

# Schutz der Vertraulichkeit von E-Mails in regulierten Branchen

Veröffentlicht: 18. Aug 2006

## Auf dieser Seite

- [Einführung](#)
- [Szenario zum Schutz der Vertraulichkeit von E-Mails](#)
- [Zusammenfassung](#)

## Download

[Dokument „Schutz der Vertraulichkeit von E-Mails in regulierten Branchen“ herunterladen](#)

## Einführung

Unternehmen sehen sich bedeutenden rechtlichen und behördlichen Herausforderungen in Bereichen wie Informationssicherheit, Datenschutz und Zuverlässigkeit gegenüber. Aufgrund dieser Herausforderungen können umfassende Änderungen an Systemen und Verfahren im gesamten Unternehmen erforderlich werden. Daher besteht bei Unternehmen Handlungsbedarf und die Notwendigkeit, sich zur Erfüllung vielfacher rechtlicher und ethischer Vorgaben auf das Strukturwachstum und zunehmende Regulierungsaufkommen bezüglich Verantwortlichkeit und Kontrolle einzurichten. Die Erfüllung aller rechtlichen und geschäftlichen Anforderungen, denen sich ein Unternehmen gegenüber sieht, und die es im alltäglichen Betrieb und bei seinen Geschäftstätigkeiten vorweisen können muss, wird unter dem Begriff „Einhaltung“ zusammengefasst. Dieser Begriff schliesst aber auch das Verständnis des rechtlichen Rahmens ein, in dem sich gerichtliche und unternehmerische Anforderungen bewegen. Um diesen Anforderungen gerecht zu werden, muss die Einhaltung jede Geschäftsabteilung und jeden Mitarbeiter umfassen. Sie lässt sich nicht durch die Umsetzung einer einzelnen Lösung oder Verfahrensweise erreichen, sondern muss in jedem Geschäftsbereich eines Unternehmens Einzug finden.

Das regulatorische Gefüge wird zunehmend komplexer. Einhaltung lässt sich oftmals nicht durch einen einfachen Prozess erreichen, und Vorschriften weichen hinsichtlich der Konkretheit ihrer Anforderungen voneinander ab. Ein Unternehmen muss daher eine umfassende Bewertung der Risiken und Auswirkungen vornehmen.

In diesem Papier werden einige der Verfahren und Technologien beschrieben, die zur Standardisierung und Abstimmung von Massnahmen zur Einhaltung von Vorschriften im Bereich der Vertraulichkeit von E-Mails verwendet werden können. Es stellt Ressourcen und Optionen vor, die viele kleine bis mittelgrosse Unternehmen bei ihren Bemühungen um die Einhaltung von Gesetzen und Vorschriften nutzen können. Das Papier soll keine genaue Anleitung zum Erreichen der Einhaltung gesetzlicher Vorschriften sein und enthält ebenso wenig rechtliche Ratschläge zu diesen Gesichtspunkten. Leser müssen sich vor der Auswahl eines Programms oder Verfahrens zur Einhaltung mit den eigenen Beratern und Rechtsanwälten absprechen.

## Zielgruppe dieses Leitfadens

Zu der Zielgruppe dieses Leitfadens gehören IT-Experten, die für die Installation, Wartung und Verwaltung von E-Mail-Diensten auf Basis von Microsoft® Exchange Server 2003 in ihren Netzwerkkumgebungen zuständig sind.

Die Angaben in diesem Leitfaden gelten für kleine und mittelgrosse Unternehmen mit vertraulichem E-Mail-Verkehr in ihren Netzwerken.

## Übersicht

Zwar enthält Microsoft Exchange Server bereits seit der ersten Produktversion Sicherheitsfunktionen für den Nachrichtenverkehr, doch wurden sie bisher in der Regel nur von Kunden mit besonderen Sicherheitsanforderungen und mit eigenem Sicherheitspersonal genutzt. Ein Verständnis der Sicherheitskonzepte für E-Mail-Nachrichten war nur von Sicherheitsexperten und Personen mit einem Hintergrund in Kryptographie gefordert. Mit der zunehmenden Unterstützung von S/MIME (Secure/Multipurpose Internet Mail Extensions) in Exchange Server 2003 sowie angesichts der Pflicht zur Einhaltung gesetzlicher Vorschriften müssen sich mittlerweile jedoch auch Administratoren mit diesen Prinzipien und Konzepten vertraut machen.

Das Messaging & Security Feature Pack für Windows Mobile 5.0 bietet Unterstützung für S/MIME-Zertifikate auf Smartphones. Darüber hinaus unterstützt Microsoft Exchange Server 2003 Service Pack 2 (SP2) S/MIME in Microsoft Outlook® Web Access (OWA).

Dieses Papier enthält eine Einführung in S/MIME und damit verbundene Konzepte und bietet ausführliche Anleitungen zur Implementierung von S/MIME. Es ist kein Hintergrundwissen im Bereich der Sicherheit erforderlich. In diesem Papier werden die allgemeinen S/MIME-Konzepte erläutert, so dass Sie diese gezielt auf Ihren Exchange Server anwenden können.

## Vorteile von S/MIME

Vor der Entwicklung von S/MIME haben Administratoren das gemeinhin verwendete E-Mail-Protokoll SMTP (Simple Mail Transfer Protocol) zur Nachrichtenübermittlung genutzt, das dem Wesen nach unsicherer war. Mitunter fanden auch unternehmenseigene Lösungen Anwendung, die mehr Sicherheit boten. Administratoren waren praktisch gezwungen, bei der Entscheidung für eine Lösung entweder Sicherheit oder Konnektivität den Vorzug zu geben. Mit S/MIME steht Administratoren nunmehr eine E-Mail-Option zur Verfügung, die mehr Sicherheit als SMTP und eine umfassende und sichere E-Mail-Konnektivität bietet.

S/MIME umfasst zwei Sicherheitsdienste:

- Digitale Signaturen
- Nachrichtenverschlüsselung

Diese beiden Dienste bilden das Kernstück der S/MIME-basierten Nachrichtensicherheit. Alle anderen mit der Nachrichtensicherheit verbundenen Konzepte unterstützen diese Dienste. Auch wenn der volle Umfang der Nachrichtensicherheit sehr komplex erscheinen mag, bilden diese beiden Dienste deren Grundlage.

Digitale Signaturen und Nachrichtenverschlüsselung schliessen sich nicht gegenseitig aus. Jeder Dienst ist jeweils auf bestimmte Sicherheitsaspekte ausgerichtet. Digitale Signaturen befassen sich mit Authentifizierungs- und Zurückweisungsgesichtspunkten, während die Nachrichtenverschlüsselung dem Schutz der Vertraulichkeit dient. Da jeder Dienst verschiedene Aspekte behandelt, müssen für jede Strategie zur Nachrichtensicherheit auch beide Dienste betrachtet werden. Die beiden Dienste sind für die gemeinsame Verwendung konzipiert, da jeder von ihnen jeweils eine Seite der Absender-Empfänger-Beziehung betrifft. Digitale Signaturen kümmern sich um Sicherheitsaspekte auf Absenderseite, während sich die Verschlüsselung hauptsächlich mit solchen auf Empfängerseite befasst.

Bei der gemeinsamen Verwendung von digitalen Signaturen und der Nachrichtenverschlüsselung profitieren Benutzer somit auch von beiden Diensten. Die Anwendung beider Dienste auf Nachrichten bedeutet keine Änderung hinsichtlich der Handhabung oder Verarbeitung dieser Dienste.

### Digitale Signaturen

Digitale Signaturen stellen den gebräuchlicheren S/MIME-Dienst dar. Wie der Name bereits andeutet, sind digitale Signaturen die digitale Entsprechung herkömmlicher, rechtsverbindlicher Unterschriften auf Papierdokumenten. Genau wie rechtsverbindliche Unterschriften bieten digitale Signaturen die folgenden Sicherheitsfunktionen:

- **Authentifizierung.** Eine Unterschrift dient zur Identitätsbestätigung. Sie beantwortet durch Bereitstellung eines Mittels zur eindeutigen Unterscheidung einer Person von allen anderen Personen und Bestätigung der Herkunft aus einer beidseitig als vertrauenswürdig angesehenen Quelle die Frage nach der Identität. Da SMTP-E-Mails keine Authentifizierung bieten, bleibt der Absender einer Nachricht letztendlich unbekannt. Die Authentifizierung durch eine digitale Signatur trägt zur Lösung dieses Problems bei, indem ein Empfänger überprüfen kann, ob eine Nachricht tatsächlich von der Person oder Organisation stammt, die sie angeblich gesendet hat.
- **Nichtabstreitbarkeit.** Durch die Eindeutigkeit einer Signatur kann verhindert werden, dass deren Eigentümer sie nicht anerkennt. Dieses Merkmal wird als Nichtabstreitbarkeit bezeichnet. Somit ist durch die Authentifizierung, die eine Signatur bietet, Nichtabstreitbarkeit gewährleistet. Das Konzept der Nichtabstreitbarkeit ist hauptsächlich im Kontext von Verträgen auf Papier bekannt: Ein unterschriebener Vertrag stellt ein rechtsverbindliches Dokument dar, und es ist schwierig, eine authentifizierte Unterschrift nicht anzuerkennen. Digitale Signaturen erfüllen die gleiche Funktion und werden besonders in einigen Bereichen mehr und mehr als rechtsverbindlich angesehen, genau wie Unterschriften auf Papier. Da SMTP-E-Mails keine Authentifizierungsfunktion bieten, ist die Nichtabstreitbarkeit nicht gewährleistet. Ein Absender kann problemlos leugnen, Verfasser einer bestimmten SMTP-E-Mail-Nachricht zu sein.
- **Datenintegrität.** Digitale Signaturen bieten als zusätzliche Sicherheitseinrichtung Datenintegrität. Die Datenintegrität resultiert aus den konkreten Vorgängen, die digitale Signaturen möglich machen. Wenn der Empfänger einer digital signierten E-Mail-Nachricht die digitale Signatur überprüft, wird dank Datenintegritätsdiensten sichergestellt, dass die empfangene Nachricht tatsächlich mit der signierten und gesendeten identisch ist und während der Übermittlung nicht geändert wurde. Jegliche Änderungen an einer signierten Nachricht während der Übermittlung führen zum Erlöschen der Signaturgültigkeit. Auf diese Art bieten digitale Signaturen eine Sicherheitsfunktion, die bei Unterschriften auf Papier nicht gegeben ist, da Papierdokumente auch nach der Unterzeichnung geändert werden können.

### Nachrichtenverschlüsselung

Die Nachrichtenverschlüsselung stellt eine Lösung für das Problem der ungewollten Informationsoffenlegung dar. SMTP-basierte Internet-E-Mails bieten keinen Schutz der Nachrichten. Sie können von jedem gelesen werden, der sie während der Übermittlung oder an ihrem Speicherort einsehen kann. S/MIME schafft hierbei durch Verschlüsselung Abhilfe.

Die Verschlüsselung bedeutet die Veränderung von Informationen auf eine Weise, dass sie weder gelesen noch verstanden werden können, bevor sie wieder in lesbare und verständliche Form gebracht werden.

Auch wenn die Nachrichtenverschlüsselung nicht so weit verbreitet ist wie digitale Signaturen, befasst sie sich mit den nach Meinung vieler Benutzer grössten Schwachstellen von Internet-E-Mails. Sie bietet zwei spezifische Sicherheitsfunktionen:

- **Vertraulichkeit.** Die Nachrichtenverschlüsselung trägt zum Schutz des Inhalts von E-Mail-Nachrichten bei. Nur der gewünschte Empfänger kann den Inhalt anzeigen, der seinen vertraulichen Charakter beibehält und von niemandem, der die Nachricht unberechtigt empfangen oder anzeigen könnte, entschlüsselt werden kann. Die Verschlüsselung schützt die Vertraulichkeit während der Übermittlung und Speicherung von Nachrichten.
- **Datenintegrität.** Genau wie digitale Signaturen bietet die Nachrichtenverschlüsselung Datenintegritätsdienste als Ergebnis der konkreten Vorgänge, die die Verschlüsselung möglich machen.

### Voraussetzungen für S/MIME

Zur Wahrung der Vertraulichkeit von E-Mails sind bestimmte Softwarekomponenten in Ihrer Umgebung erforderlich. Diese Komponenten werden im folgenden Abschnitt vorgestellt.

#### Public Key-Infrastruktur (PKI)

S/MIME-Lösungen erfordern eine PKI zur Bereitstellung von digitalen Zertifikaten mit Paaren aus öffentlichem und privatem Schlüssel und zur Aktivierung der Zertifikatszuordnung im Active Directory®-Verzeichnisdienst. Im S/MIME-Standard ist festgelegt, dass für S/MIME verwendete digitale Zertifikate dem Standard X.509 der International Telecommunications Union (ITU) entsprechen müssen. Die Version 3 von S/MIME erfordert ausdrücklich, dass digitale Zertifikate der Version 3 des Standards X.509 entsprechen. Da S/MIME ein anerkannter Standard für die Struktur von digitalen Zertifikaten zugrunde liegt, fördert der S/MIME-Standard die Verbreitung und damit auch Akzeptanz dieses Standards.

Eine PKI zur Unterstützung von S/MIME lässt sich auf zwei Arten einrichten: durch Übergabe der internen Zertifikatsinfrastruktur an eine externe Organisation oder durch Nutzung der Zertifikatsdienste in Microsoft Windows Server™ 2003.

Weitere Informationen zu den Zertifikatsdiensten in Windows Server 2003 erhalten Sie auf der Webseite [Public Key-Infrastruktur für Windows Server 2003](http://www.microsoft.com/windowsserver2003/technologies/pki/default.msp) (möglicherweise in englischer Sprache) unter [www.microsoft.com/windowsserver2003/technologies/pki/default.msp](http://www.microsoft.com/windowsserver2003/technologies/pki/default.msp).

Die PKI muss über einen Mechanismus zur Zertifikatssperrung verfügen. Die Zertifikatssperrung ist erforderlich, wenn ein Zertifikat abläuft oder möglicherweise von einem Angreifer manipuliert wurde. Durch das Sperren eines Zertifikats kann ein Administrator jedem, der dieses Zertifikat verwendet, den Zugriff verweigern. Jedes Zertifikat enthält den Speicherort seiner Zertifikatsperrliste (CRL, Certificate Revocation List).

