



IBM Systems - iSeries

Sicherheit

Digital Certificate Manager

*Version 5 Release 4*







IBM Systems - iSeries

Sicherheit

Digital Certificate Manager

*Version 5 Release 4*

**Hinweis**

Vor Verwendung dieser Informationen und des darin beschriebenen Produkts sollten die allgemeinen Informationen unter „Bemerkungen“, auf Seite 101 gelesen werden.

**Neunte Ausgabe (Februar 2006)**

Diese Ausgabe bezieht sich auf Version 5, Release 4, Modifikation 0 von IBM i5/OS (Produktnummer 5722-SS1) und alle nachfolgenden Releases und Modifikationen, es sei denn, es erfolgen anders lautende Angaben in neuen Ausgaben. Diese Version kann nicht auf allen RISC-Modellen (RISC = Reduced Instruction Set Computer) ausgeführt werden. Auf CICS-Modellen ist sie nicht ausführbar.

Diese Veröffentlichung ist eine Übersetzung des Handbuchs  
*IBM Systems - iSeries Security Digital Certificate Manager, Version 5 Release 4*,  
herausgegeben von International Business Machines Corporation, USA

© Copyright International Business Machines Corporation 1999, 2006  
© Copyright IBM Deutschland GmbH 1999, 2006

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

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

Änderung des Textes bleibt vorbehalten.

Herausgegeben von:  
SW TSC Germany  
Kst. 2877  
Februar 2006

---

# Inhaltsverzeichnis

<b>Digital Certificate Manager</b> . . . . .	<b>1</b>	Konfiguration von DCM . . . . .	45
Neuerungen in V5R4 . . . . .	1	Digital Certificate Manager starten . . . . .	46
Druckbare PDF-Datei . . . . .	2	Zertifikate erstmals definieren . . . . .	46
DCM-Konzepte . . . . .	2	Vorhandenes Zertifikat verlängern . . . . .	63
Zertifikatserweiterungen . . . . .	3	Zertifikat importieren . . . . .	65
Zertifikatsverlängerung . . . . .	3	Verwaltung mit DCM . . . . .	66
Registrierter Name . . . . .	4	Lokale Zertifizierungsinstanz zum Ausstellen von	
Digitale Signaturen . . . . .	5	Zertifikaten für andere iSeries-Systeme verwenden	
Öffentliches/privates Schlüsselpaar . . . . .	6	. . . . .	66
Zertifizierungsinstanz (CA) . . . . .	6	Anwendungen in DCM verwalten . . . . .	76
CRL-Verteilungspunkte . . . . .	7	Zertifikate nach Verfallsdatum verwalten . . . . .	79
Zertifikatsspeicher . . . . .	8	Zertifikate und Anwendungen überprüfen . . . . .	80
Chiffrierung . . . . .	10	Anwendungen ein Zertifikat zuordnen . . . . .	81
IBM Verschlüsselungskoprozessoren für iSeries	11	CRL-Verteilungspunkte verwalten . . . . .	81
Secure Sockets Layer (SSL) . . . . .	11	Zertifikatsschlüssel auf einem IBM Verschlüsse-	
Anwendungsdefinitionen . . . . .	12	lungskoprozessor speichern . . . . .	83
Gültigkeitsprüfung . . . . .	12	Anforderungsadresse für eine PKIX-Zertifizie-	
DCM-Szenarios . . . . .	14	rungsinstanz verwalten . . . . .	85
Szenario: Zertifikate für die externe Authentifizie-		LDAP-Position für Benutzerzertifikate verwalten	
rung verwenden . . . . .	14	Objekte signieren . . . . .	87
Szenario: Zertifikate für die interne Authentifizie-		Objektsignaturen prüfen . . . . .	89
rung verwenden . . . . .	22	Fehlerbehebung in DCM . . . . .	90
Planung von DCM . . . . .	32	Fehler bei Kennwörtern und allgemeine Fehler	
DCM-Setupvoraussetzungen . . . . .	32	beheben . . . . .	91
Hinweise zur Sicherung und Wiederherstellung		Fehler bei Zertifikatsspeichern und Schlüssel-	
von DCM-Daten . . . . .	32	datenbanken beheben . . . . .	93
Typen digitaler Zertifikate . . . . .	33	Fehler bei Browsern beheben . . . . .	95
Öffentliche vs. private Zertifikate . . . . .	35	Fehler beim IBM HTTP-Server für iSeries behe-	
Digitale Zertifikate für die gesicherte SSL-Kom-		ben . . . . .	97
munikation . . . . .	38	Fehler beim Zuordnen eines Benutzerzertifikats	
Digitale Zertifikate für die Benutzerauthentifizie-		beheben . . . . .	98
rung . . . . .	38	Referenzinformationen zu DCM . . . . .	99
Digitale Zertifikate und Enterprise Identity Map-			
ping . . . . .	40		
Digitale Zertifikate für VPN-Verbindungen . . . . .	41		
Digitale Zertifikate für das Signieren von Objek-			
ten . . . . .	42		
Digitale Zertifikate für die Prüfung von Objekt-			
signaturen . . . . .	44		
		<b>Anhang. Bemerkungen</b> . . . . .	<b>101</b>
		Marken . . . . .	103
		Bedingungen . . . . .	103



---

## Digital Certificate Manager

Ein digitales Zertifikat ist ein elektronischer Berechtigungsnachweis, den Sie bei elektronischen Transaktionen zur Belegung Ihrer Identität verwenden können. Digitale Zertifikate werden immer häufiger zur Verbesserung der Sicherheit in Netzwerken eingesetzt. Sie sind z. B. bei der Konfiguration und der Verwendung von Secure Sockets Layer (SSL) von zentraler Bedeutung. Durch den Einsatz von SSL können Sie gesicherte Verbindungen zwischen Benutzern und Serveranwendungen innerhalb eines nicht anerkannten Netzwerks wie z. B. dem Internet herstellen. SSL bietet Ihnen im Internet eine der besten Lösungen zum Schutz der Vertraulichkeit von sensiblen Daten wie z. B. Benutzernamen und Kennwörtern. Zahlreiche iSeries-Services und -Anwendungen wie FTP, Telnet oder HTTP-Server stellen SSL-Unterstützung zur Gewährleistung der Vertraulichkeit von Daten zur Verfügung.

iSeries verfügt über umfangreiche Unterstützungsfunktionen für digitale Zertifikate, mit deren Hilfe Sie diese bei einer Reihe von Sicherheitsanwendungen als Berechtigungsnachweis einsetzen können. Zusätzlich zu der Möglichkeit, Zertifikate zur Konfiguration von SSL zu benutzen, können Sie diese sowohl bei SSL- als auch bei VPN-Transaktionen (VPN = Virtual Private Network) als Berechtigungsnachweis für die Client-Authentifizierung benutzen. Digitale Zertifikate und die zugehörigen Sicherheitsschlüssel können auch zum Signieren von Objekten (siehe hierzu Sign objects) eingesetzt werden. Das Signieren von Objekten ermöglicht Ihnen durch Prüfung der Objektsignaturen die Feststellung von Änderungen oder Manipulationen des Objektinhalts und somit die Gewährleistung ihrer Integrität.

Die Nutzung dieser iSeries-Unterstützungsfunktionen für Zertifikate ist einfach, wenn Sie mit Digital Certificate Manager (DCM) arbeiten. Hierbei handelt es sich um eine kostenlose Funktion für die zentrale Verwaltung von Anwendungszertifikaten. DCM ermöglicht Ihnen die Verwaltung von Zertifikaten, die von einer beliebigen Zertifizierungsinstanz (CA) ausgestellt wurden. Darüber hinaus können Sie DCM verwenden, um eine eigene lokale Zertifizierungsinstanz zu erstellen und zu betreiben, mit der Sie private Zertifikate für die Anwendungen und Benutzer Ihres Unternehmens ausstellen können.

Eine durchdachte Planung und Bewertung Ihrer individuellen Anforderungen sind der Schlüssel zum effektiven Einsatz von Zertifikaten und zur Nutzung ihrer zusätzlichen Sicherheitsvorteile. Unter den folgenden Themen finden Sie Wissenswertes zur Funktionsweise von Zertifikaten und dazu, wie DCM zur Verwaltung von Zertifikaten und der Anwendungen, die diese benutzen, eingesetzt werden kann:

---

## Neuerungen in V5R4

Im Folgenden wird erläutert, welche Informationen im aktuellen Release neu hinzugefügt oder erheblich geändert wurden.

### Neue Informationen zur Zertifikatsverlängerung

In diesen neuen Informationen werden die einzelnen Arbeitsschritte erläutert, die zur Verlängerung vorhandener Zertifikate bei der lokalen Zertifizierungsinstanz oder bei einer Internet-Zertifizierungsinstanz durchgeführt werden müssen.

- „Vorhandenes Zertifikat verlängern“ auf Seite 63

### Neue Informationen zum Zertifikatsimport

In diesen neuen Informationen werden die Arbeitsschritte erläutert, die zum Importieren von Zertifikaten ausgeführt werden müssen, die in Dateien auf Ihrem oder einem anderen Server gespeichert sind.

- „Zertifikat importieren“ auf Seite 65



## Ergänzungen zu den Informationen für die Liste der entzogenen Zertifikate (CRL) und das Lightweight Directory Access Protocol (LDAP)

Diese Informationen wurden aktualisiert und enthalten jetzt Anweisungen zur Herstellung einer anonymen Bindung zu einem LDAP-Server zum Zwecke der CRL-Verarbeitung.

- „CRL-Verteilungspunkte verwalten“ auf Seite 81
- „LDAP-Position für Benutzerzertifikate verwalten“ auf Seite 86
- „CRL-Verteilungspunkte“ auf Seite 7

### Abrufen neuer oder geänderter Informationen

Um technische Änderungen zu markieren, werden im vorliegenden Dokument die folgenden Symbole verwendet:


- Das Grafiksymbol  markiert den Anfang der neuen oder geänderten Informationen.
- Das Grafiksymbol  markiert das Ende der neuen oder geänderten Informationen.

Weitere Informationen zu den Änderungen und Neuerungen im aktuellen Release finden Sie im Memorandum für Benutzer.

---

### Druckbare PDF-Datei

Auf dieser Seite finden Sie Informationen zum Drucken des gesamten Abschnitts als PDF-Datei.


Wenn Sie die PDF-Version dieses Themas anzeigen oder herunterladen wollen, müssen Sie Digital Certificate Manager  (Dateigröße ca. 600 KB bzw. 116 Seiten) auswählen.

### Speichern von PDF-Dateien

So können Sie eine PDF-Datei auf Ihrer Workstation speichern, um diese anzuzeigen oder zu drucken:

1. Klicken Sie im Browser mit der rechten Maustaste auf die PDF-Datei (bzw. klicken Sie auf den o. a. Link).
2. Klicken Sie, wenn Sie mit dem Internet Explorer arbeiten, auf **Ziel speichern unter....** Wenn Sie Netscape Communicator verwenden, müssen Sie auf **Rahmen speichern unter...** klicken.
3. Navigieren Sie zu dem Verzeichnis, in dem die PDF-Datei gespeichert werden soll.
4. Klicken Sie auf **Speichern**.

### Download von Adobe Acrobat Reader

Zur Anzeige und zum Drucken von PDF-Dateien benötigen Sie Adobe Acrobat Reader. Sie können eine Kopie dieses Produkts von der Adobe-Website ([www.adobe.com/products/acrobat/readstep.html](http://www.adobe.com/products/acrobat/readstep.html))  herunterladen.

---

### DCM-Konzepte

Anhand der folgenden Informationen können Sie sich mit digitalen Zertifikaten und deren Funktionsweise vertraut machen. Sie enthalten Angaben zu den unterschiedlichen Zertifikatstypen und wie diese im Rahmen Ihrer Sicherheitsrichtlinien eingesetzt werden können.

Bevor Sie digitale Zertifikate verwenden, um die Sicherheitsstrategie Ihres Systems und Ihres Netzwerks zu optimieren, sollten Sie die grundlegenden Merkmale digitaler Zertifikate sowie die Vorteile kennen, die diese in Bezug auf die Sicherheit bieten.



Ein digitales Zertifikat ist ein digitaler Berechtigungsnachweis, der die Identität des Zertifikatseigners bestätigt, vergleichbar mit einem Pass. Die Identifikationsdaten, die in einem digitalen Zertifikat bereitgestellt werden, werden als registrierter Subjektname (DN) bezeichnet. Eine anerkannte Instanz, die als Zertifizierungsinstanz (CA) bezeichnet wird, stellt digitale Zertifikate für Benutzer und Organisationen bzw. Unternehmen aus. Die Anerkennung der Zertifizierungsinstanz bildet die Voraussetzung für die Anerkennung des Zertifikats als gültiger Berechtigungsnachweis.

Ein digitales Zertifikat enthält darüber hinaus auch einen öffentlichen Schlüssel, der Teil eines öffentlichen/privaten Schlüsselpaars ist. Eine Vielzahl von Sicherheitsfunktionen basieren auf der Verwendung digitaler Zertifikate und der zugehörigen Schlüsselpaare. Sie können digitale Zertifikate zum Konfigurieren von SSL-Sitzungen (SSL = Secure Sockets Layer) verwenden und so private gesicherte Kommunikationssitzungen zwischen Benutzern und den verwendeten Serveranwendungen herstellen. Sie können diese Sicherheitsfunktionen auch erweitern, indem Sie viele SSL-Anwendungen so konfigurieren, dass zur gesicherten Benutzerauthentifizierung an Stelle von Benutzernamen und Kennwörtern Zertifikate verwendet werden.

Weitere Informationen zu den Konzepten digitaler Zertifikate finden Sie in den folgenden Themen:

## Zertifikatserweiterungen

Bei Zertifikatserweiterungen handelt es sich um Informationsfelder, die zusätzliche Informationen zu Zertifikaten bereitstellen.

Zertifikatserweiterungen bieten eine Möglichkeit zur Erweiterung der ursprünglichen X.509-Standards für Zertifikatsinformationen. Während bestimmte Erweiterungen angegeben werden, um die für ein Zertifikat bereitgestellten Identifikationsdaten zu ergänzen, enthalten andere Erweiterungen Informationen zu den Verschlüsselungsfunktionen des Zertifikats.

Nicht alle Zertifikate verwenden die Erweiterungsfelder zur Erweiterung des registrierten Namens (DN) und weiterer Informationen. Die Anzahl und der Typ der Erweiterungsfelder, die von einem Zertifikat verwendet werden, variieren abhängig von den Zertifizierungsinstanzen (CAs), die zur Ausstellung von Zertifikaten verwendet werden.

Die von Digital Certificate Manager (DCM) bereitgestellte lokale Zertifizierungsinstanz (CA) ermöglicht Ihnen z. B. ausschließlich die Verwendung der Zertifikatserweiterungen für den Subjektalternativenamen. Diese Erweiterungen ermöglichen die Zuordnung eines Zertifikats zu einer bestimmten IP-Adresse, einem vollständig qualifizierten Domännennamen oder einer E-Mail-Adresse. Wenn Sie das Zertifikat jedoch zum Identifizieren eines Endpunktes für eine iSeries-VPN-Verbindung (VPN = Virtual Private Network) benutzen wollen, müssen Sie Informationen für diese Erweiterungen angeben.

### Zugehörige Konzepte

„Registrierter Name“ auf Seite 4

Unter diesem Thema erfahren Sie mehr über Identifikationsmerkmale von digitalen Zertifikaten.

## Zertifikatsverlängerung

Die von Digital Certificate Manager (DCM) bei der Zertifikatsverlängerung verwendete Vorgehensweise kann abhängig vom Typ der ausstellenden Zertifizierungsinstanz (CA) variieren.

Wenn Sie zum Signieren des verlängerten Zertifikats die lokale Zertifizierungsinstanz (CA) verwenden, benutzt DCM die Informationen, die Sie bei der Erstellung eines neuen Zertifikats im aktuellen Zertifikatsspeicher angeben, und speichert das zuvor verwendete Zertifikat.

Wenn Sie zur Ausstellung des Zertifikats eine anerkannte Internet-Zertifizierungsinstanz (CA) verwenden, können Sie zur Zertifikatsverlängerung entweder das verlängerte Zertifikat aus einer Datei importieren, die Sie von der signierenden CA erhalten haben, oder Sie können mit DCM ein neues

öffentliches/privates Schlüsselpaar für das Zertifikat erstellen. DCM stellt die erste Auswahl für den Fall bereit, dass Sie es vorziehen, das Zertifikat direkt bei der Zertifizierungsinstanz zu verlängern, die dieses ausgestellt hat.

Wenn Sie sich für die Erstellung eines neuen Schlüsselpaares entscheiden, führt DCM die Verlängerung auf die gleiche Weise durch, die bei der Zertifikatserstellung verwendet wurde. DCM erstellt ein neues öffentliches/privates Schlüsselpaar für das verlängerte Zertifikat und generiert eine Zertifikatssignieranforderung (CSR), die aus einem öffentlichen Schlüssel und weiteren Informationen besteht, die für das neue Zertifikat angegeben werden. Sie können die CSR zum Anfordern eines neuen Zertifikats von VeriSign oder einer anderen öffentlichen Zertifizierungsinstanz verwenden. Nachdem Sie das signierte Zertifikat von der Zertifizierungsinstanz (CA) erhalten haben, können Sie dieses mit DCM in den entsprechenden Zertifikatsspeicher importieren. Der Zertifikatsspeicher enthält anschließend beide Kopien des Zertifikats, d. h. das ursprüngliche Dokument und das neu ausgestellte, verlängerte Zertifikat.

Wenn Sie kein neues Schlüsselpaar durch DCM generieren lassen wollen, führt Sie das Programm durch den Prozess zum Import des verlängerten, signierten Zertifikats in den Zertifikatsspeicher. Das Zertifikat befindet sich hierbei in einer Datei, die Sie von der zuständigen Zertifizierungsinstanz (CA) erhalten haben. Das importierte, verlängerte Zertifikat ersetzt dann das zuvor verwendete Zertifikat.

## Registrierter Name

Unter diesem Thema erfahren Sie mehr über Identifikationsmerkmale von digitalen Zertifikaten.

Für jede Zertifizierungsinstanz gelten bestimmte Richtlinien bei der Festlegung, welche Identifikationsdaten zur Ausstellung eines Zertifikats erforderlich sind. Einige öffentliche Internet-Zertifizierungsinstanzen fordern möglicherweise nur wenige Informationen an, wie beispielsweise einen Namen und eine E-Mail-Adresse. Andere öffentliche Zertifizierungsinstanzen fordern möglicherweise mehr Informationen und Identitätsnachweise an, bevor sie ein Zertifikat ausstellen. Zertifizierungsinstanzen, die PKIX-Standards unterstützen (PKIX = Public Key Infrastructure Exchange), verlangen möglicherweise vom Anfordernden, seine Identitätsdaten durch eine Registrierungsinstanz (RA) bestätigen zu lassen, bevor das Zertifikat ausgestellt wird. Wenn Sie vorhaben, Zertifikate als Berechtigungen zu akzeptieren und zu verwenden, sollten Sie daher die Identifikationsanforderungen der betreffenden Zertifizierungsinstanz überprüfen, um festzustellen, ob deren Anforderungen Ihren Sicherheitsbedürfnissen gerecht werden.

Beim registrierten Namen (DN = Distinguished Name) handelt es sich um einen Terminus, der die identifizierenden Informationen eines Zertifikats beschreibt und selbst Teil des Zertifikats ist. Ein Zertifikat enthält DN-Informationen sowohl für den Eigner bzw. Anforderer des Zertifikats (DN für Betreff) als auch für die Zertifizierungsinstanz (CA), die das Zertifikat ausstellt (DN für Aussteller). Abhängig von den jeweiligen Identifikationsrichtlinien der Zertifizierungsinstanz, die ein Zertifikat ausstellt, kann der DN umfangreiche Informationen beinhalten. Sie können Digital Certificate Manager (DCM) verwenden, um eine private Zertifizierungsinstanz zu betreiben und private Zertifikate auszustellen. Darüber hinaus können Sie DCM zum Generieren der DN-Informationen sowie des Schlüsselpaares für die von einer öffentlichen Internet-Zertifizierungsinstanz für Ihr Unternehmen ausgestellten Zertifikate verwenden. Die DN-Informationen, die Sie für beide Zertifikatstypen angeben können, umfassen Folgendes:

- Allgemeiner Name des Zertifikatseigners
- Organisation
- Organisationseinheit
- Standort oder Stadt
- Bundesland
- Land oder Region

Wenn Sie DCM zum Ausstellen privater Zertifikate verwenden, können Sie Zertifikatserweiterungen zur Bereitstellung folgender zusätzlicher DN-Informationen für das Zertifikat verwenden:

- Adresse der IP-Version

- Vollständig qualifizierter Domänenname
- E-Mail-Adresse

#### **Zugehörige Konzepte**

„Zertifikatserweiterungen“ auf Seite 3

Bei Zertifikatserweiterungen handelt es sich um Informationsfelder, die zusätzliche Informationen zu Zertifikaten bereitstellen.

## **Digitale Signaturen**

Eine digitale Signatur auf einem elektronischen Dokument oder einem anderen Objekt wird mit Hilfe eines bestimmten Chiffrierverfahrens erstellt und entspricht einer persönlichen Unterschrift auf einem schriftlichen Dokument.

Sie belegt den Ursprung eines Objekts und bietet die Möglichkeit, die Integrität dieses Objekts zu prüfen. Der Eigner eines digitalen Zertifikats "signiert" ein Objekt, indem er den privaten Schlüssel des Zertifikats verwendet. Der Empfänger des Objekts verwendet den zugehörigen öffentlichen Schlüssel des Zertifikats, um die Signatur zu entschlüsseln. Hierdurch können die Integrität des signierten Objekts sowie sein Absender überprüft werden.

Eine Zertifizierungsinstanz (CA) signiert die von ihr ausgestellten Zertifikate. Diese Signatur besteht aus einer Datenfolge, die mit dem privaten Schlüssel der Zertifizierungsinstanz verschlüsselt wurde. Jeder Benutzer kann dann die Signatur auf dem Zertifikat prüfen, indem er die Signatur mit Hilfe des öffentlichen Schlüssels der Zertifizierungsinstanz entschlüsselt.

Eine digitale Signatur ist eine elektronische Unterschrift, die von Ihnen oder einer Anwendung mit Hilfe des privaten Schlüssels eines digitalen Zertifikats geleistet wird. Die digitale Signatur auf einem Objekt bietet eine eindeutige elektronische Zuordnung der Identität des Signierers (Eigners des Signiererschlüssels) zum Ursprung des Objekts. Wenn Sie auf ein Objekt mit einer digitalen Signatur zugreifen, können Sie die Objektsignatur prüfen. Hierdurch können Sie feststellen, ob die Objektquelle gültig ist. (Es ist auf diese Weise z. B. möglich festzustellen, ob eine Anwendung, die Sie herunterladen möchten, tatsächlich von einer autorisierten Quelle wie beispielsweise IBM stammt.) Mit Hilfe dieses Prüfprozesses können Sie außerdem feststellen, ob an dem Objekt seit dem Erstellen der Signatur unbefugte Änderungen vorgenommen wurden.

### **Beispiel für die Funktionsweise einer digitalen Signatur**

Ein Softwareentwickler hat eine i5/OS-Anwendung erstellt, die über das Internet verteilt werden soll, da dies ein einfaches und kostengünstiges Verfahren für seine Kunden darstellt. Er ist sich darüber bewusst, dass diese Kunden beim Herunterladen von Programmen aus dem Internet begründete Bedenken haben, da das Problem mit Objekten, die als legale Programme getarnt sind und sich dann als potenziell gefährlich herausstellen (z. B. Viren) immer häufiger auftritt.

Aus diesem Grund entschließt er sich zum digitalen Signieren der Anwendung, damit seine Kunden überprüfen können, dass sein Unternehmen der legitime Absender der Anwendung ist. Er verwendet hierzu den privaten Schlüssel eines digitalen Zertifikats, das er von einer bekannten öffentlichen Zertifizierungsinstanz (CA) abgerufen hat. Nachdem die Anwendung signiert ist, stellt er sie seinen Kunden zum Download zur Verfügung. Das Download-Paket umfasst eine Kopie des digitalen Zertifikats, das zum Signieren des Objekts verwendet wurde. Wenn ein Kunde nun das Anwendungspaket herunterlädt, kann er mit Hilfe des öffentlichen Schlüssels dieses Zertifikats prüfen, ob die Anwendungssignatur gültig ist. Durch diese Vorgehensweise kann der Kunde die Anwendung identifizieren und prüfen sowie sicherstellen, dass der Inhalt des Anwendungsobjekts seit dem Erstellen der Signatur nicht geändert wurde.

#### **Zugehörige Konzepte**

„Zertifizierungsinstanz (CA)“ auf Seite 6

Eine Zertifizierungsinstanz (CA) ist eine anerkannte zentrale Verwaltungsentität, die digitale Zertifikate für Benutzer und Server ausstellen kann.

„Chiffrierung“ auf Seite 10

In diesem Abschnitt sind grundlegende Informationen zur Chiffrierung enthalten. Außerdem erfahren Sie hier, auf welche Weise digitale Zertifikate Verschlüsselungsfunktionen verwenden, um die Sicherheit der verwendeten Systeme zu gewährleisten.

„Öffentliches/privates Schlüsselpaar“

Jedes digitale Zertifikat verfügt über ein Paar zugeordneter Chiffrierschlüssel, das aus einem privaten und einem öffentlichen Schlüssel besteht.

## Öffentliches/privates Schlüsselpaar

Jedes digitale Zertifikat verfügt über ein Paar zugeordneter Chiffrierschlüssel, das aus einem privaten und einem öffentlichen Schlüssel besteht.

**Anmerkung:** Signaturüberprüfungszertifikate bilden eine Ausnahme von dieser Regel und verfügen nur über einen zugeordneten öffentlichen Schlüssel.

Ein öffentlicher Schlüssel gehört zum digitalen Zertifikat des Eigners und kann von jedem Benutzer verwendet werden. Ein privater Schlüssel wird dagegen vom Eigner des Schlüssels sicher verwahrt und steht nur diesem zur Verfügung. Durch diesen eingeschränkten Zugriff wird die Sicherheit der mit Hilfe dieses Schlüssels übertragenen Daten gewährleistet.

Der Eigner eines Zertifikats kann diese Schlüssel verwenden, um die Sicherheitsvorteile der Verschlüsselungsfunktionen, die diese Schlüssel bieten, zu nutzen. Der Zertifikatseigner kann den privaten Schlüssel eines Zertifikats zum "Signieren" und Verschlüsseln von Daten (z. B. Nachrichten, Dokumente und Codeobjekte) verwenden, die zwischen Benutzern und Servern hin- und hergesendet werden. Der Empfänger des signierten Objekts kann den im Zertifikat des Signierers enthaltenen öffentlichen Schlüssel dann zum Entschlüsseln der Signatur verwenden. Derartige digitale Signaturen stellen die Zuverlässigkeit des Objektursprungs sicher und bieten eine Möglichkeit zum Prüfen der Objektintegrität.

### Zugehörige Konzepte

„Digitale Signaturen“ auf Seite 5

Eine digitale Signatur auf einem elektronischen Dokument oder einem anderen Objekt wird mit Hilfe eines bestimmten Chiffrierverfahrens erstellt und entspricht einer persönlichen Unterschrift auf einem schriftlichen Dokument.

„Zertifizierungsinstanz (CA)“

Eine Zertifizierungsinstanz (CA) ist eine anerkannte zentrale Verwaltungsentität, die digitale Zertifikate für Benutzer und Server ausstellen kann.

## Zertifizierungsinstanz (CA)

Eine Zertifizierungsinstanz (CA) ist eine anerkannte zentrale Verwaltungsentität, die digitale Zertifikate für Benutzer und Server ausstellen kann.

Die Anerkennung der Zertifizierungsinstanz bildet die Voraussetzung für die Anerkennung des Zertifikats als gültiger Berechtigungsnachweis. Eine CA verwendet ihren privaten Schlüssel zum Erstellen einer digitalen Signatur auf dem von ihr ausgegebenen Zertifikat, mit der der Ursprung des Zertifikats bestätigt wird. Andere können den öffentlichen Schlüssel des Zertifikats der Zertifizierungsinstanz zum Überprüfen der Authentizität der Zertifikate verwenden, die von der Zertifizierungsinstanz ausgestellt und signiert werden.

Bei der Zertifizierungsinstanz kann es sich entweder um eine öffentliche, kommerzielle Entität wie z. B. VeriSign oder eine private Entität handeln, die von einem Unternehmen für interne Zwecke benutzt wird. Viele Unternehmen stellen kommerzielle CA-Services für Internet-Benutzer zur Verfügung. Digital Certificate Manager (DCM) ermöglicht die Verwaltung von Zertifikaten, die von öffentlichen und privaten Zertifizierungsinstanzen (CAs) ausgestellt wurden.

Darüber hinaus können Sie DCM verwenden, um eine eigene, private lokale Zertifizierungsinstanz zu betreiben, mit der Sie private Zertifikate für Systeme und Benutzer ausstellen können. Wird ein Benutzerzertifikat von der lokalen Zertifizierungsinstanz ausgestellt, ordnet DCM das Zertifikat automatisch dem Profil des Benutzers auf dem iSeries-System oder einer anderen Benutzeridentität zu. Ob DCM das Zertifikat einem Benutzerprofil oder einer anderen Benutzeridentität des Benutzers zuordnet, hängt davon ab, ob DCM für die Verwendung von EIM (Enterprise Identity Mapping) konfiguriert wurde. Damit wird sichergestellt, dass die Zugriffsberechtigungen für das Zertifikat mit denen des Benutzerprofils für den Eigner übereinstimmen.

### **Trusted Root-Status**

Der Terminus 'Trusted Root' bezieht sich auf eine spezielle Kennzeichnung, die einem Zertifikat der Zertifizierungsinstanz zugeordnet wird. Diese Kennzeichnung als Trusted Root ermöglicht dem Browser oder einer anderen Anwendung, von der Zertifizierungsinstanz (CA) ausgestellte Zertifikate zu authentifizieren und zu akzeptieren.

Wird ein Zertifikat der Zertifizierungsinstanz in den Browser heruntergeladen, kann dieses als Trusted Root dediziert werden. Andere Anwendungen, die den Einsatz von Zertifikaten unterstützen, müssen ebenfalls so konfiguriert werden, dass sie eine Zertifizierungsinstanz anerkennen, bevor sie die von einer bestimmten CA ausgestellten Zertifikate authentifizieren und anerkennen können.

Sie können DCM zum Aktivieren bzw. Inaktivieren des Anerkennungsstatus für ein Zertifikat der Zertifizierungsinstanz (CA) verwenden. Wenn Sie ein Zertifikat der Zertifizierungsinstanz aktivieren, können Sie angeben, dass Anwendungen dieses zum Authentifizieren und Akzeptieren von Zertifikaten verwenden, die von der Zertifizierungsinstanz ausgestellt wurden. Wenn Sie ein Zertifikat der Zertifizierungsinstanz inaktivieren, können Sie nicht mehr angeben, dass Anwendungen dieses verwenden, um die von der CA ausgestellten Zertifikate zu authentifizieren und zu akzeptieren.

### **Richtliniendaten der Zertifizierungsinstanz (CA)**

Beim Erstellen einer lokalen Zertifizierungsinstanz (CA) mit Digital Certificate Manager können Sie die Richtliniendaten für die lokale Zertifizierungsinstanz angeben. Die Richtliniendaten für eine lokale Zertifizierungsinstanz beschreiben die einer Zertifizierungsinstanz erteilten Signaturberechtigungen. Sie legen folgende Kriterien fest:

- Ob die lokale Zertifizierungsinstanz Benutzerzertifikate ausstellen und signieren kann.
- Wie lange die durch die lokale Zertifizierungsinstanz ausgestellten Zertifikate gültig sind.

#### **Zugehörige Konzepte**

„Digitale Signaturen“ auf Seite 5

Eine digitale Signatur auf einem elektronischen Dokument oder einem anderen Objekt wird mit Hilfe eines bestimmten Chiffrierverfahrens erstellt und entspricht einer persönlichen Unterschrift auf einem schriftlichen Dokument.

„Öffentliches/privates Schlüsselpaar“ auf Seite 6

Jedes digitale Zertifikat verfügt über ein Paar zugeordneter Chiffrierschlüssel, das aus einem privaten und einem öffentlichen Schlüssel besteht.

### **CRL-Verteilungspunkte**

Bei einer Liste der entzogenen Zertifikate (CRL = Certificate Revocation List) handelt es sich um eine Datei, in der alle ungültigen und widerrufenen Zertifikate einer bestimmten Zertifizierungsinstanz (CA) aufgeführt sind.

Diese Listen werden von den Zertifizierungsinstanzen in periodischen Zeitabständen aktualisiert und anderen für die Veröffentlichung in LDAP-Verzeichnissen (LDAP = Lightweight Directory Access Protocol) zur Verfügung gestellt. Einige Zertifizierungsinstanzen wie z. B. SSH in Finnland veröffentlichen die CRLs selbst in LDAP-Verzeichnissen, auf die direkt zugegriffen werden kann. Wenn eine Zertifizierungs-

instanz eigene CRLs veröffentlicht, ist das im Zertifikat an einer Erweiterung für einen CRL-Verteilungspunkt zu erkennen. Dieser wird in Form einer URI-Angabe (URI = Uniform Resource Identifier) definiert.

Digital Certificate Manager (DCM) ermöglicht das Definieren und Verwalten von Informationen zu CRL-Verteilungspunkten. Hierdurch kann die Verwendung strengerer Authentifizierungskriterien für Zertifikate gewährleistet werden, die verwendet oder als Identitätsnachweis von anderen akzeptiert werden. Die Definition des CRL-Verteilungspunktes beschreibt die Position des sowie Zugriffsinformationen für den LDAP-Server (LDAP = Lightweight Directory Access Protocol), auf dem die Liste der entzogenen Zertifikate (CRL) gespeichert ist.

- | Zur Herstellung einer Verbindung zu einem LDAP-Server müssen Sie einen DN und ein Kennwort angeben, um zu verhindern, dass das System eine anonyme Bindung zu einem LDAP-Server herstellt. Bei einer anonymen Bindung zum Server wird nicht mit den Berechtigungen gearbeitet, die für den Zugriff auf ein "kritisches" Attribut wie z. B. die Liste der entzogenen Zertifikate erforderlich ist. In diesem Fall kann DCM ein widerrufenes Zertifikat als gültig einstufen, weil der korrekte Status des Zertifikats nicht aus der Liste der entzogenen Zertifikate abgerufen werden kann. Wenn Sie über eine anonyme Bindung auf den LDAP-Server zugreifen wollen, müssen Sie das Directory-Server-Webverwaltungstool verwenden und dort die Task "Schemadateien verwalten" auswählen, um die Sicherheitsklasse (Zugriffsklasse) der Attribute **certificateRevocationList** und **authorityRevocationList** von "kritisch" in "normal" zu ändern.

Anwendungen, die eine Zertifikatsauthentifizierung durchführen, können für eine bestimmte Zertifizierungsinstanz auf den CRL-Verteilungspunkt zugreifen (sofern dieser definiert wurde), um sicherzustellen, dass die CA ein bestimmtes Zertifikat nicht widerrufen hat. DCM ermöglicht das Definieren und Verwalten der Informationen zum CRL-Verteilungspunkt, die von Anwendungen zur Ausführung der CRL-Verarbeitung während der Zertifikatsauthentifizierung benötigt werden. Die folgenden Anwendungen und Prozesse führen bei der Zertifikatsauthentifizierung z. B. eine CRL-Verarbeitung durch: VPN IKE-Server (VPN IKE = Virtual Private Networking Internet Key Exchange), Anwendungen mit SSL-Unterstützung (SSL = Secure Sockets Layer) und der Objektsignierprozess. Wird ein CRL-Verteilungspunkt definiert und einem CA-Zertifikat zugeordnet, führt DCM als Teil des Prüfprozesses für die von der angegebenen Zertifizierungsinstanz ausgestellten Zertifikate auch die CRL-Verarbeitung aus.

#### **Zugehörige Konzepte**

„Zertifikate und Anwendungen überprüfen“ auf Seite 80

Digital Certificate Manager (DCM) kann zum Überprüfen individueller Zertifikate oder der Anwendungen benutzt werden, die diese Zertifikate verwenden. Die Liste der von DCM geprüften Kriterien kann abhängig davon, ob Zertifikate oder Anwendungen geprüft werden, leicht variieren.

#### **Zugehörige Tasks**

„CRL-Verteilungspunkte verwalten“ auf Seite 81

Digital Certificate Manager (DCM) ermöglicht Ihnen das Definieren und Verwalten der Informationen zu den CRL-Verteilungspunkten (CRL = Certificate Revocation List; Liste der entzogenen Zertifikate), die von einer Zertifizierungsinstanz (CA) bei der Gültigkeitsprüfung von Zertifikaten verwendet werden.

## **Zertifikatsspeicher**

Ein Zertifikatsspeicher ist eine spezielle Schlüsseldatenbankdatei, die Digital Certificate Manager (DCM) verwendet, um digitale Zertifikate zu speichern.

Der Zertifikatsspeicher enthält den privaten Schlüssel des Zertifikats, wenn dieser nicht in einem IBM Verschlüsselungskoprocessor gespeichert wird. DCM ermöglicht es Ihnen, verschiedene Zertifikatsspeichertypen zu erstellen und zu verwalten. DCM steuert den Zugriff auf Zertifikatsspeicher über Kennwörter und darüber hinaus den Zugriff auf das IFS-Verzeichnis und die Dateien, aus denen sich der Zertifikatsspeicher zusammensetzt.

Zertifikatsspeicher werden auf der Basis der darin enthaltenen Zertifikatstypen klassifiziert. Die Verwaltungstasks, die Sie für jeden Zertifikatsspeicher ausführen können, variieren je nach dem im betreffenden Zertifikatsspeicher enthaltenen Zertifikatstyp. DCM bietet folgende vordefinierte Zertifikatsspeicher, die erstellt und verwaltet werden können:

#### **Lokale Zertifizierungsinstanz (CA)**

DCM verwendet diesen Zertifikatsspeicher zum Speichern des Zertifikats der lokalen Zertifizierungsinstanz sowie des zugehörigen privaten Schlüssels, wenn Sie eine lokale Zertifizierungsinstanz erstellen. Sie können das in diesem Zertifikatsspeicher enthaltene Zertifikat verwenden, um Zertifikate zu signieren, die Sie von der lokalen Zertifizierungsinstanz ausstellen lassen. Wenn die lokale Zertifizierungsinstanz ein Zertifikat ausstellt, speichert DCM eine Kopie des Zertifikats der Zertifizierungsinstanz (ohne den privaten Schlüssel) zum Zweck der Authentifizierung im entsprechenden Zertifikatsspeicher (z. B. \*SYSTEM). Anwendungen verwenden Zertifikate der Zertifizierungsinstanz, um den Ursprung von Zertifikaten zu bestätigen, die sie als Teil der SSL-Vereinbarung überprüfen müssen, damit Berechtigungen für Ressourcen erteilt werden können.

#### **\*SYSTEM**

DCM stellt diesen Zertifikatsspeicher für die Verwaltung von Server- oder Client-Zertifikaten zur Verfügung, die von Anwendungen verwendet werden, um an SSL-Kommunikationssitzungen teilzunehmen (SSL = Secure Sockets Layer). IBM iSeries -Anwendungen (sowie die Anwendungen vieler anderer Softwarehersteller) wurden so entwickelt, dass sie nur die im Zertifikatsspeicher \*SYSTEM enthaltenen Zertifikate verwenden. Wenn Sie DCM zum Erstellen einer lokalen Zertifizierungsinstanz verwenden, wird dieser Zertifikatsspeicher von Digital Certificate Manager im Rahmen des Erstellungsprozesses generiert. Wenn Sie die von Ihren Server- und Client-Anwendungen zu benutzenden Zertifikate von einer öffentlichen Zertifizierungsinstanz wie z. B. VeriSign abrufen möchten, müssen Sie diesen Zertifikatsspeicher selbst erstellen.

#### **\*OBJECTSIGNING**

DCM stellt diesen Zertifikatsspeicher für die Verwaltung von Zertifikaten zur Verfügung, die Sie zum digitalen Signieren von Objekten verwenden. Mit den Tasks dieses Zertifikatsspeichers können Sie außerdem digitale Signaturen auf Objekten erstellen sowie Objektsignaturen anzeigen und überprüfen. Wenn Sie DCM zum Erstellen einer lokalen Zertifizierungsinstanz verwenden, wird dieser Zertifikatsspeicher von Digital Certificate Manager im Rahmen des Erstellungsprozesses generiert. Wenn Sie die zum Signieren von Objekten benötigten Zertifikate von einer öffentlichen Zertifizierungsinstanz wie z. B. VeriSign abrufen möchten, müssen Sie diesen Zertifikatsspeicher selbst erstellen.

#### **\*SIGNATUREVERIFICATION**

DCM stellt diesen Zertifikatsspeicher für die Verwaltung von Zertifikaten zur Verfügung, die Sie zur Überprüfung der Authentizität von digitalen Signaturen auf Objekten verwenden. Zum Überprüfen einer digitalen Signatur muss dieser Zertifikatsspeicher eine Kopie des Zertifikats enthalten, das zum Signieren des Objekts verwendet wurde. Der Zertifikatsspeicher muss ferner eine Kopie des Zertifikats der Zertifizierungsinstanz enthalten, die das Objektsignierzertifikat ausgegeben hat. Diese Zertifikate können abgerufen werden, indem Objektsignierzertifikate auf dem aktuellen System in den Zertifikatsspeicher exportiert oder indem die vom Objektsignierer empfangenen Zertifikate importiert werden.

#### **Speicher für andere Systemzertifikate**

Dieser Zertifikatsspeicher stellt eine alternative Speichermöglichkeit für Server- oder Client-Zertifikate zur Verfügung, die Sie für SSL-Sitzungen verwenden. Speicher für andere Systemzertifikate sind benutzerdefinierte sekundäre Zertifikatsspeicher für SSL-Zertifikate. Mit der Auswahl "Speicher für andere Systemzertifikate" können Sie Zertifikate für Anwendungen verwalten, die von Ihnen oder anderen Benutzern geschrieben wurden und die mit Hilfe der API SSL\_Init auf ein Zertifikat zugreifen und dieses zum Aufbauen einer SSL-Sitzung verwenden. Mit Hilfe dieser API kann eine Anwendung für einen Zertifikatsspeicher an Stelle des von Ihnen speziell angegebenen Zertifikats das Standardzertifikat verwenden. Im Allgemeinen verwenden Sie diesen Zertifikatsspeicher bei der Migration von Zertifikaten von einem früheren DCM-Release oder bei der Erstellung einer speziellen Untergruppe von Zertifikaten für die Verwendung mit SSL.

**Anmerkung:** Wenn auf Ihrem System ein IBM Verschlüsselungskoprozessor installiert ist, können Sie weitere Auswahlmöglichkeiten für die Speicherung des privaten Schlüssels für Ihre Zertifikate angeben. (Eine Ausnahme bilden hierbei allerdings Objektsignierzertifikate.) Sie haben die Wahl, entweder den privaten Schlüssel auf dem Koprozessor selbst zu speichern, oder den Koprozessor zu verwenden, um den privaten Schlüssel zu verschlüsseln und ihn statt in einem Zertifikatsspeicher in einer speziellen Schlüsseldatei zu speichern.

DCM steuert den Zugriff auf Zertifikate mittels Kennwörtern. Darüber hinaus verwaltet DCM die Zugriffssteuerung über das IFS-Verzeichnis (IFS = Integrated File System) und die Dateien, aus denen sich der Zertifikatsspeicher zusammensetzt. Die Zertifikatsspeicher Lokale Zertifizierungsinstanz (CA), \*SYSTEM, \*OBJECTSIGNING und \*SIGNATUREVERIFICATION müssen in den entsprechenden Pfaden im IFS gespeichert sein; Speicher für andere Systemzertifikate können an beliebiger Stelle im IFS vorhanden sein.

### Zugehörige Konzepte

„Typen digitaler Zertifikate“ auf Seite 33

In diesen Informationen wird erläutert, welche unterschiedlichen Typen digitaler Zertifikate unterstützt werden und wie diese in Digital Certificate Manager (DCM) eingesetzt werden können.

## Chiffrierung

In diesem Abschnitt sind grundlegende Informationen zur Chiffrierung enthalten. Außerdem erfahren Sie hier, auf welche Weise digitale Zertifikate Verschlüsselungsfunktionen verwenden, um die Sicherheit der verwendeten Systeme zu gewährleisten.

Die Chiffrierung bezeichnet die Wissenschaft, die sich mit der Gewährleistung der Datensicherheit befasst. Sie ermöglicht die Speicherung von Informationen und die Übertragung von Daten an andere Personen, ohne dass Unbefugte die gespeicherten Informationen lesen oder die Kommunikation mit diesen Personen verstehen können. Durch eine Verschlüsselung wird der lesbare Text in unlesbare Daten (sog. Ciphertext) umgesetzt. Durch die Entschlüsselung wird aus den unlesbaren Daten wieder der ursprüngliche, lesbare Text hergestellt. Für beide Prozesse werden mathematische Formeln oder Algorithmen und eine geheime Datenfolge (der so genannte Schlüssel) benötigt.

Es gibt zwei Arten der Chiffrierung:

- Für die **(symmetrische) Chiffrierung mit gemeinsamen, geheimen Schlüsseln** wird ein geheimer Schlüssel gemeinsam von zwei miteinander kommunizierenden Teilnehmern verwendet. Für die Verschlüsselung und Entschlüsselung wird derselbe Schlüssel benutzt.
- Für die **(asymmetrische) Chiffrierung mit öffentlichen Schlüsseln** werden für Verschlüsselung und Entschlüsselung verschiedene Schlüssel verwendet. Ein Teilnehmer hat ein Schlüsselpaar, das aus einem öffentlichen und einem privaten Schlüssel besteht. Der öffentliche Schlüssel wird (normalerweise über ein digitales Zertifikat) frei weitergegeben. Der private Schlüssel hingegen wird vom Eigner sicher verwahrt und geheim gehalten. Die beiden Schlüssel stehen in einer mathematischen Beziehung zueinander, es ist jedoch nahezu unmöglich, den privaten Schlüssel aus dem öffentlichen Schlüssel abzuleiten. Ein Objekt wie z. B. eine Nachricht, die mit einem öffentlichen Schlüssel verschlüsselt wurde, kann nur mit dem zugeordneten privaten Schlüssel entschlüsselt werden. Wechselweise kann auch ein Server oder Benutzer einen privaten Schlüssel verwenden, um ein Objekt zu "signieren". Der Empfänger kann dann mit dem zugehörigen öffentlichen Schlüssel die digitale Signatur entschlüsseln, um den Ursprung sowie die Integrität des Objekts zu überprüfen.

### Zugehörige Konzepte

„Digitale Signaturen“ auf Seite 5

Eine digitale Signatur auf einem elektronischen Dokument oder einem anderen Objekt wird mit Hilfe eines bestimmten Chiffrierverfahrens erstellt und entspricht einer persönlichen Unterschrift auf einem schriftlichen Dokument.

„Secure Sockets Layer (SSL)“ auf Seite 11

Der ursprünglich von Netscape entwickelte SSL-Standard hat sich zum Branchenstandard für die Sitzungsverschlüsselung zwischen Clients und Servern entwickelt.



## IBM Verschlüsselungskoprocessoren für iSeries

Dieser Verschlüsselungskoprocessor stellt bewährte kryptografische Services zur Gewährleistung der Vertraulichkeit und der Integrität bereit, die Ihnen das Entwickeln sicherer e-business Anwendungen ermöglichen.

Ein IBM Verschlüsselungskoprocessor für iSeries ergänzt Ihr System durch sehr sichere kryptografische Verarbeitungsfunktionen. Wenn auf Ihrem System ein Verschlüsselungskoprocessor installiert und aktiviert ist, können Sie diesen zum Bereitstellen sichererer Speichermöglichkeiten für die privaten Schlüssel Ihrer Zertifikate verwenden.

Sie können den Verschlüsselungskoprocessor zum Speichern des privaten Schlüssels eines Server- oder Client-Zertifikats sowie eines Zertifikats einer lokalen Zertifizierungsinstanz (CA) verwenden. Der Verschlüsselungskoprocessor kann allerdings nicht verwendet werden, um den privaten Schlüssel eines Benutzerzertifikats zu speichern, weil dieser Schlüssel auf dem System des Benutzers gespeichert werden muss. Auch zum Speichern des privaten Schlüssels für ein Objektsignierzertifikat kann er nicht benutzt werden.

Sie können den privaten Schlüssel eines Zertifikats entweder direkt im Verschlüsselungskoprocessor speichern, oder den Hauptschlüssel dieses Koprocessors verwenden, um den Schlüssel zu verschlüsseln und in einer speziellen Schlüsseldatei zu speichern. Sie können diese Auswahlmöglichkeiten für Schlüsselspeicher im Rahmen der Zertifikaterstellung oder -verlängerung auswählen. Wenn Sie den Koprocessor zum Speichern eines privaten Zertifikatsschlüssels verwenden, können Sie die Einheitszuordnung des Koprocessors für diesen Schlüssel ändern.

Wenn Sie den Verschlüsselungskoprocessor zur Speicherung von privaten Schlüsseln verwenden wollen, müssen Sie sicherstellen, dass der Koprocessor vor dem Einsatz von Digital Certificate Manager (DCM) aktiviert wird. Andernfalls kann DCM die Auswahl zur Angabe der Speicherposition bei der Zertifikaterstellung oder -verlängerung nicht bereitstellen.

### Zugehörige Konzepte

„Zertifikatsschlüssel auf einem IBM Verschlüsselungskoprocessor speichern“ auf Seite 83

Dieses Thema enthält Informationen zum Einsatz eines installierten Koprocessors zur Verbesserung der Sicherheit der gespeicherten privaten Schlüssel Ihrer Zertifikate.

## Secure Sockets Layer (SSL)

Der ursprünglich von Netscape entwickelte SSL-Standard hat sich zum Branchenstandard für die Sitzungsverschlüsselung zwischen Clients und Servern entwickelt.

SSL verwendet die asymmetrische Chiffrierung mit öffentlichen Schlüsseln, um die Sitzung zwischen Server und Client zu verschlüsseln. Die Client- und die Serveranwendung vereinbaren diesen Sitzungsschlüssel während des Austauschs digitaler Zertifikate. Die Gültigkeit des Schlüssels läuft automatisch nach 24 Stunden ab und für jede Serververbindung und jeden Client wird vom SSL-Prozess ein anderer Schlüssel erstellt. Deshalb können auch unbefugte Benutzer, selbst wenn sie einen Sitzungsschlüssel abfangen und entschlüsseln (was sehr unwahrscheinlich ist), den Schlüssel nicht für spätere Sitzungen erneut verwenden.

### Zugehörige Konzepte

„Chiffrierung“ auf Seite 10

In diesem Abschnitt sind grundlegende Informationen zur Chiffrierung enthalten. Außerdem erfahren Sie hier, auf welche Weise digitale Zertifikate Verschlüsselungsfunktionen verwenden, um die Sicherheit der verwendeten Systeme zu gewährleisten.

„Typen digitaler Zertifikate“ auf Seite 33

In diesen Informationen wird erläutert, welche unterschiedlichen Typen digitaler Zertifikate unterstützt werden und wie diese in Digital Certificate Manager (DCM) eingesetzt werden können.

## Anwendungsdefinitionen

Unter diesem Thema erfahren Sie mehr zu DCM-Anwendungsdefinitionen und wie diese für die SSL-Konfiguration und zum Signieren von Objekten eingesetzt werden können.

Unter Digital Certificate Manager (DCM) können Sie zwei verschiedene Anwendungsdefinitionstypen verwalten:

- Client- oder Serveranwendungsdefinitionen, die mit SSL-Kommunikationssitzungen (SSL = Secure Sockets Layer) arbeiten.
- Objektsignieranwendungsdefinitionen zum Signieren von Objekten, um die Objektintegrität sicherzustellen.

Wenn Sie unter DCM mit SSL-Anwendungsdefinitionen und den zugehörigen Zertifikaten arbeiten wollen, muss die Anwendung in DCM zuerst als Anwendungsdefinition registriert werden, um ihr eine eindeutige Anwendungs-ID zuzuordnen. Anwendungsentwickler registrieren Anwendungen mit SSL-Unterstützung mit Hilfe einer API (QSYRGAP, QsyRegisterAppForCertUse), um die Anwendungs-ID in DCM automatisch zu erstellen. Alle IBM iSeries-Anwendungen mit SSL-Unterstützung sind in DCM registriert, so dass Sie DCM auf einfache Weise für die Zuordnung eines Zertifikats benutzen können, um die Herstellung einer SSL-Sitzung zu ermöglichen. Bei selbst geschriebenen oder gekauften Anwendungen können Sie ebenfalls eine Anwendungsdefinition definieren und die entsprechende Anwendungs-ID in DCM erstellen. Sie müssen im Zertifikatsspeicher \*SYSTEM arbeiten, um eine SSL-Anwendungsdefinition für eine Client- oder eine Serveranwendung zu erstellen.

Um ein Zertifikat zum Signieren von Objekten zu verwenden, müssen Sie zuerst eine Anwendung definieren, die mit dem Zertifikat benutzt werden soll. Anders als eine SSL-Anwendungsdefinition beschreibt eine Objektsignieranwendung keine konkrete Anwendung. Stattdessen sollte die von Ihnen erstellte Anwendungsdefinition zur Beschreibung des Typs oder der Gruppe von Objekten dienen, die signiert werden sollen. Sie müssen im Zertifikatsspeicher \*OBJECTSIGNING arbeiten, um die Definition einer Objektsignieranwendung zu erstellen.

### Zugehörige Konzepte

„Anwendungen in DCM verwalten“ auf Seite 76

Dieses Thema enthält Informationen zum Erstellen von Anwendungsdefinitionen und dazu, wie die Zertifikatzuordnung einer Anwendung verwaltet werden kann. Außerdem wird hier erklärt, wie CA-Anerkennungslisten definiert werden, die von Anwendungen zum Akzeptieren von Zertifikaten für die Client-Authentifizierung benutzt werden.

### Zugehörige Tasks

„Anwendungsdefinition erstellen“ auf Seite 76

In diesem Abschnitt werden die beiden verschiedenen Anwendungstypen beschrieben, die Sie definieren und mit denen Sie arbeiten können.

