VOMATEC®

ARIGON® PLUS

ARIGON® PLUS unter Verwendung einer mit SSL/TLS gesicherten Datenbankverbindung zum Microsoft SQL-Server

Kundeninformation

Inhaltsverzeichnis

1 Begriffe/Erklärungen

- SSL (Secure Sockets Layer)
  SSL ist ein Verschlüsselungsprotokoll, das Authentifizierung und Datenverschlüsselung zwischen Servern, Computern und Anwendungen bietet, die in einem Netzwerk arbeiten.
- TLS (Transport Layer Security)
  TLS ist ein Verschlüsselungsprotokoll, das Authentifizierung und Datenverschlüsselung zwischen Servern, Computern und Anwendungen bietet, die in einem Netzwerk arbeiten. TLS basiert auf SSL 3.0, ist aber nicht kompatibel.

2 Voraussetzungen

- Microsoft® SQL Server 2008 und höher, unabhängig von der Edition (Express, …)
- ARIGON® PLUS 4.2 Servicepack 1 und höher

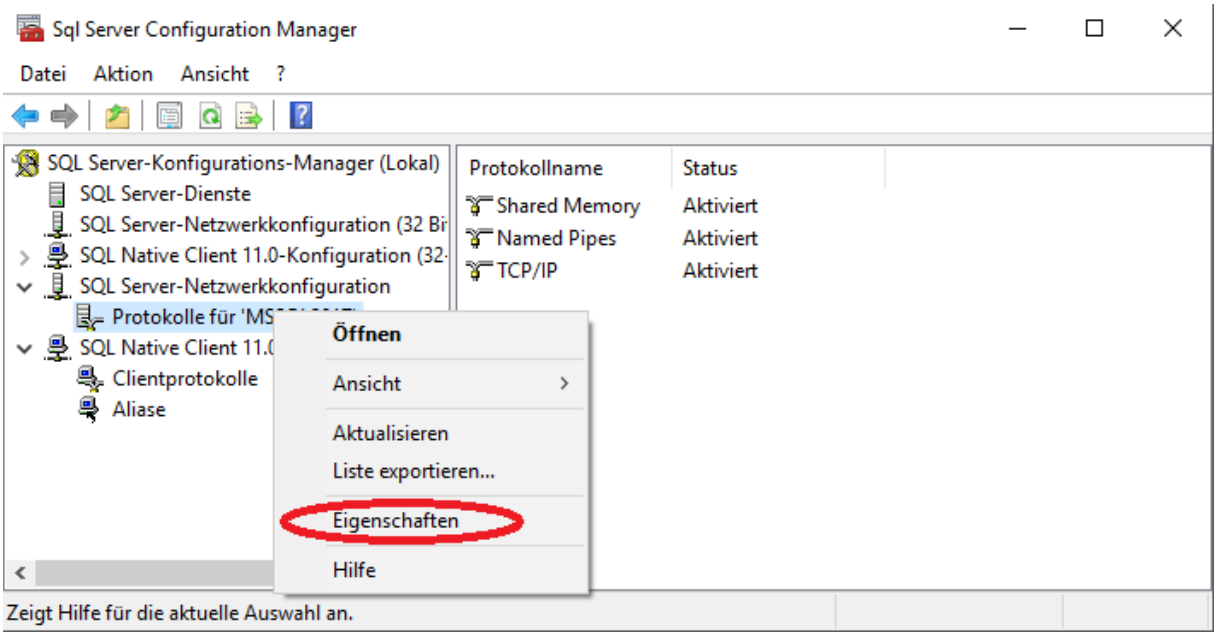
3 Konfiguration des Microsoft® SQL Servers

Der SQL Server hat folgende Möglichkeiten, um Datenbankverbindungen zu sichern:

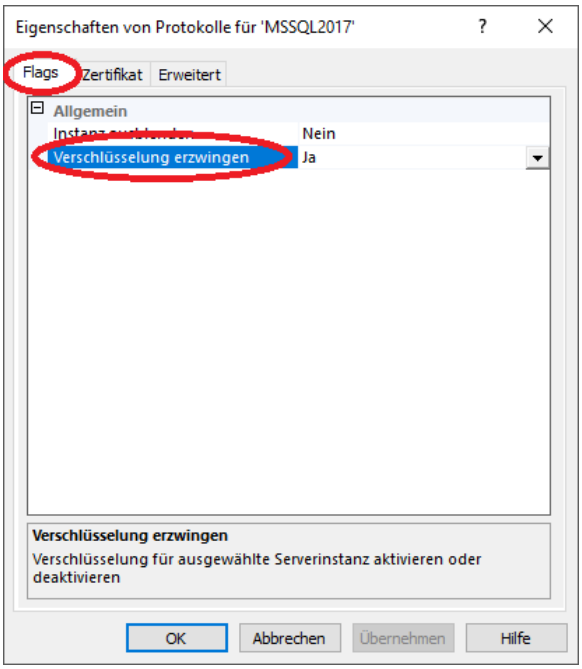
3.1 Verschlüsselung erzwingen

Im „SQL Server Configuration Manager“ kann die Verschlüsselung erzwungen werden:

Unter „SQL Server-Netzwerkkonfiguration“ rechts auf die betreffende Instanz klicken:



Daraufhin öffnet sich folgender Dialog:



Über die Einstellung „Verschlüsselung erzwingen“ auf „Ja“ wird die betreffende SQL Server Instanz so konfiguriert, dass sie ausschließlich verschlüsselte Verbindungen zulässt. Unverschlüsselte Verbindungsversuche schlagen fehl. Ist die Einstellung auf „Nein“ gesetzt, lässt die betreffende SQL Server Instanz sowohl verschlüsselte als auch nicht-verschlüsselte Verbindungen zu.

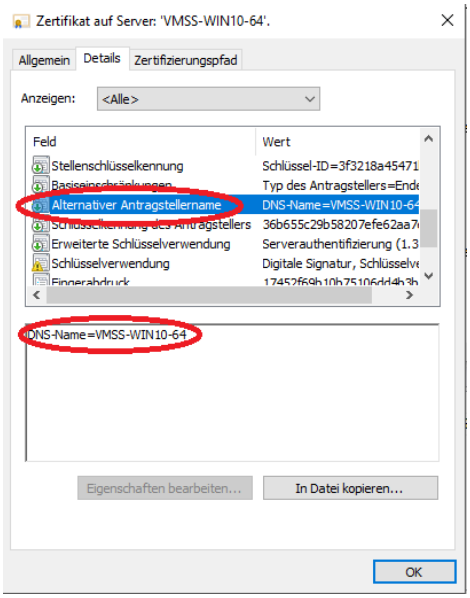
3.2 Authentifizierung des Microsoft® SQL Servers

Eine SSL/TLS-Verbindung ist immer verschlüsselt, aber hierfür muss sie nicht zwingend eine Authentifizierung des Servers beinhalten. Wenn aber eine reine Verschlüsselung ohne Authentifizierung des Servers genutzt wird, ist die Kommunikation verschlüsselt, aber anfällig gegen Man-In-The-Middle-Angriffe.

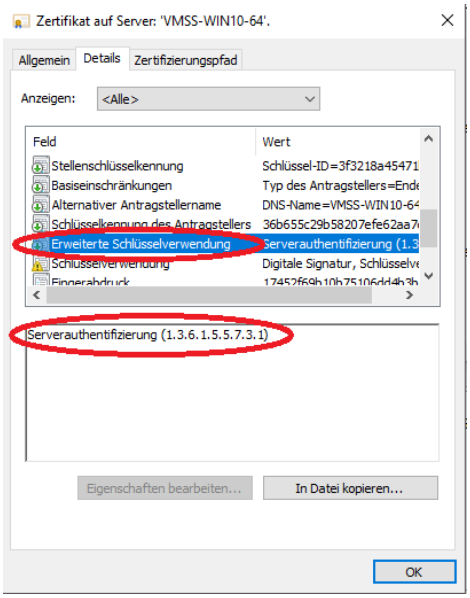
Die Authentifizierung des Microsoft® SQL Servers erfolgt über ein SSL-Serverzertifikat. Es ist also ein gültiges Zertifikat für den Host zu erstellen, auf dem der betreffende Microsoft® SQL Server installiert ist. Es kann ein selbst-signiertes Zertifikat sein, aber die Anfälligkeit gegen Man-In-The-Middle-Angriffe bliebe dann bestehen.