Weitere Informationen zur Handhabung der Zertifikatssperrung finden Sie im Artikel [Zertifikatssperrung verwalten](http://technet2.microsoft.com/WindowsServer/en/Library/de0ae267-14e6-46f8-bcc7-8ac480889b951033.msp) (möglicherweise in englischer Sprache) unter <http://technet2.microsoft.com/WindowsServer/en/Library/de0ae267-14e6-46f8-bcc7-8ac480889b951033.msp>

#### Zertifikatvorlagen

Windows Server 2003 umfasst spezielle Zertifikatvorlagen für die Ausstellung digitaler Zertifikate zur Verwendung mit S/MIME. Drei multifunktionale Benutzerzertifikatvorlagen stehen für die Ausstellung von Zertifikaten für den sicheren E-Mail-Verkehr zur Verfügung:

- **Administrator.** Ermöglicht Administratoren die Verwendung eines Zertifikats für die Authentifizierung, für die EFS-Verschlüsselung (EFS = Encrypted File System), für sichere E-Mails sowie für die Signierung von Zertifikatsvertrauenslisten.
- **Benutzer.** Ermöglicht Benutzern die Verwendung eines Zertifikats für die Authentifizierung,

für die EFS-Verschlüsselung und für sichere E-Mails.

•**Smartcard-Benutzer.** Ermöglicht Benutzern die Anmeldung per Smartcard und die Signierung von E-Mails. Darüber hinaus bietet dieses Zertifikat Clientauthentifizierung.

**Hinweis** Zur Nutzung verbesserter Sicherheitsfunktionen empfiehlt Microsoft ausdrücklich die Aktualisierung einer vorhandenen Windows Server 2003-PKI auf eine Windows Server 2003-PKI mit Service Pack 1 (SP1).

Weitere Informationen zu Zertifikatvorlagen finden Sie im Artikel [Zertifikatvorlagen](http://technet2.microsoft.com/windowsserver/en/library/7D82B420-10EF-4F20-A56F-17EE7EE352D21033.msp) (möglicherweise in englischer Sprache) im Microsoft TechNet unter <http://technet2.microsoft.com/windowsserver/en/library/7D82B420-10EF-4F20-A56F-17EE7EE352D21033.msp>.

### Active Directory

Active Directory ist eine Schlüsselkomponente für die Implementierung von S/MIME-Zertifikaten. Um Benutzern Zertifikate zur Verwendung mit E-Mail-Diensten zur Verfügung zu stellen, kann ein Administrator die automatische Registrierungsfunktion für Gruppenrichtlinien von Active Directory nutzen. Unter Windows Server 2003 verfügt Active Directory ausserdem über integrierte Unterstützung für die Nutzung als PKI-Verzeichnis für verschiedene E-Mail-Clients von Microsoft, z. B. Outlook, Outlook Express und Outlook Web Access (OWA) mit S/MIME, sowie die Möglichkeit, Benutzerkonten Zertifikaten zuzuordnen.

Weitere Informationen zur Zertifikatszuordnung finden Sie im Artikel [Zuordnen von Zertifikaten zu Benutzerkonten](http://technet2.microsoft.com/WindowsServer/en/library/0539dcf5-82c5-48e6-be8a-57bca16c7e171033.msp?mfr=true) (möglicherweise in englischer Sprache) unter <http://technet2.microsoft.com/WindowsServer/en/library/0539dcf5-82c5-48e6-be8a-57bca16c7e171033.msp?mfr=true>.

### Exchange Server 2003

Durch Berücksichtigung einer Vielzahl von E-Mail-Clients können Exchange Server 2003-Administratoren die Bereitstellung ihren Bedürfnissen entsprechend anpassen. Die S/MIME-Unterstützung für Clients von Exchange Server 2003 ähnelt der generellen Client-Unterstützung, da alle unterstützten Clients von Kunden gleichzeitig verwendet werden können. Somit kann eine S/MIME-basierte Exchange Server 2003-Lösung etwa gleichzeitig Unterstützung für Outlook-Clients, OWA-Clients sowie Outlook Express-Clients, die POP3 verwenden, bieten. Da ein E-Mail-Client jedoch die Version 3 von S/MIME unterstützen und von Exchange Server unterstützt werden muss, sind nicht alle E-Mail-Clients auch als S/MIME-Clients geeignet.

S/MIME ist auch in Exchange Server 2000 sowie Exchange Server 2007 verfügbar.

### E-Mail-Clients

Exchange Server 2003 unterstützt S/MIME-Clients über die vorhandene Unterstützung für Clientprotokolle. Wenn ein unterstützter Client wiederum S/MIME unterstützt, ist er zur Verwendung mit Exchange Server 2003 geeignet. Unterstützt er hingegen die Version 3 von S/MIME nicht, kann er dennoch zum Lesen von Nachrichten verwendet werden, in die die Signatur direkt eingefügt ist.

### Microsoft Outlook 2003

Outlook unterstützt MAPI-basierte (Messaging Application Programming Interface) Verbindungen zu Exchange Server 2003. Darüber hinaus unterstützt Outlook POP3- und

IMAP4-Verbindungen. Exchange Server 2003 S/MIME lässt sich mit jeder Version von Outlook verwenden, die digitale Zertifikate gemäss Version 3 des Standards X.509 unterstützt. Die vollständige Unterstützung für digitale Zertifikate gemäss dieser Standardversion war erstmals in Outlook 2000 Service Release 1 (SR-1) gegeben.

### **POP3- und IMAP4-Clients**

Exchange Server 2003 bietet anhand der Internet-E-Mail-Standardprotokolle POP3 and IMAP4 vollständige Unterstützung für S/MIME-Clients, sofern der E-Mail-Client S/MIME der Version 2 oder 3 unterstützt. Wenn derartige E-Mail-Clients ausserdem POP3 oder IMAP4 unterstützen, können sie als E-Mail-Clients in einem Exchange Server 2003-Nachrichtensicherheitsystem verwendet werden. Da E-Mail-Clients mit Unterstützung des S/MIME-Standards alle Nachrichtensicherheitsdienste vollständig unterstützen, können sie mit vollem Funktionsumfang als E-Mail-Clients verwendet werden. Microsoft bietet sowohl in Outlook Express 5.5 und höher als auch in Outlook 2000 SR-1a und höher Unterstützung für Version 3 von S/MIME auf POP3- und IMAP4-Clients.

**Hinweis** Unterschiedliche Internetstandards und E-Mail-Clients haben unterschiedliche Anforderungen und Handhabungsweisen für Zertifikate der Version 3 von X.509. Berücksichtigen Sie bei der Entscheidung für unterstützte E-Mail-Clients derartige Anforderungen und mögliche Kompatibilitätsprobleme.

### **Erwägungen zum Einsatz**

Nach der Implementierung und Überprüfung der einzelnen Elemente dieser Lösung sollte eine Reihe kontinuierlicher Massnahmen zur Sicherstellung des erfolgreichen Einsatzes beim Schutz der Vertraulichkeit von E-Mails in Betracht gezogen werden.

Zu diesen Erwägungen gehören:

- das **Installieren von Service Packs**. Exchange Server SP2 enthält z. B. einen verbesserten Spamschutz. Weitere Informationen finden Sie im Artikel [Spamschutzverbesserungen in Exchange Server 2003 Service Pack 2](#) (möglicherweise in englischer Sprache) im TechNet unter <http://go.microsoft.com/fwlink/?linkid=55849>.
- das **Installieren aktueller Sicherheitsupdates**. Schützen Sie alle Ihre Server mit Aktualisierungen aus dem Microsoft Download Center.
- das **Einplanen technischer Herausforderungen**. Besuchen Sie regelmässig [Microsoft Update](#) unter <http://update.microsoft.com/>, um weitere Sicherheitsupdates für Exchange Server und Windows Server herunterzuladen und zu installieren.
- das **Ausführen von Microsoft Baseline Security Analyzer (MBSA)**. Durch das Herunterladen von MBSA können Sie ermitteln, ob möglicherweise Sicherheitsupdates auf Exchange Server 2003 fehlen.
- das **Verwenden von Microsoft Exchange Server Intelligent Message Filter**. Durch Kombination von Exchange Server Intelligent Message Filter mit Outlook 2003 wird die heuristische Nachrichtenfilterung auf Serverseite verbessert und damit das Spamaufkommen reduziert. Einzelheiten dazu, wie Intelligent Message Filter stets auf dem aktuellen Stand bleibt, erfahren Sie im englischsprachigen Artikel [The "Microsoft Exchange Server Intelligent Message Filter v2 Operations Guide" is now available](#) unter <http://support.microsoft.com/?kbid=907747>.
- das **Ausführen von Microsoft Exchange Server Best Practices Analyzer**. Dieses Tool, das kostenlos heruntergeladen werden kann, sammelt Konfigurationsdaten von jedem Server in der Topologie und analysiert sie automatisch. Der resultierende Bericht enthält Einzelheiten zu kritischen Konfigurationsproblemen, zu potenziellen Problemen sowie zu nicht-standardmässigen Produkteinstellungen. Durch Berücksichtigung der Empfehlungen lassen

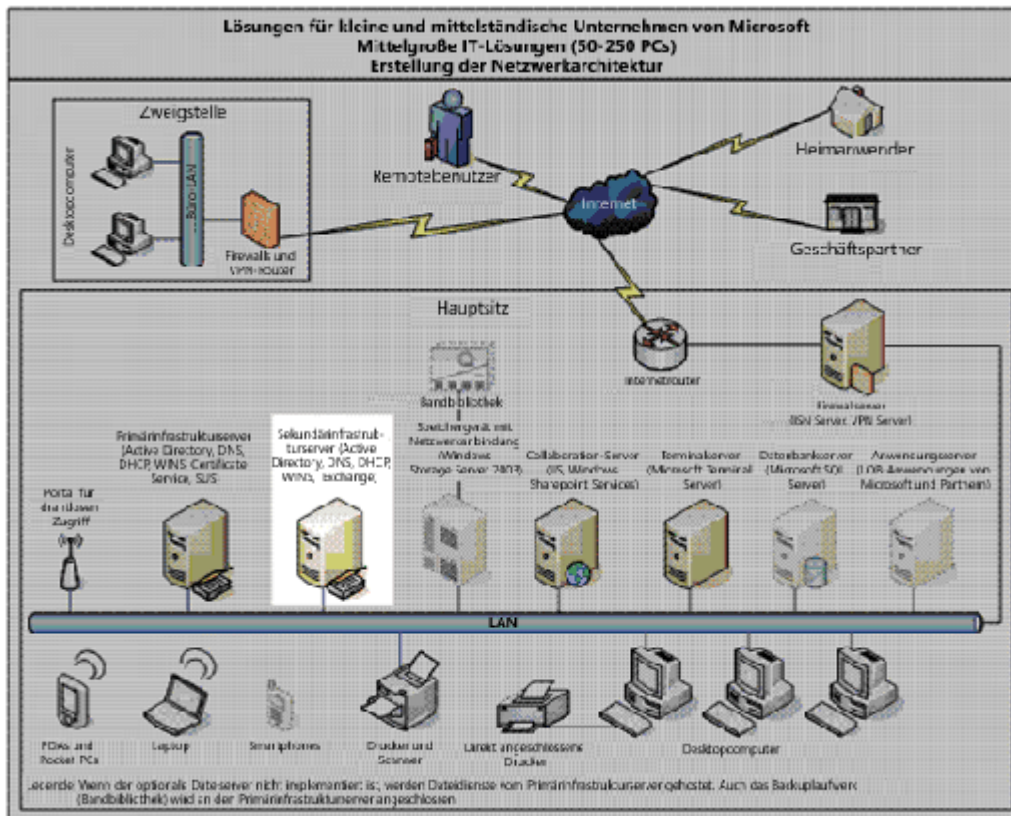
sich Leistung, Skalierbarkeit, Zuverlässigkeit und Verfügbarkeit verbessern.

- das **regelmässige Überprüfen auf aktualisierte Sicherheitsinformationen**. Technische Sicherheitsanweisungen finden Sie auf der Seite [Technische Bibliothek für Exchange Server 2003: Sicherheit und Schutz](http://www.microsoft.com/technet/prodtechnol/exchange/2003/security.mspx) unter [www.microsoft.com/technet/prodtechnol/exchange/2003/security.mspx](http://www.microsoft.com/technet/prodtechnol/exchange/2003/security.mspx).

[☐ Zum Seitenanfang](#)

## Szenario zum Schutz der Vertraulichkeit von E-Mails

Das folgende Verfahren zum Schutz der Vertraulichkeit von E-Mails bezieht sich auf Szenarien für kleine und mittelgrosse Unternehmen ähnlich dem in der Abbildung dargestellten.



**Abbildung 1. E-Mail-Dienste in mittelgrossen IT-Umgebungen**

[Bild in voller Grösse anzeigen](#)

Die Vertraulichkeit ist insbesondere für Benutzer erforderlich, die E-Mails an Empfänger sowohl an internen als auch an externen Standorten senden. Um dies zu erreichen, richten Sie Exchange Server 2003 und die E-Mail-Clients zur Unterstützung von S/MIME ein.

### Hilfe beim Schutz der Vertraulichkeit von E-Mails

Die folgenden Schritte geben die zum Schutz der Vertraulichkeit von E-Mails erforderlichen Konfigurationsverfahren wieder.

#### Bevor Sie beginnen

Vor der Implementierung von S/MIME in einer Exchange Server 2003-Umgebung müssen Sie die Auswirkung auf Nachrichten verstehen, wenn eines der folgenden Elemente bereits implementiert wurde:

- Ereignissenken
- Antivirensoftware

#### **Ereignissenken und digital signierte Nachrichten**

Ereignissenken können Aktionen auf E-Mail-Nachrichten durchführen, wenn sie von Exchange Server verarbeitet werden. Einige Ereignissenken ändern beispielsweise zu Nachrichtenfilterungszwecken den Inhalt und die Kopfzeile einer E-Mail-Nachricht. Eine gültige digitale Signatur bedeutet, dass eine Nachricht während der Übertragung nicht geändert wurde. Eine Ereignissenke, die eine E-Mail-Nachricht ändert, macht digitale Signaturen ungültig. Wenn die Nachricht beim Empfänger eingeht, ist die digitale Signatur ungültig, da die Nachricht nach der Signierung durch den Absender von der Ereignissenke geändert wurde.