## Gültigkeitsprüfung

Digital Certificate Manager (DCM) stellt Tasks zur Verfügung, mit deren Hilfe Sie ein Zertifikat oder eine Anwendung überprüfen und dadurch feststellen können, ob eine Reihe von erforderlichen Eigenschaften erfüllt ist.

### Gültigkeitsprüfung für Zertifikate

Beim Überprüfen eines Zertifikats prüft Digital Certificate Manager (DCM) eine Reihe von Zertifikatsmerkmalen, um die Authentizität und Gültigkeit des Zertifikats sicherzustellen. Die Überprüfung eines Zertifikats gewährleistet, dass die Wahrscheinlichkeit, dass Anwendungen, die das Zertifikat für die gesicherte Kommunikation oder zum Signieren von Objekten verwenden, bei dessen Einsatz auf Probleme stoßen, auf ein Minimum reduziert werden kann.

Im Rahmen des Überprüfungsprozesses stellt DCM fest, ob das ausgewählte Zertifikat noch gültig ist. Ist für die ausstellende CA ein CRL-Verteilungspunkt vorhanden, wird außerdem geprüft, ob das Zertifikat in der Liste der entzogenen Zertifikate (CRL) nicht als widerrufen aufgeführt ist.

| Wenn Sie die LDAP-Zuordnung (LDAP = Lightweight Directory Access Protocol) so konfigurieren, dass  
| eine Liste der entzogenen Zertifikate verwendet wird, überprüft DCM diese Liste bei der Gültigkeits-  
| prüfung des Zertifikats. Auf diese Weise kann sichergestellt werden, dass das Zertifikat nicht in der Liste  
| der entzogenen Zertifikate enthalten ist. Damit während der Gültigkeitsprüfung die Liste der entzogenen  
| Zertifikate korrekt überprüft werden kann, muss im Verzeichnisserver (LDAP-Server), der zur Ausfüh-  
| rung der LDAP-Zuordnung konfiguriert wurde, die richtige Liste der entzogenen Zertifikate enthalten  
| sein. Andernfalls schlägt die Gültigkeitsprüfung des Zertifikats fehl. Sie müssen einen DN für die  
| Bindung und ein Kennwort angeben, um zu verhindern, dass ein Zertifikat validiert wird, das widerrufen  
| wurde. Außerdem ist zu beachten, dass das System eine anonyme Bindung zum LDAP-Server herstellt,  
| wenn Sie bei der Konfiguration der LDAP-Zuordnung keinen DN und kein Kennwort angeben. Bei ano-  
| nymen Bindungen zum LDAP-Server sind nicht die erforderlichen Berechtigungen vorhanden, die für  
| den Zugriff auf "kritische" Attribute wie die Liste der entzogenen Zertifikate benötigt werden. In diesem  
| Fall kann DCM ein widerrufenes Zertifikat als gültig einstufen, weil der korrekte Status des Zertifikats  
| nicht aus der Liste der entzogenen Zertifikate abgerufen werden kann. Wenn Sie über eine anonyme Bin-  
| dung auf den LDAP-Server zugreifen wollen, müssen Sie das Directory-Server-Webverwaltungstool ver-  
| wenden und dort die Task "Schemadateien verwalten" auswählen, um die Sicherheitsklasse (Zugriffs-  
| klasse) der Attribute **certificateRevocationList** und **authorityRevocationList** von "kritisch" in "normal" zu  
| ändern.

DCM prüft außerdem, ob sich das Zertifikat der Zertifizierungsinstanz für die ausstellende CA im aktuel-  
len Zertifikatsspeicher befindet und ob das Zertifikat der Zertifizierungsinstanz als anerkannt markiert ist.  
Wenn für das Zertifikat ein privater Schlüssel definiert wurde (z. B. für Server-, Client- oder Objektsig-  
nierzertifikate), prüft DCM auch das öffentliche/private Schlüsselpaar, um sicherzustellen, dass dieses  
übereinstimmt. DCM verschlüsselt hierzu die Daten mit dem öffentlichen Schlüssel und prüft dann, ob  
die Daten mit dem privaten Schlüssel wieder entschlüsselt werden können.

## Gültigkeitsprüfung für Anwendungen

Beim Überprüfen einer Anwendung stellt Digital Certificate Manager (DCM) fest, ob eine Zertifikatszu-  
ordnung für die Anwendung definiert wurde und ob dieses Zertifikat gültig ist. Darüber hinaus stellt  
DCM sicher, dass bei Anwendungen, die für die Verwendung einer CA-Anerkennungsliste konfiguriert  
wurden, diese Anerkennungsliste mindestens ein Zertifikat der Zertifizierungsinstanz enthält. Anschlie-  
ßend prüft DCM, ob die Zertifikate der Zertifizierungsinstanz in der CA-Anerkennungsliste der Anwen-  
dung gültig sind. Wenn in der Anwendungsdefinition angegeben ist, dass die CRL-Verarbeitung ausge-  
führt wird und dass ein definierter CRL-Verteilungspunkt für die Zertifizierungsinstanz (CA) definiert ist,  
überprüft DCM darüber hinaus im Rahmen des Überprüfungsprozesses auch die Liste der entzogenen  
Zertifikate (CRL).

Die Überprüfung der Gültigkeit einer Anwendung kann zur Feststellung möglicher Probleme beitragen,  
die in einer Anwendung bei der Ausführung einer Funktion auftreten können, für die Zertifikate erfor-  
derlich sind. Solche Probleme können dazu führen, dass die betroffene Anwendung entweder nicht an  
einer SSL-Sitzung (SSL = Secure Sockets Layer) teilnehmen oder keine Objektsignaturen ausstellen kann.

### Zugehörige Konzepte

„Zertifikate und Anwendungen überprüfen“ auf Seite 80

Digital Certificate Manager (DCM) kann zum Überprüfen individueller Zertifikate oder der Anwen-  
dungen benutzt werden, die diese Zertifikate verwenden. Die Liste der von DCM geprüften Kriterien  
kann abhängig davon, ob Zertifikate oder Anwendungen geprüft werden, leicht variieren.

---

## DCM-Szenarios

In diesen Informationen finden Sie zwei Szenarios, in denen typische Situationen für die Implementierung von Zertifikaten schematisch dargestellt werden. Mit Hilfe dieser Szenarios können Sie die eigene Zertifikatsimplementierung im Rahmen Ihrer iSeries-Sicherheitsrichtlinien einfacher planen. Jedes Szenario umfasst darüber hinaus alle erforderlichen Konfigurationsschritte, die zum Implementieren des jeweiligen Szenarios ausgeführt werden müssen.

Digital Certificate Manager und die Unterstützungsfunktion für digitale Zertifikate Ihres iSeries-Systems ermöglichen Ihnen den Einsatz von Zertifikaten zur Verbesserung verschiedener Aspekte Ihrer Sicherheitsrichtlinien. Die Art und Weise des Einsatzes dieser digitalen Zertifikate kann abhängig von Ihren individuellen Unternehmenszielen und den geltenden Sicherheitsanforderungen variieren.

Durch die Verwendung digitaler Zertifikate wird die Sicherheit in verschiedener Hinsicht wesentlich verbessert. Digitale Zertifikate ermöglichen Ihnen über Secure Sockets Layer (SSL) den gesicherten Zugriff auf Websites und andere Internet-Services. Darüber hinaus können digitale Zertifikate auch zum Konfigurieren von VPN-Verbindungen (VPN = Virtual Private Network) benutzt werden. Der Schlüssel eines Zertifikats kann zum digitalen Signieren oder zum Prüfen der digitalen Signatur von Objekten verwendet werden, um die Authentizität dieser Objekte sicherzustellen. Derartige digitale Signaturen belegen den Ursprung eines Objekts und schützen dessen Integrität.

Die Systemsicherheit kann weiter verbessert werden, wenn Sie zur Authentifizierung und Sitzungsberechtigung zwischen Servern und Benutzern an Stelle von Benutzernamen und Kennwörtern ebenfalls digitale Zertifikate verwenden. DCM kann darüber hinaus abhängig von der gewählten Konfiguration für die Zuordnung eines Benutzerzertifikats zum entsprechenden iSeries-Benutzerprofil oder zu einer EIM-Kennung (EIM = Enterprise Identity Mapping) verwendet werden. Das Zertifikat verfügt dann über die gleichen Berechtigungen wie das zugeordnete Benutzerprofil.

Die Entscheidung über die Art des Einsatzes von Zertifikaten kann schwierig sein und hängt von einer Vielzahl verschiedener Faktoren ab. Die im vorliegenden Abschnitt bereitgestellten Szenarios beschreiben die wichtigsten Sicherheitszielsetzungen für die gesicherte Datenübertragung digitaler Zertifikate in verschiedenen prototypischen Unternehmensumfeldern. Jedes dieser Szenarios beschreibt darüber hinaus alle erforderlichen System- und Softwarevoraussetzungen und sämtliche Konfigurations-Tasks, die zur Ausführung des jeweiligen Szenarios benötigt werden.

### Zugehörige Informationen

Object Signing Scenarios

## Szenario: Zertifikate für die externe Authentifizierung verwenden

Dieses Szenario beschreibt, wann und wie Zertifikate als Authentifizierungsverfahren zum Schutz und zur Eingrenzung des Zugriffs öffentlicher Benutzer auf öffentliche bzw. Extranet-Ressourcen und -Anwendungen eingesetzt werden können.

### Situation:

Sie arbeiten für das Versicherungsunternehmen MyCo., Inc. und sind für die Verwaltung verschiedener Anwendungen auf den Intra- und Extranet-Sites Ihres Unternehmens verantwortlich. Bei einer der Anwendungen, die in Ihrem Verantwortungsbereich liegen, handelt es sich um eine Prämienkalkulationsanwendung, mit der Hunderte von unabhängigen Versicherungsagenten entsprechende Kostenschätzungen für ihre Kunden generieren können. Da die von dieser Anwendung bereitgestellten Daten z. T. sensibel sind, wollen Sie sicherstellen, dass nur registrierte Versicherungsagenten sie benutzen können. Darüber hinaus wollen Sie eine sicherere Methode für die Benutzerauthentifizierung für die Anwendung bereitstellen, als dies über die derzeit verwendeten Verfahren für die Zugriffssteuerung über Benutzernamen und zugehörige Kennwörter möglich ist. Sie befürchten außerdem, dass unbefugte Benutzer diese Informationen abfangen könnten, wenn sie über ein ungesichertes Netzwerk übertragen wer-

den. Außerdem besteht immer die Gefahr, dass mehrere Versicherungsagenten diese Informationen gemeinsam verwenden, ohne dass eine entsprechende Berechtigung hierfür vorliegt.

Nach entsprechender Prüfung der Sachverhalte haben Sie entschieden, dass der Einsatz digitaler Zertifikate das benötigte Maß an Sicherheit zur Verfügung stellen kann, den Sie zum Schutz sensibler Daten benötigen, die in diese Anwendung eingegeben und aus dieser abgerufen werden. Die Verwendung von Zertifikaten ermöglicht Ihnen die Benutzung von SSL (Secure Sockets Layer) zum Schutz bei der Übertragung von Preis- und Prämiendaten. Obwohl mittelfristig alle Versicherungsagenten für den Zugriff auf die Anwendung Zertifikate verwenden sollen, wissen Sie, dass Ihr Unternehmen und die zugehörigen Versicherungsagenten eine gewisse Zeit benötigen, um diese Umstellung zu vollziehen. Zusätzlich zum Einsatz der Client-Authentifizierung mit Zertifikaten beabsichtigen Sie, die bislang verwendete Authentifizierungsmethode mit Hilfe von Benutzernamen und Kennwörtern weiterzuverwenden, weil die Vertraulichkeit der sensiblen Daten während der Übertragung mit SSL geschützt werden kann.

Basierend auf dem Anwendungstyp und den zugehörigen Benutzern sowie der für die Zukunft angestrebten Authentifizierung aller Benutzer über Zertifikate entscheiden Sie sich für ein öffentliches Zertifikat einer bekannten Zertifizierungsinstanz (CA), um SSL für die Anwendung zu konfigurieren.

## Vorteile des Szenarios

Die Implementierung dieses Szenarios bietet die folgenden Vorteile:

- Die Verwendung digitaler Zertifikate zum Konfigurieren des SSL-Zugriffs auf die vorhandene Prämienkalkulationsanwendung stellt sicher, dass die zwischen dem Server und dem Client übertragenen Informationen geschützt und vertraulich bleiben.
- Werden digitale Zertifikate bei der Client-Authentifizierung möglichst oft eingesetzt, können autorisierte Benutzer mit größerer Sicherheit identifiziert werden. Auch dort, wo der Einsatz von digitalen Zertifikaten nicht möglich ist, kann die Client-Authentifizierung mit Hilfe von Benutzernamen und Kennwörtern geschützt und über SSL-Sitzungen vertraulich ausgeführt werden, wodurch die Sicherheit bei der Übertragung der sensiblen Daten erhöht werden kann.
- Der Einsatz *öffentlicher* digitaler Zertifikate zur Authentifizierung von Benutzern Ihrer Anwendungen und Daten ist dann sinnvoll, wenn für Sie die folgenden oder ähnliche Bedingungen zutreffen:
  - Ihre Daten und Anwendungen unterliegen unterschiedlichen Sicherheitserfordernissen.
  - Bei Ihren anerkannten Benutzern ist eine hohe Fluktuationsrate zu verzeichnen.
  - Sie stellen öffentliche Zugriffsmöglichkeiten auf Anwendungen und Daten bereit, z. B. auf einer Internet-Website oder in einer Extranet-Anwendung.
  - Sie wollen keine eigene Zertifizierungsinstanz (CA) betreiben, weil verwaltungstechnische Überlegungen wie z. B. eine große Anzahl von externen Benutzern, die auf Ihre Anwendungen und Ressourcen zugreift, gegen diese Lösung sprechen.
- Der Einsatz öffentlicher Zertifikate zum Konfigurieren der Prämienkalkulationsanwendung für die Verwendung von SSL dient im vorliegenden Szenario zur Reduzierung des Aufwands, den Benutzer zur Konfiguration des sicheren Anwendungszugriffs leisten müssen. Die Mehrzahl der Client-Softwareprodukte enthält bereits CA-Zertifikate für die meisten bekannten Zertifizierungsinstanzen.

## Ziele

Im vorliegenden Szenario möchte MyCo., Inc. digitale Zertifikate zum Schutz der Prämienkalkulationsinformationen einsetzen, die die Anwendung für berechtigte öffentliche Benutzer bereitstellt. Das Unternehmen möchte darüber hinaus eine sicherere Methode zur Authentifizierung der Benutzer implementieren, die über eine Zugriffsberechtigung für die Anwendung verfügen.

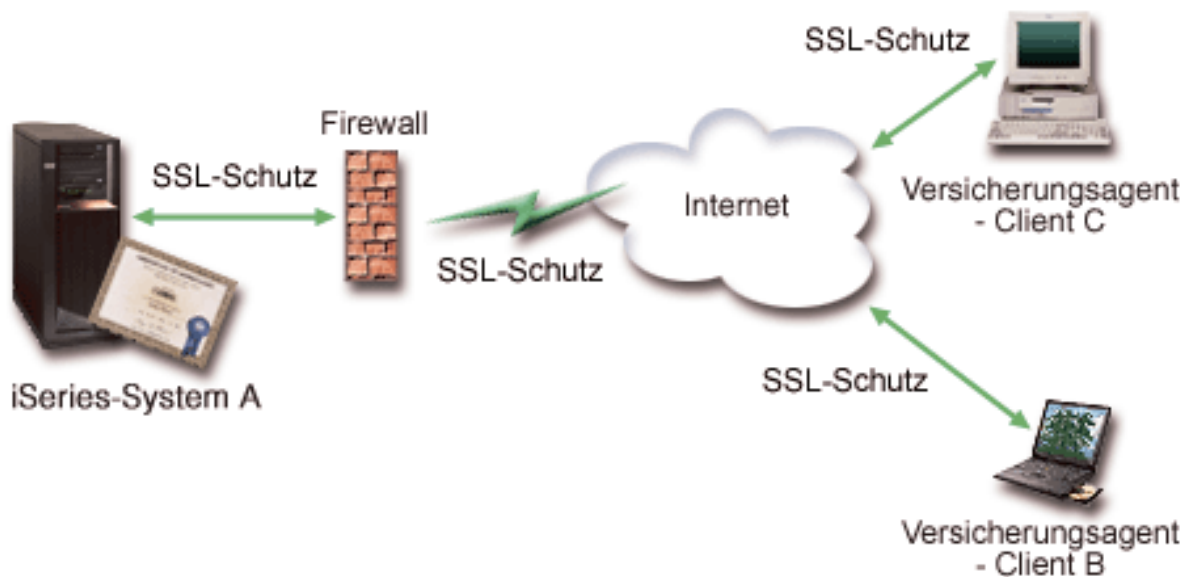
Im vorliegenden Szenario gelten die folgenden Zielsetzungen:

- Die öffentliche Prämienkalkulationsanwendung des Unternehmens muss zum Schutz der Vertraulichkeit der bereitgestellten bzw. empfangenen Daten SSL verwenden.

- Die SSL-Konfiguration muss mit öffentlichen Zertifikaten einer bekannten öffentlichen Internet-Zertifizierungsinstanz (CA) implementiert werden.
- Autorisierte Benutzer müssen einen gültigen Benutzernamen sowie das zugehörige Kennwort angeben, um im SSL-Modus auf die Anwendung zuzugreifen. Die autorisierten Benutzer müssen in der Lage sein, sich mit einer der beiden nachfolgend beschriebenen, gesicherten Methoden zu authentifizieren, um Zugriff auf die gewünschte Anwendung zu erhalten. Die Versicherungsagenten müssen entweder ein öffentliches digitales Zertifikat einer bekannten Zertifizierungsinstanz (CA) oder einen gültigen Benutzernamen sowie das zugehörige Kennwort angeben, wenn kein Zertifikat verfügbar ist.

## Details

In der folgenden Abbildung wird die Netzwerkkonfiguration für dieses Szenario dargestellt:



Die Abbildung stellt die folgenden Informationen zur Situation im vorliegenden Szenario dar:

### Öffentlicher Unternehmensserver - iSeries A

- iSeries A dient als Host für die Prämienkalkulationsanwendung des Unternehmens.
- iSeries A arbeitet mit i5/OS Version 5 Release 4 (V5R4).
- Auf iSeries A sind Digital Certificate Manager (i5/OS Option 34) und IBM HTTP-Server für i5/OS (5722-DG1) installiert und konfiguriert.
- Auf iSeries A wird die Prämienkalkulationsanwendung ausgeführt, die folgendermaßen konfiguriert wurde:
  - Die Verwendung des SSL-Modus ist erforderlich.
  - Für die Authentifizierung wird ein öffentliches Zertifikat einer bekannten Zertifizierungsinstanz (CA) verwendet, um eine SSL-Sitzung zu initialisieren.
  - Für die Benutzerauthentifizierung ist ein Benutzername sowie das zugehörige Kennwort erforderlich.
- iSeries A legt ihr Zertifikat vor, um eine SSL-Sitzung aufzubauen, wenn die Clients B und C auf die Prämienkalkulationsanwendung zugreifen.
- Nach dem Aufbau der SSL-Sitzung fordert iSeries A die Clients B und C zur Angabe eines gültigen Benutzernamens und des zugehörigen Kennworts auf, bevor diesen Einheiten der Zugriff auf die Prämienkalkulationsanwendung gewährt wird.

## Client-Systeme der Versicherungsagenten - Client B und Client C

- Die Clients B und C sind unabhängigen Versicherungsagenten zugeordnet, die auf die Prämienkalkulationsanwendung zugreifen wollen.
- Die Client-Software der Clients B und C verfügt über eine installierte Kopie eines Zertifikats der bekannten Zertifizierungsinstanz, die das entsprechende Anwendungszertifikat ausgestellt hat.
- Die Clients B und C greifen auf die Prämienkalkulationsanwendung auf iSeries A zu. Dieses System legt daraufhin sein Zertifikat bei deren Client-Software vor, um so seine Identität zu authentifizieren und eine SSL-Sitzung aufzubauen.
- Die Client-Software auf den Clients B und C wurde so konfiguriert, dass das Zertifikat der iSeries A zum Aufbau einer SSL-Sitzung akzeptiert wird.
- Nach dem Start der SSL-Sitzung müssen die Clients B und C einen gültigen Benutzernamen und das zugehörige Kennwort angeben, bevor die iSeries A diesen Einheiten den Zugriff auf die Anwendung gewährt.

## Voraussetzungen und Annahmen

Das vorliegende Szenario geht von den folgenden Voraussetzungen und Annahmen aus:

- Die Prämienkalkulationsanwendung auf der iSeries A ist eine generische Anwendung, die für den Einsatz von SSL konfiguriert werden kann. Die meisten Anwendungen einschließlich zahlreicher iSeries-Anwendungen bieten SSL-Unterstützung. Die SSL-Konfigurationsschritte dieser Anwendungen können stark voneinander abweichen. Aus diesem Grund umfasst das vorliegende Szenario keine spezifischen Anweisungen zum Konfigurieren der Prämienkalkulationsanwendung für die Verwendung von SSL. Es enthält Anweisungen zum Konfigurieren und Verwalten der Zertifikate, die bei allen Anwendungen für den Einsatz von SSL erforderlich sind.
- Die Prämienkalkulationsanwendung umfasst eventuell eine Funktion zur Anforderung von Zertifikaten für die Client-Authentifizierung. Das vorliegende Szenario enthält Anweisungen zum Einsatz von Digital Certificate Manager (DCM) für die Konfiguration der Zertifikatsanerkennung bei den Anwendungen, die diese Unterstützungsfunktion umfassen. Da die zur Konfiguration der Client-Authentifizierung auszuführenden Schritte von Anwendung zu Anwendung stark variieren können, werden im vorliegenden Szenario keine spezifischen Anweisungen zur Konfiguration der Client-Authentifizierung über Zertifikate für die Prämienkalkulationsanwendung erläutert.
- Die iSeries A entspricht den Voraussetzungen zum Installieren und zur Verwendung von Digital Certificate Manager (DCM).
- Auf der iSeries A wurde DCM zuvor noch nicht konfiguriert oder verwendet.
- Das Benutzerprofil der Person, die die im vorliegenden Szenario enthaltenen Tasks ausführt, muss über die Sonderberechtigungen \*SECADM und \*ALLOBJ verfügen.
- Auf der iSeries A ist kein IBM Verschlüsselungskoprozessor installiert.

## Konfigurations-Tasks

### Zugehörige Tasks

„Digital Certificate Manager starten“ auf Seite 46

In diesem Abschnitt erfahren Sie, wie Sie auf Ihrem System auf Digital Certificate Manager (DCM) zugreifen können.

## Planungsarbeitsblätter ausfüllen

Die folgenden Planungsarbeitsblätter enthalten die Daten, die Sie erfassen müssen, und Informationen zu den Einstellungen, die zur Vorbereitung der im vorliegenden Szenario beschriebenen Implementierung für digitale Zertifikate definiert werden müssen. Um eine erfolgreiche Implementierung zu gewährleisten, müssen Sie alle Fragen zu den vorausgesetzten Komponenten mit Ja beantworten können und alle angeforderten Daten erfasst haben, bevor die erforderlichen Konfigurations-Tasks ausgeführt werden.

Tabelle 1. Planungsarbeitsblatt für die Voraussetzungen der Zertifikatsimplementierung

Voraussetzung gemäß Arbeitsblatt	Antworten
Arbeiten Sie mit i5/OS V5R42 (5722-SS1)?	Ja
Ist auf Ihrem System die Option 34 von i5/OS installiert?	Ja
Ist auf Ihrem System IBM HTTP-Server für i5/OS (5722-DG1) installiert, und wurde die Administrationsserverinstanz gestartet?	Ja
Wurde TCP auf dem System so konfiguriert, dass ein Web-Browser und die Administrationsserverinstanz des HTTP-Servers verwendet werden können, um auf DCM zuzugreifen?	Ja
Verfügen Sie über die Sonderberechtigungen *SECADM und *ALLOBJ?	Ja

Sie müssen die folgenden Daten zu Ihrer Implementierung für digitale Zertifikate sammeln, um die für die Implementierung erforderlichen Konfigurations-Tasks auszuführen:

Tabelle 2. Planungsarbeitsblatt für die Konfiguration der Zertifikatsimplementierung

Planungsarbeitsblatt für iSeries A	Antworten
Werden Sie eine eigene lokale Zertifizierungsinstanz (CA) betreiben oder Ihre Anwendungszertifikate von einer öffentlichen Zertifizierungsinstanz abrufen?	Die Zertifikate werden von einer öffentlichen Zertifizierungsinstanz abgerufen.
Sind die Anwendungen, für die die SSL-Unterstützung aktiviert werden soll, auf der iSeries A installiert?	Ja
<p>Welche DN-Informationen werden für die Zertifikatssignieranforderung (CSR) verwendet, die mit DCM erstellt werden soll?</p> <ul style="list-style-type: none"> <li>• <b>Schlüsselgröße:</b> Gibt den Grad der Verschlüsselung eines Chiffrierschlüssels für das Zertifikat an.</li> <li>• <b>Zertifikatsbezeichnung:</b> Identifiziert das Zertifikat mit einer eindeutigen Zeichenfolge.</li> <li>• <b>Allgemeiner Name:</b> Identifiziert den Eigner des Zertifikats (z. B. eine Person, eine Entität oder Anwendung) und ist Teil des registrierten Subjektnamens (DN) des Zertifikats.</li> <li>• <b>Organisationseinheit:</b> Identifiziert den Organisationsabschnitt oder -bereich für die Anwendung, die dieses Zertifikat verwenden wird.</li> <li>• <b>Organisationsname:</b> Identifiziert Ihren Unternehmens- oder Bereichsabschnitt für die Anwendung, die dieses Zertifikat verwenden wird.</li> <li>• <b>Standort oder Stadt:</b> Identifiziert den Standort bzw. die Stadt, an dem bzw. in der sich Ihr Unternehmen befindet.</li> <li>• <b>Bundesland:</b> Identifiziert das Bundesland, in dem dieses Zertifikat verwendet werden soll.</li> <li>• <b>Land oder Region:</b> Identifiziert das Land oder die Region, in der dieses Zertifikat verwendet werden soll, mit einem zweistelligen alphabetischen Zielcode.</li> </ul>	<p><b>Schlüsselgröße:</b> 1024 <b>Zertifikatsbezeichnung:</b> Myco_public_cert <b>Allgemeiner Name:</b> myco_rate_server@myco.com <b>Organisationseinheit:</b> Rate dept <b>Organisationsname:</b> myco <b>Standort oder Stadt:</b> Any_city <b>Bundesland:</b> Any <b>Land oder Region:</b> ZZ</p>
Welche DCM-Anwendungs-ID soll der Anwendung zugeordnet werden, die für die Verwendung von SSL konfiguriert wird?	mcyo_agent_rate_app



Tabelle 2. Planungsarbeitsblatt für die Konfiguration der Zertifikatsimplementierung (Forts.)

Planungsarbeitsblatt für iSeries A	Antworten
Wird die SSL-Anwendung so konfiguriert, dass für die Client-Authentifizierung Zertifikate eingesetzt werden? Wenn ja, welche Zertifizierungsinstanzen (CAs) sollen zur CA-Anerkennungsliste der Anwendung hinzugefügt werden?	Nein

## Server- oder Client-Zertifikatsanforderung erstellen

1. Starten Sie Digital Certificate Manager.
2. Wählen Sie im Navigationsrahmen von DCM **Neuen Zertifikatsspeicher erstellen** aus, um die geführte Task zu starten und eine Reihe von Formularen auszufüllen. Diese Formulare führen Sie durch die Arbeitsschritte, die zum Erstellen eines Zertifikatsspeichers und eines Zertifikats erforderlich sind, das von den Anwendungen zum Herstellen von SSL-Sitzungen benutzt werden kann.

**Anmerkung:** Wenn Sie Fragen zum Ausfüllen eines bestimmten Formulars in dieser geführten Task haben, wählen Sie die Schaltfläche mit dem Fragezeichen (?) oben auf der Seite aus, um auf die Onlinehilfe zuzugreifen.

3. Wählen Sie als den zu erstellenden Zertifikatsspeicher **\*SYSTEM** aus, und klicken Sie anschließend auf **Weiter**.
4. Wählen Sie **Ja** aus, um bei der Erstellung des Zertifikatsspeichers **\*SYSTEM** auch ein Zertifikat zu erstellen, und klicken Sie dann auf **Weiter**.
5. Wählen Sie als Signierer des neuen Zertifikats **VeriSign oder eine andere Internet-Zertifizierungsinstanz (CA)** aus, und klicken Sie anschließend auf **Weiter**. Daraufhin wird ein Formular angezeigt, in dem Sie die Daten zur Identifikation des neuen Zertifikats eingeben können.
6. Füllen Sie das Formular aus, und klicken Sie anschließend auf **Weiter**, um eine Bestätigungsseite aufzurufen. Diese Bestätigungsseite zeigt die Zertifikatsanforderungsdaten an, die für die öffentliche Zertifizierungsinstanz (CA) angegeben werden müssen, die Ihr Zertifikat ausstellt. Die Daten für die Zertifikatssignieranforderung (CSR) bestehen aus einem öffentlichen Schlüssel, dem registrierten Namen (DN) und weiteren Informationen, die Sie für das neue Zertifikat angegeben haben.
7. Kopieren Sie die CSR-Daten, und fügen Sie diese sorgfältig in das Zertifikatsantragsformular oder eine separate Datei ein, das bzw. die die öffentliche Zertifizierungsinstanz zur Anforderung eines Zertifikats benötigt. Sie müssen alle CSR-Daten einschließlich der Zeilen zum Beginn und zum Ende der Anforderung eines neuen Zertifikats verwenden.

**Anmerkung:** Wird diese Seite verlassen, gehen die Daten verloren und können nicht wiederhergestellt werden.

8. Wird diese Seite verlassen, gehen die Daten verloren und können nicht wiederhergestellt werden.
9. Sie müssen warten, bis die Zertifizierungsinstanz das signierte, vervollständigte Zertifikat zurücksendet, bevor Sie mit dem nächsten Task-Schritt im Szenario fortfahren können.

Nachdem die Zertifizierungsinstanz das signierte und vervollständigte Zertifikat zurückgesendet hat, können Sie Ihre Anwendung für die Benutzung von SSL konfigurieren, das Zertifikat in den Zertifikatsspeicher **\*SYSTEM** importieren und es der gewünschten Anwendung für den SSL-Einsatz zuordnen.

## Anwendung für den Einsatz von SSL konfigurieren

Nachdem Sie das signierte Zertifikat von der öffentlichen Zertifizierungsinstanz (CA) zurückerhalten haben, können Sie mit den Arbeitsschritten fortfahren, die zum Aktivieren der SSL-Kommunikation (SSL = Secure Sockets Layer) für die öffentliche Anwendung erforderlich sind. Die Anwendung sollte für die Verwendung von SSL konfiguriert werden, bevor Sie mit dem signierten Zertifikat arbeiten. Bestimmte Anwendungen, z. B. IBM HTTP-Server für iSeries, generieren eine eindeutige Anwendungs-ID und registrieren diese bei Digital Certificate Manager (DCM), wenn Sie die SSL-Konfiguration der Anwendung

durchführen. Sie müssen diese Anwendungs-ID kennen, um DCM zum Zuordnen des signierten Zertifikats und zum Abschluss des SSL-Konfigurationsprozesses verwenden zu können.

Die Art und Weise, in der eine Anwendung für SSL konfiguriert werden kann, variiert abhängig von der verwendeten Anwendung. Im vorliegenden Szenario wird nicht von der Verwendung einer spezifischen Quelle für die beschriebene Prämienkalkulationsanwendung ausgegangen, weil MyCo., Inc. die Anwendung seinen Versicherungsagenten auf verschiedene Arten zur Verfügung stellen kann.

Informationen zur Konfiguration der verwendeten Anwendung für den SSL-Einsatz sind den Anweisungen in der zugehörigen Anwendungsdokumentation zu entnehmen. Weitere Informationen zum Konfigurieren zahlreicher allgemeiner IBM Anwendungen für den SSL-Einsatz finden Sie im Abschnitt Secure Sockets Layer (SSL) im iSeries Information Center.

Nach Abschluss der SSL-Konfiguration Ihrer Anwendung können Sie das signierte öffentliche Zertifikat der Anwendung so konfigurieren, dass mit diesem SSL-Sitzungen initialisiert werden können.

## Signiertes öffentliches Zertifikat importieren und zuordnen

Nach der Konfiguration Ihrer Anwendung für den Einsatz von SSL können Sie mit Digital Certificate Manager (DCM) das signierte Zertifikat importieren und der gewünschten Anwendung zuordnen.

So können Sie Ihr Zertifikat importieren und der gewünschten Anwendung zuordnen, um den Prozess der SSL-Konfiguration abzuschließen:

1. Starten Sie Digital Certificate Manager.
2. Klicken Sie im Navigationsrahmen auf **Zertifikatsspeicher auswählen**, und wählen Sie anschließend als zu öffnenden Zertifikatsspeicher **\*SYSTEM** aus.
3. Geben Sie auf der Seite **Zertifikatsspeicher und Kennwort** das Kennwort ein, das Sie bei der Erstellung des Zertifikatsspeichers angegeben haben, und klicken Sie dann auf **Weiter**.
4. Nach der Aktualisierung des Navigationsrahmens wählen Sie **Zertifikate verwalten** aus, um eine Liste mit Tasks anzuzeigen.
5. Wählen Sie in der Task-Liste **Zertifikat importieren** aus, um das Importieren des signierten Zertifikats in den Zertifikatsspeicher \*SYSTEM zu starten.

**Anmerkung:** Wenn Sie Fragen zum Ausfüllen eines bestimmten Formulars in dieser geführten Task haben, wählen Sie die Schaltfläche mit dem Fragezeichen (?) oben auf der Seite aus, um auf die Onlinehilfe zuzugreifen.

6. Wählen Sie als Nächstes in der Task-Liste **Zertifikate verwalten** die Auswahl **Zertifikat zuordnen** aus, um eine Liste mit Zertifikaten im aktuellen Zertifikatsspeicher anzuzeigen.
7. Wählen Sie ein Zertifikat in der Liste aus, und klicken Sie anschließend auf **Anwendungen zuordnen**, um eine Liste der Anwendungsdefinitionen für den aktuellen Zertifikatsspeicher anzuzeigen.
8. Wählen Sie in der Liste die gewünschte Anwendung aus, und klicken Sie anschließend auf **Weiter**. Daraufhin wird eine Seite aufgerufen, in der entweder eine Bestätigungsnachricht für die Zuordnungsauswahl oder eine Fehlermeldung angezeigt wird, wenn bei der Ausführung des Arbeitsschrittes ein Fehler aufgetreten ist.

Nach Abschluss dieser Tasks können Sie Ihre Anwendung im SSL-Modus starten und die Vertraulichkeit der von ihr bereitgestellten Daten in Zukunft schützen.

## Anwendung im SSL-Modus starten

Nach dem Importieren und Zuordnen des Zertifikats zu Ihrer Anwendung muss die Anwendung möglicherweise beendet und dann im SSL-Modus erneut gestartet werden. Dieser Arbeitsschritt ist unter bestimmten Umständen erforderlich, weil die aktive Anwendung eventuell nicht feststellen kann, dass die Zertifikatzuordnung vorhanden ist. Informationen dazu, ob für die verwendete Anwendung ein Neu-

start durchgeführt werden muss, sowie weitere spezifische Informationen zum Starten der Anwendung im SSL-Modus (siehe hierzu Application in SSL mode) finden Sie in der Dokumentation zur Anwendung.

Wenn Sie für die Client-Authentifizierung Zertifikate einsetzen wollen, können Sie nun eine CA-Anerkennungsliste für die Anwendung definieren.

### **(Optional): CA-Anerkennungsliste für eine Anwendung definieren, die zur Client-Authentifizierung Zertifikate benötigt**

Für Anwendungen, die die Verwendung von Zertifikaten für die Client-Authentifizierung in SSL-Sitzungen (SSL = Secure Sockets Layer) unterstützen, muss festgelegt werden, ob Zertifikate als gültige Identitätsnachweise akzeptiert werden. Eines der Kriterien, das von Anwendungen zum Authentifizieren eines Zertifikats angewendet wird, besteht darin, ob die Anwendung die ausstellende Zertifizierungsinstanz anerkennt.

Für die im vorliegenden Szenario beschriebene Situation ist es nicht erforderlich, dass die Prämienkalkulationsanwendung für die Client-Authentifizierung Zertifikate einsetzt. Allerdings muss die Anwendung in der Lage sein, Zertifikate für die Authentifizierung zu akzeptieren, wenn diese verfügbar sind. Zahlreiche Anwendungen unterstützen die Client-Authentifizierung mit Hilfe von Zertifikaten. Die zur Konfiguration dieser Unterstützungsfunktion erforderlichen Arbeitsschritte können von Anwendung zu Anwendung jedoch stark variieren. Diese optionale Task wird hier aufgeführt, um zu erläutern, wie DCM zum Aktivieren der Zertifikatsanerkennung für die Client-Authentifizierung verwendet werden kann. Diese bildet die Basis für die Konfiguration der Unterstützungsfunktion für die Client-Authentifizierung auf Zertifikatsbasis in Ihren Anwendungen.

Vor dem Definieren einer CA-Anerkennungsliste für eine Anwendung müssen die folgenden Bedingungen erfüllt sein:

- Die Anwendung muss die Verwendung von Zertifikaten für die Client-Authentifizierung unterstützen.
- In der DCM-Definition der Anwendung muss angegeben sein, dass sie mit einer CA-Anerkennungsliste arbeitet.

Wenn in der Anwendungsdefinition angegeben ist, dass die Anwendung eine CA-Anerkennungsliste benutzt, müssen Sie diese Liste definieren, damit die Anwendung die Client-Authentifizierung mit Zertifikaten erfolgreich ausführen kann. Hierdurch wird sichergestellt, dass von der Anwendung nur die Zertifikate von Zertifizierungsinstanzen überprüft werden können, die Sie als anerkannt definiert haben. Wenn ein Benutzer oder eine Client-Anwendung ein Zertifikat einer Zertifizierungsinstanz vorlegt, die in der CA-Anerkennungsliste nicht als anerkannt definiert wurde, wird das Zertifikat bei der Authentifizierung als ungültig zurückgewiesen.

So definieren Sie mit DCM eine CA-Anerkennungsliste für eine Anwendung:

1. Starten Sie Digital Certificate Manager.
2. Klicken Sie im Navigationsrahmen auf **Zertifikatsspeicher auswählen**, und wählen Sie anschließend als zu öffnenden Zertifikatsspeicher **\*SYSTEM** aus.
3. Geben Sie auf der Seite **Zertifikatsspeicher und Kennwort** das Kennwort ein, das Sie bei der Erstellung des Zertifikatsspeichers angegeben haben, und klicken Sie dann auf **Weiter**.
4. Nach der Aktualisierung des Navigationsrahmens wählen Sie **Zertifikate verwalten** aus, um eine Liste mit Tasks anzuzeigen.
5. Wählen Sie in der Task-Liste **Status der Zertifizierungsinstanz festlegen** aus, um eine Liste der CA-Zertifikate anzuzeigen.

**Anmerkung:** Wenn Sie Fragen zum Ausfüllen eines bestimmten Formulars in dieser geführten Task haben, wählen Sie die Schaltfläche mit dem Fragezeichen (?) oben auf der Seite aus, um auf die Onlinehilfe zuzugreifen.

6. Wählen Sie in der Liste ein oder mehrere CA-Zertifikate aus, die von Ihrer Anwendung anerkannt werden sollen, und klicken Sie dann auf **Aktivieren**, um eine Liste der Anwendungen anzuzeigen, die mit einer CA-Anerkennungsliste arbeiten.
7. Wählen Sie in der Liste die Anwendung aus, zu deren Anerkennungsliste die ausgewählte Zertifizierungsinstanz hinzugefügt werden soll, und klicken Sie dann auf **OK**. Daraufhin wird oben in der Seite eine Nachricht angezeigt, um Sie darüber zu informieren, dass die ausgewählten Anwendungen diese Zertifizierungsinstanz sowie die von dieser CA ausgestellten Zertifikate anerkennen.

Sie können Ihre Anwendung nun so konfigurieren, dass für die Client-Authentifizierung ein Zertifikat erforderlich ist. Informationen zur Vorgehensweise finden Sie in der Dokumentation zur verwendeten Anwendung.

## **Szenario: Zertifikate für die interne Authentifizierung verwenden**

Dieses Szenario beschreibt, wie Zertifikate als Authentifizierungsverfahren zum Schutz von und zur Eingrenzung des Zugriffs auf Ressourcen und Anwendungen eingesetzt werden können, auf die interne Benutzer auf Ihren internen Servern zugreifen können.

### **Situationsbeschreibung**

Sie sind der Netzwerkadministrator eines Unternehmens (MyCo., Inc.), dessen Personalabteilung sich mit Themen rechtlicher Natur sowie Fragen der Vertraulichkeit der gespeicherten Daten befasst. Die Mitarbeiter des Unternehmens haben gefordert, auf ihre persönlichen Sozial- und Krankenversicherungsdaten online zugreifen zu können. Das Unternehmen hat dieser Anforderung durch die Erstellung einer internen Website Rechnung getragen, auf der die gewünschten Informationen für die Mitarbeiter bereitgestellt werden. Sie sind für die Verwaltung dieser internen Website verantwortlich, die auf dem IBM HTTP-Server für i5/OS (powered by Apache) ausgeführt wird.

Da die Mitarbeiter in zwei geografisch getrennten Büros untergebracht sind und einige Mitarbeiter häufig geschäftlich reisen, haben Sie Bedenken wegen der Vertraulichkeit dieser Daten, die über das Internet übertragen werden müssen. Darüber hinaus werden Benutzer normalerweise mit Hilfe eines Benutzernamens und des zugehörigen Kennworts authentifiziert, um so den Zugriff auf die Unternehmensdaten einzugrenzen. Auf Grund der Vertraulichkeit dieser sensiblen Daten sind Sie nun zu der Überzeugung gelangt, dass der Schutz durch eine kennwortbasierte Authentifizierung für diese Daten nicht mehr ausreichend ist. Immerhin ist es möglich, dass diese Kennwörter gemeinsam mit anderen Personen benutzt, vergessen oder sogar unberechtigt benutzt werden.

Nach entsprechender Prüfung der Sachverhalte haben Sie entschieden, dass der Einsatz digitaler Zertifikate das benötigte Maß an Sicherheit zur Verfügung stellen kann. Die Verwendung von Zertifikaten ermöglicht Ihnen die Benutzung von SSL (Secure Sockets Layer) zum Schutz bei der Übertragung von Daten. Darüber hinaus können Sie Zertifikate an Stelle von Kennwörtern zur Verbesserung der Sicherheit bei der Authentifizierung von Benutzern einsetzen und den Zugriff auf persönliche Mitarbeiterdaten einschränken.

Aus diesem Grund haben Sie sich entschlossen, eine private lokale Zertifizierungsinstanz (CA) einzurichten und für alle Mitarbeiter Zertifikate auszustellen. Darüber hinaus werden die Mitarbeiter diese Zertifikate auch ihren iSeries-Benutzerprofilen zuordnen müssen. Durch diese Implementierung privater Zertifikate verfügen Sie über eine bessere Kontrolle über den Zugriff auf sensible Daten und können die Wahrung der Vertraulichkeit dieser Daten durch den Einsatz von SSL steuern. Darüber hinaus können Sie durch das Ausstellen eigener Zertifikate mit höherer Wahrscheinlichkeit gewährleisten, dass Ihre Daten verlässlich gesichert sind, und nur von berechtigten Personen benutzt werden können.

## Vorteile des Szenarios

Die Implementierung dieses Szenarios bietet die folgenden Vorteile:

- Die Verwendung digitaler Zertifikate zum Konfigurieren des SSL-Zugriffs auf den Webserver für persönliche Mitarbeiterdaten stellt sicher, dass die zwischen dem Server und dem Client übertragenen Informationen geschützt und vertraulich bleiben.
- Werden digitale Zertifikate bei der Client-Authentifizierung eingesetzt, können autorisierte Benutzer mit größerer Sicherheit identifiziert werden.
- Der Einsatz *privater* digitaler Zertifikate zur Authentifizierung von Benutzern für Ihre Anwendungen und Daten ist dann sinnvoll, wenn für Sie die folgenden oder ähnliche Bedingungen zutreffen:
  - Sie haben hohe Sicherheitsanforderungen, insbesondere in Bezug auf die Authentifizierung von Benutzern.
  - Sie haben ein Vertrauensverhältnis zu den Personen, an die Sie Zertifikate ausstellen.
  - Für Ihre Benutzer wurden zur Steuerung des Anwendungs- und Datenzugriffs bereits iSeries-Benutzerprofile definiert.
  - Sie wollen eine eigene Zertifizierungsinstanz (CA) betreiben.
- Der Einsatz privater Zertifikate bei der Client-Authentifizierung ermöglicht Ihnen die einfachere Zuordnung des Zertifikats zum iSeries-Benutzerprofil des autorisierten Benutzers. Diese Zertifikatszuordnung zu einem Benutzerprofil ermöglicht dem HTTP-Server während der Authentifizierung die Feststellung des Benutzerprofils des Zertifikatseigners. Der HTTP-Server kann dann auf die entsprechenden Daten zugreifen und unter dem jeweiligen Benutzerprofil ausgeführt werden bzw. Aktionen für den zugehörigen Benutzer auf der Basis der im Benutzerprofil gespeicherten Daten durchführen.

## Ziele

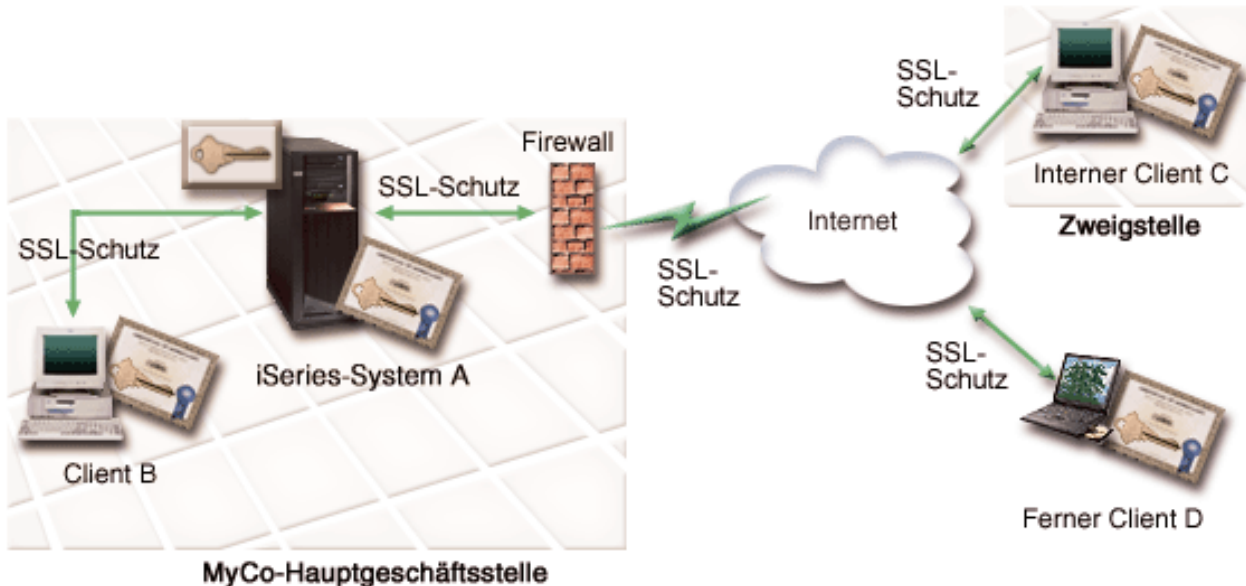
Im vorliegenden Szenario möchte MyCo., Inc. digitale Zertifikate zum Schutz der sensiblen persönlichen Daten einsetzen, die für die Mitarbeiter des Unternehmens auf der internen Website für persönliche Mitarbeiterdaten bereitgestellt werden. Das Unternehmen möchte darüber hinaus eine sicherere Methode zur Authentifizierung der Benutzer implementieren, die über eine Zugriffsberechtigung für diese Website verfügen.

Im vorliegenden Szenario gelten die folgenden Zielsetzungen:

- Die interne Website für persönliche Mitarbeiterdaten des Unternehmens muss zum Schutz der Vertraulichkeit der bereitgestellten Daten SSL verwenden.
- Die SSL-Konfiguration muss mit privaten Zertifikaten einer internen lokalen Zertifizierungsinstanz (CA) implementiert werden.
- Autorisierte Benutzer müssen ein gültiges Zertifikat vorlegen, um im SSL-Modus auf die Website für persönliche Mitarbeiterdaten zuzugreifen.

## Details

In der folgenden Abbildung wird die Netzwerkkonfiguration für dieses Szenario dargestellt:



Die Abbildung stellt die folgenden Informationen zur Situation im vorliegenden Szenario dar:

### Öffentlicher Unternehmensserver - iSeries A

- iSeries A dient als Host für die Prämienkalkulationsanwendung des Unternehmens.
- iSeries A arbeitet mit i5/OS Version 5 Release 4 (V5R4).
- Auf iSeries A sind Digital Certificate Manager (i5/OS Option 34) und IBM HTTP-Server für i5/OS (5722-DG1) installiert und konfiguriert.
- Auf iSeries A wird die Prämienkalkulationsanwendung ausgeführt, die folgendermaßen konfiguriert wurde:
  - Die Verwendung des SSL-Modus ist erforderlich.
  - Für die Authentifizierung wird ein öffentliches Zertifikat einer bekannten Zertifizierungsinstanz (CA) verwendet, um eine SSL-Sitzung zu initialisieren.
  - Für die Benutzerauthentifizierung ist ein Benutzername sowie das zugehörige Kennwort erforderlich.
- iSeries A legt ihr Zertifikat vor, um eine SSL-Sitzung aufzubauen, wenn die Clients B und C auf die Prämienkalkulationsanwendung zugreifen.
- Nach dem Aufbau der SSL-Sitzung fordert iSeries A die Clients B und C zur Angabe eines gültigen Benutzernamens und des zugehörigen Kennworts auf, bevor diesen Einheiten der Zugriff auf die Prämienkalkulationsanwendung gewährt wird.

### Client-Systeme der Versicherungsagenten - Client B und Client C

- Die Clients B und C sind unabhängigen Versicherungsagenten zugeordnet, die auf die Prämienkalkulationsanwendung zugreifen wollen.
- Die Client-Software der Clients B und C verfügt über eine installierte Kopie eines Zertifikats der bekannten Zertifizierungsinstanz, die das entsprechende Anwendungszertifikat ausgestellt hat.
- Die Clients B und C greifen auf die Prämienkalkulationsanwendung auf iSeries A zu. Dieses System legt daraufhin sein Zertifikat bei deren Client-Software vor, um so seine Identität zu authentifizieren und eine SSL-Sitzung aufzubauen.

- Die Client-Software auf den Clients B und C wurde so konfiguriert, dass das Zertifikat der iSeries A zum Aufbau einer SSL-Sitzung akzeptiert wird.
- Nach dem Start der SSL-Sitzung müssen die Clients B und C einen gültigen Benutzernamen und das zugehörige Kennwort angeben, bevor die iSeries A diesen Einheiten den Zugriff auf die Anwendung gewährt.

## Voraussetzungen und Annahmen

Das vorliegende Szenario geht von den folgenden Voraussetzungen und Annahmen aus:

- Der IBM HTTP-Server für i5/OS (powered by Apache) dient zur Ausführung der Anwendung für persönliche Mitarbeiterdaten auf der iSeries A. Das vorliegende Szenario umfasst deswegen keine speziellen Anweisungen für das Konfigurieren des HTTP-Servers für den SSL-Einsatz. Es enthält Anweisungen zum Konfigurieren und Verwalten der Zertifikate, die bei allen Anwendungen für den Einsatz von SSL erforderlich sind.
- Der HTTP-Server umfasst eine Funktion zur Anforderung von Zertifikaten für die Client-Authentifizierung. Das vorliegende Szenario enthält Anweisungen zum Einsatz von Digital Certificate Manager (DCM) für die Konfiguration der vorausgesetzten Funktionen für die Zertifikatsverwaltung im vorliegenden Szenario. Das vorliegende Szenario stellt allerdings keine spezifischen Anweisungen zu den zur Konfiguration der Client-Authentifizierung auszuführenden Schritte auf dem HTTP-Server zur Verfügung.
- Der HTTP-Server für persönliche Mitarbeiterdaten auf der iSeries A verwendet bereits eine Sicherheitsfunktion, die die Authentifizierung mit Kennwörtern durchführt.
- Die iSeries A entspricht den Voraussetzungen zum Installieren und zur Verwendung von Digital Certificate Manager (DCM).
- Auf der iSeries A wurde DCM zuvor noch nicht konfiguriert oder verwendet.
- Das Benutzerprofil der Person, die die im vorliegenden Szenario enthaltenen Tasks ausführt, muss über die Sonderberechtigungen \*SECADM und \*ALLOBJ verfügen.
- Auf der iSeries A ist kein IBM Verschlüsselungskoprozessor installiert.

## Konfigurations-Tasks

### Planungsarbeitsblätter ausfüllen

Die folgenden Planungsarbeitsblätter enthalten die Daten, die Sie erfassen müssen, und Informationen zu den Einstellungen, die zur Vorbereitung der im vorliegenden Szenario beschriebenen Implementierung für digitale Zertifikate definiert werden müssen. Um eine erfolgreiche Implementierung zu gewährleisten, müssen Sie alle Fragen zu den vorausgesetzten Komponenten mit Ja beantworten können und alle angeforderten Daten erfasst haben, bevor die erforderlichen Konfigurations-Tasks ausgeführt werden.

