STAATSMINISTERIUM
DES INNERN

Freistaat
SACHSEN

Handlungsanleitung zur Verschlüsselung von Verbindungen von Outlook 2010 zu Exchange 2010 (Microsoft Exchange 2010 RPC Encryption)

Handlungsanleitung zur Verschlüsselung von Verbindungen von Outlook 2010 zu Exchange 2010 (Microsoft Exchange 2010 RPC Encryption)

Dokumentenkontrolle:

Versionskontrolle:

Version	Datum	Kommentar
V1.0	18.07.2014	Erarbeitung durch Kernteam Verschlüsselung der AG IS
V2.0	12.12.2014	Aktualisierte und überarbeitete Fassung zur Veröffentlichung

Inhaltsverzeichnis

1. Vorbetrachtung

In der Landes- und Kommunalverwaltung kommen zahlreiche verschiedene Softwareprodukte im Bereich der E-Mail-Kommunikation zum Einsatz. Ein wichtiger Anteil davon basiert auf der Microsoft Produktlinie, d. h. auf Exchange und Outlook. Ziel ist es, durch den verstärkten Einsatz von Verschlüsselungsverfahren die Sicherheit der E-Mail-Kommunikation zu erhöhen.

Die ressortübergreifende Arbeitsgruppe Informationssicherheit der Landesverwaltung und der Arbeitskreis IT- und E-Government haben dazu Handlungsempfehlungen und einen Umsetzungsplan zum verbesserten Einsatz von Verschlüsselungsverfahren verabschiedet, nach denen u. a. die E-Mail-Verschlüsselung im und zum SVN flächendeckend eingesetzt werden soll. Die Verschlüsselung der Exchange-Server untereinander ist mit der laufenden flächendeckenden Umstellung auf Microsoft Exchange Server 2010 zu großen Teilen abgeschlossen, da Exchange 2010 zwingend eine Verschlüsselung fordert. Die Transportverschlüsselung aus dem Mail-Verbund des SVN zu den Kommunikationspartnern im Internet wird von Seiten des SVN mittels STARTTLS eingefordert und kommt bereits in vielen Fällen zum Einsatz. Bislang ungeschützt ist die Übertragungsstrecke vom Nutzer (Outlook-Client) zum zentralen E-Mail-Server (Exchange-Server) des Ressorts und zurück. Die AG IS und der AK ITEG empfehlen hier die Einschaltung der in Outlook vorhandenen, aber standardmäßig deaktivierten Verschlüsselungsoption. Im Folgenden wird das dafür notwendige Vorgehen beschrieben.

Es werden hierbei ausschließlich die Versionen Microsoft Office Outlook 2010 und Microsoft Exchange Server 2010 mit den in dieser Handlungsanleitung genannten Servicepacks betrachtet.

2. Technische und organisatorische Umsetzung in Sachsen

2.1. Ist-Stand

Um eine verschlüsselte Verbindung (RPC Encryption) von einem Outlook-Client zu einem Exchange-Server aufbauen zu können, sind sowohl auf der Client - wie auch auf der Serverseite - die entsprechenden Voraussetzungen für eine verschlüsselte Verbindung zu schaffen. Diese Voraussetzungen bestehen auf der Clientseite ab der Version Microsoft Office Outlook 2003 und auf der Serverseite ab der Version Microsoft Exchange Server 2007.

Dabei muss beachtet werden, dass der Server eine Verschlüsselung fordern oder auch nur akzeptieren kann. Akzeptiert der Server eine verschlüsselte Verbindung, steht es dem Client frei, eine Verschlüsselung zu aktivieren. Fordert hingegen der Server eine verschlüsselte Verbindung, muss der Client zwingend verschlüsselt mit dem Server kommunizieren.

Unter Microsoft Exchange Server 2010 RTM war die RPC Verschlüsselung standardmäßig aktiviert, unter Servicepack 1 bis 3 ist sie standardmäßig deaktiviert. Die derzeit eingesetzte Servicepack-Version ist SP3.

Im Anhang ist der derzeitige IST-Stand, d. h. eine Übersicht aller derzeitig erfassten Exchange 2010 Server mit der Option zur Verschlüsselung (RPC Encryption) aufgeführt. Die Option »EncryptionRequired: False« bedeutet, dass eine Verschlüsselung nur akzeptiert wird. »EncryptionRequired: True« bedeutet, eine Verschlüsselung wird vom Server gefordert.