#### **Antivirensoftware und S/MIME-Nachrichten**

Bei Verwendung einer serverbasierten Antivirenlösung verhindert die Verschlüsselung, die die Vertraulichkeit des Texts und der Anhänge von Nachrichten vor unberechtigten Benutzern schützt, dass die Antivirensoftware Nachrichten und Anhänge auf Viren überprüfen kann. Da die Antivirensoftware keine Nachrichten überprüfen kann, könnte eine verschlüsselte Nachricht einen Virus als Anhang enthalten. Treffen Sie geeignete Massnahmen in Übereinstimmung mit Ihren Sicherheitsrichtlinien zur Behandlung dieses Risiken.

Entdeckt ein Antivirenprogramm einen Virus in einer digital signierten E-Mail und entfernt ihn, kann die digitale Signatur dadurch ungültig werden, da die Nachricht während der Übermittlung geändert wurde. Auch wenn es sich um keine schädliche Änderung handelt, wird die Nachricht als geändert identifiziert und die digitale Signatur dementsprechend ungültig.

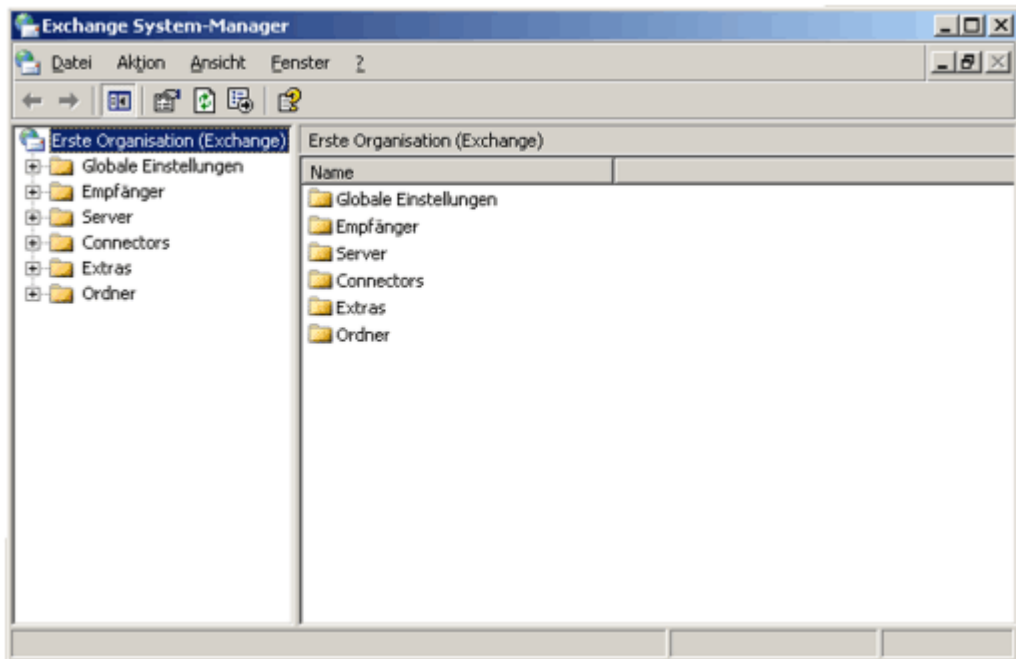
#### **Konfiguration von Exchange Server 2003 zur Wahrung der Vertraulichkeit von E-Mails**

Damit Exchange Server S/MIME-E-Mails speichern kann, muss die Nachrichtenspeicherung lediglich für die Verarbeitung von S/MIME-Signaturen konfiguriert sein. Da sowohl der Posteingang eines Benutzers als auch öffentliche Ordner als Speicherorte für S/MIME-Nachrichten in Frage kommen, können beide Speicherorte zur Aufnahme von Nachrichten mit S/MIME-Signaturen konfiguriert werden.

1.Melden Sie sich mit einem Konto an, das zu den zwei folgenden Gruppen gehört:

- Administratorengruppe auf dem lokalen Computer
- eine Gruppe, der mindestens die Rolle „Exchange-Administrator - Nur Ansicht“ auf administrativer Gruppenebene zugeordnet wurde

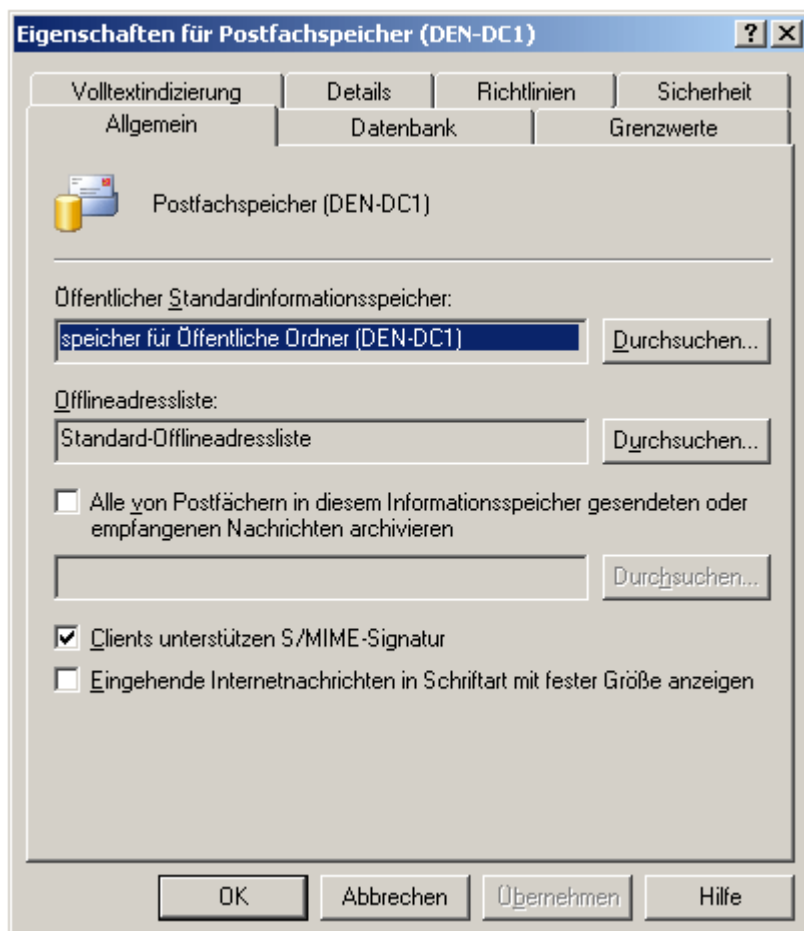
2.Klicken Sie auf **Start**, zeigen Sie auf **Alle Programme** und danach auf **Microsoft Exchange**, und klicken Sie auf **System-Manager**. Der Exchange-System-Manager (siehe Abbildung) wird angezeigt.



[Bild in voller Grösse anzeigen](#)

3. Klicken Sie auf **Server**, auf `<servername>` und danach auf **Speichergruppe**. Klicken Sie mit der rechten Maustaste auf **Postfachspeicher**, und wählen Sie **Eigenschaften**.

Aktivieren Sie auf der Seite **Eigenschaften** wie abgebildet das Kontrollkästchen **Clients unterstützen S/MIME-Signatur**.



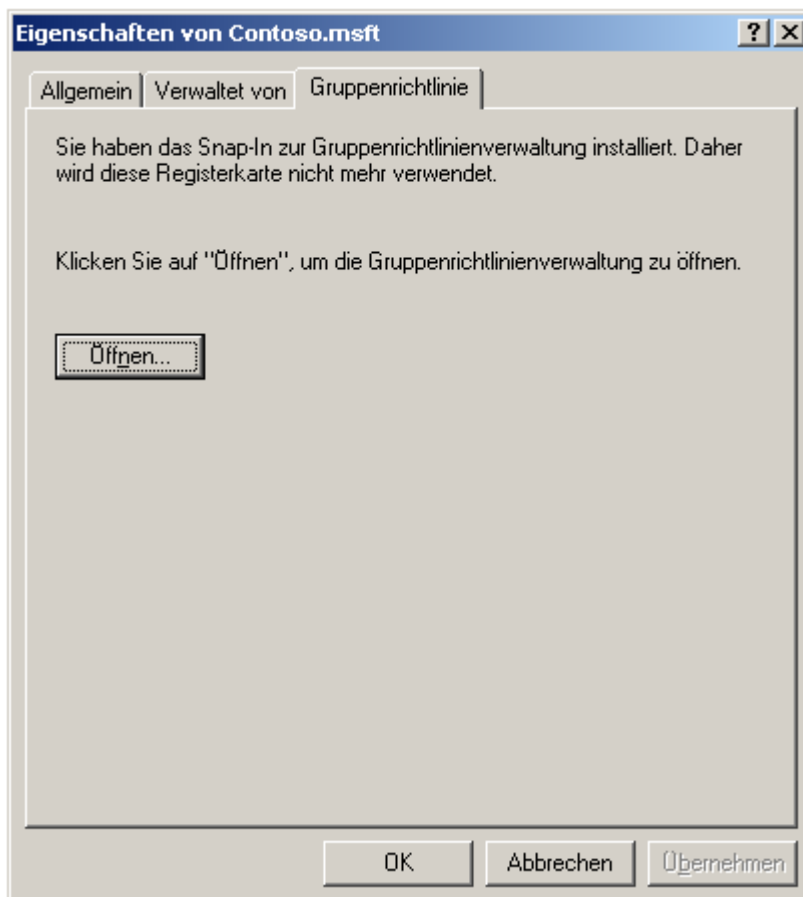
## Bereitstellung von digitalen Zertifikaten für S/MIME mit automatischer Registrierungsfunktion

Mit der automatischen Registrierungsfunktion können Clients automatisch Zertifikatsanforderungen bei einer Zertifizierungsstelle einreichen und ausgestellte Zertifikate abrufen und speichern. Microsoft Windows® XP- und Windows Server™ 2003-Clients können die automatische Registrierungsfunktion sowohl für Benutzer- als auch für Computerzertifikate nutzen. Die automatische Registrierungsfunktion reduziert die Gesamtbetriebskosten durch Reduzierung der mit der Registrierung und Erneuerung von Zertifikaten verbundenen Kosten.

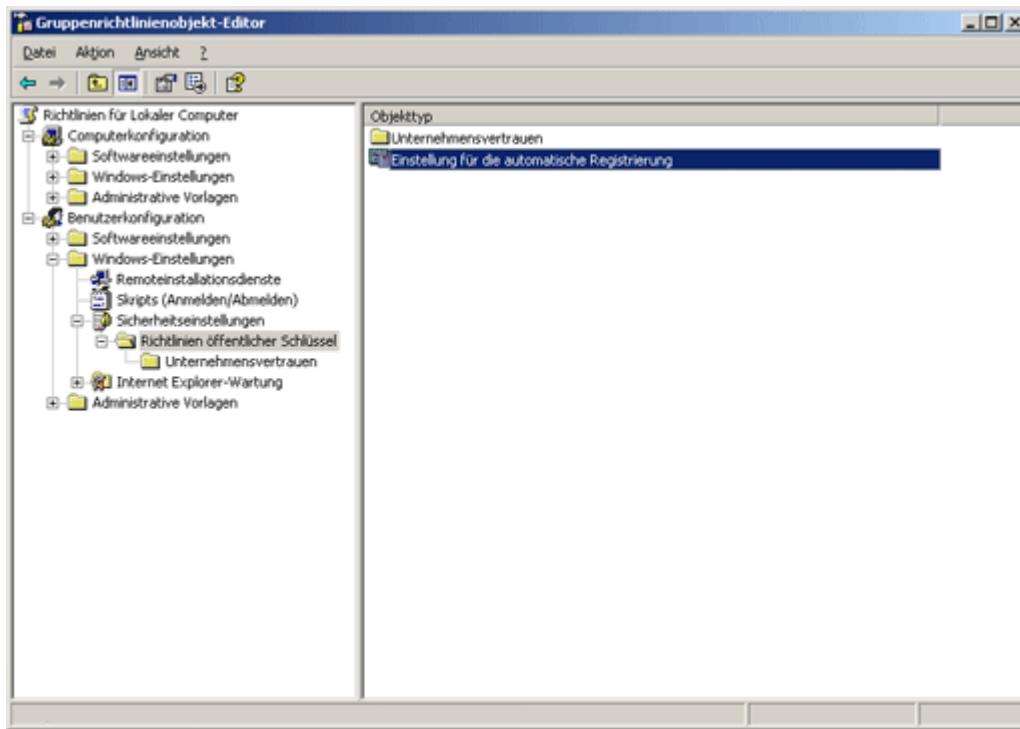
### So aktivieren Sie Einstellungen für die automatische Registrierung

1. Melden Sie sich mit Administratorrechten an.
2. Öffnen Sie unter „Verwaltung“ die Option „Active Directory-Benutzer und -Computer“.
3. Klicken Sie in der Konsolenstruktur mit der rechten Maustaste auf die Domäne, in der die Einstellungen für die automatische Registrierung implementiert werden sollen, und klicken Sie auf „Eigenschaften“.

Für die automatische Registrierungsfunktion muss das Gruppenrichtlinienobjekt (GPO) entweder mit der Domäne oder der Organisationseinheit verbunden sein, in der das Benutzer- bzw. Computerkonto vorhanden ist.