Für das Zertifikat gelten ansonsten folgende Voraussetzungen:

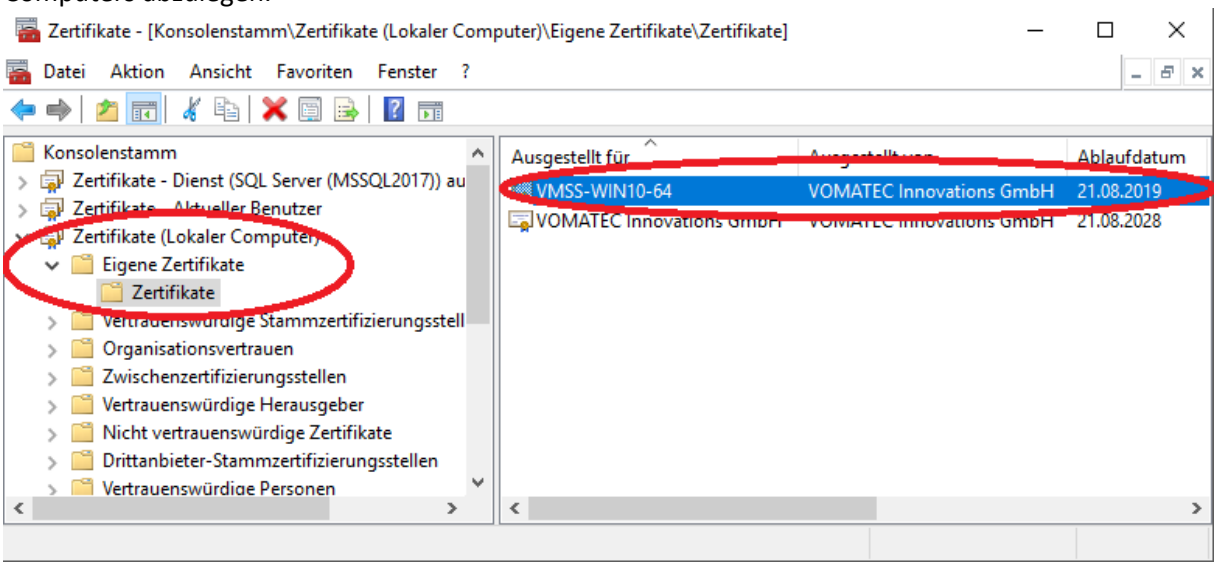
- Das Zertifikat muss exakt auf den FQDN (Fully qualified domain name) des Hosts lauten, auf dem der betreffende Microsoft® SQL Server installiert ist.



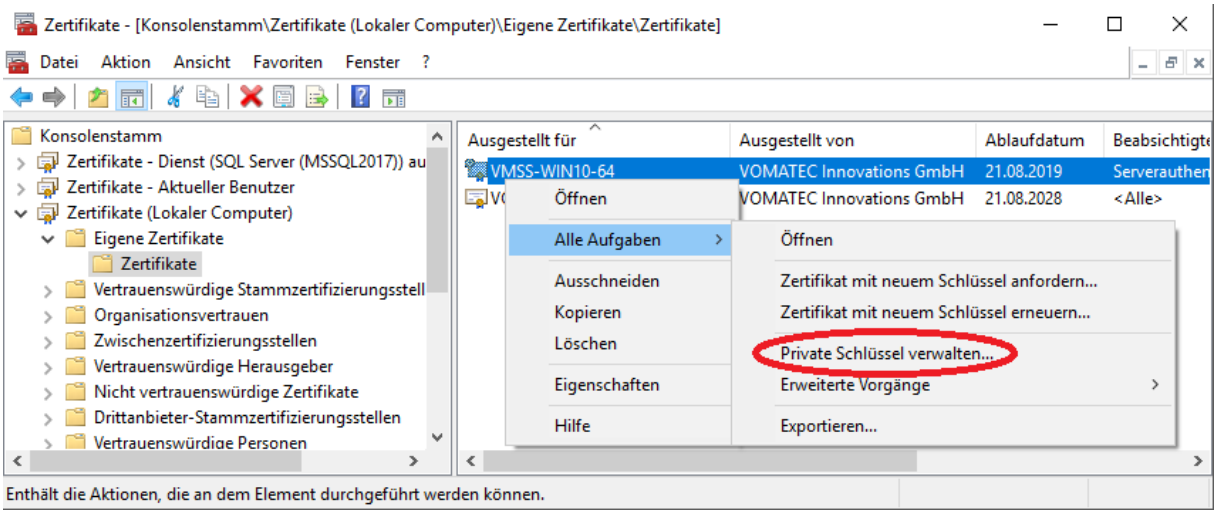
- Das Zertifikat muss als Verwendungszweck „Serverauthentifizierung“ beinhalten.