*Tabelle 3. Planungsarbeitsblatt für die Voraussetzungen der Zertifikatsimplementierung*

Voraussetzung gemäß Arbeitsblatt	Antworten
Arbeiten Sie mit i5/OS V5R4 (5722-SS1)?	Ja
Ist auf Ihrem System die Option 34 von i5/OS installiert?	Ja
Ist auf Ihrem System IBM HTTP-Server für i5/OS (5722-DG1) installiert, und wurde die Administrationsserverinstanz gestartet?	Ja
Wurde TCP auf dem System so konfiguriert, dass ein Web-Browser und die Administrationsserverinstanz des HTTP-Servers verwendet werden können, um auf DCM zuzugreifen?	Ja
Verfügen Sie über die Sonderberechtigungen *SECADM und *ALLOBJ?	Ja

Sie müssen die folgenden Daten zu Ihrer Implementierung für digitale Zertifikate sammeln, um die für die Implementierung erforderlichen Konfigurations-Tasks auszuführen:

Tabelle 4. Planungsarbeitsblatt für die Konfiguration der Zertifikatsimplementierung

Planungsarbeitsblatt für iSeries A	Antworten
Werden Sie eine eigene lokale Zertifizierungsinstanz (CA) betreiben oder Ihre Anwendungszertifikate von einer öffentlichen Zertifizierungsinstanz abrufen?	Es wird eine lokale Zertifizierungsinstanz erstellt, um Zertifikate auszustellen.
Sind die Anwendungen, für die die SSL-Unterstützung aktiviert werden soll, auf der iSeries A installiert?	Ja
<p>Welche DN-Informationen werden für die lokale Zertifizierungsinstanz (CA) verwendet?</p> <ul style="list-style-type: none"> <li>• <b>Schlüsselgröße:</b> Gibt den Grad der Verschlüsselung eines Chiffrierschlüssels für das Zertifikat an.</li> <li>• <b>Name der Zertifizierungsinstanz (CA):</b> Gibt die CA an und wird als allgemeiner Name für das Zertifikat der Zertifizierungsinstanz und den DN der Zertifizierungsinstanz für die Zertifikate verwendet, die von der CA ausgestellt werden.</li> <li>• <b>Organisationseinheit:</b> Identifiziert den Organisationsabschnitt oder -bereich für die Anwendung, die dieses Zertifikat verwenden wird.</li> <li>• <b>Organisationsname:</b> Identifiziert Ihren Unternehmens- oder Bereichsabschnitt für die Anwendung, die dieses Zertifikat verwenden wird.</li> <li>• <b>Standort oder Stadt:</b> Identifiziert den Standort bzw. die Stadt, an dem bzw. in der sich Ihr Unternehmen befindet.</li> <li>• <b>Bundesland:</b> Identifiziert das Bundesland, in dem dieses Zertifikat verwendet werden soll.</li> <li>• <b>Land oder Region:</b> Identifiziert das Land oder die Region, in der dieses Zertifikat verwendet werden soll, mit einem zweistelligen alphabetischen Zielcode.</li> <li>• <b>Gültigkeitsdauer der Zertifizierungsinstanz (CA):</b> Gibt die Anzahl der Tage an, die das Zertifikat der Zertifizierungsinstanz gültig ist.</li> </ul>	<p><b>Schlüsselgröße:</b> 1024 <b>Name der Zertifizierungsinstanz (CA):</b> Myco_CA@myco.com <b>Organisationseinheit:</b> Rate dept <b>Organisationsname:</b> myco <b>Standort oder Stadt:</b> Any_city <b>Bundesland:</b> Any <b>Land oder Region:</b> ZZ <b>Gültigkeitsdauer der Zertifizierungsinstanz (CA):</b> 1095</p>
Wollen Sie die Richtliniendaten der lokalen Zertifizierungsinstanz (CA) so definieren, dass Benutzerzertifikate für die Client-Authentifizierung ausgestellt werden können?	Ja



Tabelle 4. Planungsarbeitsblatt für die Konfiguration der Zertifikatsimplementierung (Forts.)

Planungsarbeitsblatt für iSeries A	Antworten
<p>Welche DN-Informationen werden für das Serverzertifikat verwendet, das die lokale Zertifizierungsinstanz (CA) ausstellt?</p> <ul style="list-style-type: none"> <li>• <b>Schlüsselgröße:</b> Gibt den Grad der Verschlüsselung eines Chiffrierschlüssels für das Zertifikat an.</li> <li>• <b>Zertifikatsbezeichnung:</b> Identifiziert das Zertifikat mit einer eindeutigen Zeichenfolge.</li> <li>• <b>Allgemeiner Name:</b> Identifiziert den Eigner des Zertifikats (z. B. eine Person, eine Entität oder Anwendung) und ist Teil des registrierten Subjektnamens (DN) des Zertifikats.</li> <li>• <b>Organisationseinheit:</b> Identifiziert den Organisationsabschnitt oder -bereich für die Anwendung, die dieses Zertifikat verwenden wird.</li> <li>• <b>Organisationsname:</b> Identifiziert Ihren Unternehmens- oder Bereichsabschnitt für die Anwendung, die dieses Zertifikat verwenden wird.</li> <li>• <b>Standort oder Stadt:</b> Identifiziert den Standort bzw. die Stadt, an dem bzw. in der sich Ihr Unternehmen befindet.</li> <li>• <b>Bundesland:</b> Identifiziert das Bundesland, in dem dieses Zertifikat verwendet werden soll.</li> <li>• <b>Land oder Region:</b> Identifiziert das Land oder die Region, in der dieses Zertifikat verwendet werden soll, mit einem zweistelligen alphabetischen Zielcode.</li> </ul>	<p><b>Schlüsselgröße:</b> 1024 <b>Zertifikatsbezeichnung:</b> Myco_public_cert <b>Allgemeiner Name:</b> myco_rate_server@myco.com <b>Organisationseinheit:</b> Rate dept <b>Organisationsname:</b> myco <b>Standort oder Stadt:</b> Any_city <b>Bundesland:</b> Any <b>Land oder Region:</b> ZZ</p>
<p>Welche DCM-Anwendungs-ID soll der Anwendung zugeordnet werden, die für die Verwendung von SSL konfiguriert wird?</p>	<p>mcyo_agent_rate_app</p>
<p>Wird die SSL-Anwendung so konfiguriert, dass für die Client-Authentifizierung Zertifikate eingesetzt werden? Wenn ja, welche Zertifizierungsinstanzen (CAs) sollen zur CA-Anerkennungsliste der Anwendung hinzugefügt werden?</p>	<p>JaMyco_CA@myco.com</p>

## HTTP-Server für persönliche Mitarbeiterdaten für den Einsatz von SSL konfigurieren

Die Arbeitsschritte, die zur Konfiguration von SSL (Secure Sockets Layer) auf dem HTTP-Server für persönliche Mitarbeiterdaten (powered by Apache) auf der iSeries A ausgeführt werden müssen, können abhängig von der verwendeten Serverkonfiguration variieren.

So können Sie den Server für den SSL-Einsatz konfigurieren:

1. Starten Sie die Verwaltungsschnittstelle des HTTP-Servers.
2. Wählen Sie die Indexungen **Verwalten** → **Alle Server** → **Alle HTTP-Server** aus, um eine Liste aller konfigurierten HTTP-Server anzuzeigen.
3. Wählen Sie in der Liste den Server aus, und klicken Sie dann auf **Details verwalten**.
4. Wählen Sie im Navigationsrahmen **Sicherheit** aus.
5. Wählen Sie im Formular die Indexung **SSL mit Zertifikatsauthentifizierung** aus.
6. Wählen Sie im Feld **SSL** die Einstellung **Aktiviert** aus.
7. Geben Sie im Feld **Anwendungsname für Server-Zertifikat** eine Anwendungs-ID an, unter der diese Serverinstanz auf dem System identifiziert werden kann. Alternativ hierzu können Sie auch eine Aus-

wahl in der Liste treffen. Diese Anwendungs-ID wird im Format QIBM\_HTTP\_SERVER\_[server\_name] angegeben. Beispiel: QIBM\_HTTP\_SERVER\_MYCOTEST. **Anmerkung:** Notieren Sie diese Anwendungs-ID für die spätere Verwendung. Sie müssen diese ID in DCM nochmals auswählen.

Weitere Informationen zur allgemeinen Konfiguration des HTTP-Servers beim Einsatz von SSL finden Sie unter HTTP Server for iSeries und hier insbesondere im Beispielszenario "JKL enables Secure Sockets Layer (SSL) protection on their HTTP Server (powered by Apache)". Dieses Szenario enthält Anweisungen zu allen Task-Schritten, die zur Erstellung eines virtuellen Hosts und zum Konfigurieren dieser Einheit für den SSL-Einsatz ausgeführt werden müssen. Diese lauten wie folgt:

1. Definieren eines namensbasierten virtuellen Hosts.
2. Definieren einer Listen-Direktive für den virtuellen Host.
3. Definieren der Verzeichnisse des virtuellen Hosts.
4. Definieren des Kennwortschutzes über die Basisauthentifizierung.
5. Aktivierung von SSL auf dem virtuellen Host.

Zusätzliche Informationen zum Konfigurieren der aktuellen und zukünftigen Versionen des IBM HTTP-Server für iSeries finden Sie im Abschnitt HTTP Server for iSeries.

Nach Abschluss der SSL-Konfiguration für den HTTP-Server können Sie mit DCM die Zertifikatsunterstützung konfigurieren, die für SSL und die Client-Authentifizierung benötigt wird.

## Lokale Zertifizierungsinstanz erstellen und betreiben

Nachdem Sie den HTTP-Server für persönliche Mitarbeiterdaten für den Einsatz von SSL (Secure Sockets Layer) konfiguriert haben, müssen Sie ein Zertifikat konfigurieren, das der Server zum Initialisieren von SSL einsetzen kann. Basierend auf den Zielsetzungen des vorliegenden Szenarios haben Sie sich für die Erstellung und den Betrieb einer lokalen Zertifizierungsinstanz (CA) entschieden, mit der ein Zertifikat an den Server ausgestellt werden soll.

Wenn Sie mit Digital Certificate Manager (DCM) eine lokale Zertifizierungsinstanz (CA) erstellen, werden Sie durch einen Prozess geführt, mit dem sichergestellt werden kann, dass alle Komponenten konfiguriert werden, die zum Aktivieren der SSL-Unterstützung Ihrer Anwendung erforderlich sind. Im Rahmen dieses Prozesses wird auch das von der lokalen CA ausgestellte Zertifikat der Webserveranwendung zugeordnet. Darüber hinaus wird die lokale Zertifizierungsinstanz zur CA-Anerkennungsliste der Webserveranwendung hinzugefügt. Durch die Aufnahme der lokalen CA in die Anerkennungsliste der Anwendung wird sichergestellt, dass die Anwendung Benutzer identifizieren und authentifizieren kann, die Zertifikate dieser lokalen Zertifizierungsinstanz vorlegen.

Führen Sie die folgenden Arbeitsschritte aus, um mit Digital Certificate Manager (DCM) eine lokale Zertifizierungsinstanz zu erstellen und zu betreiben und ein Zertifikat für die Serveranwendung für persönliche Mitarbeiterdaten auszustellen:

1. Starten Sie Digital Certificate Manager.
2. Wählen Sie im Navigationsrahmen **Zertifizierungsinstanz (CA) erstellen** aus, um eine Reihe von Formularen aufzurufen. Diese Formulare führen Sie durch den Erstellungsprozess für eine lokale Zertifizierungsinstanz und unterstützen Sie beim Durchführen anderer Tasks, die zur Verwendung von digitalen Zertifikaten für SSL, zum Signieren von Objekten und zur Überprüfung von Signaturen erforderlich sind.

**Anmerkung:** Wenn Sie Fragen zum Ausfüllen eines bestimmten Formulars in dieser geführten Task haben, wählen Sie die Schaltfläche mit dem Fragezeichen (?) oben auf der Seite aus, um auf die Onlinehilfe zuzugreifen.

3. Füllen Sie die Formulare für diese geführte Task aus. Beim Ausfüllen dieser Formulare führen Sie alle im Folgenden aufgeführten Tasks aus, die zur Definition einer funktionierenden lokalen Zertifizierungsinstanz (CA) erforderlich sind:

- a. Bereitstellen von Kenndaten für die lokale Zertifizierungsinstanz.
- b. Installieren des Zertifikats der lokalen Zertifizierungsinstanz auf Ihrem PC oder in Ihrem Browser, damit Ihre Software diese Zertifizierungsinstanz erkennen und die von ihr ausgestellten Zertifikate überprüfen kann.
- c. Auswählen der Richtliniendaten für Ihre lokale Zertifizierungsinstanz.

**Anmerkung:** Die Einstellungen sollten unbedingt so gewählt werden, dass die lokale Zertifizierungsinstanz Benutzerzertifikate ausstellen kann.

- d. Verwenden der neuen lokalen Zertifizierungsinstanz zum Ausstellen eines Server- oder Client-Zertifikats, das Ihre Anwendungen für SSL-Verbindungen verwenden können.
- e. Auswählen der Anwendungen, die das Server- oder Client-Zertifikat für SSL-Verbindungen verwenden können.

**Anmerkung:** Wählen Sie hierbei unbedingt die Anwendungs-ID des HTTP-Servers für persönliche Mitarbeiterdaten aus.

- f. Verwenden der neuen lokalen Zertifizierungsinstanz zum Ausstellen eines Objektsignierzertifikats, das Ihre Anwendungen zum digitalen Signieren von Objekten verwenden können. Mit dieser Sub-Task wird der Zertifikatsspeicher \*OBJECTSIGNING erstellt; dies ist der Zertifikatsspeicher, der für die Verwaltung von Objektsignierzertifikat verwendet wird.

**Anmerkung:** Obwohl in diesem Szenario keine Objektsignierzertifikate verwendet werden, müssen Sie diesen Schritt ausführen. Wenn Sie die Durchführung in dieser Phase abbrechen, wird die Task beendet und Sie müssen separate Einzel-Tasks ausführen, um die SSL-Zertifikatskonfiguration abzuschließen.

- g. Auswählen der Anwendungen, die die lokale Zertifizierungsinstanz anerkennen sollen.

**Anmerkung:** Wählen Sie unbedingt die Anwendungs-ID des HTTP-Servers für persönliche Mitarbeiterdaten (z. B. QIBM\_HTTP\_SERVER\_MYCOTEST) als eine der Anwendungen aus, die die lokale Zertifizierungsinstanz anerkennen.

Nachdem Sie die Zertifikatskonfiguration abgeschlossen haben, die für die Webserveranwendung zum Einsatz von SSL erforderlich ist, können Sie nun den Webserver so konfigurieren, dass für die Benutzerauthentifizierung Zertifikate angefordert werden.

## Client-Authentifizierung für den Webserver für persönliche Mitarbeiterdaten konfigurieren

Sie müssen die allgemeinen Authentifizierungseinstellungen für den HTTP-Server konfigurieren, wenn auf dem HTTP-Server zur Authentifizierung Zertifikate eingesetzt werden sollen. Sie können diese Einstellungen im gleichen Sicherheitsformular konfigurieren, das auch zur Konfiguration des Servers für den Einsatz von SSL (Secure Sockets Layer) benutzt wurde.

So können Sie den Server für die Client-Authentifizierung mit Hilfe von Zertifikaten konfigurieren:

1. Starten Sie die Verwaltungsschnittstelle des HTTP-Servers.
2. Rufen Sie im Browser Ihres Systems die Seite "i5/OS-Tasks" auf. Diese steht unter folgender Adresse zur Verfügung: [http://your\\_system\\_name:2001](http://your_system_name:2001).
3. Wählen Sie **IBM Web Administration for i5/OS** aus.
4. Wählen Sie die Indexungen **Verwalten** → **Alle Server** → **Alle HTTP-Server** aus, um eine Liste aller konfigurierten HTTP-Server anzuzeigen.
5. Wählen Sie in der Liste den Server aus, und klicken Sie dann auf **Details verwalten**.
6. Wählen Sie im Navigationsrahmen **Sicherheit** aus.
7. Wählen Sie im Formular die Indexzunge **Authentifizierung** aus.
8. Wählen Sie **i5/OS-Profil des Clients verwenden** aus.

9. Geben Sie im Feld **Authentifizierungsname oder -Realm** einen Namen für den Authentifizierungs-Realm ein.
10. Wählen Sie im Feld **Anforderung mit Berechtigung des Clients verarbeiten** die Einstellung **Aktiviert** aus, und klicken Sie dann auf **Anwenden**.
11. Wählen Sie im Formular die Indexzunge **Zugriffssteuerung** aus.
12. Wählen Sie **Alle authentifizierten Benutzer (gültiger Benutzername und Kennwort)** aus, und klicken Sie dann auf **Anwenden**.
13. Wählen Sie im Formular die Indexzunge **SSL mit Zertifikatsauthentifizierung** aus.
14. Vergewissern Sie sich, dass im Feld **SSL** die Einstellung **Aktiviert** ausgewählt wurde.
15. Vergewissern Sie sich, dass im Feld **Anwendungsname für Server-Zertifikat** der korrekte Wert angegeben ist, z. B. QIBM\_HTTP\_SERVER\_MYCOTEST.
16. Wählen Sie **Client-Zertifikat, sofern verfügbar, vor Verbindungsherstellung akzeptieren** aus. Klicken Sie auf **OK**.

Weitere Informationen zur allgemeinen Konfiguration des HTTP-Servers beim Einsatz von SSL finden Sie im Abschnitt HTTP Server for iSeries und hier insbesondere im Beispielszenario "JKL enables Secure Sockets Layer (SSL) protection on their HTTP Server (powered by Apache)". Dieses Szenario enthält Anweisungen zu allen Task-Schritten, die zur Erstellung eines virtuellen Hosts und zum Konfigurieren dieser Einheit für den SSL-Einsatz ausgeführt werden müssen.

Nach Abschluss der Client-Authentifizierungskonfiguration können Sie den HTTP-Server im SSL-Modus erneut starten und damit den Schutz der Daten in der Anwendung für persönliche Mitarbeiterdaten aktivieren.

## Webserver für persönliche Mitarbeiterdaten im SSL-Modus starten

Möglicherweise muss der HTTP-Server gestoppt und anschließend erneut gestartet werden, um sicherzustellen, dass die Einheit feststellen kann, ob die Zertifikatszuordnung vorhanden ist, und diese zum Initialisieren von SSL-Sitzungen verwenden kann.

So können Sie den HTTP-Server (powered by Apache) stoppen und starten:

1. Erweitern Sie die Sicht Ihres Systems im iSeries Navigator.
2. Erweitern Sie die Sicht für **Netzwerk** → **Server** → **TCP/IP** → **HTTP Administration**.
3. Klicken Sie auf **Starten**, um die Verwaltungsschnittstelle des HTTP-Servers zu starten.
4. Klicken Sie auf die Indexzunge **Verwalten**, um eine Liste aller konfigurierten HTTP-Server anzuzeigen.
5. Wählen Sie in der Liste den gewünschten Server aus, und klicken Sie dann auf **Stoppen**, wenn der Server momentan aktiv ist.
6. Klicken Sie auf **Starten**, um den Server erneut zu starten. Weitere Informationen zu den Startparametern finden Sie in der Onlinehilfe.

Bevor Benutzer auf die Webanwendung für persönliche Mitarbeiterdaten zugreifen können, müssen Sie zuerst eine Kopie des Zertifikats der lokalen Zertifizierungsinstanz in ihrer Browser-Software installieren.

### Zugehörige Informationen

HTTP Server Information Center Overview

## Kopie des Zertifikats der lokalen Zertifizierungsinstanz im Browser installieren

Wenn Benutzer auf einen Server zugreifen, der mit SSL-Verbindungen (SSL = Secure Sockets Layer) arbeitet, legt dieser Server der Client-Software dieser Benutzer ein Zertifikat vor, um seine Identität zu belegen. Die Client-Software muss das Serverzertifikat überprüfen, bevor der Server eine Verbindung herstellen kann. Zum Überprüfen des Serverzertifikats muss die Client-Software über Zugriff auf die lokal gespeicherte Kopie des Zertifikats der Zertifizierungsinstanz (CA) verfügen, die zur Ausstellung des

Serverzertifikats verwendet wurde. Wenn der Server ein Zertifikat einer öffentlichen Internet-Zertifizierungsinstanz vorlegt, muss im Browser bzw. in der Client-Software des Benutzers bereits eine Kopie des zugehörigen CA-Zertifikats vorhanden sein. Wenn der Server (wie im vorliegenden Szenario) jedoch ein Zertifikat einer privaten lokalen Zertifizierungsinstanz vorlegt, muss jeder Benutzer mit Digital Certificate Manager (DCM) eine Kopie des zugehörigen CA-Zertifikats installieren.

Jeder Benutzer (Clients B, C und D) muss die folgenden Schritte ausführen, um eine Kopie des Zertifikats der lokalen Zertifizierungsinstanz abrufen zu können:

1. Starten Sie Digital Certificate Manager.
2. Wählen Sie im Navigationsrahmen **Zertifikat der lokalen Zertifizierungsinstanz auf dem PC installieren** aus, um eine Seite anzuzeigen, über die Sie dieses CA-Zertifikat in Ihren Browser herunterladen oder in einer Datei auf Ihrem System speichern können.
3. Geben Sie die Auswahl zum Installieren des Zertifikats an. Mit dieser Auswahl können Sie das Zertifikat der lokalen Zertifizierungsinstanz als Trusted Root in Ihren Browser herunterladen. Dadurch wird sichergestellt, dass der Browser gesicherte Kommunikationssitzungen mit Webservern aufbauen kann, die ein Zertifikat von dieser Zertifizierungsinstanz verwenden. Der Browser zeigt eine Reihe von Fenstern an, um Sie beim Beenden der Installation zu unterstützen.
4. Klicken Sie auf **OK**, um zur Homepage von Digital Certificate Manager zurückzukehren.

Nachdem Benutzer nun im SSL-Modus auf den Webserver für persönliche Mitarbeiterdaten zugreifen können, müssen sie ein geeignetes Zertifikat vorlegen, um die Serverauthentifizierung durchzuführen. Aus diesem Grund müssen diese Benutzer ein entsprechendes Benutzerzertifikat der lokalen Zertifizierungsinstanz abrufen.

## Zertifikat für jeden Benutzer von der lokalen Zertifizierungsinstanz anfordern

In den vorhergehenden Schritten haben Sie den Webserver für persönliche Mitarbeiterdaten so konfiguriert, dass für die Benutzerauthentifizierung Zertifikate angefordert werden. Nun müssen die Benutzer ein gültiges Zertifikat der lokalen Zertifizierungsinstanz vorlegen, um auf den Webserver zugreifen zu können. Jeder Benutzer muss mit Hilfe von Digital Certificate Manager (DCM) über die Task **Zertifikat erstellen** ein Zertifikat abrufen. Damit ein Zertifikat von einer lokalen Zertifizierungsinstanz abgerufen werden kann, muss die Richtlinie der lokalen CA die Ausstellung von Benutzerzertifikaten durch diese CA zulassen.

Jeder Benutzer (Clients B, C und D) muss die folgenden Schritte ausführen, um ein Zertifikat abzurufen:

1. Starten Sie Digital Certificate Manager.
2. Wählen Sie im Navigationsrahmen **Zertifikat erstellen** aus.
3. Wählen Sie als Typ für das zu erstellende Zertifikat **Benutzerzertifikat** aus. Daraufhin wird ein Formular angezeigt, in dem Sie die Daten zur Identifikation des gewünschten Zertifikats eingeben können.
4. Füllen Sie das Formular aus, und klicken Sie anschließend auf **Weiter**.

**Anmerkung:** Wenn Sie Fragen zum Ausfüllen eines bestimmten Formulars in dieser geführten Task haben, wählen Sie die Schaltfläche mit dem Fragezeichen (?) oben auf der Seite aus, um auf die Onlinehilfe zuzugreifen.

5. Jetzt erstellt DCM gemeinsam mit Ihrem Browser den privaten und den öffentlichen Schlüssel für das Zertifikat. Im Browser werden möglicherweise Fenster angezeigt, um Sie durch diesen Prozess zu führen. Befolgen Sie die Browser-Anweisungen für diese Tasks. Nachdem der Browser die Schlüssel generiert hat, wird eine Bestätigungsseite angezeigt, in der Sie darüber informiert werden, dass DCM das Zertifikat erstellt hat.
6. Installieren Sie das neue Zertifikat in Ihrem Browser. Im Browser werden möglicherweise Fenster angezeigt, um Sie durch diesen Prozess zu führen. Befolgen Sie die Instruktionen, die der Browser zum Ausführen dieser Task anzeigt.

7. Klicken Sie auf **OK**, um die Task abzuschließen.

Bei der Verarbeitung ordnet Digital Certificate Manager das Zertifikat automatisch Ihrem iSeries-Benutzerprofil zu.

Nach Abschluss dieser Tasks können nur berechtigte Benutzer mit einem gültigen Zertifikat auf Daten des Webservers für persönliche Mitarbeiterdaten zugreifen und die Daten dieses Servers sind während der SSL-Übertragung geschützt.

---

## Planung von DCM

In diesen Informationen finden Sie Entscheidungshilfen dazu, wie und wann digitale Zertifikate zur Erreichung Ihrer Sicherheitsziele eingesetzt werden können. In diesen Informationen wird erläutert, welche Voraussetzungen für die Installation von DCM erforderlich sind und welche anderen Faktoren beim Einsatz von DCM zu berücksichtigen sind.

Wenn Sie Digital Certificate Manager (DCM) verwenden wollen, um die digitalen Zertifikate Ihres Unternehmens effizient zu verwalten, müssen Sie über einen Gesamtplan verfügen, wie digitale Zertifikate im Rahmen der geltenden Sicherheitsrichtlinien eingesetzt werden sollen.

Weitere Informationen zur Planung des Einsatzes von DCM und zum besseren Verständnis der Einsatzmöglichkeiten digitaler Zertifikate innerhalb Ihrer Sicherheitsrichtlinien finden Sie unter den folgenden Themen:

### DCM-Setupvoraussetzungen

In diesem Abschnitt erfahren Sie, wie Sie überprüfen können, ob auf Ihrem System die Komponenten installiert sind, die zur Ausführung von Digital Certificate Manager (DCM) benötigt werden.

Digital Certificate Manager (DCM) ist eine kostenlose iSeries-Funktion für die zentrale Verwaltung von digitalen Zertifikaten für Ihre Anwendungen. Zur erfolgreichen Verwendung von DCM müssen folgende Arbeitsschritte ausgeführt werden:

- Installieren Sie Option 34 von i5/OS. Hierbei handelt es sich um die Browser-basierte Funktion DCM.
- Installieren Sie IBM HTTP-Server für i5/OS (5722-DG1), und starten Sie anschließend die Administrationsserverinstanz.
- TCP muss auf dem System so konfiguriert sein, dass ein Web-Browser und die Administrationsserverinstanz des HTTP-Servers verwendet werden können, um auf DCM zuzugreifen.

**Anmerkung:** Sie können nur dann Zertifikate erstellen, wenn alle vorausgesetzten Programme zuvor installiert wurden. Ist ein erforderliches Programm nicht installiert, zeigt DCM eine Fehlermeldung an, in der Sie zur Installation der fehlenden Komponente aufgefordert werden.

### Hinweise zur Sicherung und Wiederherstellung von DCM-Daten

In diesem Abschnitt erfahren Sie, wie wichtige DCM-Daten zum Sicherungs- und Wiederherstellungsplan Ihres Systems hinzugefügt werden können.

Die verschlüsselten Kennwörter der Schlüsseldatenbank, die zum Zugriff auf Zertifikatsspeicher in Digital Certificate Manager (DCM) verwendet werden, werden in einer speziellen Sicherheitsdatei auf Ihrem System abgelegt, d. h. *verdeckt gespeichert*. Wenn Sie DCM zum Erstellen eines Zertifikatsspeichers auf dem System verwenden, dann führt DCM automatisch eine verdeckte Speicherung des zugehörigen Kennworts durch. Unter bestimmten Bedingungen muss die verdeckte Speicherung von Kennwörtern für Zertifikatsspeicher jedoch manuell durchgeführt werden.

Eine derartige Situation tritt z. B. ein, wenn Sie DCM zum Erstellen eines Zertifikats für ein anderes iSeries-System verwenden oder die Zertifikatsdateien auf dem Zielsystem zum Erstellen eines neuen

Zertifikatsspeichers einsetzen. In diesem Fall müssen Sie den neu erstellen Zertifikatsspeicher öffnen und die Task **Kennwort ändern** benutzen, um das Kennwort des Zertifikatsspeichers auf den Zielsystem zu ändern. Hierdurch wird sichergestellt, dass das neue Kennwort von DCM verdeckt gespeichert wird. Wenn es sich bei dem Zertifikatsspeicher um einen Speicher für andere Systemzertifikate handelt, müssen Sie auch angeben, dass die Auswahl **Automatisches Anmelden** benutzt werden soll, wenn Sie das Kennwort ändern. Weitere Informationen zur Verwendung von DCM für die Erstellung von Zertifikaten für andere iSeries-Systeme finden Sie unter "Lokale Zertifizierungsinstanz zum Ausstellen von Zertifikaten für andere iSeries-Systeme verwenden".

Darüber hinaus müssen Sie die Auswahl **Automatisches Anmelden** immer dann angeben, wenn Sie das Kennwort eines Speichers für andere Systemzertifikate ändern oder zurücksetzen.

Um sicherzustellen, dass eine Gesamtsicherung aller kritischen DCM-Daten vorhanden ist, müssen Sie wie folgt vorgehen:

- Verwenden Sie den Befehl SAV (Sichern), um alle Dateien mit den Erweiterungen .KDB und .RDB zu sichern. Jeder DCM-Zertifikatsspeicher besteht aus zwei Dateien, wobei eine über die Erweiterung .KDB und die andere über die Erweiterung .RDB verfügt.
- Mit dem Befehl SAVSYS (System sichern) und dem Befehl SAVSECDTA (Sicherheitsdaten sichern) können Sie die spezielle Sicherheitsdatei sichern, die die Kennwörter der Schlüsseldatenbank für den Zertifikatsspeicherzugriff enthält. Zum Zurücksichern der DCM-Kennwortsicherheitsdatei können Sie den Befehl RSTUSRPRF (Benutzerprofile zurücksichern) verwenden und hierbei für USRPRF (Benutzerprofil) die Einstellung \*ALL angeben.

Beim Zurücksichern sollte außerdem die Verwendung der Operation SAVSECDTA und das Risiko bedacht werden, dass die Synchronisation der aktuellen Kennwörter des Zertifikatsspeichers mit den in der DCM-Kennwortsicherheitsdatei gespeicherten Kennwörtern möglicherweise nicht mehr gewährleistet ist. Wenn Sie das Kennwort eines Zertifikatsspeichers nach der Ausführung der Operation SAVSECDTA, jedoch vor dem Zurücksichern der Daten dieser Operation ändern, ist die Synchronisation des aktuellen Kennworts für den Zertifikatsspeicher mit dem in der zurückgespeicherten Datei definierten Kennwort nicht mehr gegeben.

Um diesen Fehler zu vermeiden, müssen Sie die Task **Kennwort ändern** (unter **Zertifikatsspeicher verwalten** im Navigationsrahmen) in DCM verwenden, um die Kennwörter des Zertifikatsspeichers zu ändern, nachdem Sie die Daten der Operation SAVSECDTA zurückgespeichert haben. Hierdurch wird die korrekte Synchronisation der Kennwörter wiederhergestellt. In diesem Fall darf die Schaltfläche **Kennwort zurücksetzen** allerdings nicht verwendet werden. Diese wird angezeigt, wenn Sie einen zu öffnenden Zertifikatsspeicher auswählen. Wenn Sie das Zurücksetzen des Kennwortes anfordern, versucht DCM, das verdeckt gespeicherte Kennwort abzurufen. Wenn dieses nicht korrekt mit dem aktuellen Kennwort synchronisiert ist, schlägt die Zurücksetzung fehl. Wenn die Kennwörter für Zertifikatsspeicher nicht häufig geändert werden, ist es möglicherweise sinnvoll, die Operation SAVSECDTA bei jeder Kennwortänderung durchzuführen. Hierdurch wird sichergestellt, dass immer die aktuellste, verdeckt gespeicherte Kennwortversion zur Verfügung steht, um diese Daten im Notfall zurücksichern zu können.

#### Zugehörige Tasks

„Lokale Zertifizierungsinstanz zum Ausstellen von Zertifikaten für andere iSeries-Systeme verwenden“ auf Seite 66

Dieses Thema enthält Informationen zum Einsatz einer privaten lokalen Zertifizierungsinstanz auf einem System für die Ausstellung von Zertifikaten, die auf anderen iSeries-Systemen benutzt werden sollen.

## Typen digitaler Zertifikate

In diesen Informationen wird erläutert, welche unterschiedlichen Typen digitaler Zertifikate unterstützt werden und wie diese in Digital Certificate Manager (DCM) eingesetzt werden können.

Sie können Digital Certificate Manager (DCM) verwenden, um die folgenden Zertifikatstypen zu verwalten:

### **Zertifikate von Zertifizierungsinstanzen (CAs)**

Ein Zertifikat der Zertifizierungsinstanz ist ein digitaler Berechtigungsnachweis, der die Identität der Zertifizierungsinstanz (CA) belegt, die Eigner des Zertifikats ist. Das Zertifikat der Zertifizierungsinstanz enthält Informationen, die zur Identifizierung der Zertifizierungsinstanz benötigt werden, sowie deren öffentlichen Schlüssel. Andere können den öffentlichen Schlüssel des Zertifikats der Zertifizierungsinstanz zum Überprüfen der Authentizität der Zertifikate verwenden, die von der Zertifizierungsinstanz ausgestellt und signiert werden. Ein Zertifikat der Zertifizierungsinstanz kann von einer anderen Zertifizierungsinstanz, z. B. VeriSign, oder durch die Zertifizierungsinstanz selbst signiert sein, wenn es sich bei dieser um eine unabhängige Entität handelt. Die lokale Zertifizierungsinstanz, die mit Digital Certificate Manager erstellt und betrieben wird, ist eine unabhängige Entität. Andere können den öffentlichen Schlüssel des Zertifikats der Zertifizierungsinstanz zum Überprüfen der Authentizität der Zertifikate verwenden, die von der Zertifizierungsinstanz ausgestellt und signiert werden. Um ein Zertifikat für SSL, zum Signieren von Objekten oder Prüfen von Objektsignaturen zu verwenden, müssen Sie über eine Kopie des Zertifikats der ausstellenden Zertifizierungsinstanz verfügen.

### **Server- oder Client-Zertifikate**

Ein Server- oder Client-Zertifikat ist ein digitaler Berechtigungsnachweis, mit dem die Server- oder Client-Anwendung identifiziert wird, die das Zertifikat für die gesicherte Kommunikation verwendet. Server- oder Client-Zertifikate enthalten Identifikationsinformationen über die Organisation, die Eigner der Anwendung ist, wie beispielsweise den registrierten Namen des Systems. Das Zertifikat enthält darüber hinaus den öffentlichen Schlüssel des Systems. Ein Server benötigt ein digitales Zertifikat, um Secure Sockets Layer (SSL) für die gesicherte Kommunikation einsetzen zu können. Anwendungen, die digitale Zertifikate unterstützen, können anhand eines Serverzertifikats die Identität des Servers feststellen, wenn der Client auf diesen zugreift. Die Anwendung kann anschließend auf der Grundlage der Authentifizierung des Zertifikats eine SSL-verschlüsselte Sitzung zwischen dem Client und dem Server starten. Diese Zertifikatstypen können nur über den Zertifikatsspeicher \*SYSTEM verwaltet werden.

### **Objektsignierzertifikate**

Ein Objektsignierzertifikat ist ein Zertifikat, das Sie verwenden können, um ein Objekt digital zu "signieren". Durch das Signieren können Sie sowohl die Objektintegrität als auch den Absender oder Eigner des Objekts überprüfen. Das Zertifikat kann zum Signieren einer Vielzahl von Objekten einschließlich der meisten Objekte im IFS (Integrated File System) sowie für \*CMD-Objekte verwendet werden. Eine vollständige Liste aller signierbaren Objekte finden Sie im Abschnitt zur Objektsignierung und Signaturprüfung. Wenn Sie den privaten Schlüssel eines Objektsignierzertifikats zum Signieren eines Objekts verwenden, muss der Objektempfänger Zugriff auf eine Kopie des zugehörigen Signaturüberprüfungszertifikats haben, damit die Objektsignatur korrekt authentifiziert werden kann. Diese Zertifikatstypen können nur über den Zertifikatsspeicher \*OBJECTSIGNING verwaltet werden.

### **Signaturüberprüfungszertifikate**

Ein Signaturüberprüfungszertifikat ist eine Kopie eines Objektsignierzertifikats ohne dessen privaten Schlüssel. Der öffentliche Schlüssel des Signaturüberprüfungszertifikats wird verwendet, um die mit einem Objektsignierzertifikat erstellte digitale Signatur zu authentifizieren. Das Überprüfen der Signatur ermöglicht Ihnen, den Absender des Objekts festzustellen und zu prüfen, ob das Objekt seit dem Signieren geändert wurde. Diese Zertifikatstypen können nur über den Zertifikatsspeicher \*SIGNATUREVERIFICATION verwaltet werden.

### **Benutzerzertifikate**

Ein Benutzerzertifikat ist ein digitaler Berechtigungsnachweis, der die Identität des Clients oder Benutzers bestätigt, der Eigner des Zertifikats ist. Zahlreiche Anwendungen bieten nun Unterstützung für die Verwendung von Zertifikaten zur Authentifizierung von Benutzern gegenüber Ressourcen, an Stelle von Benutzernamen und Kennwörtern. Digital Certificate Manager (DCM) ordnet Benutzerzertifikate, die von Ihrer privaten Zertifizierungsinstanz ausgestellt werden,



automatisch dem iSeries-Benutzerprofil des betreffenden Benutzers zu. Außerdem können Sie DCM verwenden, um Benutzerzertifikate, die von anderen Zertifizierungsinstanzen ausgestellt werden, dem iSeries-Benutzerprofil des Benutzers zuzuordnen.

Wenn Sie zur Verwaltung Ihrer Zertifikate Digital Certificate Manager (DCM) verwenden, organisiert und verwaltet DCM diese Zertifikate und die zugehörigen privaten Schlüssel auf der Basis dieser Klassifizierungen in einem Zertifikatsspeicher.

**Anmerkung:** Wenn auf Ihrem System ein IBM Verschlüsselungskoprozessor installiert ist, können Sie weitere Auswahlmöglichkeiten für die Speicherung des privaten Schlüssels für Ihre Zertifikate angeben. (Eine Ausnahme bilden hierbei allerdings Objektsignierzertifikate.) Sie können den privaten Schlüssel im Verschlüsselungskoprozessor selbst speichern. Sie können den Verschlüsselungskoprozessor aber auch verwenden, um den privaten Schlüssel zu verschlüsseln und ihn anstatt in einem Zertifikatsspeicher in einer speziellen Schlüsseldatei zu speichern. Benutzerzertifikate und die zugehörigen privaten Schlüssel werden jedoch immer im Benutzersystem gespeichert, entweder in der Browser-Software oder in einer Datei, damit sie von anderen Client-Softwarepaketen verwendet werden können.

#### **Zugehörige Konzepte**

„Secure Sockets Layer (SSL)“ auf Seite 11

Der ursprünglich von Netscape entwickelte SSL-Standard hat sich zum Branchenstandard für die Sitzungsverschlüsselung zwischen Clients und Servern entwickelt.

„Zertifikatsspeicher“ auf Seite 8

Ein Zertifikatsspeicher ist eine spezielle Schlüsseldatenbankdatei, die Digital Certificate Manager (DCM) verwendet, um digitale Zertifikate zu speichern.

## **Öffentliche vs. private Zertifikate**

In diesen Informationen wird erläutert, wie der Zertifikatstyp (öffentlich oder privat) festgestellt werden kann, der die individuellen Unternehmensanforderungen des Kunden optimal erfüllt.

Sie können Zertifikate einer öffentlichen Zertifizierungsinstanz verwenden oder eine private Zertifizierungsinstanz erstellen und betreiben, mit der eigene Zertifikate ausgestellt werden. Für welche Variante Sie sich entscheiden, hängt von der geplanten Verwendung der Zertifikate ab. Nachdem Sie sich für den Zertifizierungstyp entschieden haben, der für die Ausstellung von Zertifikaten verwendet werden soll, sollten Sie den Zertifikatsimplementierungstyp auswählen, der Ihren Sicherheitsanforderungen am besten entspricht. Sie haben folgende Auswahlmöglichkeiten, um Zertifikate abzurufen:

- Kaufen der Zertifikate von einer öffentlichen Internet-Zertifizierungsinstanz (CA).
- Betreiben einer eigenen lokalen Zertifizierungsinstanz, um private Zertifikate für eigene Benutzer und Anwendungen auszustellen.
- Verwenden einer Kombination von Zertifikaten öffentlicher Internet-Zertifizierungsinstanzen und einer eigenen lokalen Zertifizierungsinstanz.

Welche dieser Auswahlmöglichkeiten zur Implementierung Sie nutzen werden, hängt von einer Reihe von Faktoren ab, wobei einer der wichtigsten Faktoren die Umgebung ist, in der die Zertifikate verwendet werden. Es folgen einige Informationen, die Ihnen helfen sollen festzustellen, welche Implementierung für Ihre Geschäftsumgebung und Ihre Sicherheitsanforderungen geeignet ist.

### **Öffentliche Zertifikate verwenden**

Öffentliche Internet-Zertifizierungsinstanzen (CAs) stellen Zertifikate für alle Personen aus, die die erforderlichen Gebühren bezahlen. Allerdings benötigt auch eine Internet-Zertifizierungsinstanz einen Nachweis der Identität des Anforderers, bevor ein Zertifikat ausgestellt wird. Die Art und Weise dieses Nachweises kann jedoch abhängig von den jeweiligen Identifikationsrichtlinien der Zertifizierungsinstanz variieren. Bevor Sie von einer Zertifizierungsinstanz Zertifikate anfordern bzw. die von der betreffenden Zertifizierungsinstanz ausgestellten Zertifikate anerkennen, sollten Sie bestimmen, ob die Strenge der

Identifikationsrichtlinien dieser Zertifizierungsinstanz Ihren Sicherheitsanforderungen entspricht. Nach der Entwicklung der PKIX-Standards (Public Key Infrastructure for X.509) stellen einige öffentliche Zertifizierungsinstanzen sehr viel strengere Identifikationsstandards für die Ausstellung von Zertifikaten bereit. Der Prozess für die Beantragung von Zertifikaten solcher PKIX-Zertifizierungsinstanzen ist zwar komplizierter, die von diesen Zertifizierungsinstanzen ausgestellten Zertifikate gewährleisten jedoch größere Sicherheit beim Zugriff auf Anwendungen durch bestimmte Benutzer. Digital Certificate Manager (DCM) ermöglicht die Verwendung und Verwaltung von Zertifikaten, die von PKIX-Zertifizierungsinstanzen ausgestellt werden, die diese neuen Zertifikatsstandards anwenden.

Darüber hinaus müssen Sie die Kosten berücksichtigen, die durch die Verwendung einer öffentlichen Zertifizierungsinstanz für die Ausstellung von Zertifikaten entstehen. Wenn Sie nur für eine begrenzte Anzahl von Server- und Client-Anwendungen und Benutzern Zertifikate benötigen, sind die Kosten für Sie wahrscheinlich nicht von entscheidender Bedeutung. Wenn Sie jedoch für eine große Anzahl *privater* Benutzer öffentliche Zertifikate zur Authentifizierung von Clients benötigen, kann der Kostenfaktor eine wichtige Rolle spielen. In diesem Fall sollten Sie außerdem den Verwaltungs- und Programmieraufwand beachten, der erforderlich ist, um Serveranwendungen so zu konfigurieren, dass sie nur eine bestimmte Untergruppe von Zertifikaten akzeptieren, die von einer bestimmten öffentlichen Zertifizierungsinstanz ausgestellt werden.

Die Verwendung der von einer öffentlichen Zertifizierungsinstanz ausgestellten Zertifikate spart Ihnen möglicherweise Zeit und Ressourcen, da zahlreiche Server-, Client- und Benutzeranwendungen so konfiguriert sind, dass sie die meisten bekannten öffentlichen Zertifizierungsinstanzen erkennen. Auch werden wahrscheinlich viele andere Unternehmen und Benutzer eher die von einer bekannten öffentlichen Zertifizierungsinstanz ausgestellten Zertifikate erkennen und anerkennen als die von Ihrer privaten lokalen Zertifizierungsinstanz ausgestellten Zertifikate.

### **Private Zertifikate verwenden**

Wenn Sie eine eigene lokale Zertifizierungsinstanz erstellen, können Sie Zertifikate an Systeme und Benutzer in einem eingeschränkteren Bereich, z. B. innerhalb Ihres Unternehmens oder Ihrer Organisation, ausstellen. Das Erstellen und Verwalten einer eigenen lokalen Zertifizierungsinstanz ermöglicht Ihnen das Ausstellen von Zertifikaten ausschließlich an die Benutzer, die als anerkannte Mitglieder Ihrer Gruppe gelten. Hierdurch lässt sich die Sicherheit verbessern, da Sie besser steuern können, wer über Zertifikate verfügt, d. h. wer auf Ihre Ressourcen zugreifen kann. Ein möglicher Nachteil der Verwendung einer eigenen lokalen Zertifizierungsinstanz liegt in dem Aufwand an Zeit und Ressourcen, den Sie hierbei investieren müssen. Mit Digital Certificate Manager (DCM) kann dieser Prozess jedoch vereinfacht werden.

Wenn Sie zum Ausstellen von Zertifikaten für Benutzer zum Zweck der Client-Authentifizierung eine lokale Zertifizierungsinstanz (CA) verwenden, müssen Sie festlegen, wo die Benutzerzertifikate gespeichert werden sollen. Wenn Benutzer Zertifikate über DCM von der lokalen Zertifizierungsinstanz abrufen müssen, werden ihre Zertifikate standardmäßig zusammen mit einem Benutzerprofil gespeichert. Sie können DCM allerdings auch so konfigurieren, dass EIM (Enterprise Identity Mapping) eingesetzt wird. Auf diese Weise werden die Zertifikate an einer LDAP-Position (LDAP = Lightweight Directory Access Protocol) gespeichert. Wenn Sie keine Benutzerzertifikate zuordnen oder diese nicht zusammen mit einem Benutzerprofil speichern wollen, können Sie APIs verwenden, um Zertifikate über das Programm an Nicht-iSeries-Benutzer auszustellen.

**Anmerkung:** Unabhängig davon, welche Zertifizierungsinstanz Sie für die Ausstellung Ihrer Zertifikate verwenden, wird vom Systemadministrator gesteuert, welche Zertifizierungsinstanzen von den Anwendungen auf dessen System anerkannt werden. Wenn in Ihrem Browser die Kopie eines Zertifikats für eine bekannte Zertifizierungsinstanz vorhanden ist, kann Ihr Browser so definiert werden, dass er von dieser Zertifizierungsinstanz ausgestellte Serverzertifikate anerkennt. Administratoren definieren CA-Zertifikate im entsprechenden DCM-Zertifikatsspeicher als anerkannt, der Kopien der meisten Zertifikate bekannter öffentlicher Zertifizierungsinstanzen enthält. Wenn ein Zertifikat der Zertifizierungsinstanz jedoch nicht

in Ihrem Zertifikatsspeicher vorhanden ist, kann Ihr Server keine von der betreffenden Zertifizierungsinstanz ausgestellten Benutzer- oder Client-Zertifikate anerkennen, bis Sie eine Kopie des CA-Zertifikats abgerufen und importiert haben. Das CA-Zertifikat muss im korrekten Dateiformat vorliegen, und Sie müssen es in Ihren DCM-Zertifikatsspeicher aufnehmen.

Möglicherweise helfen Ihnen einige allgemeine Beispiele für Szenarios über die Verwendung von Zertifikaten dabei festzustellen, ob für Ihre Geschäftsumgebung und Ihre Sicherheitsanforderungen eher öffentliche oder private Zertifikate geeignet sind.

### **Zugehörige Tasks**

Nachdem Sie entschieden haben, wie Sie Zertifikate verwenden wollen und welche Zertifikatstypen für Sie in Frage kommen, sollten Sie sich folgende Prozeduren ansehen, um sich über die Verwendung von Digital Certificate Manager für den praktischen Einsatz von Zertifikaten zu informieren:

- Der Abschnitt zum Erstellen und Betreiben einer privaten Zertifizierungsinstanz beschreibt die Tasks, die Sie ausführen müssen, wenn Sie eine lokale Zertifizierungsinstanz zur Ausstellung von privaten Zertifikaten betreiben wollen.
- Der Abschnitt zum Verwalten von Zertifikaten einer öffentlichen Internet-Zertifizierungsinstanz beschreibt die Tasks, die Sie ausführen müssen, wenn Sie Zertifikate von einer bekannten öffentlichen Zertifizierungsinstanz, auch einer PKIX-CA, verwenden wollen.
- Der Abschnitt zum Verwenden einer lokalen Zertifizierungsinstanz auf anderen iSeries-Servern beschreibt die Tasks, die Sie ausführen müssen, wenn Sie Zertifikate einer privaten lokalen Zertifizierungsinstanz auf mehreren Systemen verwenden wollen.

### **Zugehörige Konzepte**

„Zertifikate einer öffentlichen Internet-Zertifizierungsinstanz verwalten“ auf Seite 56

In diesem Abschnitt erfahren Sie, wie Sie Zertifikate einer öffentlichen Internet-Zertifizierungsinstanz verwalten können, indem Sie einen Zertifikatsspeicher erstellen.

„Öffentliche vs. private Zertifikate“ auf Seite 35

In diesen Informationen wird erläutert, wie der Zertifikatstyp (öffentlich oder privat) festgestellt werden kann, der die individuellen Unternehmensanforderungen des Kunden optimal erfüllt.

„Zertifikate erstmals definieren“ auf Seite 46

Hier erfahren Sie, wie Zertifikate einer öffentlichen Internet-Zertifizierungsinstanz verwaltet oder eine private lokale Zertifizierungsinstanz erstellt und betrieben werden kann, mit der Sie selbst Zertifikate ausstellen können.

„Digitale Zertifikate für das Signieren von Objekten“ auf Seite 42

In diesen Informationen wird erläutert, wie Zertifikate zum Sicherstellen der Objektintegrität oder zum Prüfen der digitalen Signatur von Objekten eingesetzt werden können, um deren Authentizität zu prüfen.

### **Zugehörige Tasks**

„Digitale Zertifikate und Enterprise Identity Mapping“ auf Seite 40

Durch den gemeinsamen Einsatz von Enterprise Identity Mapping (EIM) und Digital Certificate Manager (DCM) können Sie ein Zertifikat als Quellenelement einer EIM-Abgleichsoperation verwenden, um eine Zuordnung zwischen dem Zertifikat und einer Zielbenutzeridentität herzustellen, die derselben EIM-Kennung zugeordnet ist.

„Benutzerzertifikat erstellen“ auf Seite 50

In diesen Informationen wird erläutert, wie Benutzer die lokale Zertifizierungsinstanz zum Ausstellen eines Zertifikats für die Client-Authentifizierung verwenden können.

„Lokale Zertifizierungsinstanz erstellen und betreiben“ auf Seite 47

In den vorliegenden Informationen wird erläutert, wie eine lokale Zertifizierungsinstanz (CA) erstellt und betrieben werden kann, um private Zertifikate für Ihre Anwendungen auszustellen.

„Lokale Zertifizierungsinstanz zum Ausstellen von Zertifikaten für andere iSeries-Systeme verwenden“ auf Seite 66

Dieses Thema enthält Informationen zum Einsatz einer privaten lokalen Zertifizierungsinstanz auf einem System für die Ausstellung von Zertifikaten, die auf anderen iSeries-Systemen benutzt werden sollen.

### **Zugehörige Verweise**

„APIs über das Programm zum Ausstellen von Zertifikaten für Nicht-iSeries-Benutzer verwenden“ auf Seite 54

In diesen Informationen wird erläutert, wie Sie die lokale Zertifizierungsinstanz zum Ausstellen privater Zertifikate an Benutzer verwenden können, ohne dass das Zertifikat einem iSeries-Benutzerprofil zugeordnet werden muss.

## **Digitale Zertifikate für die gesicherte SSL-Kommunikation**

In diesen Informationen wird erläutert, wie Zertifikate zum Herstellen gesicherter Kommunikationssitzungen für Anwendungen benutzt werden können.

Mit Hilfe von digitalen Zertifikaten können Sie Anwendungen für die Verwendung von SSL konfigurieren (siehe hierzu *Configure applications to use the Secure Sockets Layer (SSL)*), um auf diese Weise gesicherte Kommunikationssitzungen zu gewährleisten. Beim Aufbauen einer SSL-Sitzung stellt Ihr Server stets eine Kopie seines Zertifikats für die Gültigkeitsprüfung durch den Client zur Verfügung, der die Verbindung anfordert. Verwenden einer SSL-Verbindung:

- Hierdurch wird gegenüber dem Client oder Endbenutzer die Authentizität Ihrer Site sichergestellt.
- Hierdurch wird eine verschlüsselte Kommunikationssitzung zur Verfügung gestellt, um sicherzustellen, dass Daten, die über die Verbindung gesendet werden, vertraulich bleiben.

Die Server- und Client-Anwendungen arbeiten wie folgt zusammen, um Datensicherheit zu gewährleisten:

1. Die Serveranwendung legt der Client-Anwendung (Benutzeranwendung) das Zertifikat als Nachweis für die Identität des Servers vor.
2. Die Client-Anwendung überprüft die Identität des Servers anhand einer Kopie des Zertifikats der ausstellenden Zertifizierungsinstanz (CA). (Die Client-Anwendung muss Zugriff auf eine lokal gespeicherte Kopie des betreffenden Zertifikats der Zertifizierungsinstanz haben.)
3. Die Server- und Client-Anwendungen vereinbaren einen symmetrischen Chiffrierschlüssel und verwenden diesen für die Verschlüsselung der Kommunikationssitzungen.
4. Wahlweise kann der Server den Client nun auffordern, einen Identitätsnachweis zu liefern, bevor der Zugriff auf die angeforderten Ressourcen gewährt wird. Um Zertifikate als Identitätsnachweis verwenden zu können, müssen die kommunizierenden Anwendungen das Verwenden von Zertifikaten für die Benutzerauthentifizierung unterstützen.

SSL verwendet während der einleitenden SSL-Verarbeitung Algorithmen mit asymmetrischen Schlüsseln (öffentlicher Schlüssel), um einen symmetrischen Schlüssel zu vereinbaren, der anschließend für die Verschlüsselung und Entschlüsselung der Anwendungsdaten für die betreffende SSL-Sitzung verwendet wird. Dies bedeutet, dass Ihr Server und der Client für jede Verbindung unterschiedliche Sitzungsschlüssel verwenden, die automatisch nach einer festgelegten Zeitspanne verfallen. In dem unwahrscheinlichen Fall, dass ein bestimmter Sitzungsschlüssel abgefangen und entschlüsselt wird, kann dieser Sitzungsschlüssel nicht mehr zur Ableitung zukünftiger Schlüssel verwendet werden.