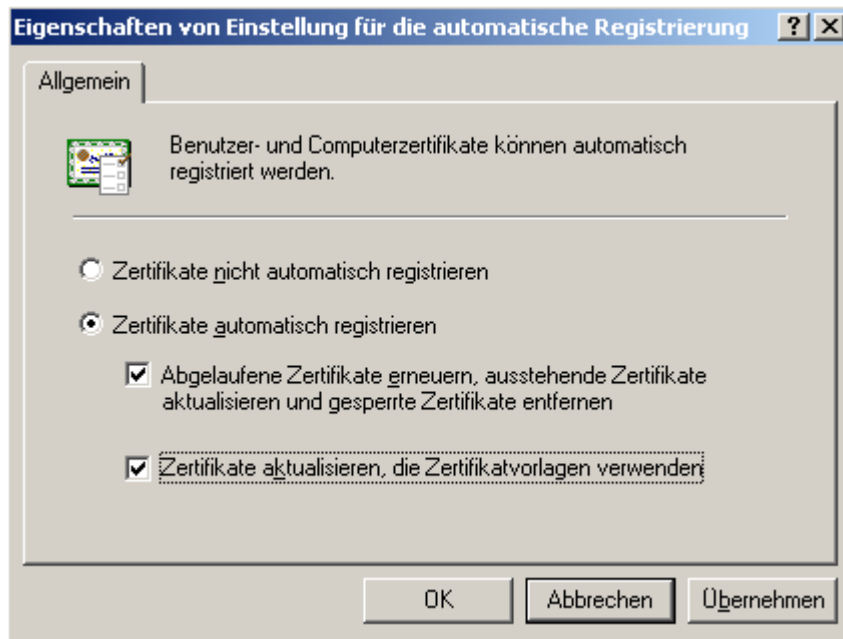
4. Klicken Sie im Dialogfeld **Eigenschaften von Domänenname** auf der Registerkarte **Gruppenrichtlinie** auf **Öffnen**, um die Group Policy Management Console zu öffnen.
5. Erstellen Sie ein mit der Domäne verbundenes Gruppenrichtlinienobjekt.
6. Erweitern Sie in der Konsolenstruktur des Gruppenrichtlinienobjekt-Editors den Eintrag **Benutzerkonfiguration**.
7. Erweitern Sie in der Konsolenstruktur wie abgebildet **Windows-Einstellungen**, dann **Sicherheitseinstellungen**, und klicken Sie auf **Richtlinien für öffentliche Schlüssel**.



[Bild in voller Grösse anzeigen](#)

8. Doppelklicken Sie im Detailbereich auf **Einstellung für die automatische Registrierung**. Vergewissern Sie sich, dass im Dialogfeld **Einstellung für die automatische Registrierung** die folgenden Einstellungen wie abgebildet ausgewählt sind:

- **Zertifikate automatisch registrieren**. Mit dieser Einstellung wird die automatische Registrierung von Zertifikaten für die Organisationseinheit des verbundenen Gruppenrichtlinienobjekts aktiviert.
- Das Kontrollkästchen **Abgelaufene Zertifikate erneuern, ausstehende Zertifikate aktualisieren und gesperrte Zertifikate entfernen**. Mit dieser Einstellung wird die automatische Registrierung bei Zertifikatserneuerungen, für die Ausstellung ausstehender Zertifikate sowie für die Entfernung gesperrter Zertifikate aus dem Zertifikatspeicher aktiviert.
- Das Kontrollkästchen **Zertifikate aktualisieren, die Zertifikatvorlagen verwenden**. Mit dieser Einstellung wird die automatische Registrierung für veraltete Zertifikatvorlagen aktiviert.



9. Klicken Sie auf **OK**.

Die automatische Registrierung ist nun für die Organisationseinheit des verbundenen Gruppenrichtlinienobjekts aktiviert.

Die Einstellungen für die automatische Registrierung werden bei der nächsten Anwendung des Gruppenrichtlinienobjekts auf den Benutzer gültig. Die automatische Benutzerregistrierung wird bei einer interaktiven Anmeldung des Benutzers sowie in den Aktualisierungsintervallen der Gruppenrichtlinie ausgelöst.

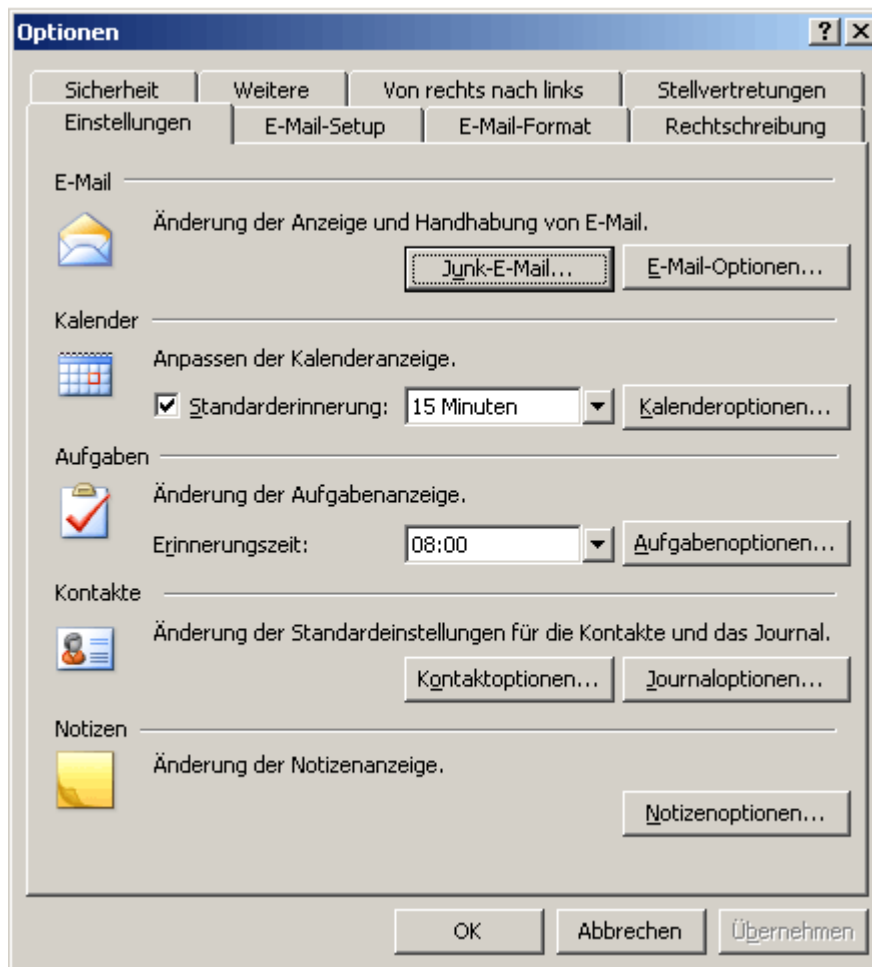
Sie können die Einstellungen für das Gruppenrichtlinienobjekt auf einem Client, auf dem Windows XP oder Windows Server 2003 ausgeführt wird, durch Erzwingen einer Gruppenrichtlinienaktualisierung manuell aktualisieren. Dies kann auch durch Ausführen von **GPUpdate /force** an einer Eingabeaufforderung auf der Zielarbeitsstation erfolgen.

### **Konfiguration von Outlook 2003 zur Wahrung der Vertraulichkeit von E-Mails**

Um eine verschlüsselte E-Mail-Nachricht versenden zu können, muss der Empfänger bereits über ein digitales Zertifikat verfügen. Bei dem Versuch, einem Benutzer ohne digitales Zertifikat eine verschlüsselte E-Mail-Nachricht zuzustellen, wird eine Fehlermeldung ausgegeben. Vergewissern Sie sich, dass Sie die Anleitungen unter „Bereitstellung von digitalen Zertifikaten für S/MIME mit automatischer Registrierungsfunktion“ weiter oben für alle Testbenutzer befolgt haben, bevor Sie E-Mail-Nachrichten an sie versenden.

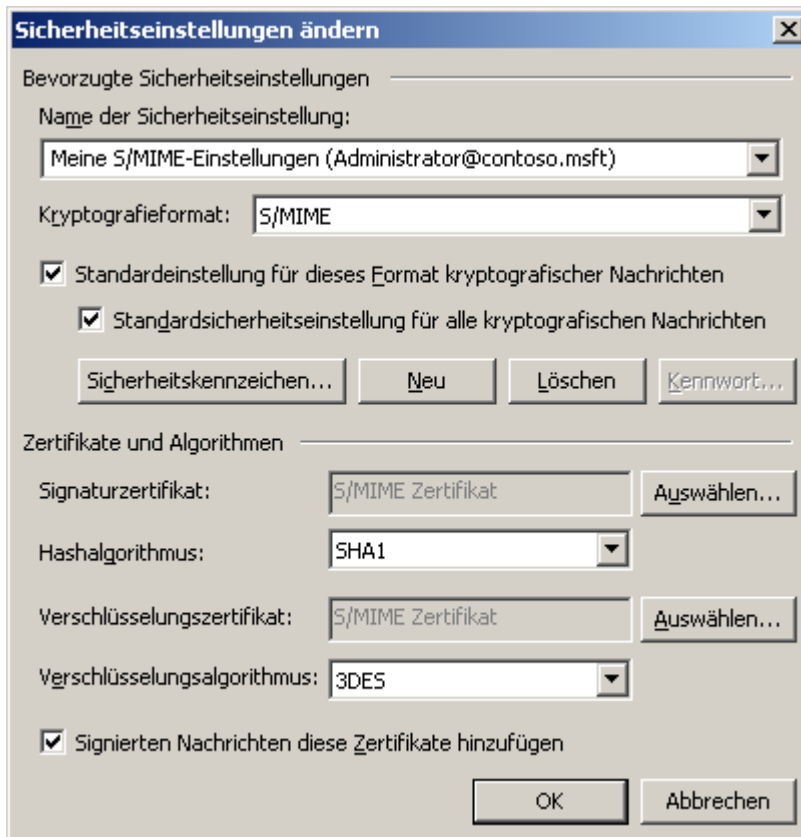
### **So konfigurieren Sie Outlook zur Wahrung der Vertraulichkeit von E-Mails**

1. Melden Sie sich bei Ihrer Domäne als Mitglied der Gruppe der Domänenbenutzer an.
2. Klicken Sie auf **Start**, zeigen Sie auf **Alle Programme** und danach auf **Microsoft Office**, und klicken Sie abschliessend auf **Microsoft Office Outlook 2003**.
3. Klicken Sie auf das Menü **Extras** und anschliessend auf **Optionen**. Das folgende Dialogfeld wird angezeigt.



4. Klicken Sie auf die Registerkarte **Sicherheit** und anschliessend auf **Einstellungen**.

5. Das Dialogfeld **Sicherheitseinstellungen ändern** enthält Standardinformationen. Klicken Sie auf **OK**, um die Standardwerte wie abgebildet zu übernehmen.

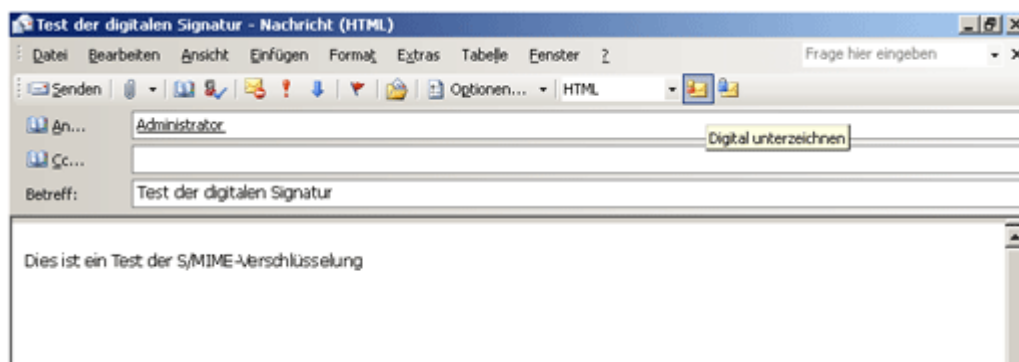


6. Klicken Sie auf **OK**, um das Dialogfeld **Optionen** zu schliessen.

Damit wurde Outlook für die Wahrung der Vertraulichkeit von E-Mails konfiguriert.

### So versenden Sie eine digital signierte Nachricht mit Outlook

1. Melden Sie sich bei Ihrer Domäne als Mitglied der Gruppe der Domänenbenutzer an.
2. Klicken Sie auf **Start**, zeigen Sie auf **Alle Programme** und danach auf **Microsoft Office**, und klicken Sie abschliessend auf **Microsoft Office Outlook 2003**.
3. Klicken Sie auf **Neu**, um eine neue Nachricht zu verfassen.
4. Fügen Sie einen Empfänger für die Testnachricht hinzu, und füllen Sie die Nachrichtfelder aus.
5. Achten Sie darauf, die Schaltfläche **Diese Nachricht digital signieren** auszuwählen. Da Sie lediglich die digitale Signatur testen möchten, wählen Sie die Schaltfläche **Nachrichteninhalte und Anlagen verschlüsseln** nicht aus.



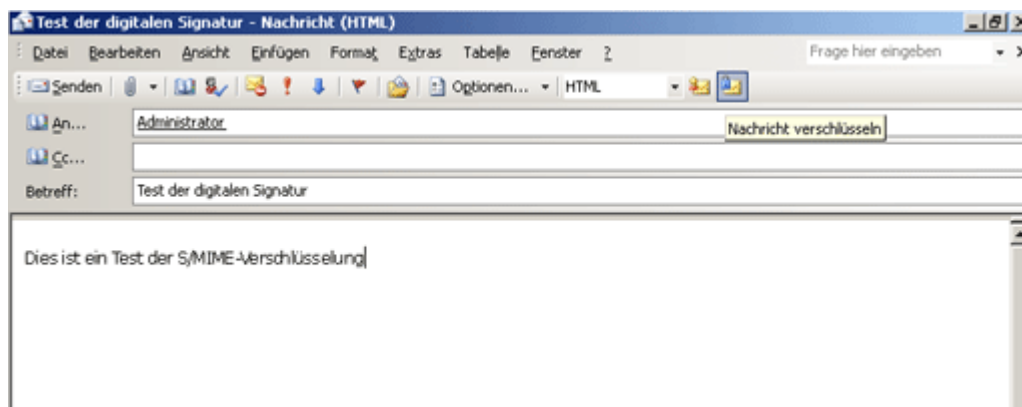
[Bild in voller Grösse anzeigen](#)

6. Klicken Sie auf **Senden**.

Damit wurde die digital signierte Nachricht an den Empfänger versendet, der daraufhin die digitale Signatur überprüfen kann.

