



# **Erweiterte Konfiguration von S/MIME v3 in MS Outlook 2000 und MS Outlook 2002/XP**

## INHALT

INHALT .....	2
Aktivierung von S/MIME v3 in MS Outlook 2000 SR 1 .....	3
Mit SR 1 aktivierbare Features sind .....	4
Policy-Konfiguration über Registry-Einträge.....	5
Verwendung von Zertifikaten ohne E-Mailadresse .....	11
MS Outlook 2000 .....	11
MS Outlook 2002/XP .....	12
Windows XP .....	12
CRL-Download Verhalten Outlook 2000 .....	13
S/MIME mit PKI und MS-EXCHANGE .....	14
Weitere Sicherheitseinstellungen.....	15
Temporärer Ordner für Outlook.....	15
Passwortcaching .....	15
Anzeige von HTML-Mails .....	15
Sicherheit von PST und OST Files .....	15
Blockieren von Attachments .....	16

## AKTIVIERUNG VON S/MIME V3 IN MS OUTLOOK 2000 SR 1

Während MS Outlook 98 und MS Outlook Express den Großteil S/MIME v2 unterstützen, sind ab MS Outlook 2000 Service Release 1 einige Features von S/MIMEv3 realisiert. Während in MS Outlook 2002 diese Features standardmäßig aktiviert sind, müssen diese für MS Outlook 2000 SR 1, obwohl installiert<sup>1</sup>, mittels eines Eintrags in der Registry aktiviert werden.

Lokalisieren Sie im Registry Editor (regedit) den Schlüssel

**HKEY\_LOCAL\_MACHINE\Software\Microsoft\Office\9.0\Outlook\Security**

Wenn kein Schlüssel für „Security“ existiert, erstellen sie einen neuen Schlüssel mit dem Namen Security ( New / Key value). Erstellen Sie in diesem Schlüssel einen neuen DWORD Eintrag mit dem Namen **EnableSRFeatures** (New / DWORD value) und setzen diesen auf den Wert **1** (modify / value auf 1 setzen).

---

<sup>1</sup> Wenn ein Upgrade aus einer Outlook 2000 Installation erfolgte, kann noch ein Extraschritt notwendig sein. Um Outlook mit hoher Verschlüsselung auszustatten benötigen Sie die Exchcsp.dll, die mittels der Datei Out128.exe, auf der CD-ROM im Support-Folder oder bei Microsoft zu finden, zu installieren ist. <http://office.microsoft.com/downloads/2000/Out128.aspx>

## MIT SR 1 AKTIVIERBARE FEATURES SIND

Die wichtigsten Features sind:

- › Ein neues Attribut wird bei signierten Nachrichten angezeigt. Das „signed by“ Feld enthält den Eintrag der „SignerInfo“ der S/MIME Nachricht, welche natürlich viel vertrauenswürdiger als das „SMTP From“ Attribut.
- › Über die Signatur und die Verschlüsselung werden detaillierte Informationen angezeigt, wie z.B. verwendete Algorithmen und Schlüssellängen.
- › In den Kontaktinformationen werden Zertifikate direkt gespeichert und nicht nur ein Pointer auf das gespeicherte Zertifikat in der Registry, somit sind diese Kontaktinformation leichter verteilbar.
- › Ein zur Verschlüsselung bestimmtes Zertifikat kann in der „Global Address List“ veröffentlicht werden. Damit können andere Benutzer mit Zugriff auf die Global Address List dieses Zertifikat für verschlüsselte Nachrichten an den Besitzer verwenden, ansonsten müsste das Zertifikat im Personal Certificate Store (other people) der Benutzer enthalten sein.
- › S/MIME v3 Features Secure Receipts (signierte Bestätigungen) und Security Labels (Klassifikationen) werden unterstützt.
- › LDAP Unterstützung für mehrere Internet LDAP Accounts.
- › ESDH (ephemeral static Diffie Hellman) Algorithmus wird unterstützt,
- › DSA Signaturalgorithmus wird kann verwendet werden, wenn der Exchange Key Management Service Server dies unterstützt.
- › In der Registry kann das Verhalten an die Security Policy der Organisation angepasst werden.

