert wurde.
newkp=0	Geben Sie 0 ein, um ein vorhandenes Administratorschlüsselpaar zu verwenden.
keysplit=1	Wenn "newkp" den Wert 1 aufweist, wird dadurch die Anzahl der privaten Schlüsselkomponenten festgelegt. **Anmerkung:** Enthält das vorhandene Schlüsselpaar mehrere private Schlüsselkomponenten, müssen alle privaten Schlüsselkomponenten im selben 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 verbunden sein.
wiz=0	Gibt an, ob diese Datei vom Installationsassistenten von CSS generiert wurde. Dieser Eintrag ist nicht erforderlich. Wenn Sie ihn in die Datei aufnehmen, sollte 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 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 in UVM registriert werden soll.
user1domain=0	Geben Sie an, ob es sich um einen lokalen oder einen Domänenaccount für Benutzer 1 handelt. 0: Angabe, dass es sich hierbei um einen lokalen Account handelt, 1: Angabe, dass es sich hierbei um einen Domänenaccount handelt.
user1ppchange=0	Geben Sie an, ob Benutzer 1 bei der nächsten Anmeldung den UVM-Verschlüsselungstext ändern soll. 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 5. 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, definieren Sie diesen Wert, um die Anzahl von Tagen bis zum Ablaufen des UVM-Verschlüsselungstextes anzugeben.

Kapitel 5. 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 über die IBM Website unter der Adresse http://www.pc.ibm.com/us/security/index.html heruntergeladen werden.

Voraussetzungen

Damit eine gesicherte 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

Weitere Informationen zur Installation und Benutzung von Tivoli Access Manager können Sie der Dokumentation auf der Website unter der Adresse http://www.tivoli.com/products/index/secureway_policy_dir/index.htm entnehmen.

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 aus, und lesen Sie die Lizenzvereinbarung. Klicken Sie dann auf **Accept Licence**.

   Sie werden danach automatisch zur Download-Seite für Client Security geführt.

4. Befolgen Sie die angezeigten Anweisungsschritte, um die erforderlichen Einheitentreiber, Readme-Dateien, Softwareprogramme, Referenzdokumente und zusätzlichen Dienstprogramme herunterzuladen.
5. Gehen Sie wie folgt vor, um Client Security zu installieren:
   a. Klicken Sie auf dem Windows-Desktop auf **Start > Ausführen**.
   b. Geben Sie in das Feld "Ausführen" `d:\verzeichnis\csec53.exe` ein. Hierbei gibt d:\verzeichnis\ den Laufwerkbuchstaben und das Verzeichnis an, 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 in das Feld "Ausführen" `d:\verzeichnis\TAMCSS.exe` ein. Hierbei gibt d:\verzeichnis\ den Laufwerkbuchstaben und das Verzeichnis an, in dem die Datei gespeichert ist. Oder klicken Sie auf **Durchsuchen**, wenn Sie die Position der Datei ermitteln möchten.
8. Klicken Sie auf **OK**.
9. Geben Sie einen Zielordner an, und klicken Sie auf **Unzip**.
   Der Assistent extrahiert die Dateien in den angegebenen Ordner. Eine Nachricht teilt mit, 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 zu der Befehlssyntax können Sie dem *Tivoli Access Manager Base Administrator Guide* entnehmen.

Gesicherte 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 erst an der gesicherten Domäne anmelden.

Das Dienstprogramm ″svrsslcfg″ ermöglicht es IBM Client Security-Anwendungen, mit dem Tivoli Access Manager-Verwaltungsserver und -Autorisierungsserver zu kommunizieren.

Das Dienstprogramm ″svrsslcfg″ ermöglicht es IBM Client Security-Anwendungen, mit dem Tivoli Access Manager-Verwaltungsserver und -Autorisierungsserver zu kommunizieren.

Das Dienstprogramm ″svrsslcfg″ führt die folgenden Tasks aus:

- Erstellt für die Anwendung eine Benutzeridentifikation. Beispiel: DemoUser/HOSTNAME
- Erstellt eine SSL-Schlüsseldatei für diesen Benutzer. Beispiel: DemoUser.kdb und DemoUser.sth
- Fügt den Benutzer der Gruppe der fernen ACL-Benutzer hinzu.

Die folgenden Parameter werden benötigt:

- **-f cfg_file** Name und Pfad der Konfigurationsdatei. Verwenden Sie TAMCSS-.conf
- **-d kdb_dir** Das Verzeichnis, das die Schlüsselringdatenbankdateien für den Server enthalten soll.
- **-n Servername** Der aktuelle Windows-Benutzername/UVM-Benutzername des gewünschten IBM Client-Benutzers.
- **-P admin_pwd** Das Tivoli Access Manager-Administratorkennwort.
- **-s server_type** Es muss ″fern″ angegeben werden.
- **-S server_pwd** Das Kennwort für den neu erstellten Benutzer. Hierbei handelt es sich um einen erforderlichen Parameter.
- **-r port_num** Die empfangsbereite Portnummer 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** Verfallszeit des Kennworts in Anzahl an Tagen.