### **Zugehörige Konzepte**

„Digitale Zertifikate für die Benutzerauthentifizierung“

Im Folgenden wird erläutert, wie Zertifikate zum Bereitstellen von Verfahren zur verbesserten Authentifizierung von Benutzern eingesetzt werden können, die auf iSeries-Systemressourcen zugreifen.

## **Digitale Zertifikate für die Benutzerauthentifizierung**

Im Folgenden wird erläutert, wie Zertifikate zum Bereitstellen von Verfahren zur verbesserten Authentifizierung von Benutzern eingesetzt werden können, die auf iSeries-Systemressourcen zugreifen.

Bisher haben Benutzer den Zugriff auf Ressourcen von einer Anwendung oder einem System mittels ihres Benutzernamens und Kennworts erhalten. Sie können die Systemsicherheit verbessern, indem Sie (an Stelle der Benutzernamen und Kennwörter) digitale Zertifikate verwenden, um Sitzungen zwischen zahlreichen Serveranwendungen und Benutzern zu authentifizieren und zu berechtigen. Außerdem können Sie Digital Certificate Manager (DCM) verwenden, um dem iSeries-Benutzerprofil eines Benutzers oder einer anderen Benutzeridentität ein Benutzerzertifikat zuzuordnen. Anschließend verfügt das Zertifikat über dieselben Berechtigungen wie die zugeordnete Benutzeridentität bzw. das zugeordnete Benutzerprofil. Alternativ hierzu können Sie APIs verwenden, um Ihre private lokale Zertifizierungsinstanz über das Programm zum Ausstellen von Zertifikaten an Benutzer anderer Systeme als iSeries zu verwenden. Diese APIs bieten Ihnen die Möglichkeit, private Zertifikate an Benutzer auszustellen, für die kein iSeries-Benutzerprofil bzw. keine andere interne Benutzeridentität angelegt werden soll.

Ein digitales Zertifikat ist ein elektronischer Berechtigungsnachweis, der die Identität der Person, die diesen Nachweis vorlegt, sicher bestätigt. In dieser Hinsicht kann ein Zertifikat mit einem Pass verglichen werden. Beide belegen die Identität einer Person, enthalten eine eindeutige Identifikationsnummer und wurden von einer bekannten Instanz ausgestellt, die den Nachweis als authentisch bestätigt hat. Im Fall eines Zertifikats ist eine Zertifizierungsinstanz (CA) die anerkannte dritte Instanz, die das Zertifikat ausstellt und es als authentischen Berechtigungsnachweis bestätigt.

Zum Zweck der Authentifizierung verwenden Zertifikate einen öffentlichen Schlüssel mit einem zugehörigen privaten Schlüssel. Die Zertifizierungsinstanz bindet diese Schlüssel, zusammen mit weiteren identifizierenden Informationen über den Zertifikatseigner, an das Zertifikat.

Immer mehr Anwendungen unterstützen neuerdings die Verwendung von Zertifikaten für die Client-Authentifizierung während einer SSL-Sitzung. Momentan unterstützen die folgenden iSeries-Anwendungen Zertifikate zur Client-Authentifizierung:

- Telnet-Server
- IBM HTTP-Server für i5/OS (powered by Apache)
- IBM Directory Server
- iSeries Access für Windows (einschließlich iSeries Navigator)
- FTP-Server

Möglicherweise werden zukünftig weitere Anwendungen verfügbar sein, die Zertifikate für die Client-Authentifizierung unterstützen. In der entsprechenden Dokumentation finden Sie Informationen darüber, ob spezifische Anwendungen über diese Unterstützungsfunktion verfügen.

Zertifikate können aus verschiedenen hier aufgeführten Gründen eine bessere Benutzerauthentifizierung bieten:

- Es besteht die Möglichkeit, dass eine Person ihr Kennwort vergisst. Daher müssen Benutzer sich ihre Benutzernamen und Kennwörter merken oder aufschreiben. Aus diesem Grund haben unbefugte Personen mehr Möglichkeiten, Kenntnis von Benutzernamen und Kennwörtern berechtigter Benutzer zu erlangen. Da Zertifikate in einer Datei oder an anderen elektronischen Position gespeichert sind, wird der Zugriff und die Vorlage des Zertifikats zur Authentifizierung von einer Client-Anwendung (und nicht vom Benutzer) durchgeführt. Hierdurch wird sichergestellt, dass Zertifikate berechtigter Benutzer nicht so leicht in die Hände unberechtigter Benutzer gelangen können, solange der unberechtigte Benutzer keinen Zugriff auf das System des berechtigten Benutzers hat. Auch können Zertifikate auf Smart Cards gespeichert werden, um sie zusätzlich vor unberechtigtem Zugriff zu schützen.
- Ein Zertifikat enthält einen privaten Schlüssel, der niemals zusammen mit dem Zertifikat zur Identifizierung gesendet wird. Stattdessen verwendet das System diesen Schlüssel während der Ver- und Entschlüsselung. Andere können den zugehörigen öffentlichen Schlüssel verwenden, um die Identität des Absenders von Objekten zu bestätigen, die mit dem privaten Schlüssel signiert sind.
- Viele Systeme fordern Kennwörter an, die höchstens acht Zeichen umfassen dürfen, wodurch diese Kennwörter schneller erraten werden können. Die Chiffrierschlüssel eines Zertifikats umfassen hun-

derte von Zeichen. Auf Grund der Schlüssellänge, zusammen mit der wahllosen Zusammenstellung der Zeichen, sind Chiffrierschlüssel sehr viel schwerer zu erraten als Kennwörter.

- Schlüssel für digitale Zertifikate bieten mehrere Verwendungsmöglichkeiten, die Kennwörter nicht bieten können, z. B. im Bereich der Datenintegrität und Vertraulichkeit. Sie können Zertifikate und die zugehörigen Schlüssel für folgende Zwecke einsetzen:
  - Gewährleisten der Datenintegrität durch das Feststellen von Änderungen an Daten.
  - Nachweisen der Ausführung einer bestimmten Aktion. Dies wird als 'Unbestreitbarkeit' (Non-repudiation) bezeichnet.
  - Sicherstellen der Vertraulichkeit bei der Datenübertragung durch Verwendung von Secure Sockets Layer (SSL) zur Verschlüsselung von Kommunikationssitzungen.

Weitere Informationen über die Konfiguration von iSeries-Anwendungen zur Verwendung von Zertifikaten für die Client-Authentifizierung während einer SSL-Sitzung finden Sie unter Secure Sockets Layer (SSL) im iSeries Information Center.

#### **Zugehörige Konzepte**

„Digitale Zertifikate für die gesicherte SSL-Kommunikation“ auf Seite 38

In diesen Informationen wird erläutert, wie Zertifikate zum Herstellen gesicherter Kommunikationssitzungen für Anwendungen benutzt werden können.


#### **Zugehörige Verweise**

„APIs über das Programm zum Ausstellen von Zertifikaten für Nicht-iSeries-Benutzer verwenden“ auf Seite 54

In diesen Informationen wird erläutert, wie Sie die lokale Zertifizierungsinstanz zum Ausstellen privater Zertifikate an Benutzer verwenden können, ohne dass das Zertifikat einem iSeries-Benutzerprofil zugeordnet werden muss.

## **Digitale Zertifikate und Enterprise Identity Mapping**

Durch den gemeinsamen Einsatz von Enterprise Identity Mapping (EIM) und Digital Certificate Manager (DCM) können Sie ein Zertifikat als Quellenelement einer EIM-Abgleichsuchoperation verwenden, um eine Zuordnung zwischen dem Zertifikat und einer Zielbenutzeridentität herzustellen, die derselben EIM-Kennung zugeordnet ist.

Bei EIM handelt es sich um eine -Technologie, mit der Sie die Benutzeridentitäten Ihres Unternehmens einschließlich der vorhandenen Benutzerprofile und Benutzerzertifikate verwalten können. Ein Benutzername und das zugehörige Kennwort stellen die am häufigsten verwendete Benutzeridentität dar. Darüber hinaus können als Benutzeridentität auch Zertifikate verwendet werden. Bestimmte Anwendungen sind so konfiguriert, dass Benutzer mit Hilfe eines Benutzerzertifikats und nicht über ihren Benutzernamen und das zugehörige Kennwort authentifiziert werden.

Sie können EIM zum Erstellen von Zuordnungen zwischen Benutzeridentitäten verwenden. Auf diese Weise kann sich ein Benutzer mit einer Benutzeridentität authentifizieren und auf die Ressourcen einer anderen Benutzeridentität zugreifen, ohne dass der Benutzer die erforderliche Benutzeridentität angeben muss. Für diese Vorgehensweise müssen Sie in EIM eine Zuordnung zwischen einer Benutzeridentität und der jeweils anderen Benutzeridentität herstellen. Benutzeridentitäten können in verschiedenen Formen (z. B. als Benutzerzertifikate) vorliegen. Sie können entweder einzelne Zuordnungen zwischen einer EIM-Kennung und den verschiedenen Benutzeridentitäten herstellen, die zu dem Benutzer gehören, der mit Hilfe der EIM-Kennung identifiziert wird. Alternativ hierzu können Sie auch Richtlinienzuordnungen erstellen, mit denen eine Gruppe von Benutzeridentitäten einer einzelnen Zielbenutzeridentität zugeordnet werden kann. Benutzeridentitäten können in verschiedenen Formen (z. B. als Benutzerzertifikate) vorliegen. Bei der Herstellung dieser Zuordnungen können die Benutzerzertifikate den entsprechenden EIM-Kennungen zugeordnet werden. Auf diese Weise wird die Verwendung von Zertifikaten für die Authentifizierung vereinfacht.

Um die EIM-Funktion zur Verwaltung von Benutzerzertifikaten zu nutzen, müssen Sie die EIM-Konfigurations-Tasks vor den jeweils erforderlichen DCM-Konfigurations-Tasks ausführen:

1. Verwenden Sie zur Konfiguration von EIM den **EIM-Konfigurationsassistenten** im **iSeries Navigator**.
2. Erstellen Sie eine EIM-Kennung für alle Benutzer, die EIM nutzen sollen.
3. Erstellen Sie eine Zielzuordnung zwischen allen EIM-Kennungen und dem Benutzerprofil der Benutzer im lokalen i5/OS-Benutzerregister, so dass alle Benutzerzertifikate, die der Benutzer über DCM zuordnet oder in DCM erstellt, dem betreffenden Benutzerprofil zugeordnet werden können. Verwenden Sie den EIM-Registerdefinitionsnamen des lokalen **i5/OS**-Benutzerregisters, das im **EIM-Konfigurationsassistenten** angegeben wurde.

Nach Ausführung der erforderlichen EIM-Konfigurations-Tasks müssen Sie die Task **LDAP-Position verwalten** verwenden, um DCM (Digital Certificate Manager) so zu konfigurieren, dass Benutzerzertifikate an einer LDAP-Position (LDAP = Lightweight Directory Access Protocol) anstatt in einem Benutzerprofil gespeichert werden. Wenn Sie EIM und DCM für die gemeinsame Verwendung konfigurieren, verarbeiten die Task **Zertifikat erstellen** für Benutzerzertifikate und die Task **Benutzerzertifikat zuordnen** Zertifikate für die EIM-Verwendung, anstatt diese einem Benutzerprofil zuzuordnen. DCM speichert das Zertifikat im konfigurierten LDAP-Verzeichnis und verwendet den registrierten Namen (DN) des Zertifikats zum Erstellen einer Quellenzuordnung für die zugehörige EIM-Kennung. Hierdurch können Betriebssysteme und Anwendungen das Zertifikat als Quelle für eine EIM-Abgleichsuchoperation verwenden, um eine Zuordnung zwischen dem Zertifikat und der Zielbenutzeridentität herzustellen, die über dieselbe EIM-Kennung verfügt.

Darüber hinaus kann bei der Konfiguration des Systems für den gemeinsamen Einsatz von DCM und EIM das Programm DCM zum Überprüfen des Verfallsdatums von Benutzerzertifikaten auf Unternehmensebene und nicht nur auf Systemebene verwendet werden.

#### **Zugehörige Konzepte**

„Öffentliche vs. private Zertifikate“ auf Seite 35

In diesen Informationen wird erläutert, wie der Zertifikatstyp (öffentlich oder privat) festgestellt werden kann, der die individuellen Unternehmensanforderungen des Kunden optimal erfüllt.

#### **Zugehörige Tasks**

„Benutzerzertifikate nach Verfallsdatum verwalten“ auf Seite 53

Digital Certificate Manager (DCM) unterstützt die Verwaltung von Zertifikaten auf der Basis des Verfallsdatums. Mit Hilfe dieser Funktion können Administratoren das Verfallsdatum von Benutzerzertifikaten auf dem lokalen iSeries-System überprüfen. Die Unterstützungsfunktion für die Verwaltung von Zertifikaten auf der Basis des Verfallsdatums kann zusammen mit EIM (Enterprise Identity Mapping) eingesetzt werden. Auf diese Weise kann DCM vom Administrator auf Unternehmensebene zum Überprüfen des Verfallsdatums von Benutzerzertifikaten verwendet werden.

„LDAP-Position für Benutzerzertifikate verwalten“ auf Seite 86

Dieses Thema enthält Informationen zum Konfigurieren von DCM für die Speicherung von Benutzerzertifikaten unter einer Verzeichnisposition auf einem LDAP-Server (Lightweight Directory Access Protocol), so dass EIM (Enterprise Identity Mapping) auch für Benutzerzertifikate eingesetzt werden kann.

#### **Zugehörige Informationen**

Enterprise Identity Mapping

## **Digitale Zertifikate für VPN-Verbindungen**

In diesen Informationen wird erläutert, wie Zertifikate bei der Konfiguration einer VPN-Verbindung (VPN = Virtual Private Network) eingesetzt werden können.

Sie können digitale Zertifikate zum Einrichten einer iSeries-VPN-Verbindung (VPN = Virtual Private Network) verwenden. Beide Endpunkte einer dynamischen VPN-Verbindung müssen sich gegenseitig authentifizieren können, um die Verbindung zu aktivieren. Die gegenseitige Endpunktauthentifizierung wird von den IKE-Servern (IKE = Internet Key Exchange) der jeweiligen Endeinheiten ausgeführt. Nach

der erfolgreichen Authentifizierung vereinbaren die IKE-Server die Verschlüsselungsverfahren und -algorithmen, die zur Sicherung der VPN-Verbindung eingesetzt werden sollen.

Eine Methode, die die IKE-Server zur gegenseitigen Authentifizierung verwenden können, ist der Einsatz eines vorab bekannten gemeinsamen Schlüssels. Der Einsatz eines solchen vorab verteilten Schlüssels ist weniger sicher, da dieser manuell an den Administrator des anderen VPN-Endpunkts übertragen werden muss. Hierbei ergibt sich das Risiko, dass der Schlüssel während der Übergabe nicht vor dem Zugriff unberechtigter Personen geschützt ist.

Dieses Risiko kann vermieden werden, indem an Stelle vorab bekannter gemeinsamer Schlüssel digitale Zertifikate zur Authentifizierung der Endpunkte benutzt werden. Der IKE-Server kann jetzt das Zertifikat des anderen Servers authentifizieren, um eine Verbindung herzustellen, über die die von den Servern zur Sicherung der Verbindung benutzten Verschlüsselungsverfahren und -algorithmen vereinbart werden können.

Digital Certificate Manager (DCM) kann zum Verwalten der Zertifikate benutzt werden, die vom IKE-Server zum Herstellen einer dynamischen VPN-Verbindung verwendet werden. Hierbei müssen Sie als erstes entscheiden, ob Sie für den IKE-Server öffentliche Zertifikate verwenden oder selbst private Zertifikate ausstellen wollen.

Bei bestimmten VPN-Implementierungen ist es erforderlich, dass das Zertifikat Informationen zu alternativen Namen des Zertifikatsinhabers wie z. B. Domännennamen oder eine E-Mail-Adresse enthält, die zusätzlich zu den Standardinformationen zum registrierten Namen definiert sind. Wenn Sie zum Ausstellen von Zertifikaten die lokale Zertifizierungsinstanz von DCM verwenden, können Sie alternative Angaben zum Namen des Zertifikatsinhabers für das Zertifikat machen. Hierdurch stellen Sie sicher, dass die VPN-Verbindung mit anderen VPN-Implementierungen kompatibel ist, die diese möglicherweise zur Authentifizierung benötigen.

Weitere Informationen zur Verwaltung von Zertifikaten für Ihre VPN-Verbindungen finden Sie in den folgenden Quellen:

- Wenn Sie DCM noch nie zum Verwalten von Zertifikaten verwendet haben, finden Sie einführende Informationen unter den folgenden Themen:
  - Unter Lokale Zertifizierungsinstanz erstellen und betreiben wird die Verwendung von DCM zum Ausstellen privater Zertifikate für Ihre Anwendungen erläutert.
  - Unter Zertifikate einer öffentlichen Internet-Zertifizierungsinstanz verwalten wird die Verwendung von DCM zum Arbeiten mit Zertifikaten einer öffentlichen Zertifizierungsinstanz erläutert.
- Wenn Sie DCM bereits zum Verwalten von Zertifikaten für andere Anwendungen einsetzen, finden Sie in den folgenden Quellen Informationen dazu, wie für eine Anwendung die Benutzung eines bereits vorhandenen Zertifikats festgelegt werden kann und wie diejenigen Zertifikate angegeben werden können, die von der Anwendung akzeptiert und authentifiziert werden:
  - Zertifikatszuordnung für eine Anwendung verwalten erläutert die Verwendung von DCM für die Zuordnung eines vorhandenen Zertifikats zu einer Anwendung wie z. B. zum IKE-Server.
  - CA-Anerkennungsliste für eine Anwendung definieren erläutert, wie Sie angeben können, welche Zertifizierungsinstanzen von einer Anwendung anerkannt werden können, wenn diese bei der Client-Authentifizierung (oder bei VPN) Zertifikate akzeptiert.

### **Zugehörige Informationen**

Configuring a VPN connection

## **Digitale Zertifikate für das Signieren von Objekten**

In diesen Informationen wird erläutert, wie Zertifikate zum Sicherstellen der Objektintegrität oder zum Prüfen der digitalen Signatur von Objekten eingesetzt werden können, um deren Authentizität zu prüfen.



IBM i5/OS bietet Unterstützung für die Verwendung von Zertifikaten zum digitalen Signieren von Objekten. Durch das digitale Signieren von Objekten können Sie die Integrität des Objekthinhalts und darüber hinaus den Ursprung des Objektes selbst überprüfen. Durch die Unterstützungsfunktion zum Signieren von Objekten werden die traditionellen iSeries-Systemtools zur Steuerung der Änderungsberechtigung für Objekte wirkungsvoll ergänzt. Mit den konventionellen Steuerungsmechanismen konnten Objekte nicht gegen unberechtigten Zugriff geschützt werden, während Sie im Internet oder in anderen nicht anerkannten Netzwerken übertragen oder auf einem anderen System als einer iSeries-Einheit gespeichert wurden. Die konventionellen Steuerungsmechanismen ermöglichen darüber hinaus nicht immer die Feststellung unbefugter Änderungen oder Manipulationen eines Objektes. Durch den Einsatz digitaler Signaturen auf Objekten steht Ihnen ein sicheres Mittel zur Feststellung solcher Änderungen an signierten Objekten zur Verfügung.

Zur Anbringung einer digitalen Signatur auf einem Objekt wird mit dem privaten Schlüssel des zugehörigen Zertifikats eine verschlüsselte mathematische Zusammenfassung der im Objekt enthaltenen Daten hinzugefügt. Durch diese Signatur können die Daten gegen unberechtigte Änderungen geschützt werden. Das Objekt und sein Inhalt werden mit der digitalen Signatur nicht, die Zusammenfassung selbst wird jedoch verschlüsselt, um unberechtigte Änderungen zu verhindern. Um zu prüfen, ob das Objekt während der Übertragung nicht geändert wurde und ob es von einer akzeptierten und legitimen Ursprungsadresse stammt, können Sie mit dem öffentlichen Schlüssel des zum Signieren verwendeten Zertifikats die digitale Signatur prüfen. Wenn die Signatur nicht mehr mit den Objektdaten übereinstimmt, wurden diese möglicherweise geändert. In diesem Fall sollten Sie das Objekt nicht verwenden und sich stattdessen an den Signierer wenden, um eine weitere Kopie des signierten Objekts anzufordern.

Wenn der Einsatz digitaler Signaturen Ihren Sicherheitsanforderungen und -richtlinien entspricht, müssen Sie prüfen, ob sich für Ihre Zwecke öffentliche oder selbst ausgestellte, private Zertifikate besser eignen. Wenn Sie Objekte in allgemein zugänglichen öffentlichen Systemen an Benutzer verteilen wollen, eignet sich voraussichtlich eine allgemein bekannte öffentliche Zertifizierungsinstanz (CA) am besten für Sie, um Objekte zu signieren. Durch die Verwendung öffentlicher Zertifikate können Sie sicher sein, dass andere Benutzer die Signaturen auf den von Ihnen verteilten Objekten einfach und kostengünstig prüfen können. Wenn Sie Objekte jedoch ausschließlich innerhalb Ihres Unternehmens verteilen wollen, ist es eventuell günstiger, mit Digital Certificate Manager (DCM) eine eigene lokale Zertifizierungsinstanz zu betreiben und Zertifikate zum Signieren von Objekten selbst auszustellen. Das Signieren von Objekten mit Hilfe von privaten Zertifikaten einer lokalen Zertifizierungsinstanz ist kostengünstiger als das Kaufen der benötigten Zertifikate von einer bekannten öffentlichen CA.

Die Signatur auf einem Objekt steht für das System, auf dem das Objekt signiert wurde, und nicht für einen speziellen Benutzer dieses Systems, obwohl der Benutzer über die entsprechenden Berechtigungen zum Verwenden des Objektsignierzertifikats verfügen muss. Sie können Digital Certificate Manager (DCM) zum Verwalten von Zertifikaten einsetzen, die Sie zum Signieren von Objekten und zum Prüfen von Objektsignaturen verwenden. Darüber hinaus können Sie DCM zum Signieren von Objekten und zum Prüfen von Objektsignaturen benutzen.

#### **Zugehörige Konzepte**

„Öffentliche vs. private Zertifikate“ auf Seite 35

In diesen Informationen wird erläutert, wie der Zertifikatstyp (öffentlich oder privat) festgestellt werden kann, der die individuellen Unternehmensanforderungen des Kunden optimal erfüllt.

„Digitale Zertifikate für die Prüfung von Objektsignaturen“ auf Seite 44

Im Folgenden wird erläutert, wie Zertifikate zum Überprüfen der digitalen Signatur auf Objekten eingesetzt werden können, um deren Authentizität zu prüfen.

#### **Zugehörige Tasks**

„Objektsignaturen prüfen“ auf Seite 89

Sie können Digital Certificate Manager (DCM) verwenden, um die Authentizität digitaler Signaturen auf Objekten zu überprüfen. Durch das Prüfen der Signatur können Sie sicherstellen, dass die in dem Objekt enthaltenen Daten nicht geändert wurden, seit das Objekt vom Eigner signiert wurde.

„Öffentliche Internet-Zertifikate für das Signieren von Objekten verwalten“ auf Seite 59  
Digital Certificate Manager (DCM) kann zum Verwalten öffentlicher Internet-Zertifikate verwendet werden, die zum Ausführen digitaler Signaturen auf Objekten eingesetzt werden.

„Zertifikate zum Prüfen von Objektsignaturen verwalten“ auf Seite 61  
Digital Certificate Manager (DCM) kann zum Verwalten der Signaturüberprüfungszertifikate verwendet werden, die zum Überprüfen der digitalen Signaturen auf Objekten eingesetzt werden.

## **Digitale Zertifikate für die Prüfung von Objektsignaturen**

Im Folgenden wird erläutert, wie Zertifikate zum Überprüfen der digitalen Signatur auf Objekten eingesetzt werden können, um deren Authentizität zu prüfen.

IBM i5/OS bietet Unterstützung für die Verwendung von Zertifikaten zum Prüfen digitaler Signaturen auf Objekten. Um zu prüfen, ob ein Objekt während der Übertragung nicht geändert wurde und ob es von einer anerkannten Ursprungsadresse stammt, können Sie mit dem öffentlichen Schlüssel des zum Signieren verwendeten Zertifikats die ursprüngliche, digitale Signatur prüfen. Wenn die Signatur nicht mehr mit den Objektdaten übereinstimmt, wurden diese möglicherweise geändert. In diesem Fall sollten Sie das Objekt nicht verwenden und sich stattdessen an den Signierer wenden, um eine weitere Kopie des signierten Objekts anzufordern.

Die Signatur auf einem Objekt steht für das System, auf dem das Objekt signiert wurde, und nicht für einen speziellen Benutzer dieses Systems. Bei der Überprüfung digitaler Signaturen müssen Sie angeben, welche Zertifizierungsinstanzen Sie anerkennen wollen und welche Zertifikate beim Signieren von Objekten als anerkannt definiert werden sollen. Wenn Sie eine Zertifizierungsinstanz (CA) anerkennen, können Sie angeben, ob Sie Signaturen anerkennen wollen, die ein Benutzer mit Hilfe eines von dieser anerkannten CA ausgestellten Zertifikats erstellt hat. Wenn Sie die Zertifizierungsinstanz nicht anerkennen, werden auch die von dieser CA ausgestellten Zertifikate bzw. die mit ihren Zertifikaten erstellten Signaturen nicht anerkannt.

### **Systemwert für das Prüfen zurückgespeicherter Objekte (QVfyOjRST)**

Wenn Sie Signaturprüfoperationen ausführen wollen, müssen Sie zu Beginn als eine der wichtigsten Entscheidungen festlegen, welchen Stellenwert Signaturen für Objekte, die auf Ihr System zurückgespeichert werden, haben sollen. Diese Einstellung können Sie mit dem Systemwert QVfyOjRST (Objektsignaturen während des Zurückspeicherns prüfen) steuern. Die Standardeinstellung dieses Systemwerts erlaubt das Zurückspeichern unsignierter Objekte, stellt jedoch sicher, dass signierte Objekte nur dann zurückgespeichert werden können, wenn die Signatur gültig ist. Das System identifiziert ein Objekt nur dann als signiert, wenn es über eine vom System anerkannte Signatur verfügt. Andere, d. h. nicht anerkannte, Objektsignaturen werden ignoriert und die entsprechenden Objekte werden behandelt wie unsignierte Objekte.

Für den Systemwert QVfyOjRST können verschiedene Werte benutzt werden. Die entsprechenden Einstellungen reichen vom Ignorieren aller Signaturen bis zum zwingenden Anfordern gültiger Signaturen für alle Objekte, die auf das System zurückgespeichert werden sollen. Dieser Systemwert ist nur für ausführbare Objekte wirksam, die zurückgespeichert werden. Für Sicherungsdateien oder IFS-Dateien gilt er hingegen nicht. Weitere Informationen zu diesem und anderen Systemwerten finden Sie im Thema zum System Value Finder im iSeries Information Center.

Sie können Digital Certificate Manager (DCM) zum Implementieren Ihrer Einstellungen für die Anerkennung von Zertifikaten und Zertifizierungsinstanzen sowie zum Verwalten der Zertifikate verwenden, die zum Überprüfen von Objektsignaturen eingesetzt werden. Darüber hinaus können Sie DCM zum Signieren von Objekten und zum Prüfen von Objektsignaturen benutzen.

## Zugehörige Konzepte

„Digitale Zertifikate für das Signieren von Objekten“ auf Seite 42

In diesen Informationen wird erläutert, wie Zertifikate zum Sicherstellen der Objektintegrität oder zum Prüfen der digitalen Signatur von Objekten eingesetzt werden können, um deren Authentizität zu prüfen.

## Zugehörige Informationen

System Value Finder

---

## Konfiguration von DCM

In diesen Informationen wird erläutert, wie die erforderlichen Komponenten so konfiguriert werden, dass DCM zur Verwaltung von Zertifikaten und der zugehörigen Schlüssel eingesetzt werden kann.

Digital Certificate Manager (DCM) stellt eine Browser-basierte Benutzerschnittstelle zur Verfügung, die Sie zum Verwalten digitaler Zertifikate für Ihre Anwendungen und Benutzer einsetzen können. Die Benutzerschnittstelle ist in zwei Hauptrahmen unterteilt, die als Navigationsrahmen und als Task-Rahmen bezeichnet werden.


Sie können den Navigationsrahmen zum Auswählen der Tasks für die Verwaltung von Zertifikaten oder der Anwendungen benutzen, die diese verwenden. Bestimmte Tasks werden zwar direkt im Haupt-Navigationsrahmen angezeigt, die Mehrzahl der Tasks im Navigationsrahmen ist jedoch in Kategorien unterteilt. Die Task-Kategorie **Zertifikate verwalten** enthält z. B. eine Vielzahl einzelner geführter Tasks. Hierzu gehören die Tasks 'Zertifikat anzeigen', 'Zertifikat verlängern', 'Zertifikat importieren' etc. Wenn es sich bei einem Element im Navigationsrahmen um eine Kategorie handelt, die mehr als eine Task enthält, wird links daneben ein Pfeil angezeigt. Dieser Pfeil zeigt an, dass nach dem Auswählen des Links für die Kategorie eine erweiterte Liste mit Tasks angezeigt wird, in der Sie die auszuführende Task dann auswählen können.

Mit Ausnahme der Kategorie **Direktaufruf** werden alle Tasks im Navigationsrahmen geführt. Hierbei müssen Sie zur schnellen und einfachen Ausführung der Task lediglich eine Reihe von Arbeitsschritten ausführen. Die Kategorie 'Direktaufruf' stellt eine Gruppe von Zertifikats- und Anwendungsverwaltungsfunktionen zur Verfügung, mit der erfahrene DCM-Benutzer schnell über eine zentrale Seitengruppe auf eine Vielzahl zugehöriger Tasks zugreifen können.

Die im Navigationsrahmen verfügbaren Tasks variieren abhängig von dem Zertifikatsspeicher, mit dem Sie arbeiten. Die Kategorien sowie die Anzahl der im Navigationsrahmen angezeigten Tasks variieren auch abhängig von den Berechtigungen, die in Ihrem i5/OS-Benutzerprofil definiert sind. Alle Tasks zum Arbeiten mit einer Zertifizierungsinstanz und zum Verwalten der von Anwendungen benutzten Zertifikate sowie andere Tasks auf Systemebene stehen nur für iSeries-Sicherheitsbeauftragte oder -Administratoren zur Verfügung. Der Sicherheitsbeauftragte oder Administrator muss über die Sonderberechtigungen \*SECADM und \*ALLOBJ verfügen, um diese Tasks anzuzeigen und zu benutzen. Benutzer ohne diese Sonderberechtigungen können hingegen nur auf Funktionen für Benutzerzertifikate zugreifen.

Wenn Sie Informationen zum Konfigurieren von DCM und zum Definieren der Systemeinstellungen für die Verwaltung von Zertifikaten benötigen, lesen Sie die Abschnitte zu folgenden Themen:

Wenn Sie weitere Informationen zur Verwendung digitaler Zertifikate in Internet-Umgebungen zur Verbesserung Ihrer System- und Netzwerksicherheit benötigen, bietet die Website von VeriSign hervorragende Informationsquellen. Die VeriSign-Website stellt eine umfangreiche Bibliothek mit Veröffentlichungen zu digitalen Zertifikaten sowie zu anderen sicherheitsbezogenen Themen aus dem Internet-Bereich

zur Verfügung. Sie können auf diese Bibliothek über das VeriSign Help Desk  zugreifen.

## Digital Certificate Manager starten

In diesem Abschnitt erfahren Sie, wie Sie auf Ihrem System auf Digital Certificate Manager (DCM) zugreifen können.

Bevor Sie mit den Funktionen von DCM arbeiten können, müssen Sie das Programm starten. Führen Sie die nachfolgenden Arbeitsschritte aus, um sicherzustellen, dass DCM erfolgreich gestartet werden kann:

1. Installieren Sie 5722 SS1 Option 34. Hierbei handelt es sich um Digital Certificate Manager (DCM).
2. Installieren Sie 5722 DG1. Hierbei handelt es sich um den IBM HTTP-Server für i5/OS.
3. So können Sie mit dem iSeries Navigator den HTTP-Server-Administrationsserver starten:
  - a. Starten Sie den **iSeries Navigator**.
  - b. Doppelklicken Sie in der Hauptverzeichnisstruktur auf Ihr System.
  - c. Erweitern Sie die Sicht für **Netzwerk > Server > TCP/IP**.
  - d. Klicken Sie mit der rechten Maustaste auf **HTTP Administration**.
  - e. Klicken Sie auf **Starten**.
4. Starten Sie den Web-Browser.
5. Rufen Sie im Browser Ihres Systems die Seite "iSeries-Tasks" auf. Diese steht unter folgender Adresse zur Verfügung: [http://your\\_system\\_name:2001](http://your_system_name:2001).
6. Wählen Sie in der Liste der Produkte auf der Seite "iSeries-Tasks" den Eintrag **Digital Certificate Manager** aus, um auf die DCM-Benutzerschnittstelle zuzugreifen.

### Zugehörige Konzepte

„Szenario: Zertifikate für die externe Authentifizierung verwenden“ auf Seite 14

Dieses Szenario beschreibt, wann und wie Zertifikate als Authentifizierungsverfahren zum Schutz und zur Eingrenzung des Zugriffs öffentlicher Benutzer auf öffentliche bzw. Extranet-Ressourcen und -Anwendungen eingesetzt werden können.

## Zertifikate erstmals definieren

Hier erfahren Sie, wie Zertifikate einer öffentlichen Internet-Zertifizierungsinstanz verwaltet oder eine private lokale Zertifizierungsinstanz erstellt und betrieben werden kann, mit der Sie selbst Zertifikate ausstellen können.

Der linke Rahmen im Fenster von Digital Certificate Manager (DCM) ist der Task-Navigationsrahmen. Sie können diesen Rahmen verwenden, um zahlreiche Tasks auszuwählen, mit denen Sie Zertifikate und die Anwendungen, die diese Zertifikate verwenden, verwalten können. Welche Tasks verfügbar sind, hängt von dem Zertifikatsspeicher ab, mit dem Sie arbeiten (falls zutreffend), und außerdem von den Sonderberechtigungen in Ihrem Benutzerprofil. Auf die meisten Tasks kann nur mit den Sonderberechtigungen \*ALLOBJ und \*SECADM zugegriffen werden. Um DCM zum Überprüfen von Objektsignaturen zu verwenden, muss Ihr Benutzerprofil außerdem über die Sonderberechtigung \*AUDIT verfügen.

Wenn Sie Digital Certificate Manager (DCM) zum ersten Mal verwenden, sind noch keine Zertifikatsspeicher vorhanden. Aus diesem Grund werden im Navigationsteilfenster beim ersten Zugriff auf DCM nur die folgenden Tasks angezeigt. Dies gilt auch nur dann, wenn Sie über die erforderlichen Sonderberechtigungen verfügen:

- Benutzerzertifikate verwalten.
- Neuen Zertifikatsspeicher erstellen.
- Zertifizierungsinstanz (CA) erstellen. (Anmerkung: Nach der Verwendung dieser Task zum Erstellen einer privaten lokalen Zertifizierungsinstanz wird sie in der Liste nicht mehr angezeigt.)
- CRL-Verteilungspunkte verwalten.
- LDAP-Position verwalten.
- PKIX-Anforderungsadresse verwalten.
- Zu iSeries-Tasks zurückkehren.

Selbst wenn auf dem System bereits Zertifikatsspeicher vorhanden sind (zum Beispiel bei der Migration von einer DCM-Vorversion), zeigt DCM im linken Navigationsrahmen nur eine eingeschränkte Anzahl von Tasks oder Task-Kategorien an. Die von DCM angezeigten Tasks oder Kategorien hängen von dem geöffneten Zertifikatsspeicher und den Sonderberechtigungen Ihres Benutzerprofils ab.

Bevor Sie mit den Tasks für die Zertifikats- und Anwendungsverwaltung arbeiten können, müssen Sie in den meisten Fällen zuerst auf den entsprechenden Zertifikatsspeicher zugreifen. Zum Öffnen eines bestimmten Zertifikatsspeichers müssen Sie im Navigationsrahmen auf **Zertifikatsspeicher auswählen** klicken.

Im Navigationsrahmen von DCM ist auch eine Schaltfläche **Gesicherte Verbindung** enthalten. Sie können diese Schaltfläche zum Aufrufen eines zweiten Browser-Fensters verwenden, in dem eine gesicherte Verbindung über SSL (Secure Sockets Layer) aufgebaut werden kann. Um diese Funktion erfolgreich nutzen zu können, müssen Sie zuerst den IBM HTTP-Server für i5/OS für die Verwendung von SSL konfigurieren, damit der Betrieb im gesicherten Modus erfolgt. Sie müssen dann den HTTP-Server im gesicherten Modus starten. Wenn Sie den HTTP-Server nicht für den SSL-Betrieb konfiguriert und entsprechend gestartet haben, wird eine Fehlermeldung angezeigt und der Browser startet keine gesicherte Sitzung.

## Einführung

Obwohl Sie Zertifikate für mehrere sicherheitsrelevante Ziele einsetzen können, hängt Ihre erste Aktion davon ab, wie Sie die benötigten Zertifikate abrufen wollen. Beim ersten Einsatz von DCM können Sie zwei grundlegende Vorgehensweisen auswählen. Die Entscheidung für eine der folgenden Vorgehensweisen hängt davon ab, ob Sie öffentliche Zertifikate verwenden oder selbst private Zertifikate ausstellen wollen.

### Zugehörige Konzepte

„Öffentliche vs. private Zertifikate“ auf Seite 35

In diesen Informationen wird erläutert, wie der Zertifikatstyp (öffentlich oder privat) festgestellt werden kann, der die individuellen Unternehmensanforderungen des Kunden optimal erfüllt.

## Lokale Zertifizierungsinstanz erstellen und betreiben

In den vorliegenden Informationen wird erläutert, wie eine lokale Zertifizierungsinstanz (CA) erstellt und betrieben werden kann, um private Zertifikate für Ihre Anwendungen auszustellen.

Nach sorgfältiger Prüfung Ihrer Sicherheitsanforderungen und -richtlinien haben Sie sich entschieden, eine lokale Zertifizierungsinstanz (CA) zu betreiben, um private Zertifikate für Ihre Anwendungen auszustellen. Sie können Digital Certificate Manager (DCM) verwenden, um eine eigene lokale Zertifizierungsinstanz zu erstellen und zu betreiben. DCM stellt Ihnen programmgeführte Anweisungen für die Erstellung einer Zertifizierungsinstanz und deren Verwendung zum Ausstellen von Zertifikaten für Ihre Anwendungen zur Verfügung. Durch die programmgeführten Anweisungen wird sichergestellt, dass Sie alles Nötige haben, um mit Hilfe digitaler Zertifikate Ihre Anwendungen für die Verwendung von SSL konfigurieren und um Objekte signieren sowie Objektsignaturen überprüfen zu können.

**Anmerkung:** Wenn Sie Zertifikate im IBM HTTP-Server für i5/OS verwenden wollen, muss der Webserver erstellt und konfiguriert werden, bevor Sie mit DCM arbeiten können. Wenn Sie einen Webserver für die Verwendung von SSL konfigurieren, wird eine Anwendungs-ID für den Server generiert. Notieren Sie diese Anwendungs-ID, damit Sie in DCM angeben können, welches Zertifikat von der zugehörigen Anwendung für SSL benutzt werden soll.

Der Server darf nicht beendet und erneut gestartet werden, bevor Sie diesem mit DCM ein Zertifikat zugeordnet haben. Wenn Sie die \*ADMIN-Instanz des Webserver vor der Zuordnung eines Zertifikats beenden und erneut starten, können Sie den Server nicht starten und DCM nicht zum Zuordnen eines Zertifikats zum Server verwenden.

So können Sie mit DCM eine lokale Zertifizierungsinstanz erstellen und betreiben:

1. Starten Sie Digital Certificate Manager.
2. Wählen Sie im Navigationsrahmen von DCM "Zertifizierungsinstanz (CA) erstellen" aus, um eine Reihe von Formularen aufzurufen. Diese Formulare führen Sie durch den Erstellungsprozess für eine lokale Zertifizierungsinstanz und unterstützen Sie beim Durchführen anderer Tasks, die zur Verwendung von digitalen Zertifikaten für SSL, zum Signieren von Objekten und zur Überprüfung von Signaturen erforderlich sind.

**Anmerkung:** Wenn Sie Fragen zum Ausfüllen eines bestimmten Formulars in dieser geführten Task haben, wählen Sie die Schaltfläche mit dem Fragezeichen (?) oben auf der Seite aus, um auf die Onlinehilfe zuzugreifen.

3. Füllen Sie alle Formulare für diese geführte Task aus. Beim Ausfüllen dieser Formulare führen Sie alle im Folgenden aufgeführten Tasks aus, die zur Definition einer funktionierenden lokalen Zertifizierungsinstanz erforderlich sind:
  - a. Auswählen der Speicherungsmethode für den privaten Schlüssel des Zertifikats der lokalen Zertifizierungsinstanz. (Dieser Schritt ist nur angegeben, wenn auf Ihrem System ein IBM Verschlüsselungskoprozessor installiert ist. Andernfalls speichert DCM die Zertifikate und die zugehörigen privaten Schlüssel im Zertifikatsspeicher der lokalen Zertifizierungsinstanz (CA)).
  - b. Bereitstellen von Kenndaten für die lokale Zertifizierungsinstanz.
  - c. Installieren des Zertifikats der lokalen Zertifizierungsinstanz auf Ihrem PC oder in Ihrem Browser, damit Ihre Software diese Zertifizierungsinstanz erkennen und die von ihr ausgestellten Zertifikate überprüfen kann.
  - d. Auswählen der Richtliniendaten für Ihre lokale Zertifizierungsinstanz.
  - e. Verwenden der neuen lokalen Zertifizierungsinstanz zum Ausstellen eines Server- oder Client-Zertifikats, das Ihre Anwendungen für SSL-Verbindungen verwenden können. (Wenn auf Ihrem System ein IBM Verschlüsselungskoprozessor installiert ist, ermöglicht Ihnen dieser Schritt anzugeben, wie der private Schlüssel des Server- oder Client-Zertifikats gespeichert werden soll. Andernfalls speichert DCM das Zertifikat und den privaten Schlüssel automatisch im Zertifikatsspeicher \*SYSTEM. DCM erstellt den Zertifikatsspeicher \*SYSTEM als Teil dieser Sub-Task.)
  - f. Auswählen der Anwendungen, die das Server- oder Client-Zertifikat für SSL-Verbindungen verwenden können.

**Anmerkung:** Wenn Sie DCM bereits zuvor für die Erstellung des Zertifikatsspeichers \*SYSTEM verwendet haben, um Zertifikate für SSL zu verwalten, die von einer öffentlichen Internet-Zertifizierungsinstanz ausgestellt wurden, führen Sie diesen und den vorherigen Schritt nicht aus.

- g. Verwenden der neuen lokalen Zertifizierungsinstanz zum Ausstellen eines Objektsignierzertifikats, das Ihre Anwendungen zum digitalen Signieren von Objekten verwenden können. Mit dieser Sub-Task wird der Zertifikatsspeicher \*OBJECTSIGNING erstellt; dies ist der Zertifikatsspeicher, der für die Verwaltung von Objektsignierzertifikat verwendet wird.
- h. Auswählen der Anwendungen, die das Objektsignierzertifikat verwenden können, um Objekten digitale Signaturen zuzuweisen.

**Anmerkung:** Wenn Sie DCM bereits zuvor für die Erstellung des Zertifikatsspeichers \*OBJECTSIGNING verwendet haben, um Objektsignierzertifikate zu verwalten, die von einer öffentlichen Internet-Zertifizierungsinstanz ausgestellt wurden, führen Sie diesen und den vorherigen Schritt nicht aus.

- i. Auswählen der Anwendungen, die Ihre lokale Zertifizierungsinstanz anerkennen sollen.

Nach Abschluss der geführten Task verfügen Sie über alle Voraussetzungen, um mit der Konfiguration von Anwendungen für den Einsatz von SSL (siehe hierzu Configuring your applications to use SSL) für die gesicherte Kommunikation zu beginnen.

Nach der Konfiguration der Anwendungen müssen Benutzer, die über eine SSL-Verbindung auf die Anwendungen zugreifen, DCM verwenden, um eine Kopie des Zertifikats der lokalen Zertifizierungsinstanz abzurufen. Jeder Benutzer muss über eine Kopie des Zertifikats verfügen, damit die Client-Software des jeweiligen Benutzers dieses verwenden kann, um im Rahmen des SSL-Vereinbarungsprozesses die Identität des Servers zu authentifizieren. Benutzer können DCM verwenden, um entweder das Zertifikat der lokalen Zertifizierungsinstanz in eine Datei zu kopieren oder dieses Zertifikat in ihren Browser herunterzuladen. Wie die Benutzer das Zertifikat der lokalen Zertifizierungsinstanz speichern, hängt von der Client-Software ab, die sie zum Aufbauen einer SSL-Verbindung zu einer Anwendung benutzen.

Sie können diese lokale Zertifizierungsinstanz auch zum Ausstellen von Zertifikaten für Anwendungen auf anderen iSeries-Systemen in Ihrem Netzwerk verwenden.

Weitere Informationen zur Verwendung von DCM zum Verwalten von Benutzerzertifikaten und zur Vorgehensweise beim Abrufen einer Kopie des Zertifikats der lokalen Zertifizierungsinstanz für die Authentifizierung von Zertifikaten der lokalen CA finden Sie in den folgenden Themen:

#### **Zugehörige Konzepte**

„Öffentliche vs. private Zertifikate“ auf Seite 35

In diesen Informationen wird erläutert, wie der Zertifikatstyp (öffentlich oder privat) festgestellt werden kann, der die individuellen Unternehmensanforderungen des Kunden optimal erfüllt.

„Benutzerzertifikate verwalten“

Digital Certificate Manager (DCM) kann zum Anfordern von Zertifikaten mit SSL oder zum Zuordnen vorhandener Zertifikate zu den entsprechenden iSeries-Benutzerprofilen verwendet werden.

#### **Zugehörige Tasks**

„Lokale Zertifizierungsinstanz zum Ausstellen von Zertifikaten für andere iSeries-Systeme verwenden“ auf Seite 66

Dieses Thema enthält Informationen zum Einsatz einer privaten lokalen Zertifizierungsinstanz auf einem System für die Ausstellung von Zertifikaten, die auf anderen iSeries-Systemen benutzt werden sollen.

„Kopie des Zertifikats der privaten Zertifizierungsinstanz abrufen“ auf Seite 55

Hier erfahren Sie, wie Sie eine Kopie des Zertifikats der privaten Zertifizierungsinstanz abrufen und auf Ihrem PC installieren können, so dass Sie von dieser CA ausgestellte Serverzertifikate authentifizieren können.

#### **Zugehörige Verweise**

„APIs über das Programm zum Ausstellen von Zertifikaten für Nicht-iSeries-Benutzer verwenden“ auf Seite 54

In diesen Informationen wird erläutert, wie Sie die lokale Zertifizierungsinstanz zum Ausstellen privater Zertifikate an Benutzer verwenden können, ohne dass das Zertifikat einem iSeries-Benutzerprofil zugeordnet werden muss.

### **Benutzerzertifikate verwalten:**

Digital Certificate Manager (DCM) kann zum Anfordern von Zertifikaten mit SSL oder zum Zuordnen vorhandener Zertifikate zu den entsprechenden iSeries-Benutzerprofilen verwendet werden.

Wenn Benutzer auf Ihre öffentlichen oder internen Server über eine SSL-Verbindung zugreifen, müssen Sie über eine Kopie des Zertifikats der Zertifizierungsinstanz (CA) verfügen, mit dem das Serverzertifikat ausgestellt wurde. Dieses CA-Zertifikat ist erforderlich, damit ihre Client-Software die Authentizität des Serverzertifikats prüfen und eine Verbindung herstellen kann. Wenn Ihr Server mit einem Zertifikat einer öffentlichen Zertifizierungsinstanz (CA) arbeitet, ist in der Software der Benutzer möglicherweise bereits eine Kopie dieses CA-Zertifikats implementiert. Es ist also weder für Sie als DCM-Administrator noch für Ihre Benutzer eine Aktion erforderlich, um an einer SSL-Sitzung teilnehmen zu können. Verwendet Ihr Server jedoch ein Zertifikat einer privaten lokalen Zertifizierungsinstanz, müssen die zugehörigen Benutzer eine Kopie dieses Zertifikats abrufen, bevor eine SSL-Sitzung mit dem Server aufgebaut werden kann.

Darüber hinaus müssen Benutzer, die auf die Ressourcen des Servers zugreifen wollen, ein gültiges Benutzerzertifikat vorlegen, wenn die verwendete Serveranwendung die Client-Authentifizierung über Zertifikate unterstützt und verlangt. Abhängig von den individuellen Sicherheitsanforderungen können Benutzer ein Zertifikat einer öffentlichen Internet-Zertifizierungsinstanz oder das Zertifikat einer lokalen Zertifizierungsinstanz vorlegen, die von Ihnen selbst betrieben wird. Wenn die Serveranwendung den Ressourcenzugriff interner Benutzer ermöglicht, die momentan über ein iSeries-Benutzerprofil verfügen, können Sie mit DCM deren Zertifikate zu den entsprechenden Benutzerprofilen hinzufügen. Durch diese Zuordnung wird sichergestellt, dass für Benutzer beim Vorlegen von Zertifikaten dieselben Zugriffsberechtigungen und -einschränkungen für Ressourcen definiert sind, die auch für deren Benutzerprofile festgelegt wurden.

Digital Certificate Manager (DCM) ermöglicht die Verwaltung von Zertifikaten, die einem iSeries-Benutzerprofil zugeordnet wurden. Wenn in Ihrem Benutzerprofil die Sonderberechtigungen \*SECADM und \*ALLOBJ definiert sind, können Sie die Zuordnung von Zertifikaten zu bestimmten Benutzerprofilen sowohl für sich selbst als auch für andere Benutzer ausführen. Ist kein Zertifikatsspeicher oder der Zertifikatsspeicher der lokalen Zertifizierungsinstanz (CA) geöffnet, können Sie für den Zugriff auf die gewünschte Task im Navigationsrahmen **Benutzerzertifikate verwalten** auswählen. Wenn ein anderer Zertifikatsspeicher geöffnet ist, stehen die Benutzerzertifikats-Tasks unter **Zertifikate verwalten** zur Verfügung.

Benutzer mit Benutzerprofilen ohne die Sonderberechtigungen \*SECADM und \*ALLOBJ sind nur zum Verwalten der eigenen Zertifikatszuordnungen berechtigt. Sie können **Benutzerzertifikate verwalten** auswählen, um auf Tasks zuzugreifen, mit deren Hilfe sie die Zertifikate anzeigen können, die ihren Benutzerprofilen zugeordnet sind, ein Zertifikat aus ihrem Benutzerprofil löschen oder ihren Benutzerprofilen ein Zertifikat einer anderen Zertifizierungsinstanz zuordnen können. Unabhängig von den Sonderberechtigungen ihrer Benutzerprofile können Benutzer ein Benutzerzertifikat von der lokalen Zertifizierungsinstanz abrufen, indem sie die Task **Zertifikat erstellen** im Haupt-Navigationsrahmen auswählen.

Weitere Informationen zur Verwendung von DCM für die Verwaltung und Erstellung von Benutzerzertifikaten finden Sie unter den folgenden Themen:

#### **Zugehörige Tasks**

„Lokale Zertifizierungsinstanz erstellen und betreiben“ auf Seite 47

In den vorliegenden Informationen wird erläutert, wie eine lokale Zertifizierungsinstanz (CA) erstellt und betrieben werden kann, um private Zertifikate für Ihre Anwendungen auszustellen.

„Kopie des Zertifikats der privaten Zertifizierungsinstanz abrufen“ auf Seite 55

Hier erfahren Sie, wie Sie eine Kopie des Zertifikats der privaten Zertifizierungsinstanz abrufen und auf Ihrem PC installieren können, so dass Sie von dieser CA ausgestellte Serverzertifikate authentifizieren können.

#### *Benutzerzertifikat erstellen:*

In diesen Informationen wird erläutert, wie Benutzer die lokale Zertifizierungsinstanz zum Ausstellen eines Zertifikats für die Client-Authentifizierung verwenden können.

Wenn Sie für die Benutzerauthentifizierung digitale Zertifikate einsetzen wollen, müssen Ihre Benutzer über die entsprechenden Zertifikate verfügen. Wenn Sie Digital Certificate Manager (DCM) zum Betreiben einer privaten lokalen Zertifizierungsinstanz (CA) einsetzen, können Sie diese CA zum Ausstellen der Zertifikate für alle Benutzer verwenden. Jeder Benutzer muss hierbei auf DCM zugreifen, um mit Hilfe der Task **Zertifikat erstellen** das benötigte Zertifikat abzurufen. Damit ein Zertifikat von einer lokalen Zertifizierungsinstanz abgerufen werden kann, muss die CA-Richtlinie die Ausstellung von Benutzerzertifikaten durch diese CA zulassen.

So rufen Sie ein Zertifikat von einer lokalen Zertifizierungsinstanz ab:

1. Starten Sie Digital Certificate Manager.



2. Wählen Sie im Navigationsrahmen **Zertifikat erstellen** aus.
3. Wählen Sie als Typ für das zu erstellende Zertifikat **Benutzerzertifikat** aus. Daraufhin wird ein Formular angezeigt, in dem Sie die Daten zur Identifikation des gewünschten Zertifikats eingeben können.
4. Füllen Sie das Formular aus, und klicken Sie anschließend auf **Weiter**.

**Anmerkung:** Wenn Sie Fragen zum Ausfüllen eines bestimmten Formulars in dieser geführten Task haben, wählen Sie die Schaltfläche mit dem Fragezeichen (?) oben auf der Seite aus, um auf die Onlinehilfe zuzugreifen.

5. Jetzt erstellt DCM gemeinsam mit Ihrem Browser den privaten und den öffentlichen Schlüssel für das Zertifikat. Im Browser werden möglicherweise Fenster angezeigt, um Sie durch diesen Prozess zu führen. Befolgen Sie die Browser-Instruktionen für diese Tasks. Nachdem der Browser die Schlüssel generiert hat, wird eine Bestätigungsseite angezeigt, in der Sie darüber informiert werden, dass DCM das Zertifikat erstellt hat.
6. Installieren Sie das neue Zertifikat in Ihrem Browser. Im Browser werden möglicherweise Fenster angezeigt, um Sie durch diesen Prozess zu führen. Befolgen Sie die Instruktionen, die der Browser zum Ausführen dieser Task anzeigt.
7. Klicken Sie auf **OK**, um die Task abzuschließen.