### So versenden Sie eine verschlüsselte Nachricht mit Outlook

1. Melden Sie sich bei Ihrer Domäne als Mitglied der Gruppe der Domänenbenutzer an.
2. Klicken Sie auf **Start**, zeigen Sie auf **Alle Programme** und danach auf **Microsoft Office**, und klicken Sie abschliessend auf **Microsoft Office Outlook 2003**.
3. Klicken Sie auf **Neu**, um eine neue Nachricht zu verfassen.
4. Fügen Sie einen Empfänger für die Testnachricht hinzu, und füllen Sie die Nachrichtfelder aus.
5. Vergewissern Sie sich, dass auf der Symbolleiste die Schaltfläche **Nachrichteninhalte und Anlagen verschlüsseln** ausgewählt ist. Da Sie lediglich die Verschlüsselung testen möchten, wählen Sie die Schaltfläche **Diese Nachricht digital signieren** nicht aus.



[Bild in voller Grösse anzeigen](#)

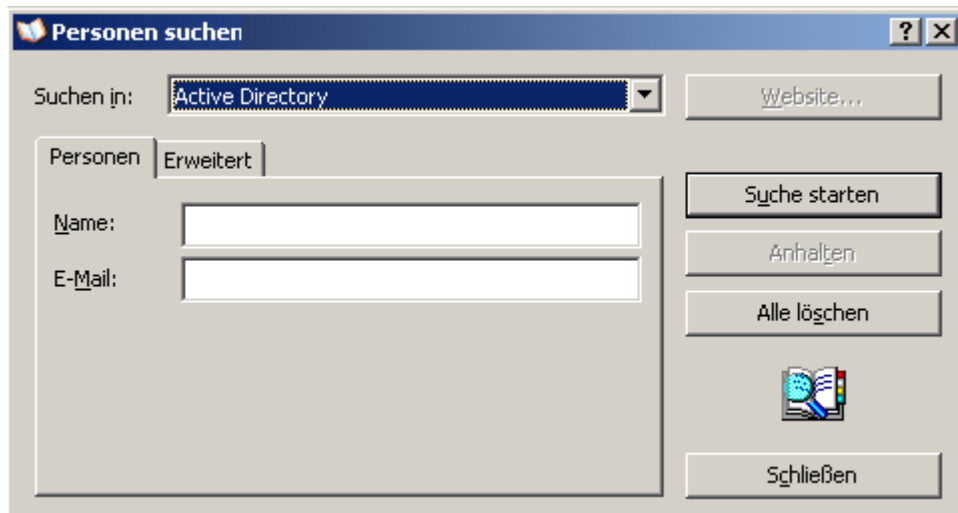
Damit wurde die verschlüsselte Nachricht an den Empfänger versendet, der diese öffnen und lesen kann.

### Konfiguration von Outlook Express zur Wahrung der Vertraulichkeit von E-Mails

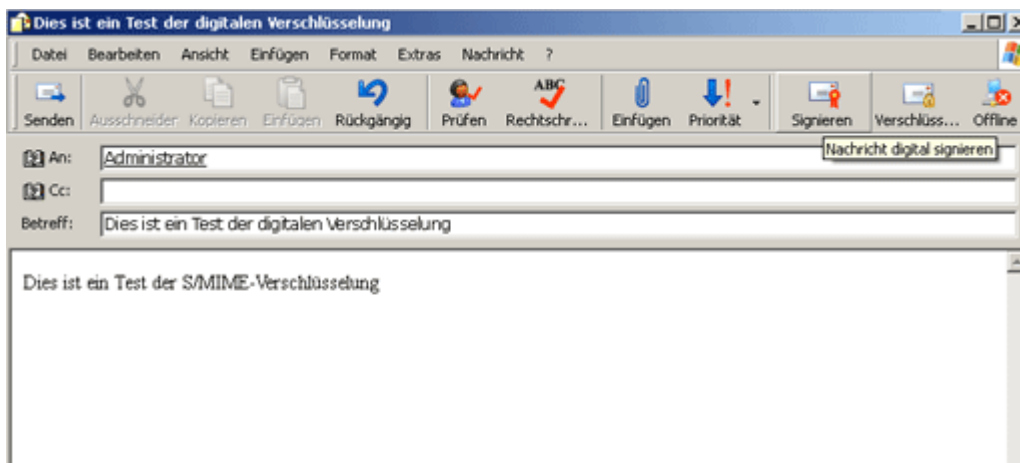
Um eine verschlüsselte E-Mail-Nachricht versenden zu können, muss der Empfänger bereits über ein digitales Zertifikat verfügen. Bei dem Versuch, einem Benutzer ohne digitales Zertifikat eine verschlüsselte E-Mail-Nachricht zuzustellen, wird eine Fehlermeldung ausgegeben. Vergewissern Sie sich, dass Sie die Anleitungen unter „Bereitstellung von digitalen Zertifikaten für S/MIME mit automatischer Registrierungsfunktion“ weiter oben für alle Testbenutzer befolgt haben, bevor Sie E-Mail-Nachrichten an sie versenden.

### So versenden Sie eine digital signierte Nachricht mit Outlook Express

1. Melden Sie sich bei Ihrer Domäne als Mitglied der Gruppe der Domänenbenutzer an.
2. Klicken Sie auf **Start**, zeigen Sie auf **Alle Programme**, und klicken Sie dann auf **Outlook Express**.
3. Geben Sie bei Aufforderung das Kennwort des Benutzers ein.
4. Klicken Sie zum Erstellen einer neuen Nachricht auf **Neue E-Mail**.
5. Klicken Sie auf **An**, um einen Empfänger aus Active Directory hinzuzufügen.
6. Klicken Sie unter **Namen eingeben oder auswählen** auf **Suchen**. Das folgende Dialogfeld wird angezeigt.



7. Klicken Sie in der Liste **Suchen in** auf **Active Directory**, geben Sie im Feld **Name** den Namen des Empfängers ein, und klicken Sie danach auf **Suche starten**.
8. Markieren Sie den Namen, und klicken Sie auf **An**.
9. Klicken Sie auf **OK**, um das Dialogfeld **Empfänger auswählen** zu schliessen.
10. Auf der Symbolleiste befinden sich zwei neue Symbole: eines zum Verschlüsseln und eines zum Signieren von Nachrichten. Stellen Sie sicher, dass die Schaltfläche **Signieren** wie abgebildet ausgewählt ist. Da Sie lediglich die digitale Signatur testen möchten, wählen Sie die Schaltfläche **Verschlüsseln** nicht aus.



[Bild in voller Grösse anzeigen](#)

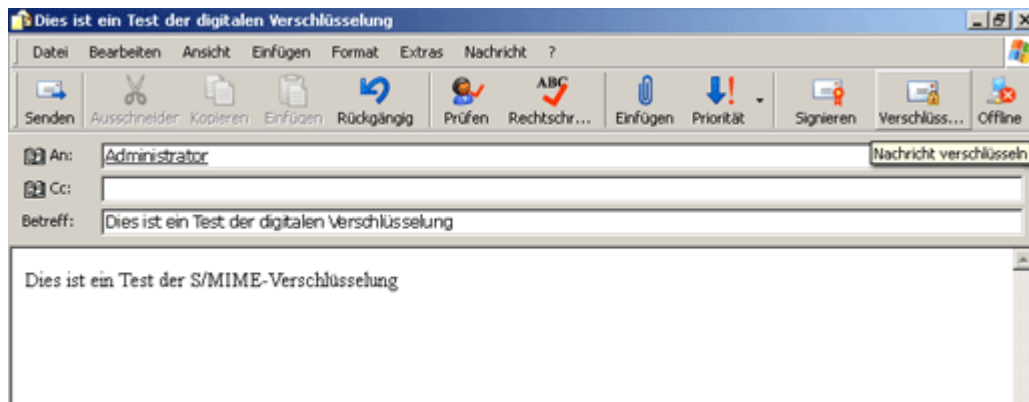
11. Klicken Sie auf **Senden**.

Damit wurde die digital signierte Nachricht an den Empfänger versendet, der daraufhin die digitale Signatur überprüfen kann.

### So versenden Sie eine verschlüsselte Nachricht mit Outlook Express

1. Melden Sie sich bei Ihrer Domäne als Mitglied der Gruppe der Domänenbenutzer an.
2. Klicken Sie auf **Start**, zeigen Sie auf **Alle Programme**, und klicken Sie dann auf **Outlook Express**.
3. Geben Sie bei Aufforderung das Kennwort des Benutzers ein.
4. Klicken Sie zum Erstellen einer neuen Nachricht auf **Neue E-Mail**.
5. Klicken Sie auf **An**, um einen Empfänger aus Active Directory hinzuzufügen.
6. Klicken Sie unter **Namen eingeben oder auswählen** auf **Suchen**.
7. Klicken Sie in der Liste **Suchen in** auf **Active Directory**, geben Sie im Feld **Name** den Empfänger ein, und klicken Sie danach auf **Suche starten**.

8. Markieren Sie den Namen, und klicken Sie auf **An**.
9. Klicken Sie auf **OK**, um das Dialogfeld **Empfänger auswählen** zu schliessen.
10. Stellen Sie sicher, dass die Schaltfläche **Verschlüsseln** auf der Symbolleiste wie abgebildet ausgewählt ist. Da Sie lediglich die Verschlüsselung testen möchten, wählen Sie die Schaltfläche **Signieren** nicht aus.



[Bild in voller Grösse anzeigen](#)

11. Klicken Sie auf **Senden**.

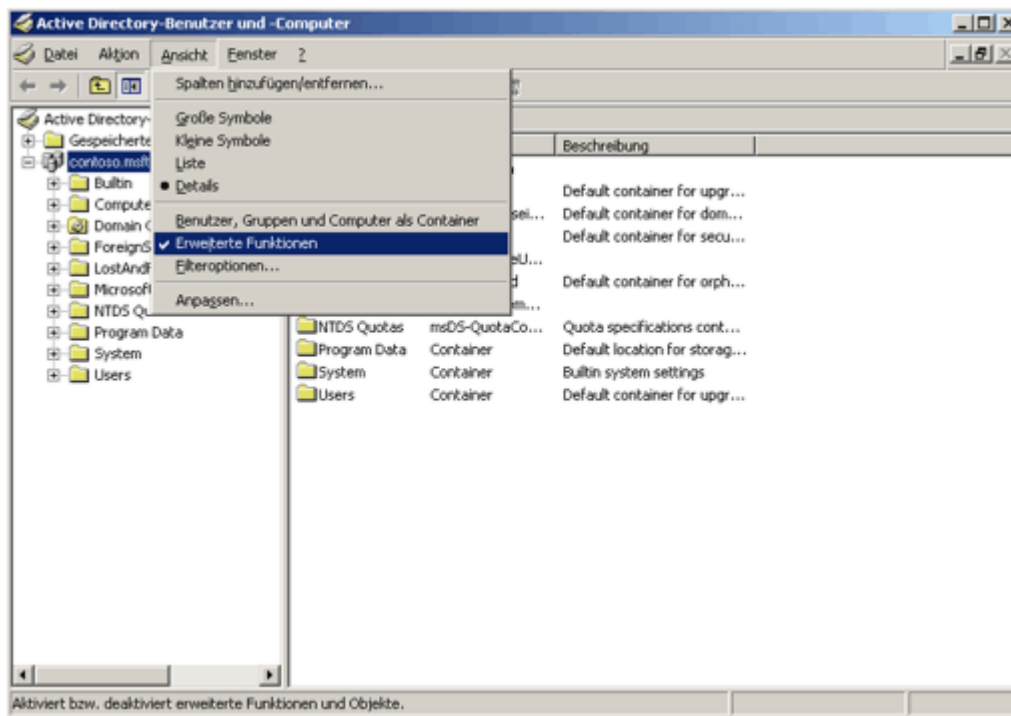
Damit wurde die verschlüsselte Nachricht an den Empfänger versendet, der diese öffnen und lesen kann.

### **Überprüfen, ob ein Benutzer ein digitales Zertifikat für S/MIME in Active Directory besitzt**

Mit „Active Directory-Benutzer und -Computer“ können Sie überprüfen, ob Active Directory-Benutzerkonten über ein digitales Zertifikat für S/MIME verfügen.

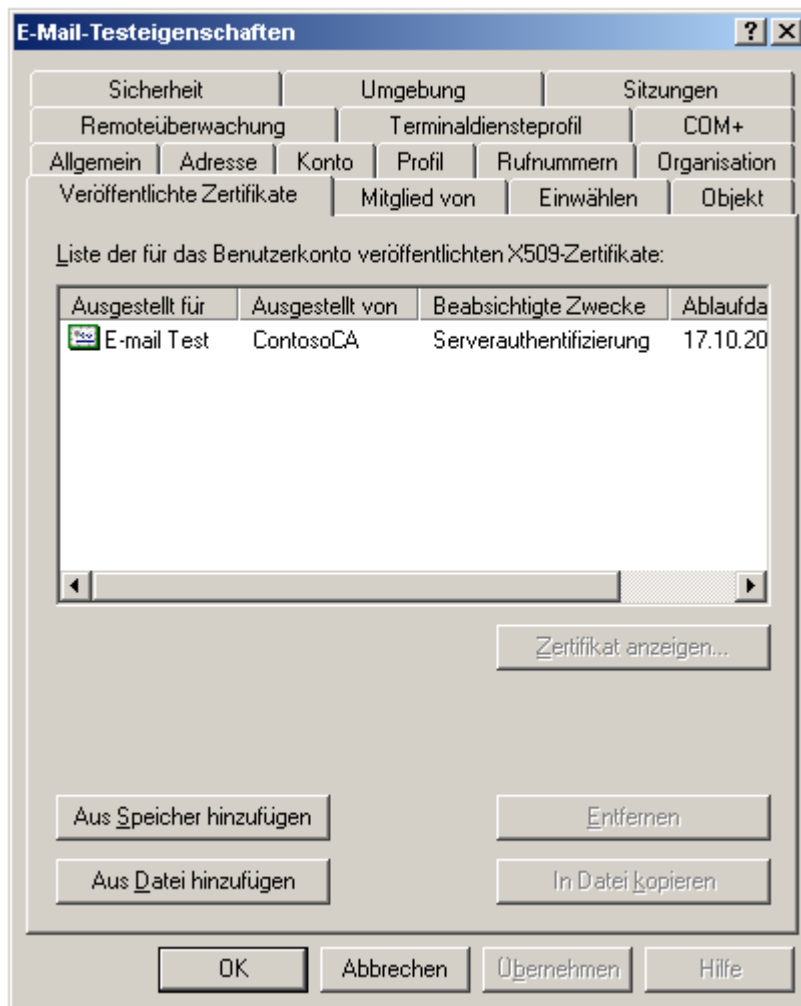
### **So überprüfen Sie, ob das Zertifikat zum Active Directory-Konto eines Benutzers hinzugefügt wurde**

1. Melden Sie sich bei Ihrer Domäne als Mitglied der Gruppe der Zertifizierungsstellenadministratoren an.
2. Klicken Sie auf **Start**, zeigen Sie auf **Alle Programme** und auf **Verwaltung**, und klicken Sie dann auf **Active Directory-Benutzer und -Computer**.
3. Klicken Sie wie abgebildet auf **Anzeigen** und danach auf **Erweiterte Funktionen**.



