



MS Exchange 2003 Konfiguration für S/MIME v3 mit Outlook Web Access

INHALT

INHALT.....	2
Registry Einstellungen am Exchange Server Rechner.....	3
Empfängerbeschränkung Einstellung.....	6

REGISTRY EINSTELLUNGEN AM EXCHANGE SERVER RECHNER

Bei der Verwendung von Exchange 2003 mit Outlook Web Access mit S/MIME-Control übernimmt der Exchange-Server Teile der Aufgaben des Clients. Daher ist der Exchange Rechner auch für die Verwendung von S/MIME zu konfigurieren. Die Konfiguration muss am Rechner (Back-End-Server), wo der Posteingang des Benutzers gespeichert ist, getroffen werden.

Lokalisieren Sie (oder fügen Sie hinzu) im Registry Editor den Schlüssel,

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\MSExchangeWeb\OWA

<i>Name des Eintrags</i>	<i>Werte und Typ</i>	<i>Beschreibung</i>
CheckCRL	0, 1 (DWORD)	Wert 1 zeigt beim Senden einer E-Mail an, dass eine CRL für ein Zertifikat nicht verfügbar war/ist und das Zertifikat nicht geprüft werden konnte. Senden ist trotzdem möglich. Standardwert ist 0.
DLExpansionTimeout	0,.. 2147483647 (DWORD)	Angabe von Millisekunden. Bei Standardwert 60000 wird der Timeoutwert für eine Verteilerliste auf 60 Sekunden gesetzt. Diese Zeit darf für den Abruf der Zertifikate für die Empfänger in einer Verteilerliste benötigen. Für mehrere Listen wird dieser Timeoutwert akkumuliert. Wert 0 sperrt das Senden von verschlüsselten Mails an Verteilerlisten. Maximumwert 2147483647 setzt den Timeout auf unendlich
CertMatchingDoNotUseProxies	0, 1 (DWORD)	Beim Finden des richtigen Empfängerzertifikates wird eine Übereinstimmung zwischen der primären SMTP-Adresse und Angabe im Subject oder Subject_Alternative_Name des Zertifikates gesucht. Wird keine gefunden wird eine Übereinstimmung zwischen Zertifikatsangaben und SMTP-Proxyadressen gesucht. Wert 1 verhindert die Ausweitung der Suche auf Proxyadressen. Standardwert ist 0.
RevocationURLRetrievalTimeout	5000,..,600000 (DWORD)	Angabe von Millisekunden die gewartet wird um eine einzelne CRL abzurufen. Standardwert: 60000 Minimum: 5000 Maximum:600000

<i>Name des Eintrags</i>	<i>Werte und Typ</i>	<i>Beschreibung</i>
CertURLRetrievalTimeout	0,...600000 (DWORD)	Angabe von Millisekunden, die gewartet wird, um alle CRLs eines Zertifikates (und Pfad) abzurufen. Standardwert ist 60000
DisableCRLCheck	0, 1 (DWORD)	Wert 1 deaktiviert generell die CRL-Überprüfung. Standardwert ist 0.
AlwaysSign	0, 1 (DWORD)	Wert 1 fordert auf alle ausgehenden OWA - Nachrichten eine Signatur. Standardwert ist 0.
AlwaysEncrypt	0, 1 (DWORD)	Wert 1 fordert auf alle ausgehenden OWA - Nachrichten eine Verschlüsselung. Standardwert ist 0.
ClearSign	0, 1 (DWORD)	Standardwert 1 fordert auf alle ausgehenden OWA - Nachrichten eine Klartext-Signatur. Wert 0 erlaubt auch opak-signierte E-Mails.
SecurityFlags	Bitmaske (DWORD)	Bei dem Schlüssel SecurityFlags handelt es sich um eine Bitmaske, mit der Funktionen von Outlook Web Access S/MIME aktiviert oder deaktiviert werden. Wenn dieser Schlüssel auf den Wert einer bestimmten Funktion gesetzt wird, führt dies zum Aktivieren der entsprechenden Funktion. Um mehrere Funktionen zu aktivieren, addieren Sie die Werte aller zu aktivierenden Funktionen, und geben Sie die Summe in den Schlüssel ein. Wenn Outlook Web Access mit S/MIME-Steurelement zum Beispiel die Zertifikatkette ohne das Stammzertifikat (0x001) und nur mit dem Signaturzertifikat (0x008) einbinden soll, addieren Sie die beiden Werte (0x001 + 0x008), und geben Sie die Summe (0x009) ein. Folgend werden die Werte aufgeführt, die im Schlüssel SecurityFlags gesetzt werden können. Standardmäßig sind alle Funktionen deaktiviert.
	0x001	Zertifikatskette ohne Stammzertifikat einschließen. OWA bindet lediglich Signatur- und Verschlüsselungszertifikate ein. Mit dieser Option werden die Zertifikatsketten ohne Stammzertifikate miteingebunden
	0x002	Zertifikatskette mit Stammzertifikat einschließen, was für einige E-Mail-Clients benötigt werden kann.
	0x004	Temporäre Puffer nicht verschlüsseln. Standardmäßig werden temporäre Dateien am Client 3DES verschlüsselt. Durch die Deaktivierung wird die Leistung des Clients erhöht, es bleiben aber unverschlüsselte Daten am Client zurück.