Bei der Verarbeitung ordnet Digital Certificate Manager das Zertifikat automatisch Ihrem iSeries-Benutzerprofil zu.

Wenn Sie dem Zertifikat einer anderen Zertifizierungsinstanz, das ein Benutzer bei der Client-Authentifizierung vorlegt, die gleichen Berechtigungen zuordnen wollen wie dem entsprechenden Benutzerprofil, kann der Benutzer mit Hilfe von DCM seinem Benutzerprofil dieses Zertifikat zuordnen.

#### **Zugehörige Konzepte**

„Öffentliche vs. private Zertifikate“ auf Seite 35

In diesen Informationen wird erläutert, wie der Zertifikatstyp (öffentlich oder privat) festgestellt werden kann, der die individuellen Unternehmensanforderungen des Kunden optimal erfüllt.

#### **Zugehörige Tasks**

„Benutzerzertifikat zuordnen“

Sie können ein eigenes Benutzerzertifikat Ihrem i5/OS-Benutzerprofil oder einer anderen Benutzeridentität zuordnen. Das Zertifikat kann von einer privaten lokalen Zertifizierungsinstanz auf einem anderen System oder von einer bekannten Internet-Zertifizierungsinstanz stammen. Bevor Sie einer Benutzeridentität ein Zertifikat zuordnen können, muss die ausstellende Zertifizierungsinstanz vom Server anerkannt werden. Darüber hinaus darf das gewünschte Zertifikat noch keinem anderen Benutzerprofil bzw. keiner anderen Benutzeridentität auf dem System zugeordnet worden sein.

„Kopie des Zertifikats der privaten Zertifizierungsinstanz abrufen“ auf Seite 55

Hier erfahren Sie, wie Sie eine Kopie des Zertifikats der privaten Zertifizierungsinstanz abrufen und auf Ihrem PC installieren können, so dass Sie von dieser CA ausgestellte Serverzertifikate authentifizieren können.

#### *Benutzerzertifikat zuordnen:*

Sie können ein eigenes Benutzerzertifikat Ihrem i5/OS-Benutzerprofil oder einer anderen Benutzeridentität zuordnen. Das Zertifikat kann von einer privaten lokalen Zertifizierungsinstanz auf einem anderen System oder von einer bekannten Internet-Zertifizierungsinstanz stammen. Bevor Sie einer Benutzeridentität ein Zertifikat zuordnen können, muss die ausstellende Zertifizierungsinstanz vom Server anerkannt werden. Darüber hinaus darf das gewünschte Zertifikat noch keinem anderen Benutzerprofil bzw. keiner anderen Benutzeridentität auf dem System zugeordnet worden sein.

Benutzer verfügen möglicherweise über Zertifikate einer externen oder einer lokalen Zertifizierungsinstanz (CA) auf einem anderen iSeries-System, bei denen Sie als der Administrator es für sinnvoll erachten, dass diese für Digital Certificate Manager (DCM) zur Verfügung gestellt werden. Hierdurch wird es

für Sie und den Benutzer möglich, DCM zum Verwalten dieser Zertifikate einzusetzen, die in den meisten Fällen für die Client-Authentifizierung eingesetzt werden. Die Task **Benutzerzertifikat zuordnen** stellt ein Verfahren bereit, mit dessen Hilfe ein Benutzer eine DCM-Zuordnung für ein Zertifikat erstellen kann, das von einer externen Zertifizierungsinstanz (CA) abgerufen wurde.

Wenn ein Benutzer ein Zertifikat zuordnet, wird dieses von DCM auf eine der beiden folgenden Arten verarbeitet:

- Das Zertifikat wird mit dem Benutzerprofil des Benutzers lokal auf dem iSeries-System gespeichert. Wenn für DCM keine LDAP-Position definiert ist, kann ein Benutzer über die Task **Benutzerzertifikat zuordnen** einem i5/OS-Benutzerprofil ein externes Zertifikat zuordnen. Durch die Zuordnung des Zertifikats zu einem Benutzerprofil wird sichergestellt, dass das Zertifikat auf dem System in Anwendungen eingesetzt werden kann, die für die Client-Authentifizierung Zertifikate benötigen.
- Das Zertifikat wird an einer LDAP-Position (LDAP = Lightweight Directory Access Protocol) gespeichert, so dass es mit EIM (Enterprise Identity Mapping) eingesetzt werden kann. Wenn eine LDAP-Position definiert ist und das iSeries-System für die Verwendung von EIM konfiguriert wurde, ermöglicht die Task **Benutzerzertifikat zuordnen** dem Benutzer das Speichern einer Kopie eines externen Zertifikats im angegebenen LDAP-Verzeichnis. DCM erstellt darüber hinaus eine EIM-Quellenzuordnung für das Zertifikat. Wenn das Zertifikat auf diese Weise gespeichert wird, kann ein EIM-Administrator das Zertifikat als gültige Benutzeridentität identifizieren, die in EIM verwendet werden kann.

**Anmerkung:** Bevor ein Benutzer ein Zertifikat einer Benutzeridentität in einer EIM-Konfiguration zuordnen kann, muss EIM für den Benutzer korrekt konfiguriert werden. Diese EIM-Konfiguration umfasst die Erstellung einer EIM-Kennung für den Benutzer und die Erstellung einer Zielzuordnung zwischen dieser EIM-Kennung und dem Benutzerprofil. Andernfalls kann DCM für das Zertifikat keine entsprechende Quellenzuordnung zur EIM-Kennung herstellen.

Um die Task **Benutzerzertifikat zuordnen** verwenden zu können, muss ein Benutzer die folgenden Voraussetzungen erfüllen:

1. Der Benutzer muss über eine gesicherte Sitzung mit dem HTTP-Server verfügen, über die er auf Digital Certificate Manager (DCM) zugreifen kann.

Ob Sie über eine gesicherte Sitzung verfügen, wird über die Portnummer in der URL-Adresse festgestellt, die Sie für den Zugriff auf DCM verwendet haben. Wenn Sie den Standardport für den DCM-Zugriff, d. h. den Port 2001 verwendet haben, verfügen Sie nicht über eine gesicherte Sitzung. Darüber hinaus muss auch der HTTP-Server für die Verwendung von SSL konfiguriert werden, bevor Sie zu einer gesicherten Sitzung wechseln können.

Wenn diese Task vom Benutzer ausgewählt wird, ruft das System ein neues Browser-Fenster auf. Wenn der Benutzer über keine gesicherte Sitzung verfügt, fordert DCM ihn auf, eine solche Sitzung zu starten und hierzu auf **Benutzerzertifikat zuordnen** zu klicken. Anschließend initialisiert DCM SSL-Vereinbarungen (SSL = Secure Sockets Layer) mit dem Browser der Benutzers. Im Rahmen dieser Vereinbarungen wird der Benutzer vom Browser möglicherweise aufgefordert anzugeben, ob die Zertifizierungsinstanz (CA), die das Zertifikat zur Identifikation des HTTP-Servers ausgestellt hat, anerkannt werden soll. Der Browser kann darüber hinaus auch anfragen, ob das Serverzertifikat selbst akzeptiert werden soll.

2. Der Benutzer muss für die Client-Authentifizierung ein Zertifikat vorlegen.

Abhängig von den Konfigurationseinstellungen des Browsers müssen Sie eventuell ein Zertifikat zur Authentifizierung auswählen. Wenn der Browser ein Zertifikat einer Zertifizierungsinstanz vorlegt, die vom System anerkannt wird, zeigt DCM in einem separaten Fenster die Zertifikatsinformationen an. Wird das vorgelegte Zertifikat nicht akzeptiert, werden Sie vom Server möglicherweise zur Eingabe Ihres Benutzernamens und des Kennwortes für die Authentifizierung aufgefordert, bevor der Zugriff gewährt wird.

3. Der Benutzer muss im Browser über ein Zertifikat verfügen, das nicht bereits der Benutzeridentität des Benutzers zugeordnet ist, der die Task ausführt. (Wenn DCM für den Einsatz mit EIM konfiguriert wurde, muss der Benutzer über ein Zertifikat im Browser verfügen, das nicht bereits an der LDAP-Position für DCM gespeichert ist.)

Nach dem Herstellen einer gesicherten Sitzung versucht DCM, ein geeignetes Zertifikat vom Browser abzurufen, um dieses Ihrer Benutzeridentität zuzuordnen. Wenn das Abrufen eines oder mehrerer Zertifikate erfolgreich ausgeführt werden konnte, können Sie die Zertifikatsinformationen anzeigen und auswählen, ob die Zuordnung zu Ihrem Benutzerprofil ausgeführt werden soll.

Wenn in DCM keine Zertifikatsinformationen angezeigt werden, konnte kein Zertifikat bereitgestellt werden, das DCM Ihrer Benutzeridentität zuordnen konnte. In diesem Fall liegt möglicherweise eines der Probleme mit Benutzerzertifikaten vor. Die im Browser enthaltenen Zertifikate können Ihrer Benutzeridentität z. B. bereits zugeordnet sein.

#### **Zugehörige Tasks**

„Benutzerzertifikat erstellen“ auf Seite 50

In diesen Informationen wird erläutert, wie Benutzer die lokale Zertifizierungsinstanz zum Ausstellen eines Zertifikats für die Client-Authentifizierung verwenden können.

„Fehler beim Zuordnen eines Benutzerzertifikats beheben“ auf Seite 98

#### **Zugehörige Informationen**

Enterprise Identity Mapping - Übersicht

*Benutzerzertifikate nach Verfallsdatum verwalten:*

Digital Certificate Manager (DCM) unterstützt die Verwaltung von Zertifikaten auf der Basis des Verfallsdatums. Mit Hilfe dieser Funktion können Administratoren das Verfallsdatum von Benutzerzertifikaten auf dem lokalen iSeries-System überprüfen. Die Unterstützungsfunktion für die Verwaltung von Zertifikaten auf der Basis des Verfallsdatums kann zusammen mit EIM (Enterprise Identity Mapping) eingesetzt werden. Auf diese Weise kann DCM vom Administrator auf Unternehmensebene zum Überprüfen des Verfallsdatums von Benutzerzertifikaten verwendet werden.

Um diese Unterstützungsfunktion für Benutzerzertifikate auf Unternehmensebene zu nutzen, muss EIM im Unternehmen konfiguriert sein und die für Benutzerzertifikate benötigten Zuordnungsinformationen enthalten. Um das Verfallsdatum von Benutzerzertifikaten zu überprüfen, die den Benutzerprofilen anderer Benutzer zugeordnet sind, müssen Sie über die Sonderberechtigungen \*ALLOBJ und \*SECADM verfügen.

Durch die Verwendung von DCM zum Anzeigen von Zertifikaten auf der Basis ihres Verfallsdatums können Sie schnell und einfach feststellen, welche Zertifikate in naher Zukunft ablaufen, so dass diese rechtzeitig verlängert werden können.

So können Sie Benutzerzertifikate auf der Basis des Verfallsdatums anzeigen und verwalten:

1. Starten Sie Digital Certificate Manager.

**Anmerkung:** Wenn Sie beim Einsatz von DCM Fragen zum Ausfüllen eines bestimmten Formulars haben, wählen Sie die Schaltfläche mit dem Fragezeichen (?) oben auf der Seite aus, um auf die Onlinehilfe zuzugreifen.

2. Wählen Sie im Navigationsrahmen **Benutzerzertifikate verwalten** aus, um eine Liste mit Tasks anzuzeigen.

**Anmerkung:** Wenn Sie momentan mit einem Zertifikatsspeicher arbeiten, wählen Sie **Zertifikate verwalten** aus, um eine Liste der Tasks anzuzeigen. Wählen Sie anschließend **Verfallsdatum prüfen** und dann **Benutzer** aus.

3. Wenn Ihr Benutzerprofil über die Sonderberechtigungen \*ALLOBJ und \*SECADM verfügt, können Sie auf der Basis des Verfallsdatums eine Methode zur Auswahl der anzuzeigenden und zu verwaltenden Benutzerzertifikate auswählen. (Wenn Ihr Benutzerprofil nicht über diese Sonderberechtigungen ver-

fügt, werden Sie von DCM aufgefordert, den Datumsbereich für das Verfallsdatum wie im nächsten Schritt beschrieben anzugeben.) Sie können hierbei eine der folgenden Auswahlmöglichkeiten verwenden:

- Wählen Sie **Benutzerprofil** aus, um Benutzerzertifikate anzuzeigen und zu verwalten, die einem bestimmten i5/OS-Benutzerprofil zugeordnet sind. Geben Sie einen Wert für **Benutzerprofilname** an, und klicken Sie dann auf **Weiter**.

**Anmerkung:** Sie können das Benutzerprofil eines anderen Benutzers nur dann angeben, wenn Sie über die Sonderberechtigungen \*ALLOBJ und \*SECADM verfügen.

- Wählen Sie **Alle Benutzerzertifikate** aus, um Benutzerzertifikate für alle Benutzer-IDs anzuzeigen und zu verwalten.
4. Geben Sie im Feld **Bereich für Verfallsdatum in Tagen (1 - 365)** die Anzahl der Tage in dem Bereich ein, in dem Benutzerzertifikate auf der Basis ihres Verfallsdatums angezeigt werden sollen, und klicken Sie dann auf **Weiter**. DCM zeigt daraufhin alle Benutzerzertifikate für das angegebene Benutzerprofil an, die zwischen dem aktuellen Datum und dem Datum ablaufen, das mit der Anzahl der angegebenen Tage übereinstimmt. Darüber hinaus zeigt DCM alle Benutzerzertifikate an, deren Verfallsdatum vor dem aktuellen Datum liegt.
  5. Wählen Sie das zu verwaltende Benutzerzertifikat aus. Sie können nun die Detailinformationen zum Zertifikat anzeigen oder das Zertifikat aus der zugehörigen Benutzeridentität entfernen.
  6. Klicken Sie nach Abschluss aller Operationen für die gewünschten Zertifikate auf **Abbrechen**, um die Task zu beenden.

#### Zugehörige Tasks

„Digitale Zertifikate und Enterprise Identity Mapping“ auf Seite 40

Durch den gemeinsamen Einsatz von Enterprise Identity Mapping (EIM) und Digital Certificate Manager (DCM) können Sie ein Zertifikat als Quellenelement einer EIM-Abgleichsoperation verwenden, um eine Zuordnung zwischen dem Zertifikat und einer Zielbenutzeridentität herzustellen, die derselben EIM-Kennung zugeordnet ist.

#### Zugehörige Informationen

Enterprise Identity Mapping - Übersicht

### APIs über das Programm zum Ausstellen von Zertifikaten für Nicht-iSeries-Benutzer verwenden:

In diesen Informationen wird erläutert, wie Sie die lokale Zertifizierungsinstanz zum Ausstellen privater Zertifikate an Benutzer verwenden können, ohne dass das Zertifikat einem iSeries-Benutzerprofil zugeordnet werden muss.

Ab i5/OS V5R3 werden zwei neue APIs zur Verfügung gestellt, die zum Ausstellen von Zertifikaten an Nicht-iSeries-Benutzer über das Programm verwendet werden können. Wenn Sie in vorherigen Releases die lokale Zertifizierungsinstanz (CA) zum Ausstellen von Zertifikaten für Benutzer verwendet haben, wurden diese Zertifikate automatisch den entsprechenden iSeries-Benutzerprofilen zugeordnet. Aus diesem Grund musste bei Verwendung der lokalen Zertifizierungsinstanz zum Ausstellen eines Client-Authentifizierungszertifikats für einen Benutzer diesem ein iSeries-Benutzerprofil zugeordnet werden. Darüber hinaus mussten alle Benutzer, die ein Zertifikat einer lokalen Zertifizierungsinstanz für die Client-Authentifizierung benötigten, Digital Certificate Manager (DCM) verwenden, um das erforderliche Zertifikat zu erstellen. Aus diesem Grund mussten alle diese Benutzer über ein Benutzerprofil auf dem iSeries-Server verfügen, auf dem DCM implementiert war, und sich auf diesem iSeries-Server anmelden können.

Die Zuordnung des Zertifikats zu einem bestimmten Benutzerprofil hat gewisse Vorteile. Dies gilt besonders bei internen Benutzern. Allerdings war die Verwendung der lokalen Zertifizierungsinstanz für die Ausstellung von Benutzerzertifikaten für eine große Anzahl von Benutzern durch diese Einschränkungen und Anforderungen relativ kompliziert. Dies war insbesondere dann der Fall, wenn den betroffenen Benutzern kein iSeries-Benutzerprofil zugeordnet werden sollte. Um diesen Benutzern kein Benutzerprofil

zuordnen zu müssen, wäre die kostenpflichtige Anforderung eines Zertifikats von einer bekannten Zertifizierungsinstanz erforderlich gewesen, wenn zur Benutzerauthentifizierung für die vorhandenen Anwendungen Zertifikate erforderlich gewesen wären.

Mit den beiden neuen APIs sind nun Unterstützungsfunktionen verfügbar, mit deren Hilfe eine Schnittstelle für die Erstellung von Benutzerzertifikaten für alle Benutzernamen bereitgestellt werden kann, die mit dem Zertifikat der lokalen Zertifizierungsinstanz signiert sind. Dieses Zertifikat wird keinem bestimmten Benutzerprofil zugeordnet. Der Benutzer muss nun auf dem iSeries-Server, auf dem DCM implementiert ist, nicht definiert sein und er benötigt nicht unbedingt DCM, um das erforderliche Zertifikat zu erstellen.

Für die beiden am häufigsten verwendeten Browser-Programme gibt es zwei APIs, die Sie aufrufen können, wenn Sie mit Net.Data ein Programm zum Ausstellen von Benutzerzertifikaten erstellen wollen. Die von Ihnen erstellte Anwendung muss über den GUI-Code (GUI = Graphical User Interface) verfügen, der zum Erstellen des Benutzerzertifikats und zum Aufrufen einer der beiden APIs für die Verwendung der lokalen Zertifizierungsinstanz zum Signieren des Zertifikats benötigt wird.

Weitere Informationen zur Verwendung dieser APIs finden Sie auf den Seiten zu folgenden Themen:

- API zum Generieren und Signieren von Benutzerzertifikatsanforderungen (QYUCGSUC).
- API zum Signieren von Benutzerzertifikatsanforderungen (QYCUSUC).

#### **Zugehörige Konzepte**

„Öffentliche vs. private Zertifikate“ auf Seite 35

In diesen Informationen wird erläutert, wie der Zertifikatstyp (öffentlich oder privat) festgestellt werden kann, der die individuellen Unternehmensanforderungen des Kunden optimal erfüllt.

„Digitale Zertifikate für die Benutzerauthentifizierung“ auf Seite 38

Im Folgenden wird erläutert, wie Zertifikate zum Bereitstellen von Verfahren zur verbesserten Authentifizierung von Benutzern eingesetzt werden können, die auf iSeries-Systemressourcen zugreifen.

#### **Zugehörige Tasks**

„Lokale Zertifizierungsinstanz erstellen und betreiben“ auf Seite 47

In den vorliegenden Informationen wird erläutert, wie eine lokale Zertifizierungsinstanz (CA) erstellt und betrieben werden kann, um private Zertifikate für Ihre Anwendungen auszustellen.

#### **Kopie des Zertifikats der privaten Zertifizierungsinstanz abrufen:**

Hier erfahren Sie, wie Sie eine Kopie des Zertifikats der privaten Zertifizierungsinstanz abrufen und auf Ihrem PC installieren können, so dass Sie von dieser CA ausgestellte Serverzertifikate authentifizieren können.

Wenn Sie auf einen Server zugreifen, der mit SSL-Verbindungen (SSL = Secure Sockets Layer) arbeitet, legt dieser Server Ihrer Client-Software ein Zertifikat vor, um seine Identität zu belegen. Die Client-Software muss das Serverzertifikat überprüfen, bevor der Server eine Verbindung herstellen kann. Zum Überprüfen des Serverzertifikats muss die Client-Software über Zugriff auf die lokal gespeicherte Kopie des Zertifikats der Zertifizierungsinstanz (CA) verfügen, die zur Ausstellung des Serverzertifikats verwendet wurde. Wenn der Server ein Zertifikat einer öffentlichen Internet-Zertifizierungsinstanz vorlegt, ist im Browser bzw. in der verwendeten Client-Software möglicherweise bereits eine Kopie des zugehörigen CA-Zertifikats vorhanden. Wenn der Server jedoch ein Zertifikat einer privaten lokalen Zertifizierungsinstanz vorlegt, müssen Sie mit Digital Certificate Manager (DCM) eine Kopie des zugehörigen CA-Zertifikats abrufen.

Sie können DCM verwenden, um das Zertifikat der lokalen Zertifizierungsinstanz direkt in Ihren Browser herunterzuladen. Alternativ hierzu können Sie das CA-Zertifikat auch in eine Datei kopieren, damit andere Client-Softwarekomponenten auf dieses zugreifen und es benutzen können. Wenn Sie sowohl den Browser als auch andere Anwendungen für die gesicherte Kommunikation verwenden, müssen Sie mögli-

cherweise beide Installationsmethoden für das Zertifikat der lokalen Zertifizierungsinstanz verwenden. Wenn Sie beide Methoden verwenden, sollten Sie das Zertifikat im Browser installieren, bevor Sie es kopieren und in eine Datei einfügen.

Wenn Sie sich bei der Serveranwendung durch Vorlage eines Zertifikats der lokalen Zertifizierungsinstanz (CA) authentifizieren müssen, müssen Sie dieses Zertifikat vor dem Anfordern eines Benutzerzertifikats von der lokalen CA in den Browser heruntergeladen.

So können Sie DCM zum Abrufen einer Kopie des CA-Zertifikats der lokalen Zertifizierungsinstanz verwenden:

1. Starten Sie Digital Certificate Manager.
2. Wählen Sie im Navigationsrahmen **Zertifikat der lokalen Zertifizierungsinstanz auf dem PC installieren** aus, um eine Seite anzuzeigen, über die Sie dieses CA-Zertifikat in Ihren Browser herunterladen oder in einer Datei auf Ihrem System speichern können.
3. Wählen Sie die Methode zum Abrufen des Zertifikats der lokalen Zertifizierungsinstanz aus.
  - a. Wählen Sie **Zertifikat installieren** aus, um dieses CA-Zertifikat als Trusted Root in Ihren Browser herunterzuladen. Dadurch wird sichergestellt, dass der Browser gesicherte Kommunikationssitzungen mit Servern aufbauen kann, die ein Zertifikat von dieser Zertifizierungsinstanz verwenden. Der Browser zeigt eine Reihe von Fenstern an, um Sie beim Beenden der Installation zu unterstützen.
  - b. Wählen Sie **Zertifikat kopieren und einfügen** aus, um eine Seite anzuzeigen, die eine speziell codierte Kopie des Zertifikats der lokalen Zertifizierungsinstanz enthält. Kopieren Sie das auf der Seite angezeigte Textobjekt in die Zwischenablage. Diese Informationen müssen später in eine Datei eingefügt werden. Diese Datei wird von einem PC-Dienstprogramm (z. B. MKKF oder IKEY-MAN) zum Speichern von Zertifikaten für die Verwendung durch Client-Programme auf dem PC verwendet. Bevor die Client-Anwendungen das Zertifikat der lokalen Zertifizierungsinstanz identifizieren und für die Authentifizierung verwenden können, müssen Sie diese so konfigurieren, dass das Zertifikat als Trusted Root anerkannt wird. Befolgen Sie die Anweisungen, die diese Anwendungen zur Verwendung der Datei zur Verfügung stellen.
4. Klicken Sie auf **OK**, um zur Homepage von Digital Certificate Manager zurückzukehren.

#### **Zugehörige Konzepte**

„Benutzerzertifikate verwalten“ auf Seite 49

Digital Certificate Manager (DCM) kann zum Anfordern von Zertifikaten mit SSL oder zum Zuordnen vorhandener Zertifikate zu den entsprechenden iSeries-Benutzerprofilen verwendet werden.

#### **Zugehörige Tasks**

„Lokale Zertifizierungsinstanz erstellen und betreiben“ auf Seite 47

In den vorliegenden Informationen wird erläutert, wie eine lokale Zertifizierungsinstanz (CA) erstellt und betrieben werden kann, um private Zertifikate für Ihre Anwendungen auszustellen.

„Benutzerzertifikat erstellen“ auf Seite 50

In diesen Informationen wird erläutert, wie Benutzer die lokale Zertifizierungsinstanz zum Ausstellen eines Zertifikats für die Client-Authentifizierung verwenden können.

## **Zertifikate einer öffentlichen Internet-Zertifizierungsinstanz verwalten**

In diesem Abschnitt erfahren Sie, wie Sie Zertifikate einer öffentlichen Internet-Zertifizierungsinstanz verwalten können, indem Sie einen Zertifikatsspeicher erstellen.

Nach genauer Prüfung Ihrer Sicherheitsanforderungen und -richtlinien haben Sie sich für die Verwendung von Zertifikaten einer öffentlichen Internet-Zertifizierungsinstanz (CA) wie z. B. VeriSign entschieden. Sie betreiben eine öffentliche Website und möchten für die Herstellung gesicherter Kommunikationssitzungen SSL (Secure Sockets Layer) verwenden, um die Wahrung der Vertraulichkeit bestimmter Datentransaktionen sicherzustellen. Da die Website öffentlich zugänglich ist, möchten Sie Zertifikate benutzen, die von den meisten Web-Browsern sofort identifiziert werden können.

Vielleicht entwickeln Sie auch Anwendungen für externe Kunden und wollen ein öffentliches Zertifikat verwenden, um die Anwendungspakete digital zu signieren. Durch das Signieren des Anwendungspakets können Ihre Kunden sicher sein, dass das Paket von Ihrem Unternehmen stammt und nicht berechnete Personen den Code während der Übertragung nicht geändert haben. Sie möchten ein öffentliches Zertifikat verwenden, damit Ihre Kunden auf einfache und kostengünstige Weise die digitale Signatur auf dem Paket prüfen können. Dieses Zertifikat kann außerdem verwendet werden, um die Signatur vor dem Versand des Pakets an den Kunden zu prüfen.

Mit den geführten Tasks in Digital Certificate Manager (DCM) können diese öffentlichen Zertifikate sowie die Anwendungen, die sie zum Herstellen von SSL-Verbindungen, Signieren von Objekten oder Prüfen der Authentizität digitaler Objektsignaturen verwenden, zentral verwaltet werden.

### **Öffentliche Zertifikate verwalten**

Wenn Sie DCM zum Verwalten von Zertifikaten einer öffentlichen Internet-Zertifizierungsinstanz einsetzen, müssen Sie als erstes einen Zertifikatsspeicher erstellen. Bei einem Zertifikatsspeicher handelt es sich um eine spezielle Schlüsseldatenbankdatei, die von DCM zum Speichern digitaler Zertifikate und der zugehörigen privaten Schlüssel benutzt wird. DCM ermöglicht Ihnen das Erstellen und Verwalten verschiedener Typen von Zertifikatsspeichern für die unterschiedlichen Zertifikatstypen, die in ihnen gespeichert werden.

Der Typ des zu erstellenden Zertifikatsspeichers sowie die nachfolgend auszuführenden Tasks zum Verwalten Ihrer Zertifikate und der Anwendungen, die mit diesen arbeiten, hängt davon ab, wie Sie die Zertifikate verwenden wollen.

**Anmerkung:** DCM ermöglicht Ihnen die Verwaltung von Zertifikaten, die von einer PKIX-Zertifizierungsinstanz (PKIX = Public Key Infrastructure for X.509) ausgestellt wurden.

Informationen über die Verwendung von DCM zum Erstellen des benötigten Zertifikatsspeichers und zum Verwalten öffentlicher Internet-Zertifikate für Ihre Anwendungen finden Sie unter den folgenden Themen:

#### **Zugehörige Konzepte**

„Öffentliche vs. private Zertifikate“ auf Seite 35

In diesen Informationen wird erläutert, wie der Zertifikatstyp (öffentlich oder privat) festgestellt werden kann, der die individuellen Unternehmensanforderungen des Kunden optimal erfüllt.

#### **Zugehörige Tasks**

„Anforderungsadresse für eine PKIX-Zertifizierungsinstanz verwalten“ auf Seite 85

Eine PKIX-Zertifizierungsinstanz (PKIX = Public Key Infrastructure for X.509) ist eine CA, die Zertifikate auf der Basis der Richtlinien der neuesten X.509-Internet-Standards zur Implementierung einer PKI ausgibt.

### **Öffentliche Internet-Zertifikate für SSL-Kommunikationssitzungen verwalten:**

Digital Certificate Manager (DCM) kann zum Verwalten öffentlicher Internet-Zertifikate verwendet werden, die von Anwendungen zum Herstellen gesicherter Kommunikationssitzungen via SSL (Secure Sockets Layer) eingesetzt werden.

Wenn Sie DCM nicht zum Betreiben einer eigenen lokalen Zertifizierungsinstanz (CA) verwenden, müssen Sie zuerst einen Zertifikatsspeicher zum Verwalten der öffentlichen Zertifikate erstellen, die für SSL verwendet werden sollen. Dieser Zertifikatsspeicher trägt den Namen \*SYSTEM. Beim Erstellen eines Zertifikatsspeichers führt Sie DCM durch die Arbeitsschritte zum Generieren der Zertifikatsanforderungsinformationen, die Sie an die öffentliche CA übergeben müssen, um ein Zertifikat abzurufen.

So können Sie DCM für die Verwaltung und Verwendung öffentlicher Internet-Zertifikate benutzen, um Anwendungen die Herstellung von SSL-Kommunikationssitzungen zu ermöglichen:

1. Starten Sie Digital Certificate Manager.
2. Wählen Sie im Navigationsrahmen von DCM **Neuen Zertifikatsspeicher erstellen** aus, um die geführte Task zu starten und eine Reihe von Formularen auszufüllen. Diese Formulare führen Sie durch die Arbeitsschritte, die zum Erstellen eines Zertifikatsspeichers und eines Zertifikats erforderlich sind, das von den Anwendungen zum Herstellen von SSL-Sitzungen benutzt werden kann.

**Anmerkung:** Wenn Sie Fragen zum Ausfüllen eines bestimmten Formulars in dieser geführten Task haben, wählen Sie die Schaltfläche mit dem Fragezeichen (?) oben auf der Seite aus, um auf die Onlinehilfe zuzugreifen.

3. Wählen Sie als den zu erstellenden Zertifikatsspeicher **\*SYSTEM** aus, und klicken Sie anschließend auf **Weiter**.
4. Wählen Sie **Ja** aus, um bei der Erstellung des Zertifikatsspeichers **\*SYSTEM** auch ein Zertifikat zu erstellen, und klicken Sie dann auf **Weiter**.
5. Wählen Sie als Signierer des neuen Zertifikats **VeriSign oder eine andere Internet-Zertifizierungsinstanz (CA)** aus, und klicken Sie anschließend auf **Weiter**. Daraufhin wird ein Formular angezeigt, in dem Sie die Daten zur Identifikation des neuen Zertifikats eingeben können.

**Anmerkung:** Wenn auf Ihrem System ein IBM Verschlüsselungskoprozessor installiert ist, können Sie unter DCM als Nächstes auswählen, wie der private Schlüssel des Zertifikats gespeichert werden soll. Andernfalls speichert DCM den privaten Schlüssel automatisch im Zertifikatsspeicher **\*SYSTEM**. Weitere Informationen und Hilfe zum Auswählen der Speicherungsart für den privaten Schlüssel finden Sie in der DCM-Onlinehilfe.

6. Füllen Sie das Formular aus, und klicken Sie anschließend auf **Weiter**, um eine Bestätigungsseite aufzurufen. Diese Bestätigungsseite zeigt die Zertifikatsanforderungsdaten an, die für die öffentliche Zertifizierungsinstanz (CA) angegeben werden müssen, die Ihr Zertifikat ausstellt. Die Daten für die Zertifikatssignieranforderung (CSR) bestehen aus einem öffentlichen Schlüssel und weiteren Informationen, die Sie für das neue Zertifikat angegeben haben.
7. Kopieren Sie die CSR-Daten, und fügen Sie diese sorgfältig in das Zertifikatsantragsformular oder eine separate Datei ein, das bzw. die die öffentliche Zertifizierungsinstanz zur Anforderung eines Zertifikats benötigt. Sie müssen alle CSR-Daten einschließlich der Zeilen zum Beginn und zum Ende der Anforderung eines neuen Zertifikats verwenden. Wird diese Seite verlassen, gehen die Daten verloren und können nicht wiederhergestellt werden. Senden Sie das Antragsformular oder die Datei an die Zertifizierungsinstanz, die Sie zum Ausstellen und Signieren Ihrer Zertifikate ausgewählt haben.

**Anmerkung:** Sie müssen warten, bis die Zertifizierungsinstanz das signierte, vervollständigte Zertifikat zurücksendet, bevor Sie diesen Vorgang beenden können.

Wenn Sie Zertifikate im HTTP-Server für Ihr System verwenden wollen, müssen Sie den Webserver erstellen und konfigurieren, bevor Sie unter DCM mit signierten, vervollständigten Zertifikaten arbeiten können. Wenn Sie einen Webserver für die Verwendung von SSL konfigurieren, wird eine Anwendungs-ID für den Server generiert. Notieren Sie diese Anwendungs-ID, damit Sie in DCM angeben können, welches Zertifikat von der zugehörigen Anwendung für SSL benutzt werden soll.

Der Server darf nicht beendet und erneut gestartet werden, bevor Sie diesem mit DCM das signierte und vervollständigte Zertifikat zugeordnet haben. Wenn Sie die **\*ADMIN**-Instanz des Webservers vor der Zuordnung eines Zertifikats beenden und erneut starten, können Sie den Server nicht starten und DCM nicht zum Zuordnen eines Zertifikats zum Server verwenden.

8. Starten Sie DCM, nachdem die öffentliche Zertifizierungsinstanz Ihr signiertes Zertifikat zurückgegeben hat.
9. Klicken Sie im Navigationsrahmen auf **Zertifikatsspeicher auswählen**, und wählen Sie anschließend als zu öffnenden Zertifikatsspeicher **\*SYSTEM** aus.
10. Geben Sie auf der Zertifikatsspeicher- und Kennwortseite das Kennwort ein, das Sie bei der Erstellung des Zertifikatsspeichers angegeben haben, und klicken Sie dann auf **Weiter**.



11. Nach der Aktualisierung des Navigationsrahmens wählen Sie **Zertifikate verwalten** aus, um eine Liste mit Tasks anzuzeigen.
12. Wählen Sie in der Task-Liste **Zertifikat importieren** aus, um das Importieren des signierten Zertifikats in den Zertifikatsspeicher \*SYSTEM zu starten. Anschließend können Sie die Anwendungen angeben, die dieses Zertifikat für die SSL-Kommunikation einsetzen sollen.
13. Wählen Sie im Navigationsrahmen **Anwendungen verwalten** aus, um eine Liste mit Tasks anzuzeigen.
14. Wählen Sie in der Task-Liste **Zertifikat neu zuordnen** aus, um eine Liste von Anwendungen mit SSL-Unterstützung anzuzeigen, für die ein Zertifikat zugeordnet werden kann.
15. Wählen Sie in der Liste eine Anwendung aus, und klicken Sie anschließend auf **Zertifikat neu zuordnen**.
16. Wählen Sie das zuvor importierte Zertifikat aus, und klicken Sie auf **Neues Zertifikat zuordnen**. Daraufhin zeigt DCM eine Nachricht an, in der die Zertifikatsauswahl für die Anwendung bestätigt wird.

**Anmerkung:** In einigen Anwendungen mit SSL-Unterstützung kann die Client-Authentifizierung auf der Basis von Zertifikaten ausgeführt werden. Wenn eine Anwendung mit dieser Unterstützungsfunktion Zertifikate authentifizieren soll, bevor der Zugriff auf Ressourcen gewährt wird, müssen Sie für die Anwendung eine CA-Anerkennungsliste definieren. Hierdurch wird sichergestellt, dass von der Anwendung nur die Zertifikate von Zertifizierungsinstanzen überprüft werden können, die Sie als anerkannt definiert haben. Wenn ein Benutzer oder eine Client-Anwendung ein Zertifikat einer Zertifizierungsinstanz vorlegt, die in der CA-Anerkennungsliste nicht als anerkannt definiert wurde, wird das Zertifikat bei der Authentifizierung als ungültig zurückgewiesen.

Nach Abschluss der geführten Task verfügen Sie über alle Voraussetzungen, um mit der Konfiguration von Anwendungen für den Einsatz von SSL (siehe hierzu *Configuring your applications to use SSL*) für die gesicherte Kommunikation zu beginnen. Bevor Benutzer über eine SSL-Sitzung auf diese Anwendungen zugreifen können, müssen Sie über eine Kopie des CA-Zertifikats der Zertifizierungsinstanz verfügen, die das Serverzertifikat ausgestellt hat. Wenn Ihr Zertifikat von einer allgemein bekannten Internet-Zertifizierungsinstanz stammt, ist in der Client-Software Ihrer Benutzer möglicherweise bereits eine Kopie des erforderlichen CA-Zertifikats vorhanden. Zum Abrufen des Zertifikats der Zertifizierungsinstanz müssen Benutzer auf die Website der gewünschten Zertifizierungsinstanz zugreifen und die dort aufgeführten Anweisungen befolgen.

### **Öffentliche Internet-Zertifikate für das Signieren von Objekten verwalten:**

Digital Certificate Manager (DCM) kann zum Verwalten öffentlicher Internet-Zertifikate verwendet werden, die zum Ausführen digitaler Signaturen auf Objekten eingesetzt werden.

Wenn Sie DCM nicht zum Betreiben einer eigenen lokalen Zertifizierungsinstanz (CA) verwenden, müssen Sie zuerst einen Zertifikatsspeicher zum Verwalten der öffentlichen Zertifikate erstellen, die für das Signieren von Objekten verwendet werden sollen. Dieser Zertifikatsspeicher trägt den Namen \*OBJECTSIGNING. Beim Erstellen eines Zertifikatsspeichers führt Sie DCM durch die Arbeitsschritte zum Generieren der Zertifikatsanforderungsinformationen, die Sie an die öffentliche Internet-Zertifizierungsinstanz (CA) übergeben müssen, um ein Zertifikat abzurufen.

Außerdem müssen Sie eine Anwendungs-ID definieren, wenn Sie ein Zertifikat zum Signieren von Objekten verwenden wollen. Mit dieser Anwendungs-ID wird gesteuert, welche Berechtigungen zum Signieren von Objekten mit einem bestimmten Zertifikat erforderlich sind. Darüber hinaus bietet sie eine weitere Ebene der Zugriffssteuerung, die über die entsprechende Funktionalität von DCM hinausgeht. Standardmäßig benötigt ein Benutzer gemäß der Anwendungsdefinition die Sonderberechtigung \*ALLOBJ, um das Zertifikat für die Anwendung zum Signieren von Objekten zu benutzen. (Die Berechtigung, die für die Anwendungs-ID erforderlich ist, kann jedoch mit dem iSeries Navigator geändert werden.)

So können Sie DCM für die Verwaltung und Verwendung öffentlicher Internet-Zertifikate zum Signieren von Objekten verwenden:

1. Starten Sie Digital Certificate Manager.
2. Wählen Sie im linken Navigationsrahmen von DCM **Neuen Zertifikatsspeicher erstellen** aus, um die geführte Task zu starten und eine Reihe von Formularen auszufüllen. Diese Formulare führen Sie durch die Arbeitsschritte, die zum Erstellen eines Zertifikatsspeichers und eines Zertifikats erforderlich sind, das zum Signieren von Objekten verwendet werden kann.

**Anmerkung:** Wenn Sie Fragen zum Ausfüllen eines bestimmten Formulars in dieser geführten Task haben, wählen Sie die Schaltfläche mit dem Fragezeichen (?) oben auf der Seite aus, um auf die Onlinehilfe zuzugreifen.

3. Wählen Sie als den zu erstellenden Zertifikatsspeicher **\*OBJECTSIGNING** aus, und klicken Sie anschließend auf **Weiter**.
4. Wählen Sie **Ja** aus, um bei der Erstellung des Zertifikatsspeichers auch ein Zertifikat zu erstellen, und klicken Sie dann auf **Weiter**.
5. Wählen Sie als Signierer des neuen Zertifikats **VeriSign oder eine andere Internet-Zertifizierungsinstanz (CA)** aus, und klicken Sie anschließend auf **Weiter**. Daraufhin wird ein Formular angezeigt, in dem Sie die Daten zur Identifikation des neuen Zertifikats eingeben können.
6. Füllen Sie das Formular aus, und klicken Sie anschließend auf **Weiter**, um eine Bestätigungsseite aufzurufen. Diese Bestätigungsseite zeigt die Zertifikatsanforderungsdaten an, die für die öffentliche Zertifizierungsinstanz (CA) angegeben werden müssen, die Ihr Zertifikat ausstellt. Die Daten für die Zertifikatssignieranforderung (CSR) bestehen aus einem öffentlichen Schlüssel und weiteren Informationen, die Sie für das neue Zertifikat angegeben haben.
7. Kopieren Sie die CSR-Daten, und fügen Sie diese sorgfältig in das Zertifikatsantragsformular oder eine separate Datei ein, das bzw. die die öffentliche Zertifizierungsinstanz zur Anforderung eines Zertifikats benötigt. Sie müssen alle CSR-Daten einschließlich der Zeilen zum Beginn und zum Ende der Anforderung eines neuen Zertifikats verwenden. Wird diese Seite verlassen, gehen die Daten verloren und können nicht wiederhergestellt werden. Senden Sie das Antragsformular oder die Datei an die Zertifizierungsinstanz, die Sie zum Ausstellen und Signieren Ihrer Zertifikate ausgewählt haben.

**Anmerkung:** Sie müssen warten, bis die Zertifizierungsinstanz das signierte, vervollständigte Zertifikat zurücksendet, bevor Sie diesen Vorgang beenden können.

8. Starten Sie DCM, nachdem die öffentliche Zertifizierungsinstanz Ihr signiertes Zertifikat zurückgegeben hat.
9. Klicken Sie im linken Navigationsrahmen auf **Zertifikatsspeicher auswählen**, und wählen Sie anschließend als zu öffnenden Zertifikatsspeicher **\*OBJECTSIGNING** aus.
10. Geben Sie auf der Zertifikatsspeicher- und Kennwortseite das Kennwort ein, das Sie bei der Erstellung des Zertifikatsspeichers angegeben haben, und klicken Sie dann auf **Weiter**.
11. Wählen Sie im Navigationsrahmen **Zertifikate verwalten** aus, um eine Liste mit Tasks anzuzeigen.
12. Wählen Sie in der Task-Liste **Zertifikat importieren** aus, um das Importieren des signierten Zertifikats in den Zertifikatsspeicher **\*OBJECTSIGNING** zu starten. Anschließend können Sie eine Anwendungsdefinition für die Verwendung des Zertifikats zum Signieren von Objekten erstellen.
13. Nach der Aktualisierung des linken Navigationsrahmens wählen Sie **Anwendungen verwalten** aus, um eine Liste mit Tasks anzuzeigen.
14. Wählen Sie in der Task-Liste **Anwendung hinzufügen** aus, um das Erstellen einer Definition für eine Objektsignieranwendung zu starten, die ein Zertifikat zum Signieren von Objekten benutzt.
15. Füllen Sie das Formular aus, um die Objektsignieranwendung zu definieren, und klicken Sie dann auf **Hinzufügen**. Diese Anwendungsdefinition dient nicht zur Beschreibung einer konkreten Anwendung, sondern zur Beschreibung des Typs von Objekten, die mit einem bestimmten Zertifikat signiert werden sollen. Informationen zum Ausfüllen des Formulars finden Sie in der Onlinehilfefunktion.

16. Klicken Sie auf **OK**, um auf die Bestätigungsnachricht für die Anwendungsdefinition zu antworten und die Task-Liste 'Anwendungen verwalten' anzuzeigen.
17. Wählen Sie in der Task-Liste **Zertifikat neu zuordnen** aus, und klicken Sie anschließend auf **Weiter**, um eine Liste mit IDs für Objektsignieranwendungen anzuzeigen, denen ein Zertifikat zugeordnet werden kann.
18. Wählen Sie in der Liste die gewünschte Anwendungs-ID aus, und klicken Sie anschließend auf **Zertifikat neu zuordnen**.
19. Wählen Sie das zuvor importierte Zertifikat aus, und klicken Sie auf **Neues Zertifikat zuordnen**.

Nach Abschluss dieser Tasks verfügen Sie über alle Voraussetzungen, um mit dem Signieren von Objekten zu beginnen, um deren Integrität zu gewährleisten.

Nach dem Verteilen der signierten Objekte müssen deren Empfänger zum Überprüfen der Signaturen auf den Objekten die DCM-Version von OS/400 V5R1 oder eine spätere DCM-Version verwenden. Hierdurch kann der Absender identifiziert und sichergestellt werden, dass die Daten nicht geändert wurden. Zum Überprüfen der Signatur muss der Empfänger über eine Kopie des Signaturüberprüfungszertifikats verfügen. Eine Kopie dieses Zertifikats muss als Bestandteil des Pakets mit den signierten Objekten zur Verfügung gestellt werden.

Der Empfänger muss außerdem über eine Kopie des CA-Zertifikats der Zertifizierungsinstanz verfügen, die das zum Signieren der Objekte verwendete Zertifikat ausgestellt hat. Wenn die Objekte mit einem Zertifikat einer allgemein bekannten Internet-Zertifizierungsinstanz signiert wurden, ist in der DCM-Version des Empfängers möglicherweise bereits eine Kopie des erforderlichen CA-Zertifikats vorhanden. Wenn nicht sicher ist, dass der Empfänger bereits eine solche Kopie besitzt, sollten Sie diese jedoch zusammen mit den signierten Objekten bereitstellen. Eine Kopie des Zertifikats der lokalen Zertifizierungsinstanz muss z. B. dann zur Verfügung gestellt werden, wenn die Objekte mit einem Zertifikat einer privaten lokalen Zertifizierungsinstanz signiert wurden. Aus Sicherheitsgründen muss das Zertifikat der Zertifizierungsinstanz in einem separaten Paket versendet oder auf Anforderung der entsprechenden Benutzer öffentlich zur Verfügung gestellt werden.

#### **Zugehörige Konzepte**

„Digitale Zertifikate für das Signieren von Objekten“ auf Seite 42

In diesen Informationen wird erläutert, wie Zertifikate zum Sicherstellen der Objektintegrität oder zum Prüfen der digitalen Signatur von Objekten eingesetzt werden können, um deren Authentizität zu prüfen.

#### **Zertifikate zum Prüfen von Objektsignaturen verwalten:**

Digital Certificate Manager (DCM) kann zum Verwalten der Signaturüberprüfungszertifikate verwendet werden, die zum Überprüfen der digitalen Signaturen auf Objekten eingesetzt werden.

Zum Signieren eines Objekts verwenden Sie den privaten Schlüssel eines Zertifikats, um die Signatur zu erstellen. Wenn Sie das signierte Objekt an andere Benutzer senden, müssen Sie eine Kopie des Zertifikats beifügen, das zum Signieren verwendet wurde. Hierzu exportieren Sie mit DCM das Objektsignierzertifikat (ohne den privaten Schlüssel) als Signaturüberprüfungszertifikat. Signaturüberprüfungszertifikate können in eine Datei exportiert werden, die anschließend an andere Benutzer verteilt werden kann. Wenn Sie die von Ihnen erstellen Signaturen prüfen wollen, können Sie alternativ hierzu ein Signaturüberprüfungszertifikat auch in den Zertifikatsspeicher \*SIGNATUREVERIFICATION exportieren.

Wenn Sie die Signatur auf einem Objekt überprüfen wollen, müssen Sie über eine Kopie des Zertifikats verfügen, das zum Signieren verwendet wurde. Mit dem öffentlichen Schlüssel des für die Signatur verwendeten Zertifikats, der in diesem enthalten ist, können Sie die Signatur prüfen, die mit dem zugehörigen privaten Schlüssel erstellt wurde. Bevor Sie die Signatur eines Objekts prüfen können, müssen Sie deshalb vom Absender der signierten Objekte eine Kopie des verwendeten Zertifikats erhalten.

Darüber hinaus benötigen Sie eine Kopie des CA-Zertifikats der Zertifizierungsinstanz, die das zum Signieren des Objekts verwendete Zertifikat ausgestellt hat. Das Zertifikat der Zertifizierungsinstanz wird zum Prüfen der Authentizität des Zertifikats verwendet, mit dem das Objekt signiert wurde. DCM stellt Kopien von CA-Zertifikaten für die meisten allgemein bekannten Zertifizierungsinstanzen zur Verfügung. Wenn das Objekt jedoch mit dem Zertifikat einer anderen öffentlichen Zertifizierungsinstanz oder einer privaten lokalen Zertifizierungsinstanz signiert wurde, müssen Sie eine Kopie des jeweiligen CA-Zertifikats abrufen, bevor Sie Objektsignaturen prüfen können.

Wenn Sie DCM zum Prüfen von Objektsignaturen verwenden wollen, müssen Sie zuerst einen Zertifikatsspeicher zum Verwalten der erforderlichen Signaturüberprüfungszertifikate erstellen. Dieser Zertifikatsspeicher trägt den Namen \*SIGNATUREVERIFICATION. Beim Erstellen wird dieser Zertifikatsspeicher von DCM automatisch mit Kopien der CA-Zertifikate der meisten allgemein bekannten, öffentlichen Zertifizierungsinstanzen aufgefüllt.

**Anmerkung:** Wenn Sie Signaturen prüfen wollen, die mit eigenen Objektsignierzertifikaten erstellt wurden, müssen Sie den Zertifikatsspeicher \*SIGNATUREVERIFICATION erstellen und die im Zertifikatsspeicher \*OBJECTSIGNING enthaltenen Zertifikate in diesen kopieren. Dies gilt auch dann, wenn die Prüfung von Signaturen vom Zertifikatsspeicher \*OBJECTSIGNING aus durchgeführt werden soll.

So können Sie DCM zum Verwalten Ihrer Signaturüberprüfungszertifikate verwenden:

1. Starten Sie Digital Certificate Manager.
2. Wählen Sie im linken Navigationsrahmen von DCM **Neuen Zertifikatsspeicher erstellen** aus, um die geführte Task zu starten und eine Reihe von Formularen auszufüllen.

**Anmerkung:** Wenn Sie Fragen zum Ausfüllen eines bestimmten Formulars in dieser geführten Task haben, wählen Sie die Schaltfläche mit dem Fragezeichen (?) oben auf der Seite aus, um auf die Onlinehilfe zuzugreifen.

3. Wählen Sie als den zu erstellenden Zertifikatsspeicher \*SIGNATUREVERIFICATION aus, und klicken Sie anschließend auf **Weiter**.

**Anmerkung:** Wenn der Zertifikatsspeicher \*OBJECTSIGNING vorhanden ist, werden Sie von DCM nun aufgefordert anzugeben, ob die Objektsignierzertifikate als Signaturüberprüfungszertifikate in den neuen Zertifikatsspeicher kopiert werden sollen. Wenn Sie die bereits vorhandenen Objektsignierzertifikate zum Prüfen der Signaturen verwenden wollen, müssen Sie **Ja** auswählen und anschließend auf **Weiter** klicken. Um Zertifikate aus dem Zertifikatsspeicher \*OBJECTSIGNING zu kopieren, muss Ihnen das entsprechende Kennwort bekannt sein.

4. Geben Sie ein Kennwort für den neuen Zertifikatsspeicher an, und klicken Sie dann auf **Weiter**, um diesen zu erstellen. Auf einer Bestätigungsseite werden Sie darüber informiert, dass der Zertifikatsspeicher erfolgreich erstellt wurde. Jetzt können Sie den Speicher zum Verwalten und Verwenden von Zertifikaten benutzen, mit denen Objektsignaturen geprüft werden können.

**Anmerkung:** Wenn Sie diesen erstellt haben, um Signaturen auf selbst signierten Objekten zu prüfen, müssen Sie jetzt keine weiteren Arbeitsschritte ausführen. Wenn Sie neue Objektsignierzertifikate erstellen, müssen diese vom Zertifikatsspeicher \*OBJECTSIGNING in diesen Zertifikatsspeicher exportiert werden. Andernfalls können die mit diesen Zertifikaten erstellten Signaturen nicht geprüft werden. Wenn Sie diesen Zertifikatsspeicher erstellt haben, um Signaturen auf Objekten zu prüfen, die Sie von anderen Quellen empfangen haben, müssen Sie noch weitere Arbeitsschritte ausführen, um die benötigten Zertifikate in den Zertifikatsspeicher zu importieren.

5. Klicken Sie im Navigationsrahmen auf **Zertifikatsspeicher auswählen**, und wählen Sie anschließend als zu öffnenden Zertifikatsspeicher \*SIGNATUREVERIFICATION aus.

6. Geben Sie auf der Zertifikatsspeicher- und Kennwortseite das Kennwort ein, das Sie bei der Erstellung des Zertifikatsspeichers angegeben haben, und klicken Sie dann auf **Weiter**.
7. Nach der Aktualisierung des Navigationsrahmens wählen Sie **Zertifikate verwalten** aus, um eine Liste mit Tasks anzuzeigen.
8. Wählen Sie in der Task-Liste **Zertifikat importieren** aus. Diese Task führt Sie durch die Arbeitsschritte, die zum Importieren der benötigten Zertifikate in den Zertifikatsspeicher ausgeführt werden müssen, damit Sie die Signaturen auf empfangenen Objekten prüfen können.
9. Wählen Sie den Typ des Zertifikats aus, das importiert werden soll. Wählen Sie **Signaturüberprüfung** aus, um das mit den signierten Objekten empfangene Zertifikat zu importieren und die Import-Task abzuschließen.

**Anmerkung:** Wenn der Zertifikatsspeicher nicht bereits eine Kopie des CA-Zertifikats für die Zertifizierungsinstanz enthält, die zur Ausstellung des Signaturüberprüfungszertifikats verwendet wurde, müssen Sie *zuerst* das Zertifikat dieser Zertifizierungsinstanz importieren. Andernfalls erhalten Sie beim Importieren des Signaturüberprüfungszertifikats möglicherweise eine Fehlermeldung.

Jetzt können Sie diese Zertifikate zum Prüfen von Objektsignaturen verwenden.

#### **Zugehörige Konzepte**

„Digitale Zertifikate für das Signieren von Objekten“ auf Seite 42

In diesen Informationen wird erläutert, wie Zertifikate zum Sicherstellen der Objektintegrität oder zum Prüfen der digitalen Signatur von Objekten eingesetzt werden können, um deren Authentizität zu prüfen.