2.2. Soll-Stand

Empfohlen wird, alle Exchange-Server so zu konfigurieren, dass diese standardmäßig von allen Outlook-Clients eine Verschlüsselung einfordern. In diesem Zusammenhang ist auf allen Outlook-Clients die Verschlüsselungsoption einzuschalten.

Um auf den Exchange- Servern eine Verschlüsselung zu fordern, muss die Option »EncryptionRequired« auf »True« gesetzt werden. Dies kann z. B. mit dem folgenden PS-Befehl geschehen:

```
„Set-RpcClientAccess -Server <ServerName> -EncryptionRequired $True”
```

Diese Verfahrensweise ist auch im Microsoft TechNet unter *http://technet.microsoft.com/en-us/library/dd439391(v=exchg.80).aspx* bzw. unter *http://theucguy.net/rpc-encryption-disabled-by-default-in/* näher beschrieben.

Hinweis: Bevor die Option »EncryptionRequired« auf »True« gesetzt wird, prüfen Sie bitte unbedingt die Clienteinstellungen, da ansonsten bei nicht aktivierter Verschlüsselungsoption am Client keine Verbindung mit dem Exchange-Server möglich ist.

Weiterhin müssen die Outlook-Clients die Option: »Daten zwischen Microsoft Outlook und Microsoft Exchange verschlüsseln« gesetzt bekommen. In Outlook ist diese Option in den Konteneinstellungen für Exchange-Konten zu finden.

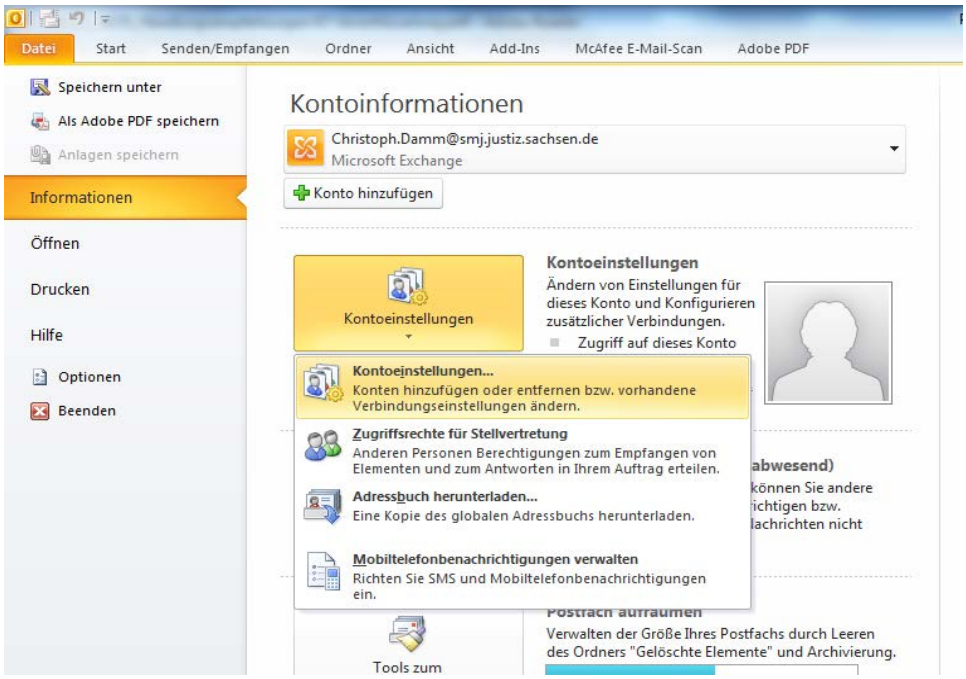


Abbildung 1: Konteneinstellung in Outlook

Das jeweilige Exchange-Konto ist zur Bearbeitung auszuwählen (Ändern-> Weitere Einstellungen).