Im Microsoft White Paper zu Outlook 2000 SR 1 erfahren sind alle Features aufgeführt, sowie detaillierte Informationen

<http://www.microsoft.com/office/ork/2000/download/Out2000SR-1.doc>.

## POLICY-KONFIGURATION ÜBER REGISTRY-EINTRÄGE

Über Registry-Einträge lassen sich die Features an die Security Policy des Unternehmens anpassen, v.a. das CRL Verhalten ist hierfür bedeutend. Einige der Einträge können auch über den Reiter Sicherheit im Outlookmenü Extras / Optionen gesteuert werden. Durch Aktivierung der Optionen in diesem Menü werden aber keine Registry-Einträge erstellt. Folgende Tabelle listet die Einträge auf, welche bei Outlook 2000 (2k) oder Outlook 2002/XP (XP) unter dem Schlüssel Security einzutragen sind:

**HKEY\_LOCAL\_MACHINE\Software\Microsoft\Office\9.0\Outlook\Security**  
 In Windows XP sind diese Einträge unter **HKEY\_CURRENT\_USER** zu machen.

<i>Name des Eintrags</i>	<i>Werte und Typ</i>	<i>Beschreibung</i>	<i>Korrespondierende Option im Menü</i>	<i>Office Version</i>
<b>EnableSRFeatures</b>	<b>0, 1 (DWORD)</b>	Wert 1 oder höher aktiviert die Outlook 2000 SR-1 security features. Standardwert ist 0.	Keine	2k
<b>UseCRLChasing</b>	<b>0, 1, 2 (DWORD)</b>	Wert 0 verwendet die Standardeinstellung des Systems Standardwert 1 fragt die CRL, immer wenn das System online ist, ab Wert 2 fragt die CRL nie ab	Keine	XP
<b>AlwaysEncrypt</b>	<b>0, 1 (DWORD)</b>	Wert 1 verschlüsselt alle ausgehenden Nachrichten Standardwert ist 0.	Nachrichten und Anlagen verschlüsseln	2k, XP
<b>AlwaysSign</b>	<b>0, 1 (DWORD)</b>	Wert 1 signiert alle ausgehenden Nachrichten Standardwert ist 0.	Nachrichten digitale Signatur hinzufügen	2k, XP
<b>ClearSign</b>	<b>0, 1 (DWORD)</b>	Wert 1 verwendet Klartextsignaturen werden für ausgehende Nachrichten. Standardwert ist 0.	Signierte Nachrichten als Klartext senden	2k, XP

<i>Name des Eintrags</i>	<i>Werte und Typ</i>	<i>Beschreibung</i>	<i>Korrespondierende Option im Menü</i>	<i>Office Version</i>
<b>RequestSecureReceipt</b>	<b>0, 1 (DWORD)</b>	Wert 1 fordert signierte Bestätigungen (secure receipts) für alle ausgehenden Nachrichten an. Standardwert ist 0.	Signaturbestätigung anfordern, wenn mit S/Mime signiert	2k, XP
<b>ForceSecurityLabel</b>	<b>0, 1 (DWORD)</b>	Wert 1 fordert auf ausgehenden Nachrichten eine Klassifikation (Security Label) Standardwert ist 0.	Keine	2k, XP
<b>ForceSecurityLabelX</b>	<b>ASN encoded BLOB (Binary)</b>	Dieser Wert spezifiziert welche benutzerdefinierte Klassifikation auf allen ausgehenden signierten Nachrichten angebracht werden muss. Standard ist, dass keine Klassifikation (security label) gefordert ist.	Keine	2k
<b>SigStatusNoCRL</b>	<b>0, 1 (DWORD)</b>	Standardwert 0 gibt fehlende CRLs während der Verifikation der Signatur als Warnung aus Wert 1 gibt fehlende CRLs als Fehler →ungültige Signatur aus.	Keine	2k, XP
<b>SigStatusNoTrustDecision</b>	<b>0, 1, 2 (DWORD)</b>	Standardwert 0 bedeutet dass eine "No Trust decision" erlaubt ist. Wert 1 bedeutet, dass eine "No Trust decision" eine Warnung ist. Wert 2 bedeutet, dass eine "No Trust decision" ein Fehler ist	Keine	2k