#### **Zugehörige Tasks**

„Objektsignaturen prüfen“ auf Seite 89

Sie können Digital Certificate Manager (DCM) verwenden, um die Authentizität digitaler Signaturen auf Objekten zu überprüfen. Durch das Prüfen der Signatur können Sie sicherstellen, dass die in dem Objekt enthaltenen Daten nicht geändert wurden, seit das Objekt vom Eigner signiert wurde.

## **| Vorhandenes Zertifikat verlängern**

| Die von Digital Certificate Manager (DCM) bei der Zertifikatsverlängerung verwendete Vorgehensweise kann abhängig vom Typ der ausstellenden Zertifizierungsinstanz (CA) variieren.

| Sie können ein Zertifikat bei der lokalen Zertifizierungsinstanz oder bei einer Internet-Zertifizierungsinstanz verlängern.

## **| Zertifikat bei einer lokalen Zertifizierungsinstanz verlängern**

| Wenn Sie zum Signieren des verlängerten Zertifikats die lokale Zertifizierungsinstanz (CA) verwenden, benutzt DCM die Informationen, die Sie bei der Erstellung eines neuen Zertifikats im aktuellen Zertifikatsspeicher angeben, und speichert das zuvor verwendete Zertifikat.

| So können Sie ein Zertifikat bei einer lokalen Zertifizierungsinstanz verlängern:

1. Klicken Sie im Navigationsrahmen auf **Zertifikatsspeicher auswählen**, und wählen Sie anschließend den Zertifikatsspeicher aus, in dem das zu verlängernde Zertifikat gespeichert ist.
2. Wählen Sie im Navigationsrahmen **Zertifikate verwalten** aus.
3. Wählen Sie im Navigationsrahmen **Zertifikat verlängern** aus.
4. Wählen Sie das zu verlängernde Zertifikat aus, und klicken Sie dann auf **Verlängern**.
5. Wählen Sie **Lokale Zertifizierungsinstanz (CA)** aus, und klicken Sie dann auf **Weiter**.
6. Füllen Sie das Formular zur Zertifikatsidentität vollständig aus. Hierbei muss die Angabe im Feld **Neue Zertifikatsbezeichnung** geändert werden, die Werte der anderen Felder können jedoch beibehalten werden.

- | 7. Wählen Sie alle Anwendungen aus, die mit dem verlängerten Zertifikat arbeiten sollen, und klicken Sie dann auf **Weiter**, um die Verlängerung des Zertifikats abzuschließen.

| **Anmerkung:** Um das Zertifikat zu verwenden, muss nicht unbedingt eine Anwendung ausgewählt werden.

### | **Zertifikat bei einer Internet-Zertifizierungsinstanz verlängern**

| Wenn Sie zur Ausstellung des Zertifikats eine anerkannte Internet-Zertifizierungsinstanz (CA) verwenden, können Sie zur Zertifikatsverlängerung die beiden folgenden Vorgehensweisen verwenden.

| Sie können das Zertifikat direkt bei der Internet-Zertifizierungsinstanz verlängern und das verlängerte Zertifikat anschließend aus der Datei importieren, die Sie von der signierenden Zertifizierungsinstanz erhalten haben. Alternativ hierzu können Sie mit DCM ein neues öffentliches/privates Schlüsselpaar und eine Zertifikatssignieranforderung für das Zertifikat erstellen und diese Daten dann an die Internet-Zertifizierungsstelle senden, um ein neues Zertifikat anzufordern. Nach Erhalt dieses Zertifikats von der Zertifizierungsinstanz können Sie den Verlängerungsprozess dann abschließen.

### | **Direkt von einer Internet-Zertifizierungsinstanz angefordertes Zertifikat importieren und verlängern:**

| Zum Importieren und Verlängern eines Zertifikats, das Sie direkt von einer Internet-Zertifizierungsinstanz angefordert haben, müssen Sie die folgenden Schritte ausführen:

- | 1. Klicken Sie im Navigationsrahmen auf **Zertifikatsspeicher auswählen**, und wählen Sie anschließend den Zertifikatsspeicher aus, in dem das zu verlängernde Zertifikat gespeichert ist.

| **Anmerkung:** Wenn Sie weitere Fragen zum Ausfüllen der Anzeige haben, können Sie in jeder Anzeige auf die Schaltfläche mit dem Fragezeichen (?) klicken, um weiterführende Informationen abzurufen.

- | 2. Wählen Sie im Navigationsrahmen **Zertifikate verwalten** aus.
- | 3. Klicken Sie im Navigationsrahmen auf **Zertifikat verlängern**.
- | 4. Wählen Sie das zu verlängernde Zertifikat aus, und klicken Sie dann auf **Verlängern**.
- | 5. Wählen Sie **VeriSign** oder eine andere Internet-Zertifizierungsinstanz (CA) aus, und klicken Sie dann auf **Weiter**.
- | 6. Wählen Sie **Nein - Verlängertes signiertes Zertifikat aus vorhandener Datei importieren** aus.
- | 7. Führen Sie die geführte Task zum Importieren des Zertifikats aus. Wenn Sie das Zertifikat direkt bei der ausstellenden Zertifizierungsinstanz verlängern wollen, gibt diese Zertifizierungsinstanz das verlängerte Zertifikat in einer Datei an Sie zurück. Vergewissern Sie sich, dass Sie den absoluten Pfad zu der Datei, in der das Zertifikat auf dem Server gespeichert ist, beim Import des Zertifikats korrekt angegeben haben. Die Datei, die das verlängerte Zertifikat enthält, kann in einem beliebigen IFS-Verzeichnis (IFS = Integrated File System) abgelegt werden.
- | 8. Klicken Sie auf **OK**, um die Task abzuschließen.

### | **Zertifikat durch Erstellung eines neuen öffentlichen/privaten Schlüsselpaares und einer Zertifikatssignieranforderung für das Zertifikat verlängern:**

| Zum Verlängern eines Zertifikats bei einer Internet-Zertifizierungsinstanz durch Erstellung eines neuen öffentlichen/privaten Schlüsselpaares und einer Zertifikatssignieranforderung für das Zertifikat müssen Sie die folgenden Schritte ausführen:

- | 1. Klicken Sie im Navigationsrahmen auf **Zertifikatsspeicher auswählen**, und wählen Sie anschließend den Zertifikatsspeicher aus, in dem das zu verlängernde Zertifikat gespeichert ist.

| **Anmerkung:** Wenn Sie weitere Fragen zum Ausfüllen der Anzeige haben, können Sie in jeder Anzeige auf die Schaltfläche mit dem Fragezeichen (?) klicken, um weiterführende Informationen abzurufen.

- | 2. Wählen Sie im Navigationsrahmen **Zertifikate verwalten** aus.

3. Klicken Sie im Navigationsrahmen auf **Zertifikat verlängern**.
4. Wählen Sie das zu verlängernde Zertifikat aus, und klicken Sie dann auf **Verlängern**.
5. Wählen Sie **VeriSign** oder eine andere Internet-Zertifizierungsinstanz (CA) aus, und klicken Sie dann auf **Weiter**.
6. Klicken Sie auf **Ja - Neues Schlüsselpaar für dieses Zertifikat erstellen** und anschließend auf **Weiter**.
7. Füllen Sie das Formular zur Zertifikatsidentität vollständig aus. Hierbei muss die Angabe im Feld **Neue Zertifikatsbezeichnung** geändert werden, die Werte der anderen Felder können jedoch beibehalten werden. Hinweis: Wenn Sie weitere Fragen zum Ausfüllen der Anzeige haben, können Sie in jeder Anzeige auf die Schaltfläche mit dem Fragezeichen (?) klicken, um weiterführende Informationen abzurufen.
8. Klicken Sie auf **OK**, um die Task abzuschließen.

## Zertifikat importieren

Im Folgenden finden Sie Informationen dazu, wie Sie Digital Certificate Manager (DCM) zum Importieren von Zertifikaten verwenden können, die in Dateien auf Ihrem Server gespeichert werden.

Sie können ein Zertifikat auch von einem anderen Server importieren, anstatt dieses auf dem aktuellen Server erneut zu erstellen. Beispiel: Sie haben auf der iSeries A die lokale Zertifizierungsinstanz verwendet, um ein Zertifikat für Ihre Einzelhandelswebanwendung zu erstellen, das zum Aufbau von SSL-Verbindungen verwendet werden soll. Ihr Unternehmen hat in der letzten Zeit expandiert und Sie haben deswegen einen neuen iSeries-Server (iSeries B) installiert, um zusätzliche Instanzen dieser sehr stark frequentierten Einzelhandelsanwendung zu unterstützen. Sie möchten, dass alle Instanzen der Einzelhandelsanwendung mit einem identischen Zertifikat arbeiten, um sich zu identifizieren und SSL-Verbindungen aufzubauen. Aus diesem Grund werden Sie möglicherweise sowohl das Zertifikat der lokalen Zertifizierungsinstanz als auch das Serverzertifikat von der iSeries A auf die iSeries B importieren wollen, anstatt die lokale Zertifizierungsinstanz auf der iSeries A zu verwenden, um ein neues, unterschiedliches Zertifikat für die iSeries B zu erstellen.

Führen Sie die folgenden Schritte aus, um ein Zertifikat mit DCM zu importieren:

1. Klicken Sie im linken Navigationsrahmen auf **Zertifikatsspeicher auswählen**, und wählen Sie anschließend den Zertifikatsspeicher aus, in den das Zertifikat importiert werden soll. Der Zertifikatsspeicher, in den das Zertifikat importiert werden soll, muss Zertifikate enthalten, die denselben Typ wie das Zertifikat aufweisen, das auf dem anderen System exportiert wurde. Wenn Sie also ein Serverzertifikat (Typ) importieren wollen, dann müssen Sie dieses in einen Zertifikatsspeicher importieren, der Serverzertifikate enthält (z. B. in den Zertifikatsspeicher \*SYSTEM oder Speicher für andere Systemzertifikate).
2. Wählen Sie im Navigationsrahmen **Zertifikate verwalten** aus.
3. Wählen Sie im Navigationsrahmen **Zertifikat importieren** aus.
4. Wählen Sie den Typ des Zertifikats aus, das importiert werden soll, und klicken Sie dann auf **Weiter**. Der zu importierende Zertifikatstyp muss mit dem Typ des exportierten Zertifikats übereinstimmen. Wenn Sie z. B. ein Serverzertifikat exportiert haben, müssen Sie für den Import ebenfalls ein Serverzertifikat auswählen.

**Anmerkung:** Wenn DCM ein Zertifikat im pkcs12-Format exportiert, befindet sich die ausstellende Zertifizierungsinstanz in der Kette des exportierten Zertifikats und wird deswegen automatisch importiert, wenn das Zertifikat selbst von DCM in den Zertifikatsspeicher importiert wird. Wird das Zertifikat jedoch nicht im pkcs12-Format exportiert und der Zertifikatsspeicher, in den importiert werden soll, kein Zertifikat der Zertifizierungsinstanz enthält, müssen Sie das Zertifikat der ausstellenden Zertifizierungsinstanz importieren, bevor das Zertifikat importiert werden kann.

5. Führen Sie die geführte Task zum Importieren des Zertifikats aus. Beim Importieren des Zertifikats müssen Sie sich vergewissern, dass der absolute Pfad, unter dem das Zertifikat auf dem Server gespeichert ist, korrekt angegeben wurde.

---

## Verwaltung mit DCM

In diesen Informationen wird erläutert, wie DCM zur Verwaltung von Zertifikaten und der Anwendungen eingesetzt werden kann, die diese benutzen. Darüber hinaus finden Sie hier Erläuterungen zum digitalen Signieren von Objekten und zum Erstellen und Betreiben einer eigenen Zertifizierungsinstanz (CA).

Nach der Konfiguration von Digital Certificate Manager (DCM) müssen im weiteren Verlauf einige Zertifikatsverwaltungs-Tasks ausgeführt werden. Weitere Informationen zur Verwendung von DCM für die Verwaltung von digitalen Zertifikaten finden Sie unter den folgenden Themen:

### Lokale Zertifizierungsinstanz zum Ausstellen von Zertifikaten für andere iSeries-Systeme verwenden

Dieses Thema enthält Informationen zum Einsatz einer privaten lokalen Zertifizierungsinstanz auf einem System für die Ausstellung von Zertifikaten, die auf anderen iSeries-Systemen benutzt werden sollen.

Möglicherweise verwenden Sie in Ihrem Netzwerk bereits eine private lokale Zertifizierungsinstanz auf einem System. Nun möchten Sie die Verwendung dieser lokalen Zertifizierungsinstanz auf ein anderes System in Ihrem Netzwerk ausdehnen. Nehmen wir an, Sie möchten, dass Ihre aktuelle lokale Zertifizierungsinstanz ein Server- oder Client-Zertifikat für eine Anwendung auf einem anderen System ausstellt, das für SSL-Kommunikationssitzungen verwendet werden soll. Es könnte aber auch sein, dass Sie die von Ihrer lokalen Zertifizierungsinstanz ausgestellten Zertifikate verwenden wollen, um Objekte zu signieren, die Sie auf einem anderen Server gespeichert haben.

Dieses Ziel können Sie durch Verwendung des Programms Digital Certificate Manager (DCM) erreichen. Einige Tasks werden auf dem System ausgeführt, auf dem die lokale Zertifizierungsinstanz betrieben wird. Andere Tasks werden auf dem sekundären System ausgeführt, auf dem sich die Anwendungen befinden, für die Sie Zertifikate ausstellen möchten. Dieses sekundäre System wird auch als Zielsystem bezeichnet. Welche Tasks Sie auf dem Zielsystem ausführen müssen, richtet sich nach dem Releasestand dieses Systems.

**Anmerkung:** Es könnte ein Problem auftreten, wenn das System, auf dem die lokale Zertifizierungsinstanz betrieben wird, ein Chiffrierprogramm verwendet, das eine stärkere Verschlüsselung durchführt als das Zielsystem. Bei OS/400 V5R2 und OS/400 V5R3 steht als einziges Chiffrierprogramm 5722-AC3 zur Verfügung, bei dem es sich um das Produkt mit der stärksten Verschlüsselung handelt. In älteren Releases konnten jedoch andere, schwächere Chiffrierprogramme (5722-AC1 oder 5722-AC2) installiert werden, die einen geringeren Umfang an Verschlüsselungsfunktionen bereitstellten. Wenn Sie das Zertifikat (und seinen privaten Schlüssel) exportieren, verschlüsselt das System die Datei, um deren Inhalt zu schützen. Wenn das System ein stärkeres Chiffrierprogramm verwendet als das Zielsystem, kann das Zielsystem die Datei während des Importprozesses nicht entschlüsseln. Der Importprozess kann somit fehlschlagen, oder das Zertifikat kann möglicherweise nicht für den Aufbau von SSL-Sitzungen verwendet werden. Dies trifft auch dann zu, wenn Sie für das neue Zertifikat eine Schlüsselgröße verwenden, die für die Verwendung mit dem Chiffrierprogramm des Zielsystems geeignet ist.

Sie können Ihre lokale Zertifizierungsinstanz verwenden, um Zertifikate für andere Systeme auszustellen, die Sie anschließend für das Signieren von Objekten benutzen können, bzw. mit denen Sie es Anwendungen ermöglichen können, SSL-Sitzungen aufzubauen. Wenn Sie die lokale Zertifizierungsinstanz verwenden, um ein Zertifikat für die Verwendung auf einem anderen System zu erstellen, enthalten die von DCM erstellten Dateien eine Kopie des Zertifikats der lokalen Zertifizierungsinstanz sowie Kopien von Zertifikaten für zahlreiche öffentliche Internet-Zertifizierungsinstanzen.

Die Tasks, die Sie in DCM ausführen müssen, können variieren. Dies richtet sich nach dem Typ des Zertifikats, das von der lokalen Zertifizierungsinstanz ausgestellt wird, sowie nach dem Releasestand und sonstigen Bedingungen auf dem Zielsystem.



## Private Zertifikate für die Verwendung auf einem anderen iSeries-System ausstellen

Wenn die lokale Zertifizierungsinstanz Zertifikate für die Verwendung auf einem anderen System ausstellen soll, müssen Sie folgende Schritte auf dem System ausführen, auf dem die lokale Zertifizierungsinstanz implementiert ist:

1. Starten Sie Digital Certificate Manager.
2. Wählen Sie im Navigationsrahmen **Zertifikat erstellen** aus, um eine Liste der Zertifikatstypen aufzurufen, die mit der lokalen Zertifizierungsinstanz erstellt werden können.

**Anmerkung:** Um diese Task auszuführen, müssen Sie keinen Zertifikatsspeicher öffnen. Bei diesen Anweisungen wird vorausgesetzt, dass Sie entweder nicht innerhalb eines bestimmten Zertifikatsspeichers arbeiten oder aber dass Sie innerhalb des Zertifikatsspeichers der lokalen Zertifizierungsinstanz arbeiten. Voraussetzung für die Ausführung dieser Tasks ist das Vorhandensein einer lokalen Zertifizierungsinstanz auf diesem System. Wenn Sie Fragen zum Ausfüllen eines bestimmten Formulars in dieser geführten Task haben, wählen Sie die Schaltfläche mit dem Fragezeichen (?) oben auf der Seite aus, um auf die Onlinehilfe zuzugreifen.

3. Wählen Sie den Typ des Zertifikats aus, das die lokale Zertifizierungsinstanz ausstellen soll, und klicken Sie anschließend auf **Weiter**, um die geführte Task zu starten und eine Reihe von Formularen auszufüllen.
4. Wählen Sie bei der Erstellung entweder **Server- oder Client-Zertifikat für anderes iSeries-System** (für SSL-Sitzungen) oder **Objektsignierzertifikat für anderes iSeries-System** (für die Verwendung auf einem anderen System) aus.

**Anmerkung:** Wenn Sie ein Objektsignierzertifikat zur Verwendung auf einem anderen System erstellen, muss auf diesem System mindestens OS/400 V5R1 installiert sein, damit das Zertifikat verwendet werden kann. Da auf dem Zielsystem mindestens OS/400 V5R1 ausgeführt werden muss, zeigt DCM auf dem lokalen Host-System keine Aufforderung zur Auswahl eines Zielreleaseformats für das neue Objektsignierzertifikat an.

5. Füllen Sie das Formular aus, und klicken Sie anschließend auf **Weiter**, um eine Bestätigungsseite aufzurufen.

**Anmerkung:** Befindet sich auf dem Zielsystem bereits ein Zertifikatsspeicher mit dem Namen \*OBJECTSIGNING oder \*SYSTEM, müssen Sie sicherstellen, dass Sie eine eindeutige Zertifikatsbezeichnung sowie einen eindeutigen Dateinamen für das Zertifikat angeben. Durch die Angabe einer eindeutigen Zertifikatsbezeichnung und eines eindeutigen Dateinamens wird sichergestellt, dass das Zertifikat problemlos in den auf dem Zielsystem vorhandenen Zertifikatsspeicher importiert wird. Auf dieser Bestätigungsseite werden die Namen der von DCM erstellten Dateien angezeigt, die an das Zielsystem übertragen werden sollen. DCM erstellt diese Dateien auf der Grundlage des auf dem Zielsystem gültigen Releasestands, den Sie angegeben haben. DCM stellt automatisch eine Kopie des Zertifikats der lokalen Zertifizierungsinstanz in diese Dateien.

DCM erstellt das neue Zertifikat in seinem eigenen Zertifikatsspeicher und generiert zwei Dateien, die Sie übertragen müssen: eine Zertifikatsspeicherdatei (mit der Erweiterung .KDB) und eine Anforderungsdatei (mit der Erweiterung .RDB).

6. Zum Übertragen der Dateien auf das Zielsystem können Sie FTP (File Transfer Protocol) im binären Modus oder eine andere Methode verwenden.

### Zugehörige Konzepte

„Hinweise zur Sicherung und Wiederherstellung von DCM-Daten“ auf Seite 32

In diesem Abschnitt erfahren Sie, wie wichtige DCM-Daten zum Sicherungs- und Wiederherstellungsplan Ihres Systems hinzugefügt werden können.

„Öffentliche vs. private Zertifikate“ auf Seite 35

In diesen Informationen wird erläutert, wie der Zertifikatstyp (öffentlich oder privat) festgestellt werden kann, der die individuellen Unternehmensanforderungen des Kunden optimal erfüllt.

### Zugehörige Tasks

„Lokale Zertifizierungsinstanz erstellen und betreiben“ auf Seite 47

In den vorliegenden Informationen wird erläutert, wie eine lokale Zertifizierungsinstanz (CA) erstellt und betrieben werden kann, um private Zertifikate für Ihre Anwendungen auszustellen.

## Privates Zertifikat für SSL verwenden

Die Zertifikate, die Ihre Anwendungen für das Aufbauen von SSL-Sitzungen aus dem Zertifikatsspeicher \*SYSTEM abrufen, werden von Ihnen mit Hilfe von Digital Certificate Manager (DCM) verwaltet. Wenn Sie DCM bisher auf dem Zielsystem noch nicht zur Verwaltung von Zertifikaten für SSL verwendet haben, ist dieser Zertifikatsspeicher auf dem Zielsystem noch nicht vorhanden.

Vom Vorhandensein des Zertifikatsspeichers \*SYSTEM hängt es ab, welche Tasks zur Verwendung der übertragenen Zertifikatsspeicherdateien ausgeführt werden, die Sie auf dem Host-System erstellt haben, auf dem die lokale Zertifizierungsinstanz implementiert ist. Wenn der Zertifikatsspeicher \*SYSTEM nicht vorhanden ist, können Sie die übertragenen Zertifikatsdateien zum Erstellen des Zertifikatsspeichers \*SYSTEM benutzen. Wenn der Zertifikatsspeicher \*SYSTEM auf dem Zielsystem vorhanden ist, können Sie entweder die übertragenen Dateien als Speicher für andere Systemzertifikate verwenden oder die übertragenen Dateien in den vorhandenen Zertifikatsspeicher \*SYSTEM importieren.

### Zertifikatsspeicher \*SYSTEM ist nicht vorhanden:

Wenn der Zertifikatsspeicher \*SYSTEM auf dem System, auf dem Sie die übertragenen Zertifikatsspeicherdateien verwenden wollen, nicht vorhanden ist, können Sie die übertragenen Zertifikatsdateien als Zertifikatsspeicher \*SYSTEM verwenden. Zum Erstellen des Zertifikatsspeichers \*SYSTEM und zum Verwenden der Zertifikatsdateien auf dem Zielsystem müssen Sie die folgenden Schritte ausführen:

1. Stellen Sie sicher, dass die Zertifikatsspeicherdateien (zwei Dateien: eine mit der Erweiterung .KDB und eine mit der Erweiterung .RDB), die Sie auf dem System erstellt haben, auf dem die lokale Zertifizierungsinstanz implementiert wurde, sich im Verzeichnis /QIBM/USERDATA/ICSS/CERT/SERVER befinden.
2. Nachdem die übertragenen Zertifikatsdateien im Verzeichnis /QIBM/USERDATA/ICSS/CERT/SERVER abgelegt wurden, müssen diese in DEFAULT.KDB und DEFAULT.RDB umbenannt werden. Durch das Umbenennen dieser Dateien im entsprechenden Verzeichnis erstellen Sie die Komponenten, die den Zertifikatsspeicher \*SYSTEM für das Zielsystem bilden. Die Zertifikatsspeicherdateien enthalten bereits Kopien von Zertifikaten für viele öffentliche Internet-Zertifizierungsinstanzen. DCM hat diese bei der Erstellung zusammen mit einer Kopie des Zertifikats der lokalen Zertifizierungsinstanz zu den Zertifikatsspeicherdateien hinzugefügt.

**Achtung:** Wenn auf Ihrem Zielsystem bereits die Dateien DEFAULT.KDB und DEFAULT.RDB im Verzeichnis /QIBM/USERDATA/ICSS/CERT/SERVER vorhanden sind, ist auch der Zertifikatsspeicher \*SYSTEM auf diesem Zielsystem definiert. Aus diesem Grund dürfen die übertragenen Dateien nicht wie angegeben umbenannt werden. Durch das Überschreiben der Standarddateien treten bei der Verwendung von DCM, des übertragenen Zertifikatsspeichers und dessen Inhalt Probleme auf. Stattdessen sollten Sie sicherstellen, dass die Dateien über eindeutige Namen verfügen und dass der übertragene Zertifikatsspeicher als **Speicher für andere Systemzertifikate** verwendet wird. Wenn Sie die Dateien als Speicher für andere Systemzertifikate verwenden, können Sie DCM nicht benutzen, um anzugeben, welche Anwendungen das Zertifikat verwenden sollen.

3. Starten Sie Digital Certificate Manager. An dieser Stelle müssen Sie das Kennwort für den Zertifikatsspeicher \*SYSTEM ändern, der durch die Umbenennung der übertragenen Dateien erstellt wurde. Wenn Sie das Kennwort ändern, kann DCM das neue Kennwort speichern, so dass Sie anschließend alle Zertifikatsverwaltungsfunktionen von DCM für den Zertifikatsspeicher verwenden können.

4. Klicken Sie im Navigationsrahmen auf **Zertifikatsspeicher auswählen**, und wählen Sie anschließend als zu öffnenden Zertifikatsspeicher **\*SYSTEM** aus.
5. Geben Sie auf der Zertifikatsspeicher- und Kennwortseite das Kennwort ein, das Sie auf dem *Host*-System für den Zertifikatsspeicher angegeben haben, als Sie das Zertifikat für das Zielsystem erstellt haben. Klicken Sie dann auf **Weiter**.
6. Wählen Sie im Navigationsrahmen **Zertifikatsspeicher verwalten** und anschließend in der Liste mit Tasks **Kennwort ändern** aus. Füllen Sie das Formular aus, um das Kennwort für den Zertifikatsspeicher zu ändern. Nach dem Ändern des Kennworts müssen Sie den Zertifikatsspeicher erneut öffnen, bevor Sie mit den darin enthaltenen Zertifikaten arbeiten können. Als Nächstes können Sie angeben, welche Anwendungen das Zertifikat für SSL-Sitzungen verwenden sollen.
7. Klicken Sie im Navigationsrahmen auf **Zertifikatsspeicher auswählen**, und wählen Sie anschließend als zu öffnenden Zertifikatsspeicher **\*SYSTEM** aus.
8. Wenn die Seite **Zertifikatsspeicher und Kennwort** angezeigt wird, geben Sie das neue Kennwort an, und klicken Sie dann auf **Weiter**.
9. Nach der Aktualisierung des Navigationsrahmens wählen Sie in diesem **Zertifikate verwalten** aus, um eine Liste mit Tasks anzuzeigen.
10. Wählen Sie in der Task-Liste **Zertifikat zuordnen** aus, um eine Liste mit Zertifikaten im aktuellen Zertifikatsspeicher anzuzeigen.
11. Wählen Sie das auf dem *Host*-System erstellte Zertifikat aus, und klicken Sie dann auf **Anwendungen zuordnen**, um eine Liste von Anwendungen mit SSL-Unterstützung anzuzeigen, denen das Zertifikat zugeordnet werden kann.
12. Wählen Sie die Anwendungen aus, die das Zertifikat für SSL-Sitzungen verwenden sollen, und klicken Sie dann auf **Weiter**. Daraufhin zeigt DCM eine Nachricht an, in der die Zertifikatsauswahl für die Anwendungen bestätigt wird.

**Anmerkung:** In einigen Anwendungen mit SSL-Unterstützung kann die Client-Authentifizierung auf der Basis von Zertifikaten ausgeführt werden. Eine Anwendung mit SSL-Unterstützung muss in der Lage sein, Zertifikate zu authentifizieren, bevor Zugriff auf Ressourcen gewährt wird. Daher müssen Sie für die Anwendung eine CA-Anerkennungsliste definieren. Hierdurch wird sichergestellt, dass von der Anwendung nur die Zertifikate von Zertifizierungsinstanzen überprüft werden können, die Sie als anerkannt definiert haben. Wenn Benutzer oder eine Client-Anwendung ein Zertifikat einer Zertifizierungsinstanz vorlegen, die in der CA-Anerkennungsliste nicht als anerkannt definiert wurde, wird das Zertifikat bei der Authentifizierung als ungültig zurückgewiesen.

Nachdem Sie diese Tasks ausgeführt haben, können die Anwendungen auf dem Zielsystem das von der lokalen Zertifizierungsinstanz auf einem anderen System ausgestellte Zertifikat verwenden. Bevor Sie jedoch SSL für diese Anwendungen nutzen können, müssen Sie die Anwendungen für die Verwendung von SSL konfigurieren (siehe hierzu *Configure the applications to use SSL*).

Bevor ein Benutzer über eine SSL-Verbindung auf die ausgewählten Anwendungen zugreifen kann, muss er mit Hilfe von DCM vom Host-System eine Kopie des Zertifikats der lokalen Zertifizierungsinstanz abrufen. Das Zertifikat der lokalen Zertifizierungsinstanz muss in eine Datei auf dem PC des Benutzers kopiert oder in seinen Browser heruntergeladen werden. Welche Vorgehensweise gewählt wird, hängt von den Anforderungen der jeweiligen Anwendung mit SSL-Unterstützung ab.

**Zertifikatsspeicher \*SYSTEM ist vorhanden - die Dateien als Speicher für andere Systemzertifikate verwenden:**

Wenn auf dem Zielsystem bereits ein Zertifikatsspeicher **\*SYSTEM** vorhanden ist, müssen Sie entscheiden, wie mit den auf das Zielsystem übertragenen Zertifikatsdateien gearbeitet werden soll. Eine Möglichkeit besteht darin, festzulegen, dass die übertragenen Zertifikatsdateien als **Speicher für andere System-**

**zertifikate** verwendet werden sollen. Die andere Möglichkeit besteht darin, das private Zertifikat und das zugehörige Zertifikat der lokalen Zertifizierungsinstanz in den vorhandenen Zertifikatsspeicher \*SYSTEM zu importieren.

Speicher für andere Systemzertifikate sind benutzerdefinierte sekundäre Zertifikatsspeicher für SSL-Zertifikate. Sie können diese erstellen und verwenden, um Zertifikate für benutzerdefinierte Anwendungen mit SSL-Unterstützung zur Verfügung zu stellen, wobei diese Anwendungen zum Registrieren einer Anwendungs-ID in der DCM-Funktion keine DCM-APIs verwenden. Mit der Auswahl "Speicher für andere Systemzertifikate" können Sie Zertifikate für Anwendungen verwalten, die von Ihnen oder anderen Benutzern geschrieben wurden und die mit Hilfe der API SSL\_Init auf ein Zertifikat zugreifen und dieses zum Aufbauen einer SSL-Sitzung verwenden. Mit Hilfe dieser API kann eine Anwendung für einen Zertifikatsspeicher an Stelle des von Ihnen speziell angegebenen Zertifikats das Standardzertifikat verwenden.

IBM iSeries -Anwendungen (sowie die Anwendungen vieler anderer Softwarehersteller) wurden so entwickelt, dass sie nur die im Zertifikatsspeicher \*SYSTEM enthaltenen Zertifikate verwenden. Wenn Sie die übertragenen Dateien als Speicher für andere Systemzertifikate verwenden, können Sie DCM nicht benutzen, um anzugeben, welche Anwendungen das Zertifikat für SSL-Sitzungen verwenden sollen. Daher können iSeries-Standardanwendungen mit SSL-Unterstützung nicht für die Verwendung dieses Zertifikats konfiguriert werden. Wenn Sie das Zertifikat für iSeries-Anwendungen benutzen wollen, müssen Sie das betreffende Zertifikat aus den übertragenen Zertifikatsspeicherdateien in den Zertifikatsspeicher \*SYSTEM importieren.

So können Sie die übertragenen Zertifikatsdateien als Speicher für andere Systemzertifikate verwenden, auf sie zugreifen und damit arbeiten:

1. Starten Sie Digital Certificate Manager.
2. Klicken Sie im Navigationsrahmen auf **Zertifikatsspeicher auswählen**, und wählen Sie anschließend als zu öffnenden Zertifikatsspeicher **Speicher für andere Systemzertifikate** aus.
3. Geben Sie auf der Zertifikatsspeicher- und Kennwortseite den vollständig qualifizierten Pfad und Dateinamen der Zertifikatsspeicherdatei (mit der Erweiterung .KDB) ein, die vom Host-System übertragen wurde. Geben Sie außerdem das Kennwort ein, das Sie für den Zertifikatsspeicher bei der Erstellung des Zertifikats für das Zielsystem auf dem *Host*-System angegeben haben, und klicken Sie dann auf **Weiter**.
4. Wählen Sie im Navigationsrahmen **Zertifikatsspeicher verwalten** und anschließend in der Liste mit Tasks **Kennwort ändern** aus. Füllen Sie das Formular aus, um das Kennwort für den Zertifikatsspeicher zu ändern.

**Anmerkung:** Stellen Sie sicher, dass **Automatisches Anmelden** ausgewählt ist, wenn Sie das Kennwort für den Zertifikatsspeicher ändern. Diese Auswahl gewährleistet, dass DCM das neue Kennwort speichert, so dass Sie für den neuen Speicher alle Zertifikatsverwaltungsfunktionen von DCM verwenden können.

Nach dem Ändern des Kennworts müssen Sie den Zertifikatsspeicher erneut öffnen, bevor Sie mit den darin enthaltenen Zertifikaten arbeiten können. Als Nächstes können Sie angeben, dass das in diesem Speicher enthaltene Zertifikat als Standardzertifikat verwendet werden soll.

5. Klicken Sie im Navigationsrahmen auf **Zertifikatsspeicher auswählen**, und wählen Sie anschließend **Speicher für andere Systemzertifikate** als zu öffnenden Zertifikatsspeicher aus.
6. Wenn die Seite **Zertifikatsspeicher und Kennwort** angezeigt wird, geben Sie den vollständig qualifizierten Pfad und den Dateinamen der Zertifikatsspeicherdatei sowie das neue Kennwort an, und klicken Sie dann auf **Weiter**.
7. Wählen Sie nach der Aktualisierung des Navigationsrahmens **Zertifikatsspeicher verwalten** und anschließend in der Task-Liste **Standardzertifikat festlegen** aus.

Nachdem Sie nun den Speicher für andere Systemzertifikate erstellt und konfiguriert haben, können alle Anwendungen, die die API SSL\_Init verwenden, das darin enthaltene Zertifikat zum Aufbauen von SSL-Sitzungen benutzen.

*Zertifikatsspeicher \*SYSTEM ist vorhanden - die im vorhandenen Zertifikatsspeicher \*SYSTEM enthaltenen Zertifikate verwenden:*

Sie können die in den übertragenen Zertifikatsspeicherdateien enthaltenen Zertifikate in einem vorhandenen Zertifikatsspeicher \*SYSTEM auf einem System verwenden. Dazu müssen Sie die Zertifikate aus den Zertifikatsspeicherdateien in den vorhandenen Zertifikatsspeicher \*SYSTEM importieren. Die Zertifikate können jedoch nicht direkt aus den Dateien mit den Erweiterungen .KDB und .RDB importiert werden, da sie nicht in einem Format vorliegen, das die DCM-Importfunktion erkennen und verwenden kann. Um die übertragenen Zertifikate in einem vorhandenen Zertifikatsspeicher \*SYSTEM verwenden zu können, müssen Sie die Dateien als Speicher für andere Systemzertifikate öffnen und anschließend in den Zertifikatsspeicher \*SYSTEM exportieren.

So können Sie auf dem Zielsystem die Zertifikate aus den Zertifikatsspeicherdateien in den Zertifikatsspeicher \*SYSTEM exportieren:

1. Starten Sie Digital Certificate Manager.
2. Klicken Sie im Navigationsrahmen auf **Zertifikatsspeicher auswählen**, und geben Sie anschließend als zu öffnenden Zertifikatsspeicher **Speicher für andere Systemzertifikate** an.
3. Geben Sie auf der Zertifikatsspeicher- und Kennwortseite den vollständig qualifizierten Pfad und Dateinamen der Zertifikatsspeicherdatei (mit der Erweiterung .KDB) ein, die vom Host-System übertragen wurde. Geben Sie außerdem das Kennwort ein, das Sie für den Zertifikatsspeicher bei der Erstellung des Zertifikats für das Zielsystem auf dem *Host*-System angegeben haben, und klicken Sie dann auf **Weiter**.
4. Wählen Sie im Navigationsrahmen **Zertifikatsspeicher verwalten** und anschließend in der Liste mit Tasks **Kennwort ändern** aus. Füllen Sie das Formular aus, um das Kennwort für den Zertifikatsspeicher zu ändern. Nach dem Ändern des Kennworts müssen Sie den Zertifikatsspeicher erneut öffnen, bevor Sie mit den darin enthaltenen Zertifikaten arbeiten können.

**Anmerkung:** Stellen Sie sicher, dass **Automatisches Anmelden** ausgewählt ist, wenn Sie das Kennwort für den Zertifikatsspeicher ändern. Diese Auswahl gewährleistet, dass DCM das neue Kennwort speichert, so dass Sie für den neuen Speicher alle Zertifikatsverwaltungsfunktionen von DCM verwenden können. Wenn Sie das Kennwort nicht ändern und "Automatisches Anmelden" auswählen, treten möglicherweise Fehler auf, wenn die Zertifikate von diesem Speicher in den Zertifikatsspeicher \*SYSTEM exportiert werden.

5. Klicken Sie im Navigationsrahmen auf **Zertifikatsspeicher auswählen**, und wählen Sie anschließend **Speicher für andere Systemzertifikate** als zu öffnenden Zertifikatsspeicher aus.
6. Wenn die Seite **Zertifikatsspeicher und Kennwort** angezeigt wird, geben Sie den vollständig qualifizierten Pfad und den Dateinamen der Zertifikatsspeicherdatei sowie das neue Kennwort an, und klicken Sie dann auf **Weiter**.
7. Wählen Sie nach der Aktualisierung des Navigationsrahmens **Zertifikate verwalten** aus, um eine Liste mit Tasks aufzurufen, und wählen Sie anschließend **Zertifikat exportieren** aus.
8. Wählen Sie als zu exportierenden Zertifikatstyp **Zertifizierungsinstanz (CA)** aus, und klicken Sie auf **Weiter**.

**Anmerkung:** Exportieren Sie zuerst das Zertifikat der lokalen Zertifizierungsinstanz in den Zertifikatsspeicher, bevor Sie das Server- oder Client-Zertifikat in den Zertifikatsspeicher exportieren. Wenn Sie das Server- oder Client-Zertifikat zuerst exportieren, tritt möglicherweise ein Fehler auf, weil das Zertifikat der lokalen Zertifizierungsinstanz nicht im Zertifikatsspeicher vorhanden ist.

9. Wählen Sie das zu exportierende Zertifikat der lokalen Zertifizierungsinstanz aus, und klicken Sie anschließend auf **Exportieren**.
10. Wählen Sie als Ausgabe für das exportierte Zertifikat **Zertifikatsspeicher** aus, und klicken Sie anschließend auf **Weiter**.
11. Geben Sie als Ziel-Zertifikatsspeicher \*SYSTEM und danach das Kennwort ein. Klicken Sie anschließend auf **Weiter**. Daraufhin wird eine Nachricht angezeigt, in der Sie entweder über den erfolgreichen Export des Zertifikats informiert werden oder Fehlerinformationen erhalten, wenn der Exportvorgang fehlgeschlagen ist.
12. Nun können Sie das Server- oder Client-Zertifikat in den Zertifikatsspeicher \*SYSTEM exportieren. Wählen Sie die Task **Zertifikat exportieren** erneut aus.
13. Wählen Sie als zu exportierenden Zertifikatstyp **Server oder Client** aus, und klicken Sie auf **Weiter**.
14. Wählen Sie das zu exportierende Server- oder Client-Zertifikat aus, und klicken Sie anschließend auf **Exportieren**.
15. Wählen Sie als Ausgabe für das exportierte Zertifikat **Zertifikatsspeicher** aus, und klicken Sie anschließend auf **Weiter**.
16. Geben Sie als Ziel-Zertifikatsspeicher \*SYSTEM und danach das Kennwort ein. Klicken Sie anschließend auf **Weiter**. Daraufhin wird eine Nachricht angezeigt, in der Sie entweder über den erfolgreichen Export des Zertifikats informiert werden oder Fehlerinformationen erhalten, wenn der Exportvorgang fehlgeschlagen ist.
17. Das Zertifikat kann nun Anwendungen zugeordnet und für SSL-Sitzungen verwendet werden. Klicken Sie im Navigationsrahmen auf **Zertifikatsspeicher auswählen**, und wählen Sie dann als zu öffnenden Zertifikatsspeicher **\*SYSTEM** aus.
18. Geben Sie auf der Zertifikatsspeicher- und Kennwortseite das Kennwort für den Zertifikatsspeicher \*SYSTEM ein, und klicken Sie dann auf **Weiter**.
19. Nach der Aktualisierung des Navigationsrahmens wählen Sie **Zertifikate verwalten** aus, um eine Liste mit Tasks anzuzeigen.
20. Wählen Sie in der Task-Liste **Zertifikat zuordnen** aus, um eine Liste mit Zertifikaten im aktuellen Zertifikatsspeicher anzuzeigen.
21. Wählen Sie das auf dem *Host*-System erstellte Zertifikat aus, und klicken Sie dann auf **Anwendungen zuordnen**, um eine Liste von Anwendungen mit SSL-Unterstützung anzuzeigen, denen das Zertifikat zugeordnet werden kann.
22. Wählen Sie die Anwendungen aus, die das Zertifikat für SSL-Sitzungen verwenden sollen, und klicken Sie dann auf **Weiter**. Daraufhin zeigt DCM eine Nachricht an, in der die Zertifikatsauswahl für die Anwendungen bestätigt wird.

**Anmerkung:** In einigen Anwendungen mit SSL-Unterstützung kann die Client-Authentifizierung auf der Basis von Zertifikaten ausgeführt werden. Eine Anwendung mit SSL-Unterstützung muss in der Lage sein, Zertifikate zu authentifizieren, bevor Zugriff auf Ressourcen gewährt wird. Daher müssen Sie für die Anwendung eine CA-Anerkennungsliste definieren. Hierdurch wird sichergestellt, dass von der Anwendung nur die Zertifikate von Zertifizierungsinstanzen überprüft werden können, die Sie als anerkannt definiert haben. Wenn Benutzer oder eine Client-Anwendung ein Zertifikat einer Zertifizierungsinstanz vorlegen, die in der CA-Anerkennungsliste nicht als anerkannt definiert wurde, wird das Zertifikat bei der Authentifizierung als ungültig zurückgewiesen.

Nachdem Sie diese Tasks ausgeführt haben, können die Anwendungen auf dem Zielsystem das von der lokalen Zertifizierungsinstanz auf einem anderen System ausgestellte Zertifikat verwenden. Bevor Sie jedoch SSL für diese Anwendungen nutzen können, müssen Sie die Anwendungen für die Verwendung von SSL konfigurieren (siehe hierzu *Configure the applications to use SSL*).

Bevor ein Benutzer über eine SSL-Verbindung auf die ausgewählten Anwendungen zugreifen kann, muss er mit Hilfe von DCM vom Host-System eine Kopie des Zertifikats der lokalen Zertifizierungsinstanz abrufen. Das Zertifikat der lokalen Zertifizierungsinstanz muss in eine Datei auf dem PC des Benutzers

kopiert oder in seinen Browser heruntergeladen werden. Welche Vorgehensweise gewählt wird, hängt von den Anforderungen der jeweiligen Anwendung mit SSL-Unterstützung ab.

## Privates Zertifikat zum Signieren von Objekten auf einem Zielsystem verwenden

Die Zertifikate, die Sie zum Signieren von Objekten aus dem Zertifikatsspeicher \*OBJECTSIGNING verwenden, werden von Ihnen mit Hilfe von Digital Certificate Manager (DCM) verwaltet. Wenn Sie DCM bisher auf dem Zielsystem noch nicht zur Verwaltung von Objektsignierzertifikaten verwendet haben, ist dieser Zertifikatsspeicher auf dem Zielsystem noch nicht vorhanden.

Vom Vorhandensein des Zertifikatsspeichers \*OBJECTSIGNING hängt ab, welche Tasks für die Verwendung der übertragenen Zertifikatsspeicherdateien, die Sie auf dem Host-System mit der lokalen Zertifizierungsinstanz erstellt haben, ausgeführt werden müssen. Wenn der Zertifikatsspeicher \*OBJECTSIGNING nicht vorhanden ist, können Sie die übertragenen Zertifikatsdateien zum Erstellen des Zertifikatsspeichers \*OBJECTSIGNING benutzen. Ist der Zertifikatsspeicher \*OBJECTSIGNING allerdings auf dem Zielsystem vorhanden, müssen Sie die übertragenen Zertifikate in diesen importieren.

### Zertifikatsspeicher \*OBJECTSIGNING ist nicht vorhanden:

Welche Tasks Sie zur Verwendung der Zertifikatsspeicherdateien ausführen müssen, die Sie auf dem Host-System mit der lokalen Zertifizierungsinstanz erstellt haben, richtet sich danach, ob Sie DCM bereits zuvor auf dem Zielsystem für die Verwaltung von Objektsignierzertifikaten verwendet haben.

So gehen Sie vor, wenn der Zertifikatsspeicher \*OBJECTSIGNING auf dem Zielsystem, das die übertragenen Zertifikatsspeicherdateien enthält, nicht vorhanden ist:

1. Stellen Sie sicher, dass die Zertifikatsspeicherdateien (zwei Dateien: eine mit der Erweiterung .KDB und eine mit der Erweiterung .RDB), die Sie auf dem System erstellt haben, auf dem die lokale Zertifizierungsinstanz implementiert wurde, sich im Verzeichnis /QIBM/USERDATA/ICSS/CERT/SIGNING befinden.
2. Nachdem die übertragenen Zertifikatsdateien im Verzeichnis /QIBM/USERDATA/ICSS/CERT/SIGNING abgelegt wurden, müssen diese ggf. in SGN0BJ.KDB und SGN0BJ.RDB umbenannt werden. Durch das Umbenennen dieser Dateien erstellen Sie die Komponenten, die den Zertifikatsspeicher \*OBJECTSIGNING für das Zielsystem bilden. Die Zertifikatsspeicherdateien enthalten bereits Kopien von Zertifikaten für viele öffentliche Internet-Zertifizierungsinstanzen. DCM hat diese bei der Erstellung zusammen mit einer Kopie des Zertifikats der lokalen Zertifizierungsinstanz zu den Zertifikatsspeicherdateien hinzugefügt.

**Achtung:** Wenn auf Ihrem Zielsystem bereits die Dateien SGN0BJ.KDB und SGN0BJ.RDB im Verzeichnis /QIBM/USERDATA/ICSS/CERT/SIGNING vorhanden sind, ist auch der Zertifikatsspeicher \*OBJECTSIGNING auf diesem Zielsystem definiert. Aus diesem Grund dürfen die übertragenen Dateien nicht wie angegeben umbenannt werden. Durch das Überschreiben der Standard-Objektsignierdateien treten bei der Verwendung von DCM, des übertragenen Zertifikatsspeichers und dessen Inhalt Probleme auf. Wenn der Zertifikatsspeicher \*OBJECTSIGNING bereits vorhanden ist, müssen Sie einen anderen Prozess verwenden, um die Zertifikate im vorhandenen Zertifikatsspeicher abzulegen.

3. Starten Sie Digital Certificate Manager. An dieser Stelle müssen Sie das Kennwort für den Zertifikatsspeicher \*OBJECTSIGNING ändern. Wenn Sie das Kennwort ändern, kann DCM das neue Kennwort speichern, so dass Sie anschließend alle Zertifikatsverwaltungsfunktionen von DCM für den Zertifikatsspeicher verwenden können.
4. Klicken Sie im Navigationsrahmen auf **Zertifikatsspeicher auswählen**, und wählen Sie anschließend als zu öffnenden Zertifikatsspeicher \*OBJECTSIGNING aus.
5. Geben Sie auf der Kennwortseite das Kennwort ein, das Sie bei der Erstellung des Zertifikatsspeichers auf dem Host-System angegeben haben, und klicken Sie dann auf **Weiter**.
6. Wählen Sie im Navigationsrahmen **Zertifikatsspeicher verwalten** und anschließend in der Liste mit Tasks **Kennwort ändern** aus. Füllen Sie das Formular aus, um das Kennwort für den Zertifikatsspeicher zu ändern. Nach dem Ändern des Kennworts müssen Sie den Zertifikatsspeicher erneut öff-

nen, bevor Sie mit den darin enthaltenen Zertifikaten arbeiten können. Anschließend können Sie eine Anwendungsdefinition für die Verwendung des Zertifikats zum Signieren von Objekten erstellen.

7. Nach dem erneuten Öffnen des Zertifikatsspeichers müssen Sie im Navigationsrahmen **Anwendungen verwalten** auswählen, um eine Liste mit Tasks aufzurufen.
8. Wählen Sie in der Task-Liste **Anwendung hinzufügen** aus, um das Erstellen einer Definition für eine Objektsignieranwendung zu starten, die ein Zertifikat zum Signieren von Objekten benutzt.
9. Füllen Sie das Formular aus, um die Objektsignieranwendung zu definieren, und klicken Sie dann auf **Hinzufügen**. Diese Anwendungsdefinition dient nicht zur Beschreibung einer konkreten Anwendung, sondern zur Beschreibung des Typs von Objekten, die mit einem bestimmten Zertifikat signiert werden sollen. Informationen zum Ausfüllen des Formulars finden Sie in der Onlinehilfefunktion.
10. Klicken Sie auf **OK**, um auf die Bestätigungsnachricht für die Anwendungsdefinition zu antworten und die Task-Liste **Anwendungen verwalten** aufzurufen.
11. Wählen Sie in der Task-Liste **Zertifikat neu zuordnen** aus, um eine Liste mit IDs für Objektsignieranwendungen anzuzeigen, denen ein Zertifikat zugeordnet werden kann.
12. Wählen Sie in der Liste die gewünschte Anwendungs-ID aus, und klicken Sie anschließend auf **Zertifikat neu zuordnen**.
13. Wählen Sie das Zertifikat aus, das die lokale Zertifizierungsinstanz auf dem Host-System erstellt hat, und klicken Sie anschließend auf **Neues Zertifikat zuordnen**.

Nach Abschluss dieser Tasks verfügen Sie über alle Voraussetzungen, um mit dem Signieren von Objekten zu beginnen, um deren Integrität zu gewährleisten.

Nach dem Verteilen der signierten Objekte müssen deren Empfänger zum Überprüfen der Signaturen auf den Objekten DCM verwenden. Hierdurch kann der Absender identifiziert und sichergestellt werden, dass die Daten nicht geändert wurden. Zum Überprüfen der Signatur muss der Empfänger über eine Kopie des Signaturüberprüfungszertifikats verfügen. Eine Kopie dieses Zertifikats muss als Bestandteil des Pakets mit den signierten Objekten zur Verfügung gestellt werden.

Der Empfänger muss außerdem über eine Kopie des CA-Zertifikats der Zertifizierungsinstanz verfügen, die das zum Signieren der Objekte verwendete Zertifikat ausgestellt hat. Wenn die Objekte mit einem Zertifikat einer allgemein bekannten Internet-Zertifizierungsinstanz signiert wurden, ist auf der DCM-Version des Empfängers bereits eine Kopie des erforderlichen CA-Zertifikats vorhanden. Falls erforderlich, sollten Sie jedoch eine Kopie des CA-Zertifikats zusammen mit den signierten Objekten in einem separaten Paket bereitstellen. Eine Kopie des Zertifikats der lokalen Zertifizierungsinstanz muss z. B. dann zur Verfügung gestellt werden, wenn die Objekte mit einem Zertifikat der lokalen Zertifizierungsinstanz signiert wurden. Aus Sicherheitsgründen muss das Zertifikat der Zertifizierungsinstanz in einem separaten Paket versendet oder auf Anforderung der entsprechenden Benutzer öffentlich zur Verfügung gestellt werden.

### **Zertifikatsspeicher \*OBJECTSIGNING ist vorhanden:**

Sie können die in den übertragenen Zertifikatsspeicherdateien enthaltenen Zertifikate in einem vorhandenen Zertifikatsspeicher \*OBJECTSIGNING auf einem System verwenden. Dazu müssen Sie die Zertifikate aus den Zertifikatsspeicherdateien in den vorhandenen Zertifikatsspeicher \*OBJECTSIGNING importieren. Die Zertifikate können jedoch nicht direkt aus den Dateien mit den Erweiterungen .KDB und .RDB importiert werden, da sie nicht in einem Format vorliegen, das die DCM-Importfunktion erkennen und verwenden kann. Die Zertifikate können in den vorhandenen Zertifikatsspeicher \*OBJECTSIGNING aufgenommen werden, indem die übertragenen Dateien auf dem Zielsystem als Speicher für andere Systemzertifikate geöffnet werden. Anschließend können Sie die Zertifikate direkt in den Zertifikatsspeicher \*OBJECTSIGNING exportieren. Es muss sowohl eine Kopie des Objektsignierzertifikats selbst als auch eine Kopie des Zertifikats der lokalen Zertifizierungsinstanz aus den übertragenen Dateien exportiert werden.



So können Sie auf dem Zielsystem die Zertifikate aus den Zertifikatsspeicherdateien direkt in den Zertifikatsspeicher \*OBJECTSIGNING exportieren:

1. Starten Sie Digital Certificate Manager.
2. Klicken Sie im Navigationsrahmen auf **Zertifikatsspeicher auswählen**, und geben Sie anschließend als zu öffnenden Zertifikatsspeicher **Speicher für andere Systemzertifikate** an.
3. Geben Sie auf der Zertifikatsspeicher- und Kennwortseite den vollständig qualifizierten Pfad und Dateinamen der Zertifikatsspeicherdateien ein. Geben Sie außerdem das Kennwort ein, das Sie bei der Erstellung dieser Dateien auf dem Host-System angegeben haben, und klicken Sie dann auf **Weiter**.
4. Wählen Sie im Navigationsrahmen **Zertifikatsspeicher verwalten** und anschließend in der Liste mit Tasks **Kennwort ändern** aus. Füllen Sie das Formular aus, um das Kennwort für den Zertifikatsspeicher zu ändern.

**Anmerkung:** Stellen Sie sicher, dass **Automatisches Anmelden** ausgewählt ist, wenn Sie das Kennwort für den Zertifikatsspeicher ändern. Diese Auswahl gewährleistet, dass DCM das neue Kennwort speichert, so dass Sie für den neuen Speicher alle Zertifikatsverwaltungsfunktionen von DCM verwenden können. Wenn Sie das Kennwort nicht ändern und "Automatisches Anmelden" auswählen, treten möglicherweise Fehler auf, wenn die Zertifikate von diesem Speicher in den Zertifikatsspeicher \*OBJECTSIGNING exportiert werden.