#### [Bild in voller Grösse anzeigen](#)

4. Klicken Sie im linken Fensterbereich auf den Ordner **Benutzer**.
5. Doppelklicken Sie im rechten Fensterbereich auf einen der Testbenutzer.
6. Klicken Sie auf die Registerkarte **Veröffentlichte Zertifikate**.
7. In der **Liste der für das Benutzerkonto veröffentlichten X509-Zertifikate** (siehe Abbildung) werden das digitale Zertifikat des Benutzers aus der Windows-Zertifizierungsstelle sowie alle weiteren für diesen Benutzer in Active Directory gespeicherten digitalen Zertifikate angezeigt.



Damit ist die Überprüfung, ob das Zertifikat zum Active Directory-Benutzerkonto hinzugefügt wurde, abgeschlossen.

### Überprüfen, ob Exchange Server für die Wahrung der Vertraulichkeit von E-Mails konfiguriert wurde

Sie können mit Exchange Server System Manager überprüfen, ob Exchange Server zur Unterstützung von Clients, die S/MIME verwenden, konfiguriert wurde.

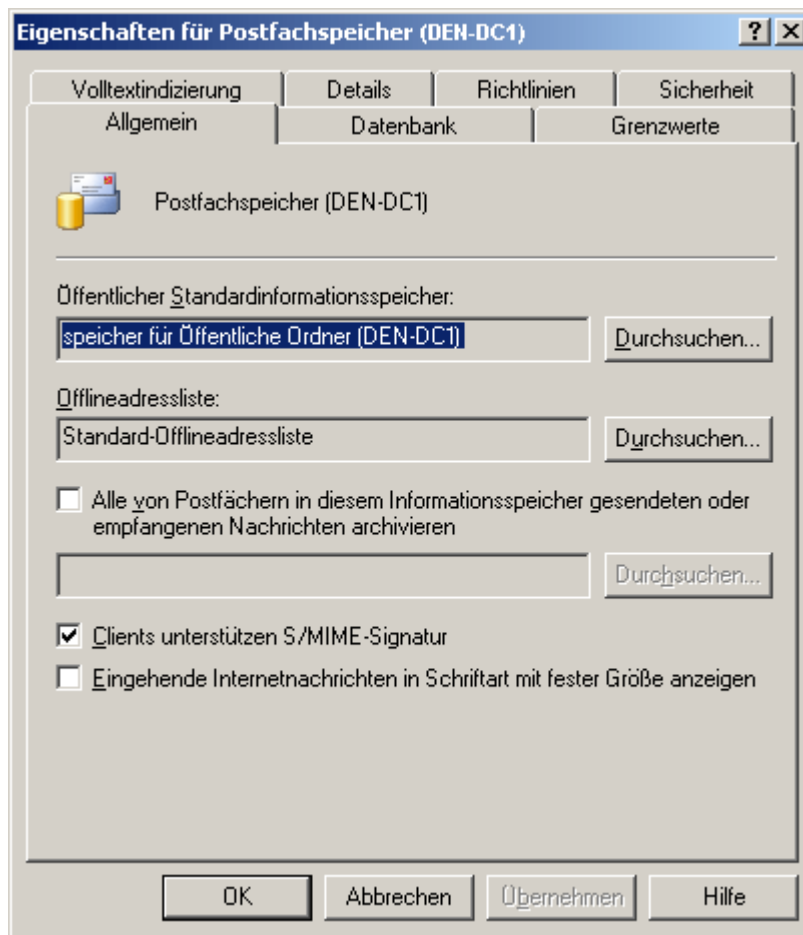
1. Melden Sie sich mit einem Konto an, das zu den zwei folgenden Gruppen gehört:

- Administratorengruppe auf dem lokalen Computer
- eine Gruppe, der mindestens die Rolle „Exchange-Administrator - Nur Ansicht“ auf administrativer Gruppenebene zugeordnet wurde

2. Klicken Sie auf **Start**, zeigen Sie auf **Alle Programme** und danach auf **Microsoft Exchange**, und klicken Sie auf **System-Manager**.

3. Klicken Sie auf **Server**, auf `<servername>` und danach auf **Speicherguppe**. Klicken Sie mit der rechten Maustaste entweder auf **Postfachspeicher** oder auf **Informationsspeicher für Öffentliche Ordner**, und klicken Sie danach auf **Eigenschaften**.

4. Überprüfen Sie auf der Seite **Eigenschaften**, ob das Kontrollkästchen **Clients unterstützen S/MIME-Signatur** auf der Registerkarte **Allgemein** wie abgebildet aktiviert ist.



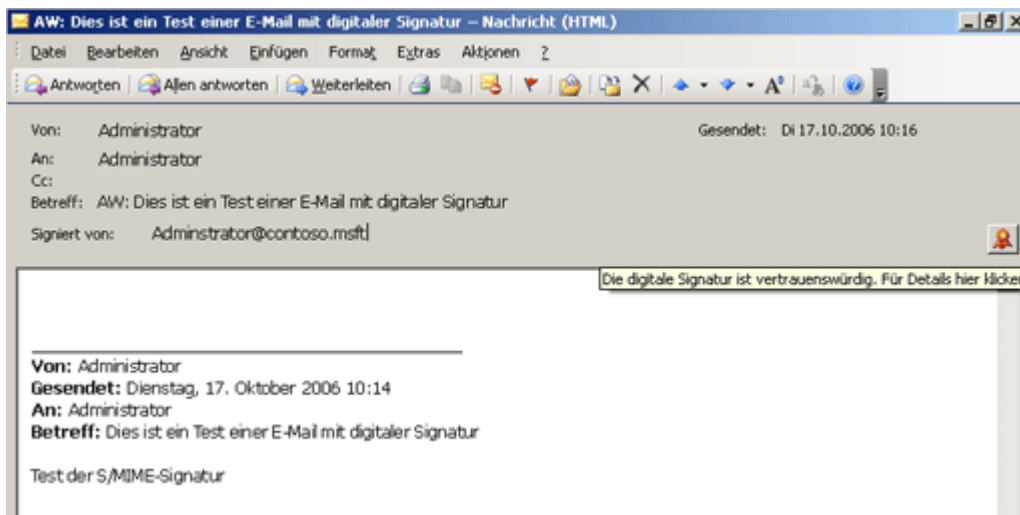
Damit ist die Überprüfung, ob Exchange Server zur Wahrung der Vertraulichkeit von E-Mails konfiguriert wurde, abgeschlossen.

### **Überprüfung, ob Outlook 2003 zur Wahrung der Vertraulichkeit konfigurierte E-Mails empfangen kann**

Sie können mit Outlook 2003 überprüfen, ob Sie E-Mail-Nachrichten empfangen können, die für digitale Signaturen und Verschlüsselung konfiguriert wurden.

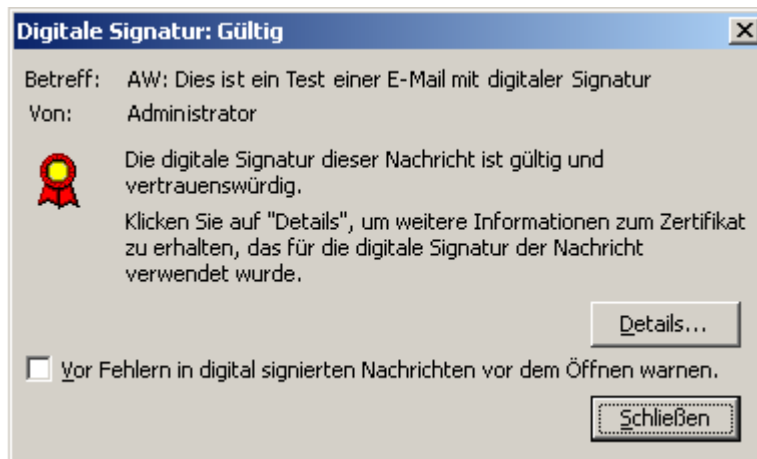
### **So zeigen Sie eine digital signierte Nachricht in Outlook an**

1. Melden Sie sich bei Ihrer Domäne als Mitglied der Gruppe der Domänenbenutzer an.
2. Klicken Sie auf **Start**, zeigen Sie auf **Alle Programme** und danach auf **Microsoft Office**, und klicken Sie abschliessend auf **Microsoft Office Outlook 2003**.
3. Doppelklicken Sie im Posteingang auf die digital signierte Testnachricht.
4. Wenn die Nachricht geöffnet wird, klicken Sie auf die Schaltfläche **Signatur überprüfen** (siehe Abbildung), um die Signatur zu überprüfen.



### [Bild in voller Grösse anzeigen](#)

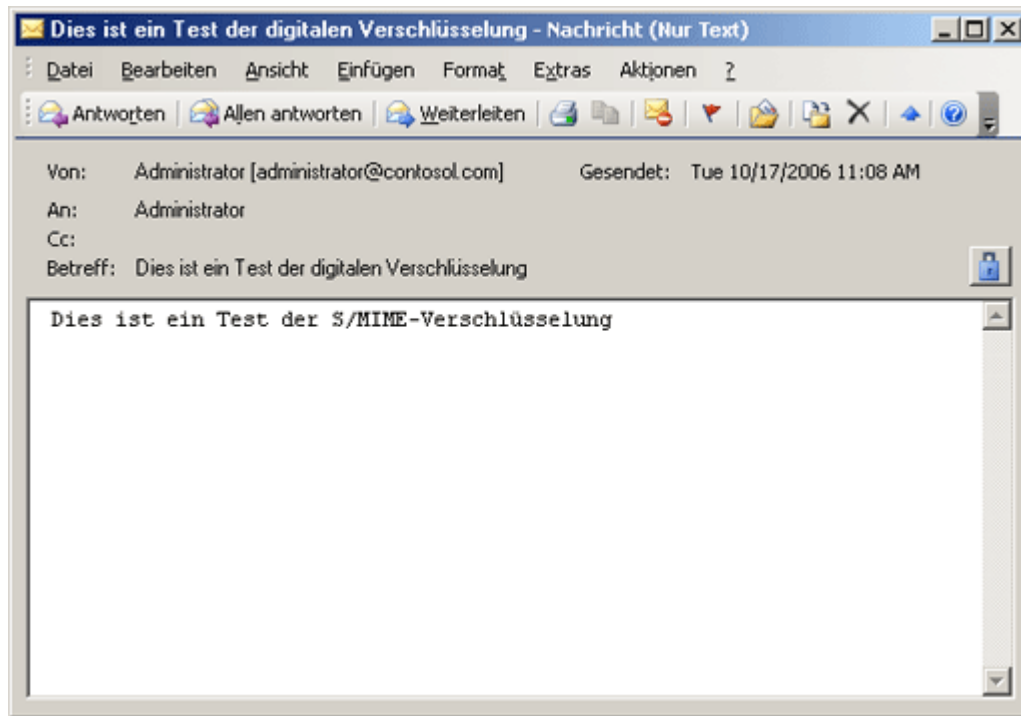
Nach Klicken auf **Signatur überprüfen** wird das Dialogfeld **Digitale Signatur** geöffnet (siehe Abbildung), in dem die Gültigkeit der digitalen Signatur bestätigt wird.



Damit ist die Überprüfung der digitalen Signatur der Nachricht abgeschlossen.