<i>Name des Eintrags</i>	<i>Werte und Typ</i>	<i>Beschreibung</i>	<i>Korrespondierende Option im Menü</i>	<i>Office Version</i>
PromoteErrorsAsWarnings	0, 1 (DWORD)	Standardwert 0 werden "Error Level 2" Fehler als Fehler ausgegeben Wert 1 werden "Level 2 Errors" als Warnung ausgegeben. Level 2 Fehler sind: Unbekannter Signaturalgorithmus Kein Signaturzertifikat gefunden Bad Attribute Sets Kein Ausstellerzertifikat gefunden Keine CRL gefunden Abgelaufene CRL Root Trust Problem Abgelaufene CTL	Keine	2k, XP
PublishtoGalDisabled	0, 1 (DWORD)	Wert 1 deaktiviert die "In GAL veröffentlichen" Schaltfläche. Standardwert ist 0.	In GAL veröffentlichen	2k, XP
FIPSMoDe	0, 1 (DWORD)	Wert 1 versetzt Outlook in den FIPS 140-1 Modus. Standardwert ist 0.	Keine	2k, XP
WarnAboutInvalid	0, 1, 2 (DWORD)	Wert 0 zeigt die "Show and Ask check box" (Secure E-Mail Problem dialog box). Wert 1 zeigt diese Dialog Box immer an Standardwert 2 zeigt diese Box nie an.	Secure E-Mail Problem dialog box	2k, XP
DisableContinueEncryption	0, 1, (DWORD)	Standardwert 0 zeigt die "Continue Encrypting" Schaltfläche bei der "Encryption Errors" dialog box an. Wert 1 versteckt diese Schaltfläche.	Continue Encrypting button auf der Encryption Errors dialog box	2k, XP

<i>Name des Eintrags</i>	<i>Werte und Typ</i>	<i>Beschreibung</i>	<i>Korrespondierende Option im Menü</i>	<i>Office Version</i>
<b>RespondtoReceiptRequest</b>	0, 1, 2, 3 (DWORD)	Standardwert 0 sendet immer eine signierte Bestätigung auf eine entsprechende Anforderung, und fragt nach Passwort/PIN wenn notwendig. Wert 1 verlangt eine Benutzereingabe, wenn eine Anforderung kommt. Wert 2 verwendet nie eine Bestätigung. Wert 3 erzwingt den Versand einer Bestätigung.	Keine	2k, XP
<b>NeedEncryptionString</b>	String	Bei erfolglosem Versuch der Entschlüsselung einer Nachricht wird dieser String angezeigt.	Standardstring	2k, XP
<b>Options</b>	0, 1, (DWORD)	Standardwert 0 zeigt eine Warnung wenn ein Benutzer eine Nachricht mit einer ungültigen Signatur lesen will Wert 1 unterdrückt diese Warnung	Keine	XP
<b>MinEncKey</b>	40, 64, 128, 168 (DWORD)	Setzt die Minimum-Schlüssellänge für verschlüsselte ausgehende Nachrichten	Keine	XP
<b>RequiredCA</b>	String	Setzt den Namen der benötigten Zertifizierungsstelle	Keine	XP
<b>EnrollPageURL</b>	String	Setzt die URL für die Zertifizierungsstelle bei Anforderung einer neuen digital ID eines Benutzers	Digitale ID anfordern Button	XP

Weitere Registry-Einträge finden sich unter:

HKEY\_CURRENT\_USER\Software\Microsoft\Cryptography\SMIME\SecurityPolicies\Default