Nach dem Ändern des Kennworts müssen Sie den Zertifikatsspeicher erneut öffnen, bevor Sie mit den darin enthaltenen Zertifikaten arbeiten können.

5. Klicken Sie im Navigationsrahmen auf **Zertifikatsspeicher auswählen**, und wählen Sie anschließend **Speicher für andere Systemzertifikate** als zu öffnenden Zertifikatsspeicher aus.
6. Geben Sie auf der Zertifikatsspeicher- und Kennwortseite den vollständig qualifizierten Pfad und Dateinamen der Zertifikatsspeicherdatei sowie das neue Kennwort ein, und klicken Sie dann auf **Weiter**.
7. Wählen Sie nach der Aktualisierung des Navigationsrahmens **Zertifikate verwalten** aus, um eine Liste mit Tasks aufzurufen, und wählen Sie anschließend **Zertifikat exportieren** aus.
8. Wählen Sie als zu exportierenden Zertifikatstyp **Zertifizierungsinstanz (CA)** aus, und klicken Sie auf **Weiter**.

**Anmerkung:** Die Wortwahl bei der Beschreibung dieser Task lässt vermuten, dass Sie, wenn Sie mit einem Speicher für andere Systemzertifikate arbeiten, immer mit Server- oder Client-Zertifikaten arbeiten. Der Grund hierfür ist, dass dieser Zertifikatsspeichertyp für die Verwendung als sekundärer Speicher neben dem Zertifikatsspeicher \*SYSTEM gedacht ist. Die Verwendung der Export-Task in diesem Zertifikatsspeicher ist jedoch der einfachste Weg, um die Zertifikate aus den übertragenen Dateien in den vorhandenen Zertifikatsspeicher \*OBJECTSIGNING einzufügen.

9. Wählen Sie das zu exportierende Zertifikat der lokalen Zertifizierungsinstanz aus, und klicken Sie anschließend auf **Exportieren**.

**Anmerkung:** Exportieren Sie zuerst das Zertifikat der lokalen Zertifizierungsinstanz in den Zertifikatsspeicher, bevor Sie das Objektsignierzertifikat in den Zertifikatsspeicher exportieren. Wenn Sie das Objektsignierzertifikat zuerst exportieren, tritt möglicherweise ein Fehler auf, weil das Zertifikat der lokalen Zertifizierungsinstanz nicht im Zertifikatsspeicher vorhanden ist.

10. Wählen Sie als Ausgabe für das exportierte Zertifikat **Zertifikatsspeicher** aus, und klicken Sie anschließend auf **Weiter**.
11. Geben Sie als Ziel-Zertifikatsspeicher \*OBJECTSIGNING und anschließend das zugehörige Kennwort für \*OBJECTSIGNING ein, und klicken Sie dann auf **Weiter**.
12. Nun können Sie das Objektsignierzertifikat in den Zertifikatsspeicher \*OBJECTSIGNING exportieren. Wählen Sie die Task **Zertifikat exportieren** erneut aus.

13. Wählen Sie als zu exportierenden Zertifikatstyp **Server oder Client** aus, und klicken Sie auf **Weiter**.
14. Wählen Sie das zu exportierende Zertifikat aus, und klicken Sie anschließend auf **Exportieren**.
15. Wählen Sie als Ausgabe für das exportierte Zertifikat **Zertifikatsspeicher** aus, und klicken Sie anschließend auf **Weiter**.
16. Geben Sie als Ziel-Zertifikatsspeicher \*OBJECTSIGNING und anschließend das zugehörige Kennwort für \*OBJECTSIGNING ein, und klicken Sie dann auf **Weiter**. Daraufhin wird eine Nachricht angezeigt, in der Sie entweder über den erfolgreichen Export des Zertifikats informiert werden oder Fehlerinformationen erhalten, wenn der Exportvorgang fehlgeschlagen ist.

**Anmerkung:** Um dieses Zertifikat zum Signieren von Objekten zu verwenden, müssen Sie nun eine Zertifikatzuordnung zu einer Objektsignieranwendung vornehmen.

## Anwendungen in DCM verwalten

Dieses Thema enthält Informationen zum Erstellen von Anwendungsdefinitionen und dazu, wie die Zertifikatzuordnung einer Anwendung verwaltet werden kann. Außerdem wird hier erklärt, wie CA-Anerkennungslisten definiert werden, die von Anwendungen zum Akzeptieren von Zertifikaten für die Client-Authentifizierung benutzt werden.

Digital Certificate Manager (DCM) kann zum Ausführen verschiedener Verwaltungsaufgaben für Anwendungen mit SSL-Unterstützung sowie für Objektsignieranwendungen benutzt werden. Sie können z. B. angeben, welche Zertifikate Ihre Anwendungen für SSL-Kommunikationssitzungen (SSL = Secure Sockets Layer) verwenden. Die Tasks für die Anwendungsverwaltung, die ausgeführt werden können, hängen vom jeweiligen Anwendungstyp und von dem Zertifikatsspeicher ab, mit dem Sie arbeiten. Anwendungen können nur über den Zertifikatsspeicher \*SYSTEM oder \*OBJECTSIGNING verwaltet werden.

Obwohl die Mehrzahl der von DCM bereitgestellten Tasks für die Anwendungsverwaltung leicht verständlich ist, werden Ihnen einige dieser Tasks möglicherweise noch nicht vertraut sein. Weitere Informationen zu diesen Tasks finden Sie unter den folgenden Themen:

### Zugehörige Konzepte

„Anwendungsdefinitionen“ auf Seite 12

Unter diesem Thema erfahren Sie mehr zu DCM-Anwendungsdefinitionen und wie diese für die SSL-Konfiguration und zum Signieren von Objekten eingesetzt werden können.

## Anwendungsdefinition erstellen

In diesem Abschnitt werden die beiden verschiedenen Anwendungstypen beschrieben, die Sie definieren und mit denen Sie arbeiten können.

Es gibt zwei Arten von Anwendungsdefinitionen, mit denen in DCM gearbeitet werden kann. Dies sind zum einen Anwendungsdefinitionen für Server- und Client-Anwendungen, die mit SSL arbeiten, und zum anderen Anwendungsdefinitionen, die Sie zum Signieren von Objekten benutzen.

Wenn Sie unter DCM mit SSL-Anwendungsdefinitionen und den zugehörigen Zertifikaten arbeiten wollen, muss die Anwendung in DCM zuerst als Anwendungsdefinition registriert werden, um ihr eine eindeutige Anwendungs-ID zuzuordnen. Anwendungsentwickler registrieren Anwendungen mit SSL-Unterstützung mit Hilfe einer API (QSYRGAP, QsyRegisterAppForCertUse), mit der die Anwendungs-ID in DCM automatisch erstellt werden kann. Alle IBM iSeries-Anwendungen mit SSL-Unterstützung sind in DCM registriert, so dass Sie diesen mit DCM auf einfache Weise ein Zertifikat zuordnen können, um den Aufbau einer SSL-Sitzung zu ermöglichen. Bei selbst geschriebenen oder gekauften Anwendungen können Sie ebenfalls eine Anwendungsdefinition definieren und die entsprechende Anwendungs-ID in DCM erstellen. Sie müssen im Zertifikatsspeicher \*SYSTEM arbeiten, um eine SSL-Anwendungsdefinition für eine Client- oder eine Serveranwendung zu erstellen.

Um ein Zertifikat zum Signieren von Objekten zu verwenden, müssen Sie zuerst eine Anwendung definieren, die mit dem Zertifikat benutzt werden soll. Anders als eine SSL-Anwendungsdefinition beschreibt

eine Objektsignieranwendung keine konkrete Anwendung. Stattdessen sollte die von Ihnen erstellte Anwendungsdefinition zur Beschreibung des Typs oder der Gruppe von Objekten dienen, die signiert werden sollen. Sie müssen im Zertifikatsspeicher \*OBJECTSIGNING arbeiten, um die Definition einer Objektsignieranwendung zu erstellen.

So erstellen Sie eine Anwendungsdefinition:

1. Starten Sie Digital Certificate Manager.
2. Klicken Sie auf **Zertifikatsspeicher auswählen**, und wählen Sie anschließend den gewünschten Zertifikatsspeicher aus. (Hierbei handelt es sich abhängig vom Typ der zu erstellenden Anwendungsdefinition entweder um den Zertifikatsspeicher \*SYSTEM oder \*OBJECTSIGNING.)

**Anmerkung:** Wenn Sie Fragen zum Ausfüllen eines bestimmten Formulars in dieser geführten Task haben, wählen Sie die Schaltfläche mit dem Fragezeichen (?) oben auf der Seite aus, um auf die Onlinehilfe zuzugreifen.

3. Geben Sie auf der Zertifikatsspeicher- und Kennwortseite das Kennwort ein, das Sie bei der Erstellung des Zertifikatsspeichers angegeben haben, und klicken Sie dann auf **Weiter**.
4. Wählen Sie im Navigationsrahmen **Anwendungen verwalten** aus, um eine Liste mit Tasks anzuzeigen.
5. Wählen Sie in der Task-Liste **Anwendung hinzufügen** aus, um ein Formular zum Definieren der Anwendung anzuzeigen.

**Anmerkung:** Wenn Sie im Zertifikatsspeicher \*SYSTEM arbeiten, fordert DCM Sie nun auf auszuwählen, ob Sie eine Server- oder eine Client-Anwendungsdefinition hinzufügen wollen.

6. Füllen Sie das Formular aus, und klicken Sie anschließend auf **Hinzufügen**. Die Daten, die Sie für die Anwendungsdefinition angeben können, variieren abhängig vom Anwendungstyp, der definiert werden soll. Wenn Sie eine Serveranwendung definieren, kann auch angegeben werden, ob diese für die Client-Authentifizierung Zertifikate einsetzen kann, und ob die Client-Authentifizierung überhaupt erforderlich ist. Darüber hinaus können Sie angeben, dass die Anwendung mit einer CA-Anerkennungsliste arbeiten muss, um Zertifikate zu authentifizieren.

#### **Zugehörige Konzepte**

„Anwendungsdefinitionen“ auf Seite 12

Unter diesem Thema erfahren Sie mehr zu DCM-Anwendungsdefinitionen und wie diese für die SSL-Konfiguration und zum Signieren von Objekten eingesetzt werden können.

## **Zertifikatzuordnung für eine Anwendung verwalten**

Sie müssen mit Digital Certificate Manager (DCM) einer Anwendung ein Zertifikat zuordnen, bevor diese Anwendung eine gesicherte Funktion ausführen kann. Hierzu gehört z. B. das Herstellen einer SSL-Sitzung (SSL = Secure Sockets Layer) oder das Signieren eines Objekts.

So können Sie einer Anwendung ein Zertifikat zuordnen oder die Zertifikatzuordnung für eine Anwendung ändern:

1. Starten Sie Digital Certificate Manager.
2. Klicken Sie auf **Zertifikatsspeicher auswählen**, und wählen Sie anschließend den gewünschten Zertifikatsspeicher aus. (Hierbei handelt es sich abhängig vom Typ der Anwendung, der ein Zertifikat zugeordnet werden soll, um den Zertifikatsspeicher \*SYSTEM oder \*OBJECTSIGNING.)

**Anmerkung:** Wenn Sie Fragen zum Ausfüllen eines bestimmten Formulars in dieser geführten Task haben, wählen Sie die Schaltfläche mit dem Fragezeichen (?) oben auf der Seite aus, um auf die Onlinehilfe zuzugreifen.

3. Geben Sie auf der Zertifikatsspeicher- und Kennwortseite das Kennwort ein, das Sie bei der Erstellung des Zertifikatsspeichers angegeben haben, und klicken Sie dann auf **Weiter**.
4. Wählen Sie im Navigationsrahmen **Anwendungen verwalten** aus, um eine Liste mit Tasks anzuzeigen.

5. Wenn Sie im Zertifikatsspeicher \*SYSTEM arbeiten, wählen Sie den zu verwaltenden Anwendungstyp aus. (Geben Sie hierbei für die Anwendung entweder **Server** oder **Client** an.)
6. Wählen Sie in der Task-Liste **Zertifikat neu zuordnen** aus, um eine Liste von Anwendungen anzuzeigen, für die ein Zertifikat zugeordnet werden kann.
7. Wählen Sie in der Liste eine Anwendung aus, und klicken Sie anschließend auf **Zertifikat neu zuordnen**, um eine Liste der Zertifikate anzuzeigen, die der Anwendung zugeordnet werden können.
8. Wählen Sie ein Zertifikat in der Liste aus, und klicken Sie dann auf **Neues Zertifikat zuordnen**. Daraufhin zeigt DCM eine Nachricht an, in der die Zertifikatsauswahl für die Anwendung bestätigt wird.

**Anmerkung:** Wenn Sie einer SSL-Anwendung, die den Einsatz von Zertifikaten für die Client-Authentifizierung unterstützt, ein Zertifikat zuordnen wollen, müssen Sie für die Anwendung eine CA-Anerkennungsliste definieren. Hierdurch wird sichergestellt, dass von der Anwendung nur die Zertifikate von Zertifizierungsinstanzen überprüft werden können, die Sie als anerkannt definiert haben. Wenn ein Benutzer oder eine Client-Anwendung ein Zertifikat einer Zertifizierungsinstanz vorlegt, die in der CA-Anerkennungsliste nicht als anerkannt definiert wurde, wird das Zertifikat bei der Authentifizierung als ungültig zurückgewiesen.

Wenn Sie ein Zertifikat für eine Anwendung ändern oder entfernen, ist nicht sicher, ob dies durch die Anwendung erkannt wird, wenn sie während der Änderung der Zertifikatszuordnung ausgeführt wird. iSeries Access für Windows-Server können die von Ihnen vorgenommenen Zertifikatsänderungen z. B. automatisch anwenden. Telnet-Server, IBM HTTP-Server für i5/OS oder andere Anwendungen müssen jedoch möglicherweise gestoppt und anschließend erneut gestartet werden, damit die Zertifikatsänderungen angewendet werden können.

Ab OS/400 V5R2 können Sie die Task Zertifikat zuordnen verwenden, um ein Zertifikat in einem Arbeitsgang mehreren Anwendungen zuzuordnen.

### **CA-Anerkennungsliste für eine Anwendung definieren**

Für Anwendungen, die die Verwendung von Zertifikaten für die Client-Authentifizierung in SSL-Sitzungen (SSL = Secure Sockets Layer) unterstützen, muss festgelegt werden, ob Zertifikate als gültige Identitätsnachweise akzeptiert werden. Eines der Kriterien, das von Anwendungen zum Authentifizieren eines Zertifikats angewendet wird, besteht darin, ob die Anwendung die ausstellende Zertifizierungsinstanz anerkennt.

Digital Certificate Manager (DCM) kann zum Definieren der Zertifizierungsinstanzen verwendet werden, die von einer Anwendung bei der Client-Authentifizierung für Zertifikate anerkannt werden. Diese anerkannten Zertifizierungsinstanzen werden über eine CA-Anerkennungsliste verwaltet.

Vor dem Definieren einer CA-Anerkennungsliste für eine Anwendung müssen die folgenden Bedingungen erfüllt sein:

- Die Anwendung muss die Verwendung von Zertifikaten für die Client-Authentifizierung unterstützen.
- In der Definition der Anwendung muss angegeben sein, dass sie mit einer CA-Anerkennungsliste arbeitet.

Wenn in der Anwendungsdefinition angegeben ist, dass die Anwendung eine CA-Anerkennungsliste benutzt, müssen Sie diese Liste definieren, damit die Anwendung die Client-Authentifizierung mit Zertifikaten erfolgreich ausführen kann. Hierdurch wird sichergestellt, dass von der Anwendung nur die Zertifikate von Zertifizierungsinstanzen überprüft werden können, die Sie als anerkannt definiert haben. Wenn Benutzer oder eine Client-Anwendung ein Zertifikat einer Zertifizierungsinstanz vorlegen, die in der CA-Anerkennungsliste nicht als anerkannt definiert wurde, wird das Zertifikat bei der Authentifizierung als ungültig zurückgewiesen.

Wenn Sie der Anerkennungsliste für eine Anwendung eine Zertifizierungsinstanz hinzufügen, müssen Sie sicherstellen, dass diese CA auch aktiviert ist.

So definieren Sie eine CA-Anerkennungsliste für eine Anwendung:

1. Starten Sie Digital Certificate Manager.
2. Klicken Sie auf **Zertifikatsspeicher auswählen**, und wählen Sie anschließend als zu öffnenden Zertifikatsspeicher **\*SYSTEM** aus.

**Anmerkung:** Wenn Sie Fragen zum Ausfüllen eines bestimmten Formulars in dieser geführten Task haben, wählen Sie die Schaltfläche mit dem Fragezeichen (?) oben auf der Seite aus, um auf die Onlinehilfe zuzugreifen.

3. Geben Sie auf der Zertifikatsspeicher- und Kennwortseite das Kennwort ein, das Sie bei der Erstellung des Zertifikatsspeichers angegeben haben, und klicken Sie dann auf **Weiter**.
4. Wählen Sie im Navigationsrahmen **Anwendungen verwalten** aus, um eine Liste mit Tasks anzuzeigen.
5. Wählen Sie in der Task-Liste **Anerkennungsliste der Zertifizierungsinstanz definieren** aus.
6. Wählen Sie den Anwendungstyp (Server oder Client) aus, für den die Liste definiert werden soll, und klicken Sie anschließend auf **Weiter**.
7. Wählen Sie in der Liste eine Anwendung aus, und klicken Sie anschließend auf **Weiter**, um eine Liste der CA-Zertifikate anzuzeigen, die zum Definieren der Anerkennungsliste benutzt werden.
8. Wählen Sie die Zertifizierungsinstanzen aus, die die Anwendung anerkennen soll, und klicken Sie dann auf **OK**. Daraufhin zeigt DCM eine Nachricht an, um die Auswahl für die Anerkennungsliste zu bestätigen.

**Anmerkung:** Sie können in der Liste entweder einzelne Zertifizierungsinstanzen auswählen oder angeben, dass die Anwendung alle oder keine der in der Liste enthaltenen CAs anerkennen soll. Darüber hinaus können Sie die CA-Zertifikate auch anzeigen oder überprüfen, bevor Sie zur Anerkennungsliste hinzugefügt werden.

## Zertifikate nach Verfallsdatum verwalten

Digital Certificate Manager (DCM) stellt Unterstützungsfunktionen bereit, mit deren Hilfe Sie die Informationen zum Verfallsdatum von Zertifikaten verwalten können. Auf diese Weise können Administratoren Server-, Client-, Objektsignier- und Benutzerzertifikate auf dem lokalen System auf der Basis des Verfallsdatums verwalten.

**Anmerkung:** Wenn Sie DCM so konfigurieren, dass mit EIM (Enterprise Identity Mapping) gearbeitet wird, können Sie Benutzerzertifikate nach Verfallsdatum verwalten, und zwar unternehmensweit.

Wenn Sie DCM zum Anzeigen von Zertifikaten auf der Basis ihres Verfallsdatums verwenden, können Sie schnell und einfach feststellen, bei welchen Zertifikaten das Verfallsdatum unmittelbar bevorsteht. Die betroffenen Zertifikate können dann rechtzeitig verlängert werden.

**Anmerkung:** Da Sie zur Überprüfung der Objektsignaturen auch dann ein Signaturüberprüfungszertifikat verwenden können, wenn das Zertifikat abgelaufen ist, stellt DCM keine Unterstützung für die Überprüfung des Verfallsdatums dieser Zertifikate zur Verfügung.

So können Sie Server-, Client- oder Objektsignierzertifikate auf der Basis des Verfallsdatums anzeigen und verwalten:

1. Starten Sie Digital Certificate Manager.
2. Klicken Sie im Navigationsrahmen auf **Zertifikatsspeicher auswählen**, und wählen Sie anschließend als zu öffnenden Zertifikatsspeicher **\*OBJECTSIGNING** oder **\*SYSTEM** aus.

**Anmerkung:** Wenn Sie beim Einsatz von DCM Fragen zum Ausfüllen eines bestimmten Formulars haben, wählen Sie die Schaltfläche mit dem Fragezeichen (?) oben auf der Seite aus, um auf die Onlinehilfe zuzugreifen.

3. Geben Sie das Kennwort für den Zertifikatsspeicher ein, und klicken Sie anschließend auf **Weiter**.
4. Nach der Aktualisierung des Navigationsrahmens wählen Sie **Zertifikate verwalten** aus, um eine Liste mit Tasks anzuzeigen.
5. Wählen Sie in der Task-Liste **Verfallsdatum prüfen** aus.
6. Wählen Sie den Typ des Zertifikats aus, das geprüft werden soll. Wenn Sie im Zertifikatsspeicher \*SYSTEM arbeiten, wählen Sie den **Server oder Client** aus. Wenn Sie hingegen im Zertifikatsspeicher \*OBJECTSIGNING arbeiten, müssen Sie **Objektsignierung** auswählen.
7. Geben Sie im Feld **Bereich für Verfallsdatum in Tagen (1 - 365)** die Anzahl der Tage in dem Bereich ein, in dem Zertifikate auf der Basis ihres Verfallsdatums angezeigt werden sollen, und klicken Sie dann auf **Weiter**. Digital Certificate Manager (DCM) zeigt alle Zertifikate an, die zwischen dem aktuellen Datum und dem Datum ablaufen, das mit der angegebenen Anzahl von Tagen übereinstimmt. Darüber hinaus zeigt DCM alle Zertifikate an, deren Verfallsdatum vor dem aktuellen Datum liegt.
8. Wählen Sie ein Zertifikat aus, das verwaltet werden soll. Sie können nun die Detailinformationen zum Zertifikat anzeigen, das Zertifikat löschen oder verlängern.
9. Klicken Sie nach Abschluss aller Operationen für die gewünschten Zertifikate auf **Abbrechen**, um die Verarbeitung zu beenden.

## Zertifikate und Anwendungen überprüfen

Digital Certificate Manager (DCM) kann zum Überprüfen individueller Zertifikate oder der Anwendungen benutzt werden, die diese Zertifikate verwenden. Die Liste der von DCM geprüften Kriterien kann abhängig davon, ob Zertifikate oder Anwendungen geprüft werden, leicht variieren.

### Gültigkeitsprüfung für Anwendungen

Das Überprüfen einer Anwendungsdefinition mit DCM trägt zur Vermeidung von Zertifikatsproblemen bei Anwendungen bei, wenn diese eine Funktion ausführen, für die Zertifikate benötigt werden. Solche Probleme können dazu führen, dass die betroffene Anwendung entweder nicht an einer SSL-Sitzung (SSL = Secure Sockets Layer) teilnehmen oder keine Objektsignaturen ausstellen kann.

Beim Überprüfen einer Anwendung stellt DCM fest, ob eine Zertifikatszuordnung für die Anwendung definiert wurde und ob dieses Zertifikat gültig ist. Darüber hinaus stellt DCM sicher, dass bei Anwendungen, die für die Verwendung einer CA-Anerkennungsliste konfiguriert wurden, diese Anerkennungsliste mindestens ein Zertifikat der Zertifizierungsinstanz enthält. Anschließend prüft DCM, ob die Zertifikate der Zertifizierungsinstanz in der CA-Anerkennungsliste der Anwendung gültig sind. Wenn in der Anwendungsdefinition angegeben ist, dass die CRL-Verarbeitung ausgeführt wird und dass ein definierter CRL-Verteilungspunkt für die Zertifizierungsinstanz (CA) definiert ist, überprüft DCM darüber hinaus im Rahmen des Überprüfungsprozesses auch die Liste der entzogenen Zertifikate (CRL).

### Gültigkeitsprüfung für Zertifikate

Beim Überprüfen eines Zertifikats prüft Digital Certificate Manager (DCM) eine Reihe von Kriterien, um die Authentizität und Gültigkeit des Zertifikats sicherzustellen. Die Überprüfung eines Zertifikats gewährleistet, dass die Wahrscheinlichkeit, dass Anwendungen, die das Zertifikat für die gesicherte Kommunikation oder zum Signieren von Objekten verwenden, bei dessen Einsatz auf Probleme stoßen, auf ein Minimum reduziert werden kann.

Im Rahmen des Überprüfungsprozesses stellt DCM fest, ob das ausgewählte Zertifikat noch gültig ist. Ist für die ausstellende CA ein CRL-Verteilungspunkt vorhanden, wird außerdem geprüft, ob das Zertifikat in der Liste der entzogenen Zertifikate (CRL) nicht als widerrufen aufgeführt ist. DCM prüft auch, ob sich das Zertifikat der Zertifizierungsinstanz für die ausstellende CA im aktuellen Zertifikatsspeicher befindet und als aktiviert und anerkannt markiert ist. Wenn für das Zertifikat ein privater Schlüssel definiert wurde (z. B. für Server-, Client- oder Objektsignierzertifikate), prüft DCM auch das

öffentliche/private Schlüsselpaar, um sicherzustellen, dass dieses übereinstimmt. DCM verschlüsselt hierzu die Daten mit dem öffentlichen Schlüssel und prüft dann, ob die Daten mit dem privaten Schlüssel wieder entschlüsselt werden können.

### **Zugehörige Konzepte**

„CRL-Verteilungspunkte“ auf Seite 7

Bei einer Liste der entzogenen Zertifikate (CRL = Certificate Revocation List) handelt es sich um eine Datei, in der alle ungültigen und widerrufenen Zertifikate einer bestimmten Zertifizierungsinstanz (CA) aufgeführt sind.

„Gültigkeitsprüfung“ auf Seite 12

Digital Certificate Manager (DCM) stellt Tasks zur Verfügung, mit deren Hilfe Sie ein Zertifikat oder eine Anwendung überprüfen und dadurch feststellen können, ob eine Reihe von erforderlichen Eigenschaften erfüllt ist.

## **Anwendungen ein Zertifikat zuordnen**

Digital Certificate Manager (DCM) ermöglicht Ihnen die schnelle und einfache Zuordnung eines Zertifikats zu mehreren Anwendungen. Das Zuordnen eines Zertifikats zu mehreren Anwendungen ist nur im Zertifikatsspeicher \*SYSTEM oder \*OBJECTSIGNING möglich.

So können Sie eine Zertifikatszuordnung zu einer oder mehreren Anwendungen durchführen:

1. Starten Sie Digital Certificate Manager.
2. Klicken Sie im Navigationsrahmen auf **Zertifikatsspeicher auswählen**, und wählen Sie anschließend als zu öffnenden Zertifikatsspeicher **\*OBJECTSIGNING** oder **\*SYSTEM** aus.

**Anmerkung:** Wenn Sie beim Einsatz von DCM Fragen zum Ausfüllen eines bestimmten Formulars haben, wählen Sie die Schaltfläche mit dem Fragezeichen (?) oben auf der Seite aus, um auf die Onlinehilfe zuzugreifen.

3. Geben Sie das Kennwort für den Zertifikatsspeicher ein, und klicken Sie anschließend auf **Weiter**.
4. Nach der Aktualisierung des Navigationsrahmens wählen Sie **Zertifikate verwalten** aus, um eine Liste mit Tasks anzuzeigen.
5. Wählen Sie in der Task-Liste **Zertifikat zuordnen** aus, um eine Liste mit Zertifikaten im aktuellen Zertifikatsspeicher anzuzeigen.
6. Wählen Sie ein Zertifikat in der Liste aus, und klicken Sie anschließend auf **Anwendungen zuordnen**, um eine Liste der Anwendungsdefinitionen für den aktuellen Zertifikatsspeicher anzuzeigen.
7. Wählen Sie in der Liste eine oder mehrere Anwendungen aus, und klicken Sie dann auf **Weiter**. Daraufhin wird eine Seite aufgerufen, in der entweder eine Bestätigungsnachricht für die Zuordnungsauswahl oder eine Fehlernachricht angezeigt wird, wenn bei der Ausführung des Arbeitsschrittes ein Fehler aufgetreten ist.

## **CRL-Verteilungspunkte verwalten**

Digital Certificate Manager (DCM) ermöglicht Ihnen das Definieren und Verwalten der Informationen zu den CRL-Verteilungspunkten (CRL = Certificate Revocation List; Liste der entzogenen Zertifikate), die von einer Zertifizierungsinstanz (CA) bei der Gültigkeitsprüfung von Zertifikaten verwendet werden.

DCM oder eine andere Anwendung, die CRL-Informationen verarbeitet, kann mit Hilfe der Liste der entzogenen Zertifikate feststellen, ob die ausstellende CA das verwendete Zertifikat nicht widerrufen hat. Wenn Sie einen CRL-Verteilungspunkt für eine Zertifizierungsinstanz definieren, können Anwendungen, die die Verwendung von Zertifikaten für die Client-Authentifizierung unterstützen, auf die Liste der entzogenen Zertifikate (CRL) zugreifen.

Darüber hinaus können Anwendungen, die die Verwendung von Zertifikaten für die Client-Authentifizierung unterstützen, die CRL-Verarbeitung ausführen, um strengere Authentifizierungskriterien für die Zertifikate anzulegen, die als gültige Identitätsnachweise akzeptiert werden. Damit eine Anwendung bei der

Gültigkeitsprüfung von Zertifikaten eine definierte Liste der entzogenen Zertifikate benutzen kann, muss in der DCM-Anwendungsdefinition die Ausführung der CRL-Verarbeitung als erforderlich festgelegt werden.

## Funktionsweise der CRL-Verarbeitung

Wenn Sie mit DCM ein Zertifikat oder eine Anwendung überprüfen, wird die CRL-Verarbeitung standardmäßig im Rahmen des Prüfprozesses ausgeführt. Wenn für die Zertifizierungsinstanz, die das zu prüfende Zertifikat ausgestellt hat, kein CRL-Verteilungspunkt definiert wurde, kann die CRL-Prüfung von DCM nicht ausgeführt werden. DCM kann jedoch versuchen, andere wichtige Informationen zum Zertifikat zu überprüfen. Hierbei wird z. B. festgestellt, ob die CA-Signatur auf dem Zertifikat gültig und die ausstellende Zertifizierungsinstanz anerkannt ist.

## CRL-Verteilungspunkt definieren

So definieren Sie einen CRL-Verteilungspunkt für eine bestimmte Zertifizierungsinstanz:

1. Starten Sie Digital Certificate Manager.
2. Wählen Sie im Navigationsrahmen **CRL-Verteilungspunkte verwalten** aus, um eine Liste mit Tasks anzuzeigen.

**Anmerkung:** Wenn Sie Fragen zum Ausfüllen eines bestimmten Formulars in dieser geführten Task haben, wählen Sie die Schaltfläche mit dem Fragezeichen (?) oben auf der Seite aus, um auf die Onlinehilfe zuzugreifen.

3. Wählen Sie in der Task-Liste **CRL-Verteilungspunkt hinzufügen** aus, um ein Formular anzuzeigen, in dem Sie den CRL-Verteilungspunkt und die Art und Weise beschreiben können, in der DCM oder die Anwendung auf den Verteilungspunkt zugreifen soll.
4. Füllen Sie das Formular aus, und klicken Sie anschließend auf **OK**. Sie müssen dem CRL-Verteilungspunkt einen eindeutigen Namen zuordnen, den LDAP-Server, der als Host-Einheit für die CRL dient, sowie Verbindungsinformationen angeben, die definieren, wie auf den LDAP-Server zugegriffen werden kann. Nun muss die Definition des CRL-Verteilungspunktes einer bestimmten Zertifizierungsinstanz zugeordnet werden.
5. Wählen Sie im Navigationsrahmen **Zertifikate verwalten** aus, um eine Liste mit Tasks anzuzeigen.
6. Wählen Sie in der Task-Liste den Eintrag **CRL-Verteilungspunkt neu zuordnen** aus, um eine Liste der CA-Zertifikate anzuzeigen.
7. Wählen Sie in der Liste das CA-Zertifikat aus, dem die erstellte Definition des CRL-Verteilungspunktes zugeordnet werden soll, und klicken Sie anschließend auf **CRL-Verteilungspunkt neu zuordnen**. Daraufhin wird eine Liste mit CRL-Verteilungspunkten angezeigt.
8. Wählen Sie in der Liste den CRL-Verteilungspunkt aus, der der Zertifizierungsinstanz zugeordnet werden soll, und klicken Sie dann auf **Neu zuordnen**. Daraufhin wird oben in der Seite eine Nachricht angezeigt, um Sie darüber zu informieren, dass der CRL-Verteilungspunkt dem Zertifikat der Zertifizierungsinstanz (CA) zugeordnet wurde.

| **Anmerkung:** Um eine anonyme Bindung zu einem LDAP-Server für die CRL-Verarbeitung herzustellen,  
| müssen Sie das Directory-Server-Webverwaltungstool verwenden und dort die Task  
| "Schemadateien verwalten" auswählen, um die Sicherheitsklasse (Zugriffsklasse) der Attri-  
| bute certificateRevocationList und authorityRevocationList von "kritisch" in "normal" zu  
| ändern und sowohl das Feld **Anmelde-DN** als auch das Feld **Kennwort** leer zu lassen.

Nach dem Definieren eines CRL-Verteilungspunktes für eine bestimmte Zertifizierungsinstanz können DCM oder andere Anwendungen diesen zur Ausführung der CRL-Verarbeitung benutzen. Bevor die CRL-Verarbeitung jedoch funktioniert, muss die entsprechende Liste der entzogenen Zertifikate auf dem Directory Services-Server gespeichert werden. Darüber hinaus müssen Sie sowohl für den Directory-Server (LDAP) als auch für die Client-Anwendungen die Benutzung von SSL konfigurieren und den Anwendungen in DCM ein Zertifikat zuordnen.



### **Zugehörige Konzepte**

„CRL-Verteilungspunkte“ auf Seite 7

Bei einer Liste der entzogenen Zertifikate (CRL = Certificate Revocation List) handelt es sich um eine Datei, in der alle ungültigen und widerrufenen Zertifikate einer bestimmten Zertifizierungsinstanz (CA) aufgeführt sind.

### **Zugehörige Informationen**

IBM Directory Server for iSeries (LDAP)

Enable SSL on the Directory Server

## **Zertifikatsschlüssel auf einem IBM Verschlüsselungskoprozessor speichern**

Dieses Thema enthält Informationen zum Einsatz eines installierten Koprozessors zur Verbesserung der Sicherheit der gespeicherten privaten Schlüssel Ihrer Zertifikate.

Wenn ein IBM Verschlüsselungskoprozessor (siehe hierzu IBM Cryptographic Coprocessor) auf Ihrem System installiert ist, können Sie diesen einsetzen, um die Sicherheit beim Speichern der privaten Zertifikatsschlüssel zu verbessern. Sie können den Koprozessor zum Speichern des privaten Schlüssels eines Server-, Client- oder CA-Zertifikats der lokalen Zertifizierungsinstanz verwenden. Der Koprozessor kann allerdings nicht zum Speichern des privaten Schlüssels eines Benutzerzertifikats eingesetzt werden, da dieser Schlüssel auf dem System des jeweiligen Benutzers gespeichert werden muss. Auch zum Speichern des privaten Schlüssels für ein Objektsignierzertifikat kann er nicht benutzt werden.

Bei der Speicherung des privaten Zertifikatsschlüssels kann der Koprozessor auf die beiden folgenden Arten eingesetzt werden:

- Direktes Speichern des privaten Zertifikatsschlüssels auf dem Koprozessor selbst.
- Verschlüsseln des privaten Zertifikatsschlüssels mit dem Hauptschlüssel des Koprozessors und anschließende Speicherung in einer speziellen Schlüsseldatei.

Diese beiden Auswahlmöglichkeiten für die Speicherung des Schlüssels können während der Erstellung oder Verlängerung eines Zertifikats ausgewählt werden. Wenn Sie den Koprozessor zum Speichern eines privaten Zertifikatsschlüssels verwenden, können Sie die Einheitszuordnung des Koprozessors für diesen Schlüssel ändern.

Wenn Sie den Koprozessor zur Speicherung von privaten Schlüsseln verwenden wollen, müssen Sie sicherstellen, dass der Koprozessor vor dem Einsatz von Digital Certificate Manager (DCM) aktiviert wird. Andernfalls wird in DCM bei der Erstellung oder Verlängerung von Zertifikaten keine Seite angezeigt, auf der Sie eine Auswahl für die Speicherung angeben können.

Beim Erstellen oder Verlängern von Server- oder Client-Zertifikaten können Sie die Auswahl für die Speicherung des privaten Schlüssels nach der Auswahl des Typs der Zertifizierungsinstanz angeben, die das aktuelle Zertifikat signiert. Wenn Sie die Erstellung oder Verlängerung für eine lokale CA durchführen, geben Sie die Auswahl für die Speicherung des privaten Schlüssels als ersten Arbeitsschritt an.

### **Zugehörige Konzepte**

„IBM Verschlüsselungskoprozessoren für iSeries“ auf Seite 11

Dieser Verschlüsselungskoprozessor stellt bewährte kryptografische Services zur Gewährleistung der Vertraulichkeit und der Integrität bereit, die Ihnen das Entwickeln sicherer e-business Anwendungen ermöglichen.

## **Privaten Schlüssel eines Zertifikats direkt auf dem Koprozessor speichern**

Um die Sicherheit beim Zugriff auf private Zertifikatsschlüssel sowie bei deren Verwendung zu erhöhen, können Sie diese direkt auf dem IBM Verschlüsselungskoprozessor speichern. Diese Auswahl für die Speicherung der Schlüssel kann während der Erstellung oder Verlängerung von Zertifikaten in Digital Certificate Manager (DCM) ausgewählt werden.

So können Sie mit Hilfe der Seite **Speicherposition für Schlüssel auswählen** einen privaten Zertifikatschlüssel direkt auf dem Koprozessor speichern:

1. Geben Sie als Auswahl für die Speicherung **Hardware** an.
2. Klicken Sie auf **Weiter**. Daraufhin wird die Seite **Beschreibung für Verschlüsselungseinheit auswählen** angezeigt.
3. Wählen Sie in der Einheitenliste die Einheit aus, auf der der private Zertifikatsschlüssel gespeichert werden soll.
4. Klicken Sie auf **Weiter**. DCM zeigt weitere Seiten für die aktuelle Task an, in denen z. B. Informationen zur Identifikation des zu erstellenden oder zu verlängernden Zertifikats angegeben werden können.

### **Hauptschlüssel des Koprozessors zum Verschlüsseln des privaten Zertifikatschlüssels verwenden**

Um die Sicherheit beim Zugriff auf private Zertifikatsschlüssel sowie bei deren Verwendung zu erhöhen, können Sie den Hauptschlüssel des IBM Verschlüsselungskoprozessors verwenden, um diese zu verschlüsseln und in einer speziellen Schlüsseldatei zu speichern. Diese Auswahl für die Speicherung der Schlüssel kann während der Erstellung oder Verlängerung von Zertifikaten in Digital Certificate Manager (DCM) ausgewählt werden.

Bevor Sie mit dieser Auswahl arbeiten können, müssen Sie über die Webkonfigurationsschnittstelle des IBM Verschlüsselungskoprozessors (siehe hierzu IBM Cryptographic Coprocessor) eine entsprechende Schlüsselspeicherdatei erstellen. Außerdem müssen Sie über die Webkonfigurationsschnittstelle des Koprozessors die Schlüsselspeicherdatei der Einheitenbeschreibung des zu verwendenden Koprozessors zuordnen. Auf die Webkonfigurationsschnittstelle des Koprozessors kann über die iSeries-Task-Seite zugegriffen werden.

Wenn auf Ihrem System mehrere Koprozessoren installiert und aktiviert sind, können mehrere Einheiten den privaten Zertifikatsschlüssel gemeinsam benutzen. Damit Einheitenbeschreibungen einen privaten Schlüssel gemeinsam benutzen können, muss für alle Einheiten derselbe Hauptschlüssel definiert sein. Die Verteilung desselben Hauptschlüssels an mehrere Einheiten wird als *Klonen* bezeichnet. Durch die gemeinsame Benutzung des Schlüssels kann die SSL-Lastausgleichsfunktion (SSL = Secure Sockets Layer) benutzt werden, die zur Leistungssteigerung bei gesicherten Sitzungen beitragen kann.

So können Sie mit Hilfe der Seite **Speicherposition für Schlüssel auswählen** den Hauptschlüssel des Koprozessors zum Verschlüsseln von privaten Zertifikatsschlüsseln und zum Speichern der Schlüssel in einer speziellen Schlüsselspeicherdatei verwenden:

1. Geben Sie als Auswahl für die Speicherung **Hardwareverschlüsselt** an.
2. Klicken Sie auf **Weiter**. Daraufhin wird die Seite **Beschreibung für Verschlüsselungseinheit auswählen** angezeigt.
3. Wählen Sie in der Einheitenliste die Einheit aus, die zum Verschlüsseln des privaten Zertifikatsschlüssels verwendet werden soll.
4. Klicken Sie auf **Weiter**. Wenn auf Ihrem System mehrere Koprozessoren installiert und aktiviert sind, wird die Seite **Zusätzliche Beschreibungen für Verschlüsselungseinheiten auswählen** angezeigt.

**Anmerkung:** Andernfalls zeigt DCM weitere Seiten für die aktuelle Task an, in denen z. B. Informationen zur Identifikation des zu erstellenden oder zu verlängernden Zertifikats angegeben werden können.

5. Wählen Sie in der Einheitenliste den Namen einer oder mehrerer Einheitenbeschreibungen für die gemeinsame Benutzung des privaten Zertifikatsschlüssels aus.

**Anmerkung:** Die ausgewählten Einheitenbeschreibungen müssen über den gleichen Hauptschlüssel wie die Einheit verfügen, die auf der vorherigen Seite ausgewählt wurde. Um die Übereinstimmung des Hauptschlüssels auf den Einheiten zu überprüfen, verwenden Sie die Task zum Überprüfen des Hauptschlüssels in der Webkonfigurationsschnittstelle des

Verschlüsselungskoprozessor IBM 4758. Auf die Webkonfigurationsschnittstelle des Koprozessors kann über die iSeries-Task-Seite zugegriffen werden.

6. Klicken Sie auf **Weiter**. DCM zeigt weitere Seiten für die aktuelle Task an, in denen z. B. Informationen zur Identifikation des zu erstellenden oder zu verlängernden Zertifikats angegeben werden können.

## Anforderungsadresse für eine PKIX-Zertifizierungsinstanz verwalten

Eine PKIX-Zertifizierungsinstanz (PKIX = Public Key Infrastructure for X.509) ist eine CA, die Zertifikate auf der Basis der Richtlinien der neuesten X.509-Internet-Standards zur Implementierung einer PKI ausgibt.

Bei PKIX-Zertifizierungsinstanzen werden strengere Identifikationskriterien für die Ausstellung eines Zertifikats angelegt. Hierbei muss der Antragsteller seine Identität normalerweise über eine Registrierungsstelle (RA = Registration Authority) belegen. Nachdem der Antragsteller den von der Registrierungsstelle geforderten Identitätsnachweis erbracht hat, wird diese Identität durch die RA zertifiziert. Abhängig von den für die Zertifizierungsinstanz definierten Verfahren muss entweder die Registrierungsstelle oder der Antragsteller der CA den zertifizierten Antrag vorlegen. Da diese Standards immer häufiger verwendet werden, stehen auch immer mehr PKIX-konforme Zertifizierungsinstanzen zur Verfügung. Die Verwendung einer PKIX-konformen Zertifizierungsinstanz ist dann sinnvoll, wenn die Sicherheitsanforderungen Ihres Unternehmens eine strikte Zugriffssteuerung für Ressourcen erforderlich machen, die Ihren Benutzern über Anwendungen mit SSL-Unterstützung zur Verfügung stehen. Lotus Domino bietet z. B. eine solche PKIX-Zertifizierungsinstanz für die allgemeine Benutzung an.

Wenn Sie mit einer PKIX-Zertifizierungsinstanz Zertifikate für Ihre Anwendungen ausstellen wollen, können Sie diese Zertifikate mit Digital Certificate Manager (DCM) verwalten. Zu diesem Zweck definieren Sie mit DCM eine URL-Adresse für eine PKIX-Zertifizierungsinstanz. Durch das Festlegen dieser URL-Adresse wird Digital Certificate Manager (DCM) so konfiguriert, dass eine Auswahl für eine PKIX-Zertifizierungsinstanz (CA) für das Abrufen signierter Zertifikate bereitgestellt wird.

Wenn Sie DCM zum Verwalten von Zertifikaten einer PKIX-Zertifizierungsinstanz verwenden wollen, müssen Sie DCM so konfigurieren, dass auf die Position dieser CA zugegriffen werden kann. Führen Sie hierzu die folgenden Arbeitsschritte aus:

1. Starten Sie Digital Certificate Manager.
2. Wählen Sie im Navigationsrahmen **PKIX-Anforderungsadresse verwalten** aus, um ein Formular anzuzeigen, in dem Sie die URL-Adresse für die PKIX-Zertifizierungsinstanz und die zugehörige Registrierungsstelle angeben können.
3. Geben Sie die vollständig qualifizierte URL-Adresse für die PKIX-Zertifizierungsinstanz ein, die zum Anfordern eines Zertifikats verwendet werden soll (z. B. <http://www.thawte.com>), und klicken Sie anschließend auf **Hinzufügen**. Durch das Hinzufügen der URL-Adresse wird DCM so konfiguriert, dass eine Auswahl für eine PKIX-Zertifizierungsinstanz (CA) für das Abrufen signierter Zertifikate hinzugefügt wird.

Nach dem Hinzufügen einer Anforderungsadresse für eine PKIX-Zertifizierungsinstanz fügt DCM eine Auswahl für eine PKIX-CA zu den verschiedenen Zertifizierungsinstanzen hinzu, die bei Verwendung der Task **Zertifikat erstellen** zum Ausstellen eines Zertifikats angegeben werden können.

**Anmerkung:** Die PKIX-Standards werden im Request For Comments (RFC) 2560 erläutert.

### Zugehörige Konzepte

„Zertifikate einer öffentlichen Internet-Zertifizierungsinstanz verwalten“ auf Seite 56

In diesem Abschnitt erfahren Sie, wie Sie Zertifikate einer öffentlichen Internet-Zertifizierungsinstanz verwalten können, indem Sie einen Zertifikatsspeicher erstellen.

## LDAP-Position für Benutzerzertifikate verwalten

Dieses Thema enthält Informationen zum Konfigurieren von DCM für die Speicherung von Benutzerzertifikaten unter einer Verzeichnisposition auf einem LDAP-Server (Lightweight Directory Access Protocol), so dass EIM (Enterprise Identity Mapping) auch für Benutzerzertifikate eingesetzt werden kann.

Standardmäßig speichert Digital Certificate Manager (DCM) die Benutzerzertifikate, die von der lokalen Zertifizierungsinstanz (CA) ausgestellt werden, zusammen mit den i5/OS-Benutzerprofilen. Sie können Digital Certificate Manager (DCM) zusammen mit EIM (Enterprise Identity Mapping) so konfigurieren, dass bei der Ausstellung von Benutzerzertifikaten durch die lokale Zertifizierungsinstanz (CA) die öffentliche Kopie des Zertifikats unter einer Verzeichnisposition des LDAP-Servers (LDAP = Lightweight Directory Access Protocol) gespeichert wird. Wenn Sie EIM und DCM gemeinsam konfigurieren, können Sie Benutzerzertifikate unter einer LDAP-Verzeichnisposition speichern, um die Zertifikate anderen Anwendungen einfacher zur Verfügung zu stellen. Durch diese kombinierte Konfiguration ist es außerdem möglich, EIM zur Verwaltung von Benutzerzertifikaten als Benutzeridentität innerhalb des Unternehmens einzusetzen.

**Anmerkung:** Wenn ein Benutzer ein Zertifikat einer anderen CA an der LDAP-Position speichern soll, muss dieser die Task **Benutzerzertifikat zuordnen** ausführen.

Bei EIM handelt es sich um eine **@server**-Technologie, mit der die Benutzeridentitäten Ihres Unternehmens einschließlich der i5/OS-Benutzerprofile und der zugehörigen Benutzerzertifikate verwaltet werden können. Wenn Sie EIM zur Verwaltung von Benutzerzertifikaten verwenden wollen, müssen Sie vor der Ausführung der erforderlichen DCM-Konfigurations-Tasks die folgenden EIM-Konfigurations-Tasks ausführen:

1. Verwenden Sie zur Konfiguration von EIM den **EIM-Konfigurationsassistenten** im iSeries Navigator.
2. Erstellen Sie das X.509-Register in der EIM-Domäne, das für Zertifikatszuordnungen verwendet werden soll.
3. Verwenden Sie die Menüauswahl "Eigenschaften für den Konfigurationsordner" in der EIM-Domäne, und geben Sie dann den Namen des X.509-Registers ein.
4. Erstellen Sie eine EIM-Kennung für alle Benutzer, die EIM nutzen sollen.
5. Erstellen Sie im lokalen i5/OS-Benutzerregister eine Zielzuordnung zwischen den einzelnen EIM-Kennungen und den Benutzerprofilen der Benutzer. Verwenden Sie den EIM-Registerdefinitionsnamen des lokalen i5/OS-Benutzerregisters, das im **EIM-Konfigurationsassistenten** angegeben wurde.

**Anmerkung:** Weitere Informationen zum Konfigurieren von EIM finden Sie im Abschnitt Enterprise Identity Mapping im iSeries Information Center.

Nach Abschluss der erforderlichen EIM-Konfigurations-Tasks müssen Sie die folgenden Tasks ausführen, um die Konfigurationsmaßnahmen für den gemeinsamen Einsatz von EIM und DCM abzuschließen:

1. Verwenden Sie in DCM die Task **LDAP-Position verwalten**, um das LDAP-Verzeichnis anzugeben, das von DCM zum Speichern eines Benutzerzertifikats verwendet werden soll, das die lokale Zertifizierungsinstanz (CA) erstellt. Die LDAP-Position muss sich nicht auf dem lokalen iSeries-System befinden, und es ist auch nicht erforderlich, dass diese sich auf demselben LDAP-Server befindet, der auch von EIM verwendet wird. Bei der Konfiguration der LDAP-Position in DCM verwendet DCM das angegebene LDAP-Verzeichnis, um alle von der lokalen Zertifizierungsinstanz (CA) ausgestellten Benutzerzertifikate zu speichern. DCM verwendet die LDAP-Position außerdem zum Speichern der Benutzerzertifikate, die mit der Task **Benutzerzertifikat zuordnen** verarbeitet wurden. Diese werden normalerweise zusammen mit einem Benutzerprofil gespeichert.
2. Führen Sie den Befehl CVTUSRCERT (**Benutzerzertifikate konvertieren**) aus. Dieser Befehl dient zum Kopieren vorhandener Benutzerzertifikate an die gewünschte LDAP-Verzeichnisposition. Der Befehl kopiert allerdings nur die Zertifikate von Benutzern, für die eine Zielzuordnung zwischen einer EIM-Kennung und dem entsprechenden Benutzerprofil vorhanden ist. Der Befehl erstellt dann eine Quellenzuordnung zwischen den einzelnen Zertifikaten und der jeweils zugehörigen EIM-Kennung. Der Befehl verwendet den registrierten Subjektnamen (DN) des Zertifikats, den DN des Ausstellers

und einen Hash-Code dieser DNs sowie den öffentlichen Zertifikatsschlüssel, um den Namen der Benutzeridentität für die Quellenzuordnung zu definieren.

- | **Anmerkung:** Um eine anonyme Bindung zu einem LDAP-Server für die CRL-Verarbeitung herzustellen,  
| müssen Sie das Directory-Server-Webverwaltungstool verwenden und dort die Task  
| "Schemadateien verwalten" auswählen, um die Sicherheitsklasse (Zugriffsklasse) der Attri-  
| bute certificateRevocationList und authorityRevocationList von "kritisch" in "normal" zu  
| ändern und sowohl das Feld **Anmelde-DN** als auch das Feld **Kennwort** leer zu lassen.

#### Zugehörige Tasks

„Digitale Zertifikate und Enterprise Identity Mapping“ auf Seite 40

Durch den gemeinsamen Einsatz von Enterprise Identity Mapping (EIM) und Digital Certificate Manager (DCM) können Sie ein Zertifikat als Quellenelement einer EIM-Abgleichsuchoperation verwenden, um eine Zuordnung zwischen dem Zertifikat und einer Zielbenutzeridentität herzustellen, die derselben EIM-Kennung zugeordnet ist.

## Objekte signieren

Dieses Thema enthält Informationen zum Einsatz von DCM für die Verwaltung von Zertifikaten, die zum digitalen Signieren von Objekten verwendet werden, um die Integrität dieser Objekte zu gewährleisten.

Zum Signieren von Objekten gibt es drei Methoden. Sie können ein Programm zum Aufrufen der API für das Signieren von Objekten (siehe hierzu Sign Object API) schreiben oder Digital Certificate Manager (DCM) zum Signieren von Objekten verwenden (siehe hierzu Digital Certificate Manager (DCM) to sign objects). Ab OS/400 V5R2 können Sie die Management Central-Funktion zum Signieren von Objekten verwenden (siehe hierzu Management Central feature to sign objects), wenn diese zur Verteilung auf andere Systeme gepackt werden. Diese Funktion steht im iSeries Navigator zur Verfügung.

Sie können die mit DCM verwalteten Zertifikate zum Signieren aller Objekte benutzen, die im integrierten Dateisystem (IFS) Ihres Computers gespeichert sind. Eine Ausnahme bilden hierbei allerdings Objekte, die in einer Bibliothek gespeichert sind. Nur die Objekte, die im QSYS.LIB-Dateisystem gespeichert sind, können signiert werden. Hierzu gehören die \*PGM-, \*SRVPGM-, \*MODULE-, \*SQLPKG- sowie die \*FILE-Komponenten (nur Sicherungsdatei). Ab OS/400 V5R2 besteht auch die Möglichkeit, Befehlsobjekte (\*CMD) zu signieren. Auf anderen Systemen gespeicherte Objekte können nicht signiert werden.

Sie können Objekte mit Zertifikaten signieren, die Sie von einer öffentlichen Internet-Zertifizierungsinstanz (CA) gekauft oder selbst mit einer privaten lokalen Zertifizierungsinstanz in DCM erstellt haben. Der Signierzertifikatsprozess ist unabhängig davon, ob Sie öffentliche oder private Zertifikate verwenden, identisch.