<i>Name des Eintrags</i>	<i>Werte und Typ</i>	<i>Beschreibung</i>
	0x008	Bei signierten Mails nur Signaturzertifikat einschließen. Standardmäßig werden bei zwei Zertifikaten zur Absicherung des Mailverkehrs beide, sowohl Signatur- als auch Verschlüsselungszertifikat, mit eingeschlossen.
	0x040	Getrennte Einzelnachrichten für sichtbare und unsichtbare Empfänger. Wird standardmäßig für jeden unsichtbaren Empfänger eine eigene Nachricht versandt, was einzelne Behandlung für jeden unsichtbaren zulässt, wird mit dieser Einstellung für alle unsichtbaren Empfänger dieselbe Nachricht versandt
	0x080	Eine einzige verschlüsselte Nachricht für alle Empfänger. Mit dieser Einstellung wird an alle sichtbaren und unsichtbaren Empfänger eine einzige Nachricht versandt.
	0x100	S/MIME Informationen in Nachricht einschließen. Mit Aktivierung dieser Option fügt OWA Informationen über unterstützte Algorithmen und Schlüssellängen hinzu, was für einige Mailclients wichtig sein kann.
	0x200	Empfängerkopfzeilen kopieren. Mit dieser Option werden die Empfängerkopfzeilen „from, to, cc“ in den zu signierenden Teil übernommen. Der Empfänger kann so einen Manipulation der Header erkennen.
SmartCardOnly	0, 1 (DWORD)	Mit Wert 1 können mit OWA nur Smart Card basierte Zertifikate am OWA – Client verwendet werden.
TripleWrap	0, 1 (DWORD)	Mit Standartwert 1 werden signierte, verschlüsselte Nachrichten „triple wrapped“, d.h. eine Nachricht wird, signiert, verschlüsselt und noch einmal signiert. Wert 0, die zweite Signatur nach der Verschlüsselung wird nicht angebracht.
EncryptionAlgorithms	(Reg_SZ)	<p>Eine durch Semikolons getrennte Liste der symmetrischen Verschlüsselungsalgorithmen, die beim Verschlüsseln von Nachrichten mit OWA verwendet werden sollen. Die Reihenfolge spiegelt die Priorität wieder. Für Dritt-CSPs kann auch der OID des CSP angegeben werden. Bei variablen Schlüssellängen für einen Algorithmus, muss die Länge mit angegeben werden, Standard: 3DES, RC2_128</p> <ul style="list-style-type: none"> • Format: {Algorithmus-ID}[:zu verwendende Schlüssellänge][,OID eines Kryptografiedienstanbieters, der die Algorithmus-ID unterstützt]; {Algorithmus-ID}[:zu verwendende Schlüssellänge][,OID eines Kryptografiedienstanbieters, der die Algorithmus-ID unterstützt] • RC2: 6602; 40, 56, 64, 128 Bit • DES: 6601; 56 Bit • 3DES: 6603; 168 Bit

<i>Name des Eintrags</i>	<i>Werte und Typ</i>	<i>Beschreibung</i>
DefaultSigningAlgorithm	(Reg_SZ)	Erlaubt die Angabe des Hash-Verfahrens für das Signaturverfahren. Standard: SHA-1 <ul style="list-style-type: none">• SHA-1: 8004• MD5: 8003
UseKeyIdentifier	0, 1 (DWORD)	Mit Standardwert 0 codiert OWA das zum Entschlüsseln notwendige Zertifikate mit Aussteller und Seriennummer. Mit Wert 1 wird der SubjectKeyIdentifier des Zertifikates dafür verwendet. Nicht alle Clients unterstützen diese Option, doch kann diese Einstellung, bei einem Zertifikatsrenewal mit demselben Schlüsselpaar, das Zertifikatshandling erleichtern.

EMPFÄNGERBESCHRÄNKUNG EINSTELLUNG

Empfängerbeschränkungen können im Active-Directory auf Globaler und Benutzerebene eingestellt werden. Sie funktionieren zusammen mit DLExpansionTimeout.

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
www.cryptas.com
www.cryptasmedia.com