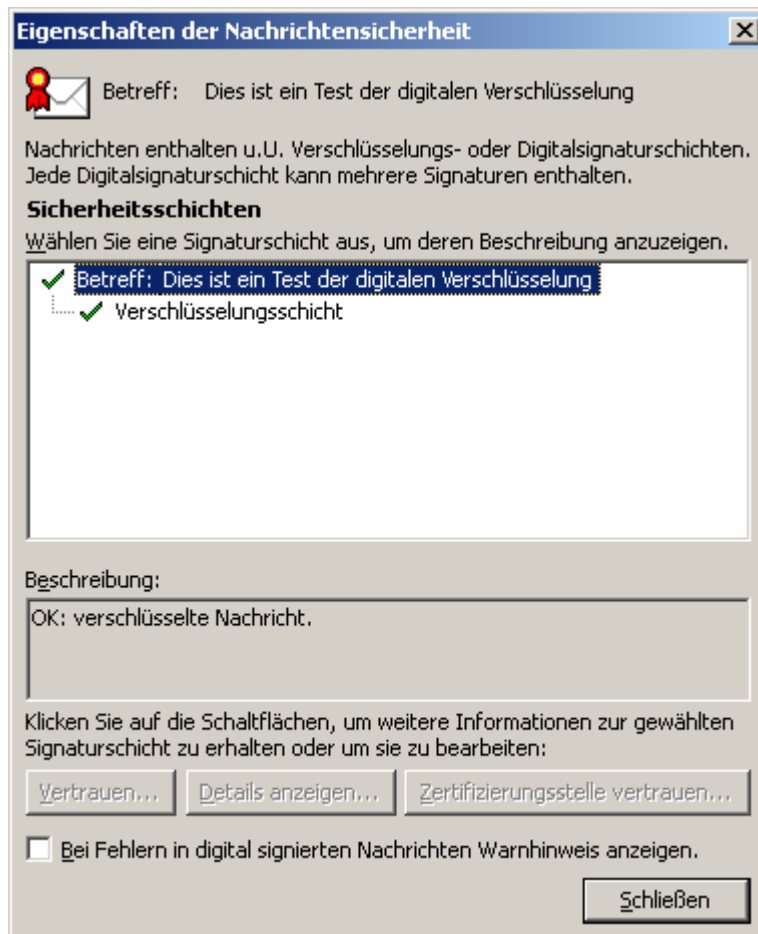
### **So zeigen Sie eine verschlüsselte Nachricht in Outlook an**

1. Melden Sie sich bei Ihrer Domäne als Mitglied der Gruppe der Domänenbenutzer an.
2. Klicken Sie auf **Start**, zeigen Sie auf **Alle Programme** und danach auf **Microsoft Office**, und klicken Sie abschliessend auf **Microsoft Office Outlook 2003**.
3. Doppelklicken Sie im Posteingang auf die verschlüsselte Testnachricht.
4. Wenn die Nachricht geöffnet wird, klicken Sie auf die Schaltfläche **Verschlüsselung überprüfen** (siehe Abbildung), um die Verschlüsselung zu überprüfen.



#### [Bild in voller Grösse anzeigen](#)

5. Nach Klicken auf **Verschlüsselung überprüfen** wird das Dialogfeld **Eigenschaften der Nachrichtensicherheit** geöffnet, in dem die Gültigkeit der verschlüsselten Nachricht bestätigt wird.



Damit ist die Überprüfung der Verschlüsselung der Nachricht abgeschlossen.

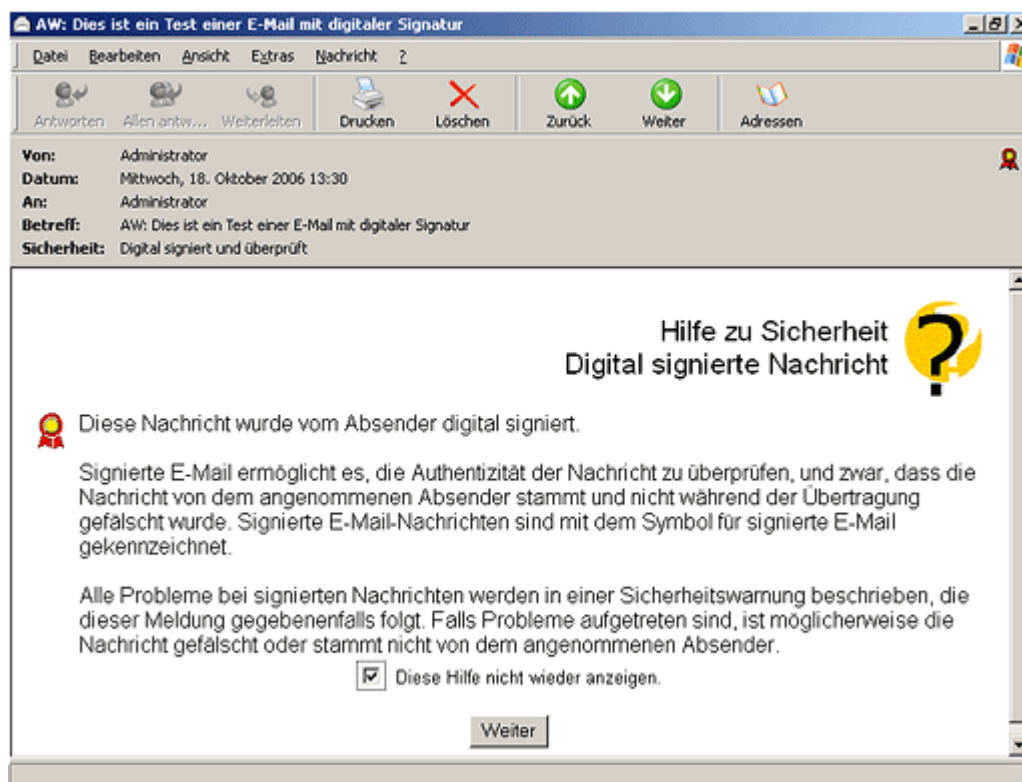
Nach Ausführung dieser Schritte haben Sie alle Elemente der Verwendung von S/MIME in Outlook 2003 getestet. Diese Informationen geben Ihnen Aufschluss über die Funktionsweise eines S/MIME-Systems, das Outlook verwendet, für Ihre Benutzer.

### Überprüfung, ob Outlook Express zur Wahrung der Vertraulichkeit konfigurierte E-Mails empfangen kann

Sie können mit Outlook Express überprüfen, ob Sie E-Mail-Nachrichten empfangen können, die für digitale Signaturen und Verschlüsselung konfiguriert wurden.

### So zeigen Sie eine digital signierte Nachricht in Outlook Express an

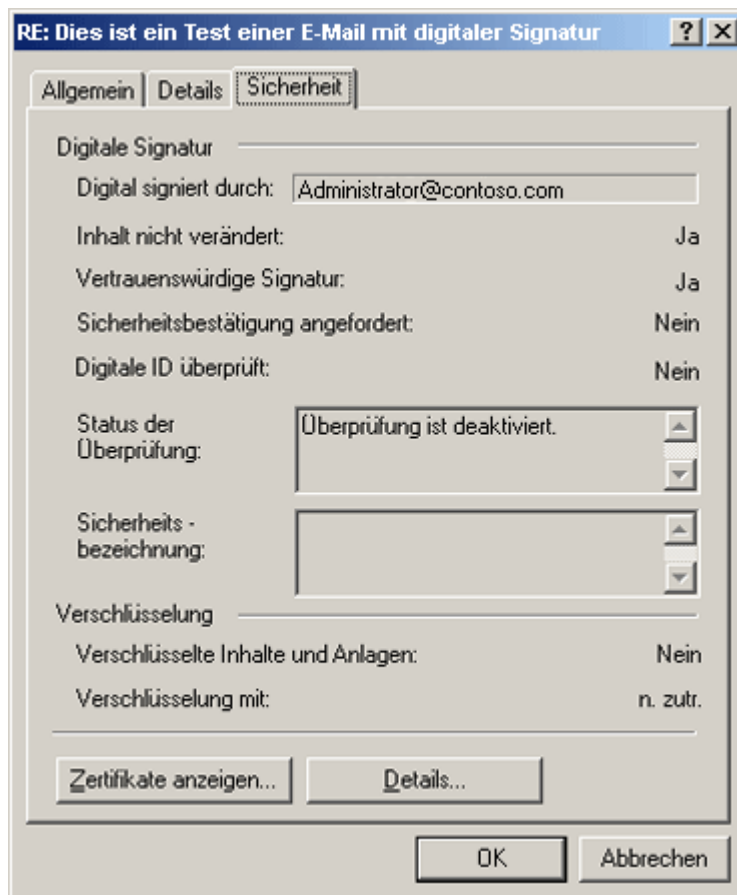
1. Melden Sie sich bei Ihrer Domäne als Mitglied der Gruppe der Domänenbenutzer an.
2. Klicken Sie auf **Start**, zeigen Sie auf **Alle Programme**, und klicken Sie dann auf **Outlook Express**.
3. Geben Sie bei Aufforderung das Kennwort des Benutzers ein.
4. Doppelklicken Sie im Posteingang auf die digital signierte Testnachricht.
5. Wenn die Nachricht geöffnet wird, zeigt Outlook Express folgende Meldung zur Erläuterung von digitalen Signaturen an. Aktivieren Sie das Kontrollkästchen **Diesen Hilfebildschirm nicht mehr anzeigen**, und klicken Sie auf **Weiter**.



### [Bild in voller Größe anzeigen](#)

6. Klicken Sie zur Überprüfung der Signatur auf die Schaltfläche **Signatur überprüfen**.

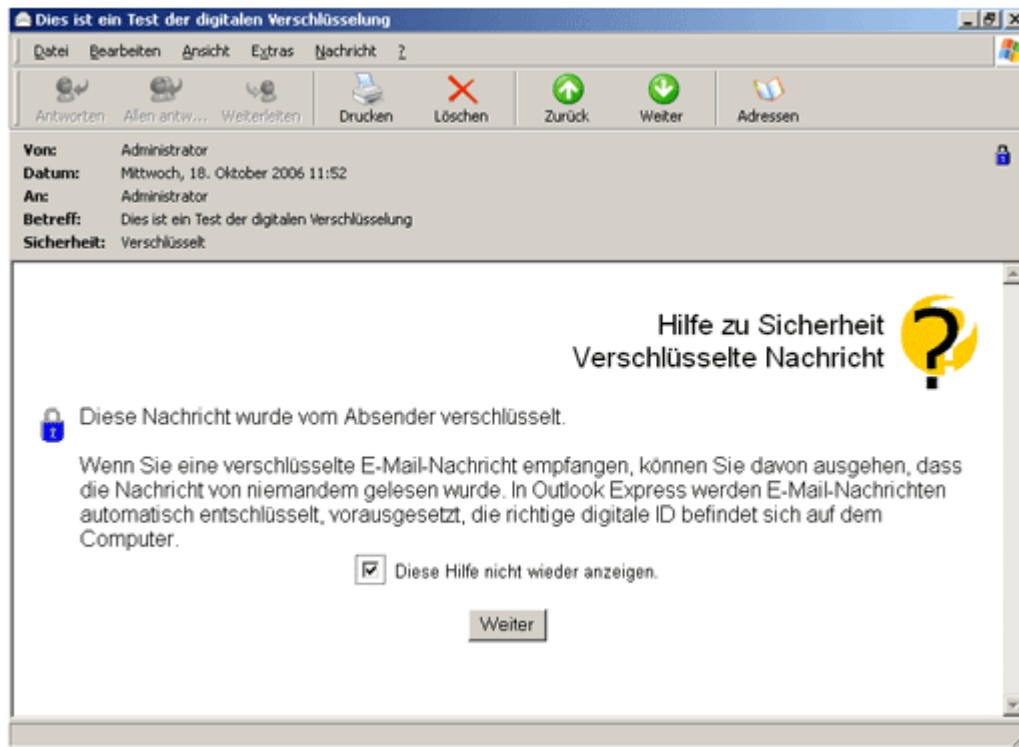
Nach Klicken auf **Signatur überprüfen** wird das Dialogfeld **Digitale Signatur wird getestet** geöffnet, in dem die Gültigkeit der digitalen Signatur bestätigt wird.



Damit ist die Überprüfung der digitalen Signatur der Nachricht abgeschlossen.

### So zeigen Sie eine verschlüsselte Nachricht in Outlook Express an

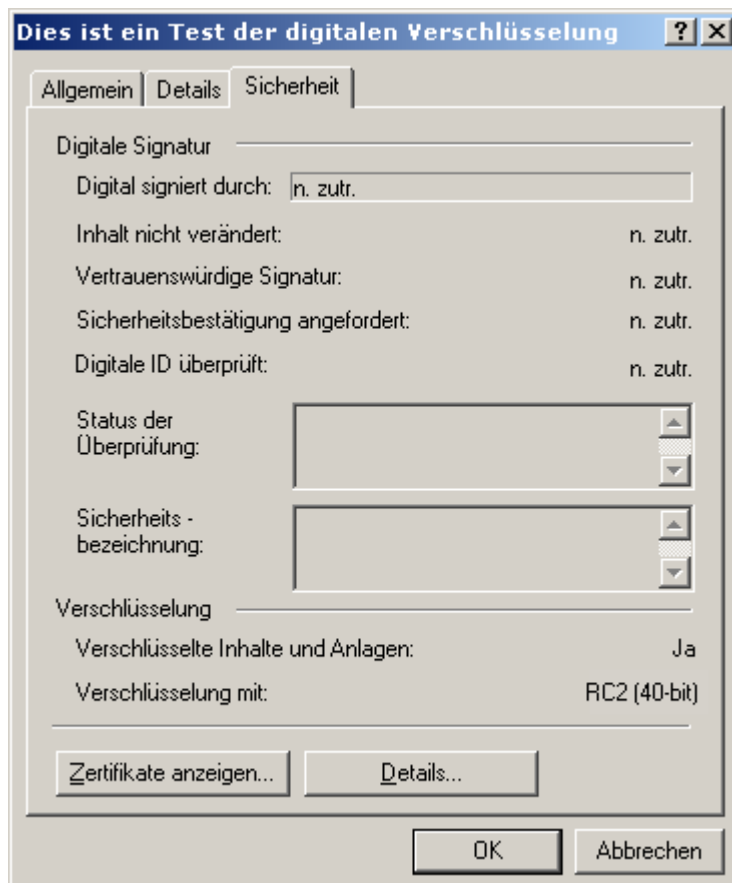
1. Melden Sie sich bei Ihrer Domäne als Mitglied der Gruppe der Domänenbenutzer an.
2. Klicken Sie auf **Start**, zeigen Sie auf **Alle Programme**, und klicken Sie dann auf **Outlook Express**.
3. Geben Sie bei Aufforderung das Kennwort des Benutzers ein.
4. Doppelklicken Sie im Posteingang auf die verschlüsselte Testnachricht.
5. Wenn die Nachricht geöffnet wird, zeigt Outlook Express folgende Meldung zur Erläuterung der Verschlüsselung an. Aktivieren Sie das Kontrollkästchen **Diesen Hilfebildschirm nicht mehr anzeigen**, und klicken Sie auf **Weiter**.



[Bild in voller Grösse anzeigen](#)

6. Klicken Sie zur Überprüfung der Signatur auf **Verschlüsselung überprüfen**.

Nach Klicken auf **Verschlüsselung überprüfen** wird das Dialogfeld **Verschlüsselung** geöffnet, in dem die Gültigkeit der verschlüsselten Nachricht bestätigt wird.