<i>Name des Eintrags</i>	<i>Werte und Typ</i>	<i>Beschreibung</i>	<i>Korrespondierende Option im Menü</i>	<i>Office Version</i>
<b>ShowWithMultiLabels</b>	0, 1 (DWORD)	Standardwert 0 zeigt eine Nachricht, wenn ein Signature-layer unterschiedliche Labels in unterschiedlichen Signaturen hat. Wert 1 unterdrückt diese Nachricht.	Keine	
<b>CertErrorWithLabel</b>	0, 1, 2 (DWORD)	Standardwert 0 verarbeitet eine Nachricht wenn diese ein Label hat, das Zertifikat aber einen Fehler aufweist. Wert 1 verhindert den Zugriff auf Nachrichten mit Fehlern beim Zertifikat Wert 2 ignoriert das Label und gewährt Zugriff, der Benutzer sieht noch den Fehler des Zertifikats	Keine	

Weitere Registry-Einträge zur spezifischen Konfiguration finden sich unter Einträgen für Cryptographic Service Provider, die unter Umständen helfen können:

#### HKEY\_CURRENT\_USER\Software\Microsoft\Cryptography\Defaults\Provider

<i>Name des Eintrags</i>	<i>Werte und Typ</i>	<i>Beschreibung</i>	<i>Korrespondierende Option im Menü</i>	<i>Office Version</i>
MaxPWTime	0, Zahl (DWORD)	Wert 0 zwingt einen Benutzer immer sein Passwort einzugeben, wenn ein Schlüsselset benötigt wird. Eine positive Zahl gibt die Minuten für die Passwortzeit an, wo er ein Passwort speichern kann. Standardwert 999	Keine	
DefPWTime	Zahl (DWORD)	Setzt den Standardwert für die Passwortzeit	Keine	

## VERWENDUNG VON ZERTIFIKATEN OHNE E-MAILADRESSE

In S/MIME v2 müssen in den verwendeten Zertifikaten verpflichtend E-Mailadressen enthalten sein. Um unabhängig von Änderungen der E-Mailadresse zu sein, bzw. ein Zertifikat mit mehreren E-Mailadressen verwenden zu können, ist in S/MIME Version 3 E-Mailadresse im Zertifikat nicht mehr verpflichtend. Ist eine E-Mailadresse im Zertifikat angegeben muss diese laut S/MIME-Standard natürlich trotzdem mit der Absenderadresse zusammenpassen.

Der Empfang von mit solchen Zertifikaten signierten Nachrichten bereitet Outlook „kein Problem“ bereitet, sprich es wird NIE ein Fehler der Signatur angezeigt, dafür gibt es das neue angezeigte Attribut „signed by“.

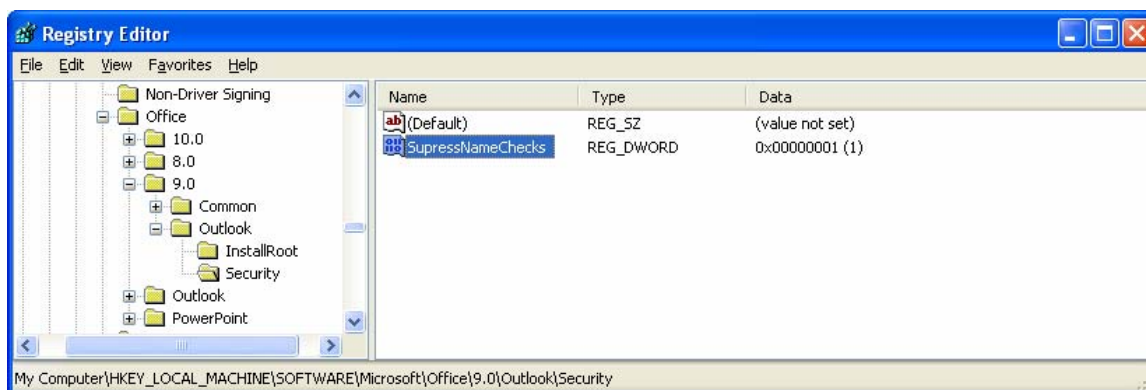
Um Outlook 2000 und Outlook 2002 aber zu ermöglichen solche Zertifikate, sprich ohne E-Mailadresse oder fremder E-Mailadresse, selbst zu verwenden ist eine Änderung des SupressNameCheck Eintrags in der Registry notwendig.