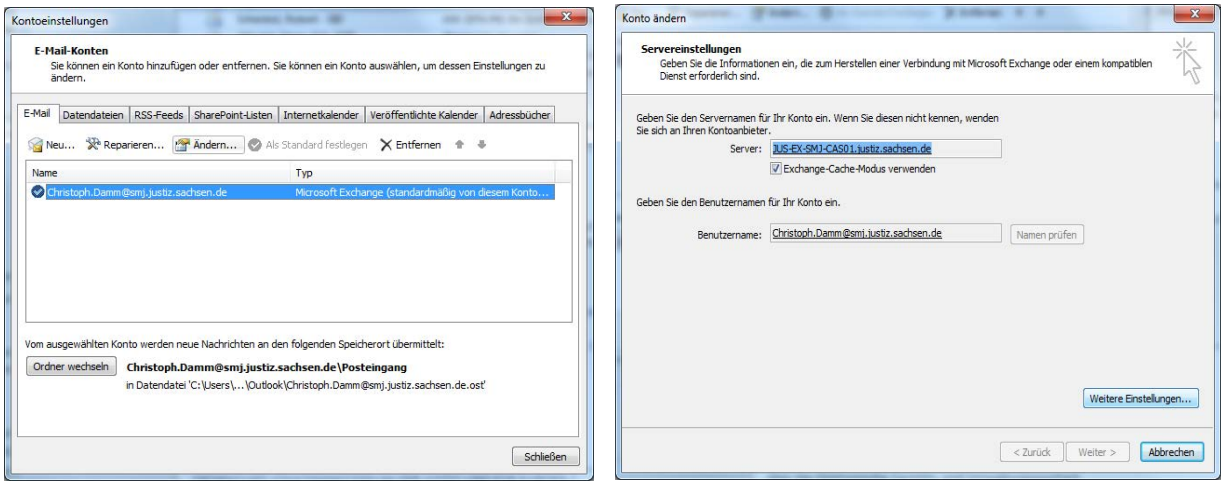


Abbildung 2: Exchange-Konto zur Bearbeitung auswählen

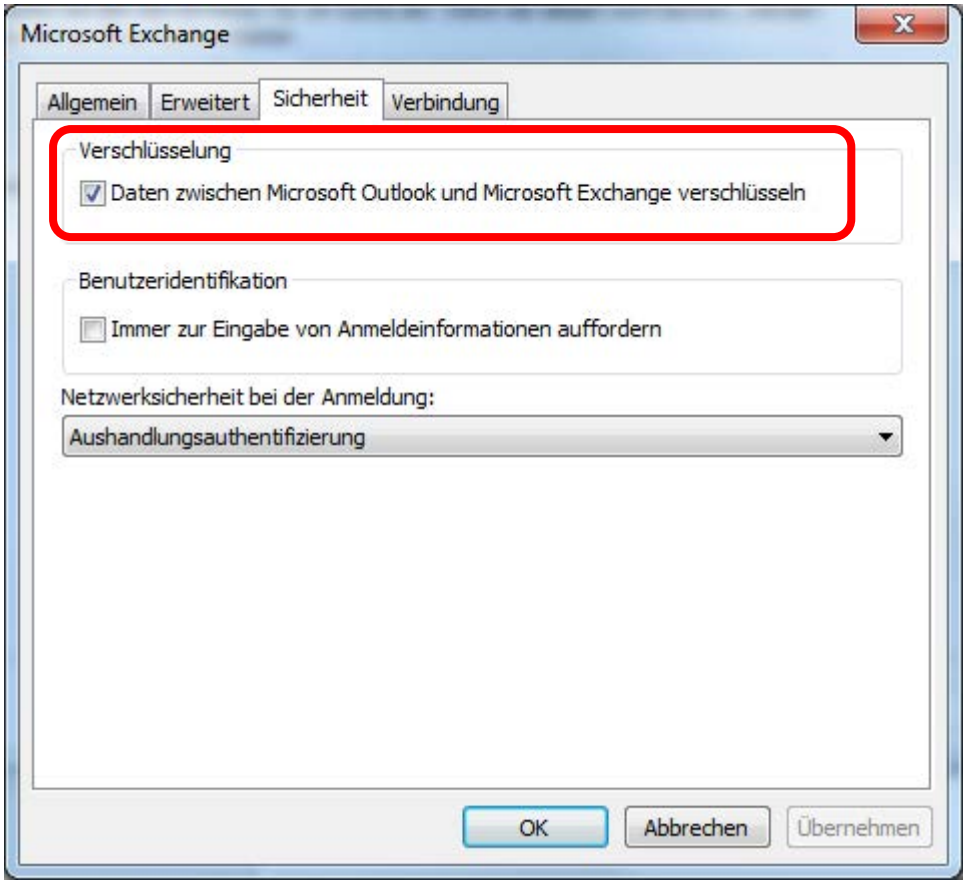
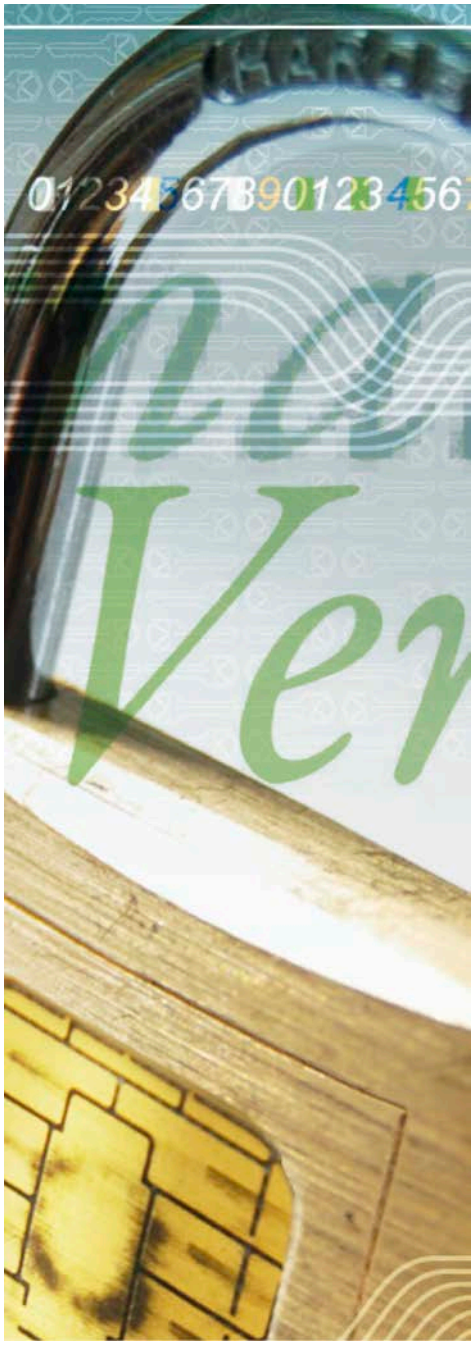