Gehen Sie wie folgt vor, um eine gesicherte 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 Hostnamen des IBM Clients an. Beispiel: –n DemoUser/MyHostName. Den IBM Client-Hostnamen können Sie herausfinden, indem Sie in die MSDOS-Befehlszeile “hostname” eingeben. Das Dienstprogramm ″svrsslcfg″ erstellt dann 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 der 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 Chip können Sie mit dem Administratordienstprogramm die Benutzerauthentifizierung konfigurieren und die UVM-Sicherheitspolicy bearbeiten. Ausführliche Anweisungen zur Installation und Verwendung von Client Security sind im *Client Security Installationshandbuch* und im *Client Security Administratorhandbuch* enthalten.

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 > Integriertes IBM Sicherheits-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 unter ″Informationen zur Konfiguration von Tivoli Access Manager″ den vollständigen Pfad zur Konfigurationsdatei TAMCSS.conf aus. Beispiel: `C:\TAMCSS\TAMCSS.conf`

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

   Die Anzeige ″Administratorkennwort eingeben″ erscheint.
8. Geben Sie das Administratorkennwort in das entsprechende Feld ein, und klicken Sie auf **OK**.

   Die Seite 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 > Integriertes IBM Sicherheits-Subsystem**.
2. Geben Sie das Administratorkennwort ein, und klicken Sie auf **OK**.

   Das Fenster "Administratordienstprogramm" wird angezeigt. Ausführliche Informationen zur Verwendung des Administratordienstprogramms sind im *Client Security Administratorhandbuch* enthalten.
3. Klicken Sie im Administratordienstprogramm auf die Schaltfläche **Anwendungsunterstützung und Policies konfigurieren** und anschließend auf **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 Datei für eine globale Policy gesteuert. Die Datei für eine globale Policy, die sog. UVM-Policy-Datei, enthält Authentifizierungsbestimmungen für Aktionen, die auf dem IBM Client-System ausgeführt werden, wie z. B. am System anmelden, Bildschirmschoner löschen 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: Bei der Aktivierung des Tivoli Access Manager zur Steuerung eines Objekts 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.

EditiervorgangSie 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 im Verzeichnis \Program Files\IBM\Security\UVM_Policy\globalpolicy.gvm gespeichert. Nur ein Benutzer, der 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 UVM hinzugefügt sind, ihren Fingerabdruck registrieren lassen, 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 **Anwendungspolicy**.

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

   Die Anzeige "Administratorkennwort eingeben" erscheint.
3. Geben Sie das Administratorkennwort in das entsprechende Feld ein, und klicken Sie auf **OK**.

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

Fehlerbehebungsinformationen zu Lotus Notes

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 werden und aktiv sein, damit 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 neu.

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 Notes-ID-Datei 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 von früheren Versionen von Client Security verschlüsselt wurden, nicht entschlüsseln, da in dieser Version die Implementierung der Dateiverschlüsselung geändert wurde.

Kapitel 6. 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 maßgeschneidert anpassen können.

Das integrierte IBM Sicherheits-Subsystem wurde auf die Einhaltung der Normen für bestimmte Hardwareangebote der Sicherheitsauthentifizierung von folgenden Unternehmen geprüft:

- Targus für Lesegerät für Fingerabdrücke
- Gemplus für Smart-Card-Lösungen
- Ensure Technologies für berührungslose Ausweise

Auf der Website http://www.pc.ibm.com/us/security/index.html finden Sie Verknüpfungen zu diesen Unternehmen 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 der 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 7. 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 ″IBM Sicherheits-Subsystem″ klicken.)

Signieren Sie die Policy-Datei gemäß den angezeigten Anweisungen, nachdem Sie auf ″Übernehmen″ klicken. (**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 die Verschlüsselungstext-Policies nach der Implementierung über Remotezugriff aktualisieren. Das Aktualisieren der Policy-Datei des Verschlüsselungstexts ermöglicht es Ihnen, die Verschlüsselungstextanforderungen zu 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 beim nächsten Ändern des Verschlüsselungstexts von Simone, der neue Verschlüsselungstext nun zwölf Zeichen umfasst. 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 soll. Was geschieht im folgenden Szenario? Ihr Verschlüsselungstext ″Leben″ mit einem Ablaufzeitraum von 30 Tagen ist 10 Tage alt. Eine neue Policy-Datei für den Verschlüsselungstext wird an den Client-Computer gesendet. Laut dieser muss der Verschlüsselungstext alle 15 Tage geändert werden. Läuft der Verschlüsselungstext nun in 5 oder in 20 Tagen ab? Der Verschlüsselungstext läuft, wie in der ursprünglichen Policy angegeben, in 20 Tagen ab. Die Policy des Verschlüsselungstextablaufs tritt in Kraft, wenn der Verschlüsselungstext implementiert wird. Die Policy mit der Änderung nach 15 Tagen beginnt, wenn Simone ihren Verschlüsselungstext nach 20 Tagen ändert.

Wenn Sie die Merkmale 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 andere Schutzrechte von IBM verletzen. Die Verantwortung für den Betrieb von Fremdprodukten, Fremdprogrammen oder Fremdservices liegt jedoch beim Kunden.

Für in diesen 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):

Director of Licensing
IBM Corporation
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. Die IBM Produktspezifikationen oder Gewährleistungen werden durch die in dieser Dokumentation enthaltenen Informationen nicht beeinflusst oder geänderDie Informationen in diesem Dokument beeinflussen oder ändern nicht die IBM Produktspezifikationen oder Gewährleistungen. 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.