### MS OUTLOOK 2000

Lokalisieren Sie im Registry Editor (regedit) den Schlüssel

**HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Office\9.0\Outlook\Security**

Wenn kein Schlüssel für „Security“ existiert, erstellen sie einen neuen Schlüssel mit dem Namen Security ( New / Key value). Erstellen Sie in diesem Schlüssel einen neuen DWORD Eintrag mit dem Namen SupressNameChecks (New / DWORD value) (Achtung: Sup(p)ress nur mit einem p schreiben!) und setzen diesen auf den Wert 1 (modify / value auf 1 setzen).



## MS OUTLOOK 2002/XP

Lokalisieren Sie im Registry Editor (regedit) den Schlüssel

**HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Office\10.0\Outlook\Security**

Und gehen Sie wie bei Outlook 2000 vor. Erstellen Sie einen Schlüssel mit Namen Security und erstellen Sie darin einen neuen DWORD Eintrag mit dem Namen SuppressNameChecks und setzen diesen auf den Wert 1.

## WINDOWS XP

In Windows XP sind diese Einträge unter HKEY\_CURRENT\_USER zu machen.

**HKEY\_CURRENT\_USER\SOFTWARE\Microsoft\Office\10.0\Outlook\Security**

Erstellen Sie darin einen neuen DWORD Eintrag mit dem Namen SuppressNameChecks und setzen diesen auf den Wert 1.

## CRL-DOWNLOAD VERHALTEN OUTLOOK 2000

Das CRL – Verhalten kann wie schon in „Policy-Konfiguration über Registry-Einträge“ gezeigt mit dem SigStatusNoCRL Eintrag in

**HKEY\_LOCAL\_MACHINE \SOFTWARE \Microsoft \Office\9.0\Outlook\Security**

gesteuert werden. Während in Outlook 2002/XP der CRL-Download standardmäßig aktiviert ist (UseCRLChasing), ist um Outlook 2000 SR 1 ebenfalls dazu zu veranlassen, ein Eintrag in der Registry vorzunehmen.

Lokalisieren Sie im Registry Editor den Schlüssel

**HKEY\_LOCAL\_MACHINE \SOFTWARE \Microsoft \Cryptography**

und fügen Sie, wenn nicht vorhanden den {7801ebd0-cf4b-11d0-851f-0060979387ea} Schlüssel hinzu. Fügen Sie einen REG\_DWORD Eintrag namens **PolicyFlags** mit dem Wert 0x00010000 hinzu.

Eine weitere Einstellmöglichkeit ist in den Internetoptionen sind unter dem Reiter Erweitert, Bereich Sicherheit ebenfalls Einstellungen über die online CRL-Prüfung möglich. In den temporären Internet Dateien sollte die CRL dann zu finden sein.

Wenn Outlook den CRL Check, trotz vorhandener CRL, weiterhin als nicht durchgeführt anzeigt, kann auch noch der Hotfix Q308707 notwendig sein.

Die Prüfung von CRLs kann bei Offline Rechner natürlich länger dauern, dieses Verhalten muss berücksichtigt werden. Grundsätzlich sucht Outlook nur dann nach einer neuen CRL, wenn die existierende gecachte CRL abläuft. Durch das Importieren von CRLs auf den lokalen Rechner und das Registrieren dieser im lokalen Zertifikatsspeicher, kann die Prüfung noch verkürzt werden. Im Allgemeinen wird von Outlook zuerst der lokale Zertifikatsspeicher durchsucht, danach die im Zertifikat angegebenen CRL Distribution Points.

## S/MIME MIT PKI UND MS-EXCHANGE

Vor allem mit der Verwendung einer Enterprise-CA können Konfigurationen für S/MIME sinnvoll sein, die ansonsten etablierte Workflows des Unternehmens umgehen könnten.