Damit ist die Überprüfung der Verschlüsselung der Nachricht abgeschlossen.

Nach Ausführung dieser Schritte haben Sie alle Elemente der Verwendung von S/MIME in Outlook Express getestet. Diese Informationen geben Ihnen Aufschluss über die Funktionsweise eines S/MIME-Systems, das Outlook Express verwendet, für Ihre Benutzer.

### **Fehlerbehebung bei E-Mails zur Wahrung der Vertraulichkeit**

In diesem Abschnitt werden einige häufig auftretende Probleme in Verbindung mit Exchange Server 2003-basierten S/MIME-Systemen behandelt. Es handelt sich hierbei nicht um eine vollständige Liste, sie enthält jedoch Informationen zu Problemen, die in Ihrer Bereitstellung auftreten könnten, sowie Empfehlungen zur Lösung dieser Probleme.

#### **Problem: Digitale Signatur eines Absenders kann nicht überprüft werden**

Dieses Problem kann auftreten, wenn das digitale Zertifikat der Stammzertifizierungsstelle oder der Zwischenzertifizierungsstelle des Absenders nicht im Zertifikatspeicher des lokalen Computers auf dem Exchange Server des Empfängers vorhanden ist.

#### **Lösung**

Importieren Sie zur Behebung dieses Problems das digitale Zertifikat für die Stammzertifizierungsstelle bzw. Zwischenzertifizierungsstelle des Absenders in den Ordner „Vertrauenswürdige Stammzertifizierungsstellen“ im Zertifikatspeicher des lokalen Computers auf dem Exchange Server des Empfängers. Durch das Importieren des digitalen Zertifikats für eine Stammzertifizierungsstelle wird jedes digitale Zertifikat, das von der Hierarchie der Stammzertifizierungsstelle ausgestellt wurde, als vertrauenswürdig eingestuft. Unternehmen, die gemäß ihren Sicherheitsrichtlinien diese Einstufung nicht vornehmen dürfen, können alternativ Strategien zur gegenseitigen Zertifizierung in Betracht ziehen. Weitere Informationen zur Implementierung der gegenseitigen Zertifizierung bei Verwendung der Windows Server 2003-Zertifizierungsstelle finden Sie im Artikel [Planen und Implementieren der gegenseitigen Zertifizierung und qualifizierten Unterordnung unter Windows Server 2003](http://go.microsoft.com/fwlink/?LinkId=17806) (möglicherweise in englischer Sprache) unter <http://go.microsoft.com/fwlink/?LinkId=17806>.

#### **So importieren Sie das digitale Zertifikat für die Stammzertifizierungsstelle des Absenders in den Speicher vertrauenswürdiger Stammzertifizierungsstellen**

1. Melden Sie sich mit einem Konto, das zur Gruppe der lokalen Administratoren gehört, beim Exchange Server des Empfängers an.
2. Klicken Sie auf **Start** und auf **Ausführen**, und geben Sie **mmc** ein. Klicken Sie danach auf **OK**.
3. Klicken Sie auf **Datei** und danach auf **Snap-In hinzufügen/entfernen**.
4. Klicken Sie auf der Registerkarte **Eigenständig** auf **Hinzufügen**.
5. Markieren Sie **Zertifikate**, und klicken Sie auf **Hinzufügen**. Wählen Sie bei Aufforderung **Computerkonto** aus, und klicken Sie auf **Weiter**.
6. Wählen Sie auf der Seite **Computer auswählen** die Option **Lokalen Computer (der Computer, auf dem diese Konsole ausgeführt wird)** aus, und klicken Sie danach auf **Fertig stellen**.
7. Erweitern Sie in MMC **Zertifikate – Lokaler Computer** und danach **Vertrauenswürdige Stammzertifizierungsstellen**.
8. Klicken Sie im Detailbereich mit der rechten Maustaste, zeigen Sie auf **Alle Aufgaben**, und klicken Sie auf **Importieren**.
9. Klicken Sie auf der ersten Seite des Zertifikatsimport-Assistenten auf **Weiter**.
10. Geben Sie im Dialogfeld **Dateiname** den Namen und den Speicherort der Datei ein, die das

- digitale Zertifikat der Stammzertifizierungsstelle enthält, und klicken Sie auf **Weiter**.
11. Klicken Sie auf der Seite **Zertifikatspeicher** auf **Alle Zertifikate in folgendem Speicher speichern**, vergewissern Sie sich, dass **Vertrauenswürdige Stammzertifizierungsstellen** im Dialogfeld **Zertifikatspeicher** angezeigt wird, und klicken Sie danach auf **Weiter**.
  12. Klicken Sie auf der letzten Seite des Assistenten auf **Fertig stellen**.

Nach dem Import des digitalen Zertifikats für die Stammzertifizierungsstelle des Absenders kann Exchange Server das digitale Zertifikat des Absenders für den Empfänger überprüfen.

### **So importieren Sie das digitale Zertifikat für die Zwischenzertifizierungsstelle des Absenders in den Zwischenzertifizierungsstellenspeicher**

1. Melden Sie sich mit einem Konto, das zur Gruppe der lokalen Administratoren gehört, beim Exchange Server des Empfängers an.
2. Klicken Sie auf **Start** und auf **Ausführen**, und geben Sie **mmc** ein. Klicken Sie danach auf **OK**.
3. Klicken Sie auf **Datei** und danach auf **Snap-In hinzufügen/entfernen**.
4. Klicken Sie auf der Registerkarte **Eigenständig** auf **Hinzufügen**.
5. Markieren Sie **Zertifikate**, und klicken Sie auf **Hinzufügen**. Wählen Sie bei Aufforderung **Computerkonto** aus, und klicken Sie auf **Weiter**.
6. Wählen Sie auf der Seite **Computer auswählen** die Option **Lokalen Computer (der Computer, auf dem diese Konsole ausgeführt wird)** aus, und klicken Sie danach auf **Fertig stellen**.
7. Erweitern Sie in MMC **Zertifikate – Lokaler Computer** und danach **Zwischenzertifizierungsstelle**.
8. Klicken Sie im Detailbereich mit der rechten Maustaste, zeigen Sie auf **Alle Aufgaben**, und klicken Sie auf **Importieren**.
9. Klicken Sie auf der ersten Seite des Zertifikatsimport-Assistenten auf **Weiter**.
10. Geben Sie im Dialogfeld **Dateiname** den Namen und den Speicherort der Datei ein, die das digitale Zertifikat der Stammzertifizierungsstelle enthält, und klicken Sie auf **Weiter**.
11. Klicken Sie auf der Seite **Zertifikatspeicher** auf **Alle Zertifikate in folgendem Speicher speichern**, vergewissern Sie sich, dass **Zwischenzertifizierungsstelle** im Dialogfeld **Zertifikatspeicher** angezeigt wird, und klicken Sie danach auf **Weiter**.
12. Klicken Sie auf der letzten Seite des Assistenten auf **Fertig stellen**.

Nach dem Import des digitalen Zertifikats für die Zwischenzertifizierungsstelle des Absenders kann Exchange Server das digitale Zertifikat des Absenders für den Empfänger erfolgreich überprüfen.

#### **Problem: Kein Zugriff auf die Zertifikatsperrliste**

Dieses Problem kann auftreten, wenn auf den im digitalen Zertifikat angegebenen Verteilungspunkt für die Zertifikatsperrliste (CRL) nur über eine Firewall zugegriffen werden kann, oder wenn der Exchange Server des Benutzers keine Zugriffsrechte für den CRL-Verteilungspunkt hat.

#### **Lösung**

Durch eine der folgenden Massnahmen können Sie das Problem beheben:

- Laden Sie die Zertifikatsperrliste manuell vom CRL-Verteilungspunkt herunter, und importieren Sie sie in den Zertifikatspeicher des lokalen Computers auf dem Exchange Server des Benutzers.
- Installieren und konfigurieren Sie einen Firewall-Client für die zutreffenden Protokolle auf

dem Exchange Server des Empfängers.

- Weisen Sie dem LocalSystem-Konto auf dem Exchange Server des Benutzers explizit das Recht zum Zugriff auf den CRL-Verteilungspunkt zu, oder konfigurieren Sie den CRL-Verteilungspunkt so um, dass für ihn keine Authentifizierung erforderlich ist.

### So importieren Sie eine Zertifikatsperrliste manuell

1. Melden Sie sich mit einem Konto, das zur Gruppe der lokalen Administratoren gehört, beim Exchange Server des Empfängers an.
2. Laden Sie die Zertifikatsperrliste von dem im digitalen Zertifikat angegebenen CRL-Verteilungspunkt herunter.
3. Klicken Sie mit der rechten Maustaste auf die Datei mit der Erweiterung **.cer** oder **.crl**, klicken Sie auf **Zertifikat installieren** oder **Zertifikatsperrliste installieren**, und klicken Sie danach auf **Weiter**.
4. Wenn der Zertifikatsimport-Assistent geöffnet wird, klicken Sie auf **Zertifikatspeicher automatisch auswählen (auf dem Zertifikattyp basierend)**.

#### Problem: Unterschiedliche Zertifikate bei Verwendung unterschiedlicher E-Mail-Clients

Dieses Problem kann auftreten, da es in Active Directory zwei Attribute gibt, unter denen digitale S/MIME-Zertifikate abgelegt werden können: das Attribut **userCertificate** und das Attribut **userSMIMECertificate**. Standardmässig untersucht Outlook zuerst das Attribut **userSMIMEZertifikat** und verwendet jegliches dort gefundene geeignete S/MIME-Zertifikat. Andere E-Mail-Clients, beispielsweise OWA, betrachten möglicherweise zuerst das Attribut **userCertificate** und verwenden entsprechend die dort gefundenen geeigneten S/MIME-Zertifikate.

Sind verschiedene digitale Zertifikate unter **userCertificate** und **userSMIMECertificate** abgelegt, könnten Outlook und OWA unterschiedliche digitale Zertifikate verwenden, da sie auf unterschiedliche Active Directory-Attribute verweisen.

#### Lösung

Vergewissern Sie sich, dass die gleichen Zertifikate unter beiden Attributen **userCertificate** und **userSMIMECertificate** abgelegt sind, um dieses Problem zu beheben. Weitere Informationen finden Sie im Artikel [Outlook 2003 verwendet weiterhin alte Zertifikate nach Migration von Schlüsselverwaltungsserver zu Public Key Infrastructure](http://go.microsoft.com/fwlink/?linkid=3052&kbid=822504) unter <http://go.microsoft.com/fwlink/?linkid=3052&kbid=822504>.

#### Problem: Outlook Express versucht, E-Mail-Nachrichten automatisch zu signieren

Wird eine signierte Nachricht bei Verwendung von Outlook Express beantwortet oder weitergeleitet, wird standardmässig die digitale Signatur für diese Nachricht aktiviert. Versucht ein Benutzer ohne gültiges Signaturzertifikat die Nachricht zu senden, zeigt Outlook Express eine Fehlermeldung an, dass keine digitale ID vorhanden ist, und versendet die Nachricht nicht.

#### Lösung

Deaktivieren Sie zur Behebung dieses Problems die digitale Signatur für die betroffene Nachricht. Weitere Informationen finden Sie im Artikel [Sie erhalten beim Versuch, eine digital signierte E-Mail-Nachricht zu beantworten oder weiterzuleiten, eine Fehlermeldung](http://go.microsoft.com/fwlink/?linkid=3052&kbid=816830) unter <http://go.microsoft.com/fwlink/?linkid=3052&kbid=816830>.

[☐ Zum Seitenanfang](#)

## Zusammenfassung

Mit der anhaltenden Ausweitung des Internets haben sich E-Mails grundlegend verändert. Sie sind nicht mehr lediglich ein unternehmensinternes Tool, sondern sie verbinden nunmehr Leute über Unternehmen und Länder hinweg – und ermöglichen sogar den Informationsaustausch zwischen Menschen auf der Erde und im Weltraum, als würden sich diese im gleichen Gebäude befinden. E-Mails sind wohl zum bisher grössten Nutzen des Internets geworden. In dem Masse, in dem Personen und Unternehmen E-Mails mehr und mehr zu einem Bestandteil ihres Lebens machen, wächst auch deren Bedeutung.

Die beispiellose Ausbreitung von E-Mails ist dank der weltweiten Annahme des zugrunde liegenden Protokolls bzw. der Sprache für Internet-E-Mails möglich: SMTP. Der SMTP-Standard ermöglicht es unterschiedlichen E-Mail-Systemen, die mit dem Internet verbunden sind, Informationen miteinander auszutauschen.

Trotz aller Vorteile, die SMTP dem Internet beschert hat, weist es ein grundlegendes Problem auf: Der SMTP-Standard wurde ursprünglich für die Übermittlung kurzer und relativ unwichtiger Nachrichten in einem geschlossenen Netzwerk konzipiert, nicht jedoch zur Übermittlung wichtiger und vertraulicher Informationen in einer eng verknüpften Welt. Niemand konnte bei der Entwicklung von SMTP die Rolle voraussehen, die es heutzutage spielt. Deshalb wurde SMTP nicht mit einem Schutz für die Art von Informationen versehen, wie sie mittlerweile jeden Tag über Netzwerke hinweg übertragen werden. Es wurde zur Übertragung einfacherer Informationen über einfachere Netzwerke hinweg konzipiert, was auch im Namen „Simple Mail Transfer Protocol“ (einfaches Mailübertragungsprotokoll) zum Ausdruck kommt. SMTP überträgt zum Beispiel Informationen auf eine Art über das Internet, die jedem die Einsichtnahme in Nachrichten erlaubt.

Glücklicherweise hat sich S/MIME als ein Standard etabliert, der SMTP-E-Mail-Nachrichten mit Sicherheitsfunktionen ausstattet. Mit S/MIME kann der Inhalt von E-Mail-Nachrichten verschlüsselt werden, während digitale Signaturen zur Überprüfung der Identität eines vorgeblichen Absenders einer E-Mail-Nachricht dienen.

Zur Implementierung von S/MIME für E-Mails ist eine Lösung erforderlich, die mehrere Produkte und Technologien umfasst.