### Voraussetzungen für das Signieren von Objekten

Bevor Sie mit DCM (oder der API zum Signieren von Objekten) Objekte signieren können, müssen Sie sicherstellen, dass bestimmte Voraussetzungen erfüllt sind:

- Der Zertifikatsspeicher \*OBJECTSIGNING muss entweder beim Erstellen einer lokalen Zertifizierungsinstanz oder beim Verwalten von Objektsignierzertifikaten einer öffentlichen Internet-Zertifizierungsinstanz erstellt worden sein.
- Der Zertifikatsspeicher \*OBJECTSIGNING muss mindestens ein Zertifikat enthalten. Hierbei kann es sich um ein mit der lokalen Zertifizierungsinstanz selbst erstelltes Zertifikat oder um ein Zertifikat einer öffentlichen Internet-Zertifizierungsinstanz handeln.
- Sie müssen eine Definition für eine Objektsignieranwendung erstellt haben, die zum Signieren von Objekten verwendet werden kann.
- Sie müssen der Objektsignieranwendung ein bestimmtes Zertifikat zugeordnet haben, das zum Signieren von Objekten eingesetzt werden soll.

## DCM zum Signieren von Objekten verwenden

So können Sie DCM zum Signieren eines oder mehrerer Objekte verwenden:

1. Starten Sie Digital Certificate Manager.
2. Klicken Sie im Navigationsrahmen auf **Zertifikatsspeicher auswählen**, und wählen Sie anschließend als zu öffnenden Zertifikatsspeicher **\*OBJECTSIGNING** aus.

**Anmerkung:** Wenn Sie beim Einsatz von DCM Fragen zum Ausfüllen eines bestimmten Formulars haben, wählen Sie die Schaltfläche mit dem Fragezeichen (?) oben auf der Seite aus, um auf die Onlinehilfe zuzugreifen.

3. Geben Sie das Kennwort für den Zertifikatsspeicher **\*OBJECTSIGNING** ein, und klicken Sie anschließend auf **Weiter**.
4. Nach der Aktualisierung des Navigationsrahmens wählen Sie **Signierbare Objekte verwalten** aus, um eine Liste mit Tasks anzuzeigen.
5. Wählen Sie in der Task-Liste den Eintrag **Objekt signieren** aus, um eine Liste mit Anwendungsdefinitionen anzuzeigen, die zum Signieren von Objekten eingesetzt werden können.
6. Wählen Sie eine Anwendung aus, und klicken Sie dann auf **Objekt signieren**, um ein Formular zur Angabe der Position der zu signierenden Objekte anzuzeigen.

**Anmerkung:** Wenn der ausgewählten Anwendung kein Zertifikat zugeordnet ist, kann es nicht zum Signieren eines Objekts verwendet werden. Sie müssen zuerst die Task **Zertifikat neu zuordnen** unter **Anwendungen verwalten** verwenden, um der Anwendungsdefinition ein Zertifikat zuzuordnen.

7. Geben Sie im entsprechenden Feld den vollständig qualifizierten Pfad und Dateinamen des Objekts oder Objektverzeichnis ein, das signiert werden soll, und klicken Sie anschließend auf **Weiter**. Alternativ hierzu können Sie auch eine Verzeichnisposition eingeben und auf **Durchsuchen** klicken, um den Verzeichnisisinhalt anzuzeigen und die zu signierenden Objekte auszuwählen.

**Anmerkung:** Sie müssen den Objektnamen mit einem führenden Schrägstrich beginnen, da andernfalls ein Fehler ausgegeben wird. Darüber hinaus können bestimmte Platzhalterzeichen verwendet werden, um die Verzeichniskomponente zu beschreiben, die signiert werden soll. Diese Platzhalterzeichen sind der Stern (\*), der zur Angabe einer beliebigen Anzahl von Zeichen dient, sowie das Fragezeichen (?), das für ein beliebiges einzelnes Zeichen steht. Beispiel: Um alle Objekte in einem bestimmten Verzeichnis zu signieren, können Sie die Zeichenfolge `/mydirectory/*` eingeben. Um alle Programme in einer bestimmten Bibliothek zu signieren, geben Sie z. B. die Zeichenfolge `/QSYS.LIB/QGPL.LIB/*.PGM` ein. Sie können diese Platzhalterzeichen nur im letzten Teil des Pfadnamens angeben. Bei Angabe an einer anderen Position, z. B. bei `/mydirectory*/filename`, erhalten Sie hingegen eine Fehlermeldung. Wenn Sie die Funktion "Durchsuchen" zum Anzeigen einer Liste mit dem Inhalt von Bibliotheken und Verzeichnissen verwenden wollen, muss das Platzhalterzeichen im Pfadnamen angegeben werden, bevor Sie auf **Durchsuchen** klicken.

8. Geben Sie die zum Signieren der ausgewählten Objekte zu verwendenden Auswahlmöglichkeiten für die Verarbeitung an, und klicken Sie anschließend auf **Weiter**.

**Anmerkung:** Wenn Sie die Jobergebnisse sofort prüfen wollen, kann die Ergebnisdatei direkt im Browser angezeigt werden. Die Ergebnisse für den aktuellen Job werden am Ende der Ergebnisdatei angefügt. Die Datei kann also zusätzlich zu den aktuellen Jobergebnissen auch Ergebnisse zuvor ausgeführter Jobs enthalten. Mit Hilfe des Datumfeldes in der Datei können Sie feststellen, welche Zeilen innerhalb der Datei sich auf den aktuellen Job beziehen. Das Datumfeld wird im Format `JJJJMMTT` angegeben. Im ersten Feld der

Datei wird entweder die Nachrichten-ID angegeben (wenn während der Verarbeitung des Objekts ein Fehler aufgetreten ist) oder das Datum angezeigt, zu dem der Job verarbeitet wurde.

9. Geben Sie den vollständig qualifizierten Pfad und Dateinamen an, der für das Speichern der Ergebnisse der Objektsignierjobs verwendet werden soll, und klicken Sie anschließend auf **Weiter**. Alternativ hierzu können Sie auch eine Verzeichnisposition eingeben und auf **Durchsuchen** klicken, um den Verzeichnisinhalt anzuzeigen und eine Datei zum Speichern der Jobergebnisse auszuwählen. Daraufhin wird eine Nachricht angezeigt, in der Sie darüber informiert werden, dass der Job zum Signieren von Objekten übergeben wurde. Die Jobergebnisse werden unter dem Job **QOBSGNBAT** im Jobprotokoll aufgeführt.

## Objektsignaturen prüfen

Sie können Digital Certificate Manager (DCM) verwenden, um die Authentizität digitaler Signaturen auf Objekten zu überprüfen. Durch das Prüfen der Signatur können Sie sicherstellen, dass die in dem Objekt enthaltenen Daten nicht geändert wurden, seit das Objekt vom Eigner signiert wurde.

### Voraussetzungen für die Signaturprüfung

Bevor Sie mit DCM Objektsignaturen prüfen können, müssen Sie sicherstellen, dass bestimmte Voraussetzungen erfüllt sind:

- Der Zertifikatsspeicher **\*SIGNATUREVERIFICATION** zum Verwalten der Signaturüberprüfungszertifikate muss erstellt worden sein.

**Anmerkung:** Sie können Signaturen prüfen, während Sie im Zertifikatsspeicher **\*OBJECTSIGNING** arbeiten. Dies gilt allerdings nur für die Prüfung von Signaturen auf Objekten, die im selben System signiert wurden. Die Arbeitsschritte, die hierbei in DCM ausgeführt werden müssen, sind in allen Zertifikatsspeichern identisch. Der Zertifikatsspeicher **\*SIGNATUREVERIFICATION** muss allerdings vorhanden sein und eine Kopie des Zertifikats enthalten, mit dem das Objekt signiert wurde. Dies gilt auch dann, wenn Sie die Signaturprüfung ausführen, während Sie im Zertifikatsspeicher **\*OBJECTSIGNING** arbeiten.

- Der Zertifikatsspeicher **\*SIGNATUREVERIFICATION** muss eine Kopie des Zertifikats enthalten, mit dem die Objekte signiert wurden.
- Der Zertifikatsspeicher **\*SIGNATUREVERIFICATION** muss außerdem eine Kopie des Zertifikats der Zertifizierungsinstanz enthalten, mit dem das für das Signieren der Objekte verwendete Zertifikat ausgestellt wurde.

### DCM zum Überprüfen von Objektsignaturen verwenden

So können Sie DCM zum Überprüfen von Objektsignaturen verwenden:

1. Starten Sie Digital Certificate Manager.
2. Klicken Sie im Navigationsrahmen auf **Zertifikatsspeicher auswählen**, und wählen Sie anschließend als zu öffnenden Zertifikatsspeicher **\*SIGNATUREVERIFICATION** aus.

**Anmerkung:** Wenn Sie beim Einsatz von DCM Fragen zum Ausfüllen eines bestimmten Formulars haben, wählen Sie die Schaltfläche mit dem Fragezeichen (?) oben auf der Seite aus, um auf die Onlinehilfe zuzugreifen.

3. Geben Sie das Kennwort für den Zertifikatsspeicher **\*SIGNATUREVERIFICATION** ein, und klicken Sie anschließend auf **Weiter**.
4. Nach der Aktualisierung des Navigationsrahmens wählen Sie **Signierbare Objekte verwalten** aus, um eine Liste mit Tasks anzuzeigen.
5. Wählen Sie in der Task-Liste **Objektsignatur überprüfen** aus, um die Position der Objekte anzugeben, deren Signaturen überprüft werden sollen.
6. Geben Sie im entsprechenden Feld den vollständig qualifizierten Pfad und Dateinamen des Objekts oder Objektverzeichnisses ein, dessen Signaturen überprüft werden sollen, und klicken Sie anschlie-

ßend auf **Weiter**. Alternativ hierzu können Sie auch eine Verzeichnisposition eingeben und auf **Durchsuchen** klicken, um den Verzeichnisisinhalt anzuzeigen und die Objekte auszuwählen, deren Signatur überprüft werden soll.

**Anmerkung:** Darüber hinaus können bestimmte Platzhalterzeichen verwendet werden, um die Verzeichniskomponente zu beschreiben, die überprüft werden soll. Diese Platzhalterzeichen sind der Stern (\*), der zur Angabe einer beliebigen Anzahl von Zeichen dient, sowie das Fragezeichen (?), das für ein beliebiges einzelnes Zeichen steht. Beispiel: Um alle Objekte in einem bestimmten Verzeichnis zu signieren, können Sie die Zeichenfolge /mydirectory/\* eingeben. Um alle Programme in einer bestimmten Bibliothek zu signieren, geben Sie z. B. die Zeichenfolge /QSYS.LIB/QGPL.LIB/\*.PGM ein. Sie können diese Platzhalterzeichen nur im letzten Teil des Pfadnamens angeben. Bei Angabe an einer anderen Position, z. B. bei /mydirectory\*/filename, erhalten Sie hingegen eine Fehlermeldung. Wenn Sie die Funktion "Durchsuchen" zum Anzeigen einer Liste mit dem Inhalt von Bibliotheken und Verzeichnissen verwenden wollen, muss das Platzhalterzeichen im Pfadnamen angegeben werden, bevor Sie auf **Durchsuchen** klicken.

7. Geben Sie die zum Überprüfen der Signatur der ausgewählten Objekte zu verwendenden Auswahlmöglichkeiten für die Verarbeitung an, und klicken Sie anschließend auf **Weiter**.

**Anmerkung:** Wenn Sie die Jobergebnisse sofort prüfen wollen, kann die Ergebnisdatei direkt im Browser angezeigt werden. Die Ergebnisse für den aktuellen Job werden am Ende der Ergebnisdatei angefügt. Die Datei kann also zusätzlich zu den aktuellen Jobergebnissen auch Ergebnisse zuvor ausgeführter Jobs enthalten. Mit Hilfe des Datumfeldes in der Datei können Sie feststellen, welche Zeilen innerhalb der Datei sich auf den aktuellen Job beziehen. Das Datumfeld wird im Format JJJJMMTT angegeben. Im ersten Feld der Datei wird entweder die Nachrichten-ID angegeben (wenn während der Verarbeitung des Objekts ein Fehler aufgetreten ist) oder das Datum angezeigt, zu dem der Job verarbeitet wurde.

8. Geben Sie den vollständig qualifizierten Pfad und Dateinamen an, der für das Speichern der Ergebnisse der Signaturüberprüfungsjobs verwendet werden soll, und klicken Sie anschließend auf **Weiter**. Alternativ hierzu können Sie auch eine Verzeichnisposition eingeben und auf **Durchsuchen** klicken, um den Verzeichnisisinhalt anzuzeigen und eine Datei zum Speichern der Jobergebnisse auszuwählen. Daraufhin wird eine Nachricht angezeigt, in der Sie darüber informiert werden, dass der Job zum Überprüfen von Objektsignaturen übergeben wurde. Die Jobergebnisse werden unter dem Job **QOBSJGNBAT** im Jobprotokoll aufgeführt.

Sie können DCM auch zum Anzeigen von Informationen über das Zertifikat verwenden, das zum Signieren eines Objekts verwendet wurde. Hierdurch ist es möglich festzustellen, ob das Objekt von einer anerkannten Quelle stammt, bevor Sie damit arbeiten.

#### **Zugehörige Konzepte**

„Digitale Zertifikate für das Signieren von Objekten“ auf Seite 42

In diesen Informationen wird erläutert, wie Zertifikate zum Sicherstellen der Objektintegrität oder zum Prüfen der digitalen Signatur von Objekten eingesetzt werden können, um deren Authentizität zu prüfen.

#### **Zugehörige Tasks**

„Zertifikate zum Prüfen von Objektsignaturen verwalten“ auf Seite 61

Digital Certificate Manager (DCM) kann zum Verwalten der Signaturüberprüfungszertifikate verwendet werden, die zum Überprüfen der digitalen Signaturen auf Objekten eingesetzt werden.

---

## **Fehlerbehebung in DCM**

In diesen Informationen wird erläutert, wie einige der allgemeineren Fehler behoben werden, die bei der Verwendung von DCM auftreten können.



Beim Arbeiten mit Digital Certificate Manager (DCM) und mit Zertifikaten können möglicherweise Fehler auftreten, die den fehlerfreien Abschluss der von Ihnen durchgeführten Arbeitsschritte verhindern. Viele der häufig auftretenden Fehler oder Probleme können den im Folgenden beschriebenen Kategorien zugeordnet werden.

## Fehler bei Kennwörtern und allgemeine Fehler beheben

Die folgende Tabelle enthält Hinweise auf Informationen, die Ihnen bei der Behebung allgemeinerer Fehler bei Kennwörtern und anderen allgemeinen Problemen helfen, die beim Arbeiten mit Digital Certificate Manager (DCM) möglicherweise auftreten.

Fehler	Mögliche Lösung
Sie finden keine zusätzlichen Hilfeinformationen zu DCM.	Klicken Sie in DCM auf das Hilfesymbol mit dem Fragezeichen (?). Außerdem können Sie im Information Center und auf externen IBM Websites im Internet nach Informationen suchen.
Ihr Kennwort für die lokale Zertifizierungsinstanz (CA) und den Zertifikatsspeicher *SYSTEM wird nicht akzeptiert.	Bei Kennwörtern muss die Groß-/Kleinschreibung beachtet werden. Prüfen Sie, ob die Einstellung der Sperrtaste für die Groß-/Kleinschreibung identisch ist mit der Einstellung, die bei der Zuordnung des Kennworts aktiv war.
Wenn Sie versuchen, einen Zertifikatsspeicher zu öffnen, erhalten Sie eine Fehlermeldung, in der Sie darüber informiert werden, dass Ihr Kennwort abgelaufen ist.	Sie müssen das Kennwort für den Zertifikatsspeicher ändern. Klicken Sie auf die Schaltfläche <b>OK</b> , um das Kennwort zu ändern.
Der Versuch, das Kennwort bei der Verwendung der Task <b>Zertifikatsspeicher auswählen</b> zurückzusetzen, ist fehlgeschlagen.	Die Rücksetzfunktion kann nur verwendet werden, wenn das Kennwort in DCM gespeichert wurde. DCM speichert das Kennwort automatisch, wenn Sie einen Zertifikatsspeicher erstellen. Wird hingegen das Kennwort eines Speichers für andere Systemzertifikate geändert (oder zurückgesetzt), müssen Sie <b>Automatisches Anmelden</b> auswählen, damit DCM das Kennwort weiterhin verdeckt speichert.
	Wenn ein Zertifikatsspeicher von einem System auf ein anderes versetzt wird, muss außerdem das Kennwort des Zertifikatsspeichers auf dem neuen System geändert werden, um sicherzustellen, dass es von DCM automatisch verdeckt gespeichert wird. Zum Ändern des Kennworts müssen Sie das ursprüngliche Kennwort des Zertifikatsspeichers angeben, wenn dieser auf dem neuen System geöffnet werden soll. Die Auswahl zum Zurücksetzen des Kennworts kann erst dann verwendet werden, wenn der Zertifikatsspeicher mit dem ursprünglichen Kennwort geöffnet und das Kennwort geändert wurde, um es zu verdecken. Wird das Kennwort nicht geändert und verdeckt gespeichert, kann es von DCM und SSL nicht automatisch wiederhergestellt werden, wenn es für die verschiedenen Funktionen benötigt wird. Wird ein Zertifikatsspeicher versetzt, der als Speicher für andere Systemzertifikate verwendet wird, müssen Sie beim Ändern des Kennworts <b>Automatisches Anmelden</b> auswählen, um sicherzustellen, dass DCM das neue Kennwort für diesen Zertifikatsspeichertyp verdeckt speichert.

Fehler	Mögliche Lösung
	Prüfen Sie den Wert für das Attribut <b>Allow new digital certificates</b> unter <b>Work with system security</b> der System-serviceprogramme (SST = System Service Tools). Wird dieses Attribut auf den Wert 2 (Nein) eingestellt, kann das Kennwort des Zertifikatsspeichers nicht zurückgesetzt werden. Sie können den Wert dieses Attributs mit Hilfe des Befehls STRSST anzeigen oder ändern, indem Sie die SST-Benutzer-ID und das zugehörige Kennwort eingeben. Wählen Sie anschließend <b>Work with system security</b> aus. Als Service-Tool-Benutzer-ID wird normalerweise QSECOFR verwendet.
Sie können keine Ursprungsangabe für ein CA-Zertifikat finden, um dieses in Ihrem System empfangen zu können.	Bestimmte Zertifizierungsinstanzen stellen ihre CA-Zertifikate nicht ohne Weiteres zur Verfügung. Wenn Sie das CA-Zertifikat einer Zertifizierungsinstanz nicht abrufen können, wenden Sie sich an den zuständigen VAR, der möglicherweise spezielle oder finanzielle Einstellungen mit der Zertifizierungsinstanz vereinbart hat.
Sie finden den Zertifikatsspeicher *SYSTEM nicht.	Die Dateiadresse des Zertifikatsspeichers *SYSTEM muss /qibm/userdata/icss/cert/server/default.kdb lauten. Wenn dieser Zertifikatsspeicher nicht vorhanden ist, muss er mit DCM erstellt werden. Verwenden Sie hierzu die Task <b>Neuen Zertifikatsspeicher erstellen</b> .
DCM hat einen Fehler ausgegeben, der durch die ausgeführten Fehlerbehebungsmaßnahmen nicht beseitigt werden konnte.	Löschen Sie den Inhalt des Browser-Caches. Definieren Sie als Cache-Größe den Wert 0, beenden und starten Sie den Browser anschließend erneut.
Auf dem LDAP-Server treten Probleme auf. Die Zertifikatszuordnungen können z. B. nicht angezeigt werden, wenn die Informationen zur gesicherten Anwendung direkt nach der Zuordnung eines Zertifikats aufgerufen werden sollen. Dieser Fehler tritt häufiger auf, wenn über den iSeries Navigator ein Netscape Communications-Browser aufgerufen wird. Ihre Vorgabe für den Browser-Cache ist so eingestellt, dass das Dokument im Cache mit dem Dokument im Netzwerk <b>Einmal pro Sitzung</b> verglichen wird.	Ändern Sie die Standardvorgabe so, dass die Cache-Prüfung jedes Mal durchgeführt wird.
Wenn Sie DCM zum Importieren eines Zertifikats verwenden, das von einer externen Zertifizierungsinstanz wie z. B. Entrust signiert wurde, erhalten Sie eine Fehlermeldung, in der Sie darüber informiert werden, dass die Gültigkeitsperiode den aktuellen Tag nicht einschließt oder nicht mit der Gültigkeitsperiode des Ausstellers übereinstimmt.	Das System verwendet zur Angabe der Gültigkeitsperiode das allgemeine Zeitformat. Warten Sie einen Tag und wiederholen Sie die Operation dann. Prüfen Sie auch, ob auf Ihrem System der korrekte Wert für die WEZ-Abweichung (dpsysval qutcoffset) definiert ist. Wenn Sie die Sommerzeit berücksichtigen müssen, ist diese Abweichung möglicherweise falsch definiert.
Sie haben einen Base-64-Fehler erhalten, als Sie versuchten, ein Entrust-Zertifikat zu importieren.	Für das Zertifikat wird ein spezielles Format wie z. B. das PEM-Format aufgelistet. Wenn die Kopierfunktion Ihres Browsers nicht einwandfrei arbeitet, werden möglicherweise zusätzliche Daten (z. B. Leerstellen am Anfang aller Zeilen) kopiert, die nicht zum Zertifikat gehören. In diesem Fall weist das Zertifikat nicht das richtige Format auf, wenn Sie versuchen, es auf dem System zu verwenden. Dieses Problem wird durch manche Webseitenentwürfe verursacht. Andere Webseiten sind hingegen so strukturiert, dass dieses Problem nicht auftritt. Überprüfen Sie unbedingt die Darstellung des ursprünglichen Zertifikats mit den Ergebnissen der Einfügeoperation. Diese Ergebnisse müssen mit den Originaldaten übereinstimmen.

## Fehler bei Zertifikatsspeichern und Schlüsseldatenbanken beheben

Die folgende Tabelle enthält Hinweise auf Informationen, die Ihnen bei der Behebung allgemeinerer Fehler in Zertifikatsspeichern und Schlüsseldatenbanken helfen, die beim Arbeiten mit Digital Certificate Manager (DCM) möglicherweise auftreten.

<b>Fehler</b>	<b>Mögliche Lösung</b>
Das System konnte die Schlüsseldatenbank nicht lokalisieren oder hat festgestellt, dass diese ungültig ist.	Prüfen Sie das Kennwort und den Dateinamen auf Tippfehler. Prüfen Sie, ob mit dem Dateinamen auch der Pfad einschließlich des führenden Schrägstrichs angegeben wurde.

Fehler	Mögliche Lösung
<p>Die Erstellung der Schlüsseldatenbank ist fehlgeschlagen oder die Erstellung einer lokalen Zertifizierungsinstanz ist fehlgeschlagen.</p>	<p>Prüfen Sie, ob ein Dateinamenkonflikt vorliegt. Der Konflikt kann in einer anderen als der angeforderten Datei begründet sein. DCM versucht, Benutzerdaten in selbst erstellten Verzeichnissen zu schützen. Dies gilt auch dann, wenn diese Dateien eine Erstellung der Dateien im Bedarfsfall verhindern.</p> <p>Beheben Sie dieses Problem, indem Sie alle einen Konflikt auslösenden Dateien in ein anderes Verzeichnis kopieren und die entsprechenden Dateien mit einer DCM-Funktion löschen, falls dies möglich ist. Wenn die Ausführung dieser Operation unter DCM nicht erfolgreich war, müssen die Dateien manuell aus dem ursprünglichen IFS-Verzeichnis gelöscht werden, wo sie zu Konflikten mit DCM führen. Dokumentieren Sie genau, welche Dateien an eine andere Speicherposition verschoben wurden und wo sich diese jetzt befinden. Mit Hilfe der Kopien können Sie diese bei Bedarf wiederherstellen. Nach dem Verschieben der folgenden Dateien muss eine neue lokale Zertifizierungsinstanz erstellt werden:</p> <pre data-bbox="769 806 1370 1331"> /QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.KDB /QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.TEMP.KDB /QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.RDB /QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.STH /QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.STH.OLD /QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.KYR /QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.POL /QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.BAK /QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.TEMP /QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.STHBAK /QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.TEMP.STH /QIBM/USERDATA/ICSS/CERT/CERTAUTH/CA.TXT /QIBM/USERDATA/ICSS/CERT/CERTAUTH/CA.BAK /QIBM/USERDATA/ICSS/CERT/CERTAUTH/CA.TMP /QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.POLTMP /QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.POLBAK /QIBM/USERDATA/ICSS/CERT/DOWNLOAD/CERTAUTH/CA.CACRT /QIBM/USERDATA/ICSS/CERT/DOWNLOAD/CERTAUTH/CA.CATMP /QIBM/USERDATA/ICSS/CERT/DOWNLOAD/CERTAUTH/CA.CABAK /QIBM/USERDATA/ICSS/CERT/DOWNLOAD/CLIENT/*.USRCRT </pre> <p>Nach dem Verschieben der folgenden Dateien müssen Sie einen neuen Zertifikatsspeicher *SYSTEM und ein neues Systemzertifikat erstellen:</p> <pre data-bbox="769 1457 1344 1875"> /QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.KDB /QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.BAK /QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.RDB /QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.STH /QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.STH.OLD /QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.STHBAK /QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.TMP /QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.TEMP.STH /QIBM/USERDATA/ICSS/CERT/SERVER/SRV.TMP /QIBM/USERDATA/ICSS/CERT/SERVER/SRV.BAK /QIBM/USERDATA/ICSS/CERT/SERVER/SRV.TXT /QIBM/USERDATA/ICSS/CERT/SERVER/SRV.SGN /QIBM/USERDATA/ICSS/CERT/SERVER/SGN.TMP /QIBM/USERDATA/ICSS/CERT/SERVER/SGN.BAK /QIBM/USERDATA/ICSS/CERT/SERVER/EXPSRV.TMP /QIBM/USERDATA/ICSS/CERT/SERVER/EXPSGN.TMP </pre>

Fehler	Mögliche Lösung
	Möglicherweise fehlt ein vorausgesetztes Lizenzprogramm (LPP), dessen Installation unter DCM erforderlich ist. Prüfen Sie die Liste der Voraussetzungen für DCM, und stellen Sie sicher, dass alle Lizenzprogramme korrekt installiert sind.
Das System weist eine CA-Textdatei zurück, die im Binärmodus von einem anderen System übertragen wurde. Es akzeptiert die Datei, wenn diese im ASCII-Code (ASCII = American National Standard Code for Information Interchange) übertragen wird.	Schlüsselringe und Schlüsseldatenbanken sind binär und müssen deshalb anders behandelt werden. Sie müssen FTP (File Transfer Protocol) für CA-Textdateien im ASCII-Modus, für Binärdateien jedoch im Binärmodus verwenden. Hierzu gehören z. B. die Dateien mit den folgenden Erweiterungen: .kdb, .kyr, .sth, .rdb etc.
Das Kennwort einer Schlüsseldatenbank kann nicht geändert werden. Ein Zertifikat in der Schlüsseldatenbank ist nicht mehr gültig.	Nachdem Sie überprüft haben, dass der Fehler nicht auf einem falschen Kennwort beruht, müssen Sie das ungültige Zertifikat im Zertifikatsspeicher suchen und aus diesem löschen. Versuchen Sie anschließend erneut, das Kennwort zu ändern. Wenn der Zertifikatsspeicher abgelaufene Zertifikate enthält, sind diese nicht mehr gültig. Aus diesem Grund wird die Kennwortänderung von der entsprechenden Funktion des Zertifikatsspeichers möglicherweise nicht zugelassen und der Verschlüsselungsprozess wird die privaten Schlüssel der abgelaufenen Zertifikate nicht verschlüsseln. Hierdurch wird die Änderung des Kennworts verhindert und das System gibt eventuell die Meldung aus, dass einer der Gründe hierfür eine Beschädigung des Zertifikatsspeichers ist. Die ungültigen (abgelaufenen) Zertifikate müssen aus dem Zertifikatsspeicher entfernt werden.
Sie wollen Zertifikate für einen Internet-Benutzer verwenden und benötigen deswegen Prüflisten. DCM stellt jedoch keine Funktionen für Prüflisten zur Verfügung.	Geschäftspartner, die Anwendungen so codieren, dass Prüflisten eingesetzt werden sollen, müssen ihren Code so definieren, dass die Prüfliste wie gewohnt ihrer Anwendung zugeordnet wird. Sie müssen außerdem den Code schreiben, mit dem festgestellt wird, wann die Identität des Internet-Benutzers ordnungsgemäß geprüft ist, damit das Zertifikat zur Prüfliste hinzugefügt werden kann. Weitere Informationen hierzu finden Sie unter dem Thema zur API QsyAddVldCertificate im Information Center. Informationen zum Konfigurieren einer gesicherten HTTP-Serverinstanz für den Einsatz der Prüfliste finden Sie unter HTTP Server for iSeries.

## Fehler bei Browsern beheben

Die folgende Tabelle enthält Hinweise auf Informationen, die Ihnen bei der Behebung allgemeinerer Browser-bezogener Fehler helfen, die beim Arbeiten mit Digital Certificate Manager (DCM) möglicherweise auftreten.

Fehler	Mögliche Lösung
Microsoft Internet Explorer lässt die Auswahl eines anderen Zertifikats erst dann zu, wenn Sie eine neue Browser-Sitzung starten.	Starten Sie eine neue Browser-Sitzung für den Internet Explorer.

Fehler	Mögliche Lösung
<p>Der Internet Explorer listet nicht alle auswählbaren Client-/Benutzerzertifikate in einer Browser-Auswahlliste auf. Es werden nur Zertifikate angezeigt, die von der anerkannten Zertifizierungsinstanz ausgestellt wurden und die Sie auf der gesicherten Site verwenden können.</p>	<p>Eine Zertifizierungsinstanz muss sowohl von der Schlüssel-datenbank als auch von der gesicherten Anwendung anerkannt werden. Prüfen Sie, ob Sie bei der Anmeldung am PC für den Internet Explorer-Browser den gleichen Benutzernamen verwendet haben, der zum Speichern des Benutzerzertifikats im Browser benutzt wurde. Rufen Sie ein weiteres Benutzerzertifikat von dem System ab, auf das Sie zugreifen. Der Systemadministrator muss sich vergewissern, dass der Zertifikatsspeicher (Schlüssel-datenbank) die Zertifizierungsinstanz, die die Benutzer- und Systemzertifikate signiert hat, weiterhin anerkennt.</p>
<p>Internet Explorer 5 empfängt das Zertifikat der Zertifizierungsinstanz, kann die Datei jedoch nicht öffnen bzw. kann die Platte nicht finden, auf der das Zertifikat gespeichert wurde.</p>	<p>Dies ist eine neue Browser-Funktion für Zertifikate, die vom Browser des Internet Explorer noch nicht anerkannt sind. Sie können auf dem PC eine Position auswählen.</p>
<p>Sie haben eine Browser-Warnung erhalten, in der Sie darüber informiert werden, dass Systemname und Systemzertifikat nicht übereinstimmen.</p>	<p>Bestimmte Browser behandeln die Groß- und Kleinschreibung bei Systemnamen unterschiedlich. Geben Sie die URL-Adresse in Bezug auf die Groß-/Kleinschreibung in exakt der gleichen Schreibweise ein wie das Systemzertifikat. Alternativ hierzu können Sie das Systemzertifikat auch mit dem Namen erstellen, der in seiner Groß-/Kleinschreibung für die Benutzer am geläufigsten ist. Wenn Sie Zweifel haben, sollte der Server- und der Systemname nicht geändert werden. Darüber hinaus sollten Sie prüfen, ob der Domänennamensserver korrekt konfiguriert ist.</p>
<p>Sie haben den Internet Explorer mit HTTPS an Stelle von HTTP gestartet und eine Warnung erhalten, dass gesicherte und nicht gesicherte Sitzungen gemischt verwendet werden.</p>	<p>Diese Warnung kann ignoriert werden. Das Problem wird in einem späteren Release von Internet Explorer behoben.</p>
<p>Netscape Communicator 4.04 für Windows hat die hexadezimalen Werte A1 und B1 in der polnischen Codepage in B2 und 9A konvertiert.</p>	<p>Dies ist ein Browser-Fehler, der sich auf die NLS-Unterstützung auswirkt. Verwenden Sie einen anderen Browser oder dieselbe Version des Browsers auf einer anderen Plattform, z. B. Netscape Communicator 4.04 für AIX.</p>
<p>In einem Benutzerprofil wurden in Netscape Communicator 4.04 die NLS-Zeichen für Benutzerzertifikate in Großbuchstaben korrekt, die Kleinbuchstaben jedoch falsch angezeigt.</p>	<p>Bestimmte landessprachliche Zeichen, die korrekt als ein Zeichen eingegeben wurden, werden bei der Anzeige später anders dargestellt. Die hexadezimalen Werte A1 und B1 werden in der Windows-Version von Netscape Communicator 4.04 für die polnische Codepage z. B. in die Werte B2 und 9A umgesetzt, was dazu führt, dass andere NLS-Zeichen angezeigt werden.</p>
<p>Der Browser gibt wiederholt die Meldung an den Benutzer aus, dass die Zertifizierungsinstanz noch nicht anerkannt wurde.</p>	<p>Definieren Sie mit DCM den <b>CA-Status</b> als <b>aktiviert</b>, um die Zertifizierungsinstanz als anerkannt zu markieren.</p>
<p>Internet Explorer-Anforderungen weisen die Herstellung einer HTTPS-Verbindung zurück.</p>	<p>Dieses Problem beruht auf der Browser-Funktion oder deren Konfiguration. Der Browser stellt keine Verbindung zu einer Site her, die mit einem Systemzertifikat arbeitet, das möglicherweise selbst signiert oder aus einem bestimmten Grund nicht gültig ist.</p>

Fehler	Mögliche Lösung
Netscape Communicator-Browser- und -Serverprodukte implementieren Root-Zertifikate von Unternehmen, z. B. von VeriSign, als Voraussetzung für die Unterstützung der SSL-Kommunikation. Dies gilt besonders in Bezug auf die Authentifizierung. Alle Root-Zertifikate laufen in periodischen Zeitabständen ab. Bestimmte Root-Zertifikate für Netscape-Browser und -Server sind zwischen dem 25. Dezember 1999 und dem 31. Dezember 1999 abgelaufen. Wenn dieses Problem nicht am bzw. vor dem 14. Dezember 1999 behoben wurde, wird eine Fehlermeldung ausgegeben.	Frühere Versionen des Browsers (Netscape Communicator 4.05 oder früher) arbeiten mit Zertifikaten, für die ein Ablaufdatum definiert ist. Sie müssen für den Browser einen Upgrade auf die aktuelle Netscape Communicator-Version durchführen. Informationen zu den Root-Zertifikaten von Browsern stehen auf vielen Sites zur Verfügung und können z. B. unter folgenden Adressen abgerufen werden: <a href="http://home.netscape.com/security/">http://home.netscape.com/security/</a> und <a href="http://www.verisign.com/server/cus/rootcert/webmaster.html">http://www.verisign.com/server/cus/rootcert/webmaster.html</a> . Kostenlose Browser-Downloads stehen unter <a href="http://www.netcenter.com">http://www.netcenter.com</a> zur Verfügung.

## Fehler beim IBM HTTP-Server für iSeries beheben

Fehler	Mögliche Lösung
Hypertext Transfer Protocol Secure (HTTPS) arbeitet nicht.	Prüfen Sie, ob der HTTP-Server für die Verwendung von SSL korrekt konfiguriert wurde. Unter V5R1 oder späteren Versionen muss in der Konfigurationsdatei über die Verwaltungsschnittstelle des HTTP-Servers <b>SSLAppName</b> definiert sein. Darüber hinaus muss in der Konfiguration ein virtueller Host definiert sein, der den SSL-Port benutzt und für den bei <b>SSL</b> die Einstellung <b>Aktiviert</b> angegeben ist. Außerdem müssen zwei <b>Listen</b> -Direktiven vorhanden sein, in denen ein Port für SSL und einer für andere Protokolle definiert ist. Diese werden auf der Seite <b>Allgemeine Einstellungen</b> definiert. Stellen Sie sicher, dass die Serverinstanz erstellt und das Serverzertifikat signiert wurde.
Die Arbeitsschritte zum Registrieren einer HTTP-Serverinstanz als gesicherte Anwendung müssen geklärt werden.	Rufen Sie auf Ihrem System die Verwaltungsschnittstelle des HTTP-Servers auf, um die erforderlichen Konfigurationseinstellungen für den HTTP-Server zu definieren. Als Erstes müssen Sie einen virtuellen Host zur Aktivierung von SSL definieren. Nach dem Definieren eines virtuellen Hosts müssen Sie angeben, dass der virtuelle Host den SSL-Port verwendet, der zuvor in der <b>Listen</b> -Direktive (auf der Seite <b>Allgemeine Einstellungen</b> ) definiert wurde. Als Nächstes müssen Sie auf der Seite <b>SSL mit Zertifikatsauthentifizierung</b> unter <b>Sicherheit</b> SSL auf dem zuvor konfigurierten virtuellen Host aktivieren. Alle Änderungen müssen in der Konfigurationsdatei angewendet werden. Beachten Sie hierbei, dass durch die Registrierung Ihrer Instanz nicht automatisch die zu verwendenden Zertifikate ausgewählt werden. Bevor Sie die Serverinstanz stoppen und erneut starten, müssen Sie der Anwendung mit DCM ein bestimmtes Zertifikat zuordnen.
Sie haben Schwierigkeiten, den HTTP-Server für die Verwendung von Prüflisten und für die optionale Client-Authentifizierung zu konfigurieren.	Informationen zu den Auswahlmöglichkeiten beim Konfigurieren der Instanz finden Sie unter HTTP Server for iSeries.
Netscape Communicator wartet, bis die Konfigurationsanweisung im HTTP-Server-Code abgelaufen ist, bevor die Auswahl eines anderen Zertifikats zugelassen wird.	Ein hoher Wert für Zertifikate erschwert das Registrieren eines zweiten Zertifikats, da der Browser weiterhin das erste Zertifikat verwendet.

Fehler	Mögliche Lösung
<p>Sie versuchen, den Browser zur Vorlage des X.509-Zertifikats beim HTTP-Server anzuweisen, damit das Zertifikat als Eingabe für die API QsyAddVldCertificate verwendet werden kann.</p>	<p>Sie müssen die Einstellungen <b>SSLEnable</b> und <b>SSLClientAuth ON</b> verwenden, damit der HTTP-Server die Umgebungsvariable <b>HTTPS_CLIENT_CERTIFICATE</b> laden kann. Informationen zu diesen APIs sind im Abschnitt API Finder im Information Center enthalten. Weitere Einzelheiten finden Sie unter den Themen zu folgenden Prüflisten und zertifikatsbezogenen APIs:</p> <ul style="list-style-type: none"> <li>• QsyListVldCertificates und QSYLSTVC</li> <li>• QsyRemoveVldCertificate und QRMVVC</li> <li>• QsyCheckVldCertificate und QSYCHKVC</li> <li>• QsyParseCertificate und QSYPARSC etc.</li> </ul>
<p>Der HTTP-Server benötigt für die Rückmeldung zu viel Zeit, oder es tritt eine Zeitlimitüberschreitung auf, wenn eine Auflistung der Zertifikate in der Prüfliste angefordert wird und diese mehr als 10.000 Einträge enthält.</p>	<p>Erstellen Sie einen Stapeljob, der nach Zertifikaten sucht, die bestimmten Kriterien entsprechen, und diese löscht. Hierbei können z. B. alle Zertifikate erfasst werden, die abgelaufen sind oder von einer bestimmten Zertifizierungsinstanz stammen.</p>
<p>Der HTTP-Server kann mit der Einstellung <b>Aktiviert</b> für <b>SSL</b> nicht gestartet werden und die Fehlermeldung HTP8351 wird im Jobprotokoll aufgezeichnet. Das Fehlerprotokoll für den HTTP-Server enthält eine Fehlermeldung, in der Sie darüber informiert werden, dass die SSL-Initialisierungsoperation fehlgeschlagen und der Rückkehrcode 107 generiert wurde, als die Ausführung des HTTP-Servers fehlgeschlagen ist.</p>	<p>Der Fehlercode 107 gibt an, dass das Zertifikat abgelaufen ist. Ordnen Sie der Anwendung mit DCM ein anderes Zertifikat (z. B. QIBM_HTTP_SERVER_MY_SERVER) zu. Wenn es sich bei der Serverinstanz, deren Start fehlgeschlagen ist, um den *ADMIN-Server handelt, müssen Sie für <b>SSL</b> temporär die Einstellung <b>Inaktiviert</b> angeben, damit DCM auf diesem Server verwendet werden kann. Anschließend können Sie DCM zum Zuordnen eines anderen Zertifikats zur Anwendung QIBM_HTTP_SERVER_ADMIN benutzen und für <b>SSL</b> wieder <b>Aktiviert</b> angeben.</p>

## Fehler beim Zuordnen eines Benutzerzertifikats beheben

Wenn Sie die Task **Benutzerzertifikat zuordnen** verwenden, zeigt Digital Certificate Manager (DCM) Zertifikatsinformationen an, die Sie vor dem Registrieren des Zertifikats genehmigen müssen. Wenn DCM kein Zertifikat anzeigen kann, liegt als Ursache möglicherweise eines der folgenden Probleme vor:

1. Ihr Browser hat Sie nicht zur Auswahl eines Zertifikats für die Vorlage beim Server aufgefordert. Dieser Fall kann eintreten, wenn der Browser ein vorher verwendetes Zertifikat im Cache gespeichert hat, das für den Zugriff auf einen anderen Server verwendet wurde. Löschen Sie den Inhalt des Browser-Caches, und wiederholen Sie die Operation. Anschließend wird der Browser Sie zur Auswahl eines Zertifikats auffordern.
2. Dieser Fall kann auch eintreten, wenn Sie den Browser so konfigurieren, dass keine Auswahlliste angezeigt wird, und der Browser in der Liste der vom Server anerkannten CAs nur ein Zertifikat einer Zertifizierungsinstanz (CA) enthält. Prüfen Sie die Konfigurationseinstellungen des Browsers, und ändern Sie diese bei Bedarf. Anschließend wird der Browser Sie zur Auswahl eines Zertifikats auffordern. Wenn Sie kein Zertifikat einer Zertifizierungsinstanz (CA) vorlegen können, das vom Server anerkannt wird, können Sie kein Zertifikat zuordnen. Wenden Sie sich in diesem Fall an den zuständigen DCM-Administrator.
3. Das gewünschte Zertifikat wurde unter DCM bereits registriert.
4. Die Zertifizierungsinstanz, die das Zertifikat ausgestellt hat, ist auf dem System bzw. in der Anwendung nicht als anerkannt definiert. Aus diesem Grund ist das vorgelegte Zertifikat ungültig. Wenden Sie sich an den Systemadministrator, um festzustellen, ob die ausstellende Zertifizierungsinstanz korrekt ist. Ist dies der Fall, muss der Systemadministrator das Zertifikat der Zertifizierungsinstanz möglicherweise in den Zertifikatsspeicher \*SYSTEM **importieren**. Alternativ hierzu kann der Administrator auch die Task **Status der Zertifizierungsinstanz festlegen** verwenden, um die CA auf dem System als anerkannt zu definieren und das Problem zu beheben.



5. Sie verfügen über kein Zertifikat, das registriert werden kann. In diesem Fall können Sie im Browser nach Benutzerzertifikaten suchen, um das Problem zu beheben.
6. Das zu registrierende Zertifikat ist abgelaufen oder unvollständig. Sie müssen das Zertifikat entweder verlängern oder eine Verbindung zur ausstellenden Zertifizierungsinstanz herstellen, um das Problem zu beheben.
7. Der IBM HTTP-Server für i5/OS ist nicht so konfiguriert, dass das Zertifikat via SSL registriert und die Client-Authentifizierung auf der gesicherten Verwaltungsserverinstanz ausgeführt werden kann. Wenn keiner der hier aufgeführten Tipps für die Fehlerbehebung erfolgreich ist, wenden Sie sich an den Systemadministrator, um das Problem zu melden.

Um ein **Benutzerzertifikat zuordnen** zu können, müssen Sie über eine SSL-Sitzung eine Verbindung zu Digital Certificate Manager (DCM) herstellen. Ist SSL nicht aktiv, wenn Sie die Task **Benutzerzertifikat zuordnen** auswählen, gibt DCM eine Nachricht aus, in der Sie zur Verwendung von SSL aufgefordert werden. Im Nachrichtenfenster ist eine Schaltfläche enthalten, mit der Sie über SSL eine Verbindung zu DCM herstellen können. Wird diese Schaltfläche im Nachrichtenfenster nicht angezeigt, sollten Sie das Problem dem Systemadministrator melden. In diesem Fall muss eventuell der Webserver erneut gestartet werden, um die Konfigurationsanweisungen für die Verwendung von SSL zu aktivieren.

#### Zugehörige Tasks

„Benutzerzertifikat zuordnen“ auf Seite 51

Sie können ein eigenes Benutzerzertifikat Ihrem i5/OS-Benutzerprofil oder einer anderen Benutzeridentität zuordnen. Das Zertifikat kann von einer privaten lokalen Zertifizierungsinstanz auf einem anderen System oder von einer bekannten Internet-Zertifizierungsinstanz stammen. Bevor Sie einer Benutzeridentität ein Zertifikat zuordnen können, muss die ausstellende Zertifizierungsinstanz vom Server anerkannt werden. Darüber hinaus darf das gewünschte Zertifikat noch keinem anderen Benutzerprofil bzw. keiner anderen Benutzeridentität auf dem System zugeordnet worden sein.


---

## Referenzinformationen zu DCM

Auf dieser Seite finden Sie Links auf andere Informationsquellen zu digitalen Zertifikaten, PKI (Public Key Infrastructure) und Digital Certificate Manager sowie weitere Referenzinformationen.

Da die Verwendung digitaler Zertifikate immer mehr Verbreitung findet, hat sich auch die Zahl der verfügbaren Informationsquellen erhöht. Im Folgenden ist eine kleine Liste anderer Informationsquellen aufgeführt, in denen Sie mehr zu digitalen Zertifikaten und den Möglichkeiten finden, wie diese zur Verbesserung der Sicherheitsrichtlinien Ihres Systems eingesetzt werden können:

- **VeriSign Help Desk-Website**  Die VeriSign-Website stellt eine umfangreiche Bibliothek mit Veröffentlichungen zu digitalen Zertifikaten sowie zu anderen sicherheitsbezogenen Themen aus dem Internet-Bereich zur Verfügung.
- **IBM eServer iSeries Wired Network Security: OS/400 V5R1 DCM and Cryptographic Enhancements (IBM Form SG24-6168)**  Dieses IBM Redbook behandelt schwerpunktmäßig funktionale Erweiterungen des Netzwerksicherheitssystems für OS/400 V5R1. Es behandelt zahlreiche Themen wie z. B. zum Einsatz der iSeries-Objektsignierfunktionen, zu Digital Certificate Manager (DCM) sowie zur SSL-Unterstützung des IBM 4758 PCI Cryptographic Coprocessor etc.
- **AS/400 Internet Security: Developing a Digital Certificate Infrastructure (IBM Form SG24-5659)**  Dieses Redbook beschreibt die Einsatzmöglichkeiten digitaler Zertifikate auf dem iSeries-Server. Es enthält Erläuterungen dazu, wie die verschiedenen Server und Clients für die Verwendung von Zertifikaten konfiguriert werden können. Darüber hinaus enthält diese Veröffentlichung Informationen und Codebeispiele, in denen die Benutzung der OS/400-APIs zur Verwaltung und zum Einsatz digitaler Zertifikate in Benutzeranwendungen beschrieben wird.

- **RFC Index Search Engine**  Diese Website stellt ein Repository zur Verfügung, das nach RFCs (Requests for Comments) durchsucht werden kann. RFCs beschreiben die Standards für Internet-Protokolle wie z. B. SSL, PKIX sowie andere Standards, die sich auf die Verwendung digitaler Zertifikate beziehen.

---

## Anhang. Bemerkungen

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

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

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

IBM Europe  
Director of Licensing  
92066 Paris La Defense Cedex  
France

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

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.

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

Lizenznehmer des Programms, die Informationen zu diesem Produkt wünschen mit der Zielsetzung: (i) den Austausch von Informationen zwischen unabhängig voneinander erstellten Programmen und anderen Programmen (einschließlich des vorliegenden Programms) sowie (ii) die gemeinsame Nutzung der ausgetauschten Informationen zu ermöglichen, wenden sich an folgende Adresse:

IBM Corporation  
Software Interoperability Coordinator, Department YBWA  
3605 Highway 52 N  
Rochester, MN 55901  
U.S.A.

Die Bereitstellung dieser Informationen kann unter Umständen von bestimmten Bedingungen - in einigen Fällen auch von der Zahlung einer Gebühr - abhängig sein.

- | Die Lieferung des im Handbuch aufgeführten Lizenzprogramms sowie des zugehörigen Lizenzmaterials
- | erfolgt auf der Basis der IBM Rahmenvereinbarung sowie der Allgemeinen Geschäftsbedingungen der
- | IBM, der IBM Internationalen Nutzungsbedingungen für Programmpakete, der IBM Lizenzvereinbarung
- | für Maschinencode oder einer äquivalenten Vereinbarung.

Alle in diesem Dokument enthaltenen Leistungsdaten stammen aus einer gesteuerten Umgebung. Die Ergebnisse, die in anderen Betriebsumgebungen erzielt werden, können daher erheblich von den hier erzielten Ergebnissen abweichen. Einige Daten stammen möglicherweise von Systemen, deren Entwicklung noch nicht abgeschlossen ist. Eine Gewährleistung, dass diese Daten auch in allgemein verfügbaren Systemen erzielt werden, kann nicht gegeben werden. Darüber hinaus wurden einige Daten unter Umständen durch Extrapolation berechnet. Die tatsächlichen Ergebnisse können abweichen. Benutzer dieses Dokuments sollten die entsprechenden Daten in ihrer spezifischen Umgebung prüfen.

Die oben genannten Erklärungen bezüglich der Produktstrategien und Absichtserklärungen von IBM stellen die gegenwärtige Absicht der IBM dar, unterliegen Änderungen oder können zurückgenommen werden, und repräsentieren nur die Ziele der IBM.

Alle von IBM angegebenen Preise sind empfohlene Richtpreise und können jederzeit ohne weitere Mitteilung geändert werden. Händlerpreise können u. U. von den hier genannten Preisen abweichen.

Diese Veröffentlichung enthält Beispiele für Daten und Berichte des alltäglichen Geschäftsablaufes. Sie sollen nur die Funktionen des Lizenzprogrammes illustrieren; sie können Namen von Personen, Firmen, Marken oder Produkten enthalten. Alle diese Namen sind frei erfunden; Ähnlichkeiten mit tatsächlichen Namen und Adressen sind rein zufällig.

#### COPYRIGHTLIZENZ:

Diese Veröffentlichung enthält Musteranwendungsprogramme, die in Quellsprache geschrieben sind. Sie dürfen diese Musterprogramme kostenlos kopieren, ändern und verteilen, wenn dies zu dem Zweck geschieht, Anwendungsprogramme zu entwickeln, verwenden, vermarkten oder zu verteilen, die mit der Anwendungsprogrammierschnittstelle konform sind, für die diese Musterprogramme geschrieben werden. Diese Beispiele wurden nicht unter allen denkbaren Bedingungen getestet. Daher kann IBM die Zuverlässigkeit, Wartungsfreundlichkeit oder Funktion dieser Programme weder zusagen noch gewährleisten.

Kopien oder Teile der Musterprogramme bzw. daraus abgeleiteter Code müssen folgenden Copyrightvermerk beinhalten:

© (Name Ihrer Firma) (Jahr). Teile des vorliegenden Codes wurden aus Musterprogrammen der IBM Corp. abgeleitet. © Copyright IBM Corp. \_Jahr/Jahre angeben\_. Alle Rechte vorbehalten.

---

## Marken

Folgende Namen sind in gewissen Ländern (oder Regionen) Marken der International Business Machines Corporation:

- | AIX
- | AS/400
- | Domino
- | eServer
- | i5/OS
- | IBM
- | iSeries
- | Lotus
- | Net.Data
- | OS/400

Microsoft, Windows und das Windows-Logo sind in gewissen Ländern Marken der Microsoft Corporation.

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

---

## Bedingungen

Die Berechtigungen zur Nutzung dieser Veröffentlichungen werden Ihnen auf der Basis der folgenden Bedingungen gewährt.

**Persönliche Nutzung:** Sie dürfen diese Veröffentlichungen für Ihre persönliche, nicht kommerzielle Nutzung unter der Voraussetzung vervielfältigen, dass alle Eigentumsvermerke erhalten bleiben. Sie dürfen diese Veröffentlichungen oder Teile der Veröffentlichungen ohne ausdrückliche Genehmigung von IBM weder weitergeben oder anzeigen noch abgeleitete Werke davon erstellen.

**Kommerzielle Nutzung:** Sie dürfen diese Veröffentlichungen nur innerhalb Ihres Unternehmens und unter der Voraussetzung, dass alle Eigentumsvermerke erhalten bleiben, vervielfältigen, weitergeben und anzeigen. Sie dürfen diese Veröffentlichungen oder Teile der Veröffentlichungen ohne ausdrückliche Genehmigung von IBM außerhalb Ihres Unternehmens weder vervielfältigen, weitergeben oder anzeigen noch abgeleitete Werke davon erstellen.

Abgesehen von den hier gewährten Berechtigungen erhalten Sie keine weiteren Berechtigungen, Lizenzen oder Rechte (veröffentlicht oder stillschweigend) in Bezug auf die Veröffentlichungen oder darin enthaltene Informationen, Daten, Software oder geistiges Eigentum.

IBM behält sich das Recht vor, die in diesem Dokument gewährten Berechtigungen nach eigenem Ermessen zurückzuziehen, wenn sich die Nutzung der Veröffentlichungen für IBM als nachteilig erweist oder wenn die obigen Nutzungsbestimmungen nicht genau befolgt werden.

Sie dürfen diese Informationen nur in Übereinstimmung mit allen anwendbaren Gesetzen und Verordnungen, einschließlich aller US-amerikanischen Exportgesetze und Verordnungen, herunterladen und exportieren.

IBM übernimmt keine Gewährleistung für den Inhalt dieser Informationen. Diese Veröffentlichungen werden auf der Grundlage des gegenwärtigen Zustands (auf "as-is"-Basis) und ohne eine ausdrückliche oder stillschweigende Gewährleistung für die Handelsüblichkeit, die Verwendungsfähigkeit oder die Freiheit der Rechte Dritter zur Verfügung gestellt.





**IBM**