Vor allem der „In GAL veröffentlichen“ Button könnte deaktiviert werden müssen.

HKEY\_LOCAL\_MACHINE\Software\Microsoft\Office\9.0\Outlook\Security

**PublishtoGalDisabled**

Typ DWORD – Wert „1“

Diese Schaltfläche ist dazu gedacht, ein Zertifikat im Unternehmensverzeichnis zu veröffentlichen, das aus einer externen Quelle kommt. Wenn ein Benutzer auf diese Schaltfläche klickt, veröffentlicht Outlook in Active Directory die Signatur (ExchangeUserSignature) und die Zertifikate (ExchangeUser certificates) des Benutzers im PKCS #7-Format im **userSMIMECertificate**-Attribut des Benutzerobjekts. Die Zertifikate (ExchangeUser certificates) des Benutzers werden auch im DER-Format im **userCertificate**-Attribut des Benutzerobjekts in Active Directory veröffentlicht.

Zusätzlich könnte die Schaltfläche „Digitale ID anfordern“ auf eine Webseite geführt werden, wo ein Zertifikat der Enterprise-CA beantragt werden kann. Wenn PKI-Administratoren ein webbasiertes Registrierungsformular zur Verfügung gestellt haben, sollten die Outlook-Administratoren diese Schaltfläche anpassen, damit die Benutzer auf diese angepasste Seite gelangen. Die URL der Seite kann durch Verwendung von Gruppenrichtlinien erfolgen, bzw. über folgenden Registrierungsschlüssel auf dem Client des Benutzers festgelegt werden:

HKEY\_CURRENT\_USER\Software\Microsoft\Office\10.0\Outlook\Security

**EnrollPageURL**

Typ STRING - Wert

## WEITERE SICHERHEITSEINSTELLUNGEN

### *Temporärer Ordner für Outlook*

HKEY\_CURRENT\_USER\Software\Microsoft\Office\10.0\Outlook\Security

OutlookSecureTempFolder

spezifiziert den Ordner für den temporären Speicher, in dem Outlook Attachments vor dem Öffnen speichert.

### *Passwortcaching*

HKEY\_CURRENT\_USER\Software\Microsoft\Office\10.0\Outlook\Security

EnableRememberPwd

DWORD

Auf Wert 0 gesetzt, wird das Speichern von POP, IMAP oder http-Passwörter für den Zugriff auf Mailserver verhindert.

<http://support.microsoft.com/?kbid=299377>

### *Anzeige von HTML-Mails*

HKEY\_CURRENT\_USER\Software\Microsoft\Office\10.0\Outlook\Options\Mail

ReadAsPlain

DWORD

Auf Wert 1 gesetzt werden HTML-Mails als Plaintext angezeigt.

<http://support.microsoft.com/?kbid=307594>

### *Sicherheit von PST und OST Files*

HKEY\_CURRENT\_USER\Software\Microsoft\Office\10.0\Outlook\PST

PSTNullFreeOnClose

DWORD

Wert 1 zwingt Outlook, in .pst und .ost Dateien gelöschte Informationen zu beim Schließen von Outlook zu überschreiben. <http://support.microsoft.com/?kbid=245776>

## *Blockieren von Attachments*

HKEY\_CURRENT\_USER\Software\Policies\Microsoft\Office\10.0\Outlook\Security

Level1Add

Level1Remove

SZ

Mit diesen Einträgen können Datei-Extensions die zu blockieren sind selbst zu bestimmen, und nicht die Standard-Blockierungen zu verwenden. Level1Remove SZ Wert „crt;“ entblockt beispielsweise .crt-Dateien.

CRYPTAS it-Security & Media GmbH  
Modecenterstrasse 22/B2  
A-1030 Wien, Austria  
T +43 (1) 798 96 96 – 0  
F +43 (1) 798 96 96 – 99  
info@cryptas.com

[www.cryptoshop.com](http://www.cryptoshop.com)  
[www.cryptas.com](http://www.cryptas.com)  
[www.cryptasmedia.com](http://www.cryptasmedia.com)