Abbildung 3: Einschalten der Verschlüsselungsoption in Outlook

Alternativ kann das Setzen der Verschlüsselungsoption für eine größere Anzahl von Outlook-Clients per Gruppenrichtlinie erfolgen.

Nach Einschaltung der Verschlüsselungsoption erfolgt die Verbindung der Outlook-Clients zum Exchange-Server komplett verschlüsselt. Das Schlüsselmanagement erfolgt intern und erfordert keine gesonderte Pflege.



Herausgeber & Redaktion
Sächsisches Staatsministerium des Innern
Wilhelm-Buck-Straße 4
01097 Dresden

Verteilerhinweis

Diese Informationsschrift wird von der Sächsischen Staatsregierung im Rahmen ihrer verfassungsmäßigen Verpflichtung zur Information der Öffentlichkeit herausgegeben. Sie darf weder von Parteien noch von deren Kandidaten oder Helfern im Zeitraum von sechs Monaten vor einer Wahl zum Zwecke der Wahlwerbung verwendet werden. Dies gilt für alle Wahlen.

Missbräuchlich ist insbesondere die Verteilung auf Wahlveranstaltungen, an Informationsständen der Parteien sowie das Einlegen, Aufdrucken oder Aufkleben parteipolitischer Informationen oder Werbemittel. Untersagt ist auch die Weitergabe an Dritte zur Verwendung bei der Wahlwerbung. Auch ohne zeitlichen Bezug zu einer bevorstehenden Wahl darf die vorliegende Druckschrift nicht so verwendet werden, dass dies als Parteinahme des Herausgebers zu Gunsten einzelner politischer Gruppen verstanden werden könnte.

Diese Beschränkungen gelten unabhängig vom Vertriebsweg, also unabhängig davon, auf welchem Wege und in welcher Anzahl diese Informationsschrift dem Empfänger zugegangen ist. Erlaubt ist jedoch den Parteien, diese Informationsschrift zur Unterrichtung ihrer Mitglieder zu verwenden.