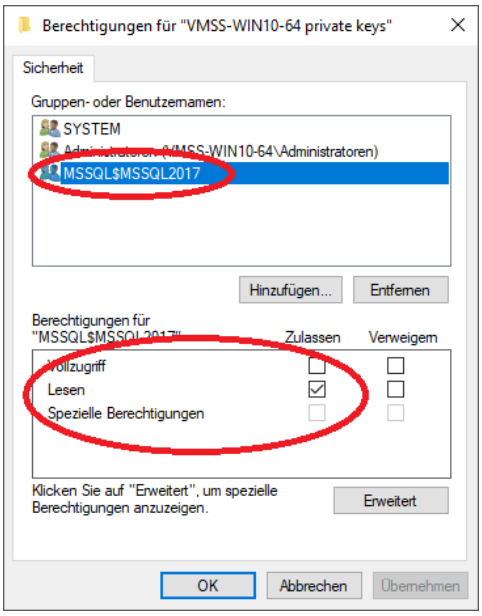
Das oben erzeugte Zertifikat ist anschließend im Zertifikatsspeicher „Eigene Zertifikate“ des lokalen Computers abzulegen:



Anschließend muss dem Benutzerkonto, unter dem der Microsoft® SQL Server betrieben wird, lesender Zugriff auf den privaten Schlüssel des oben erzeugten Zertifikats gewährt werden:

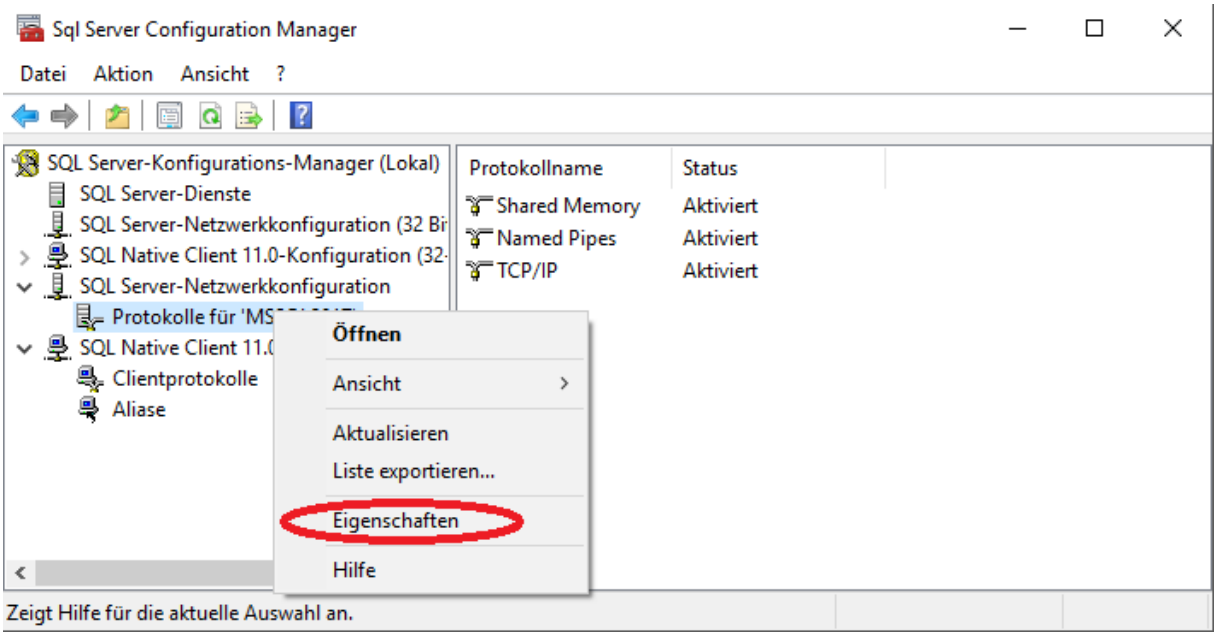


Daraufhin öffnet sich folgender Dialog, wo die entsprechenden Einstellungen („Benutzerkonto des Microsoft® SQL Servers“ und „Lesender Zugriff“) vorzunehmen sind:

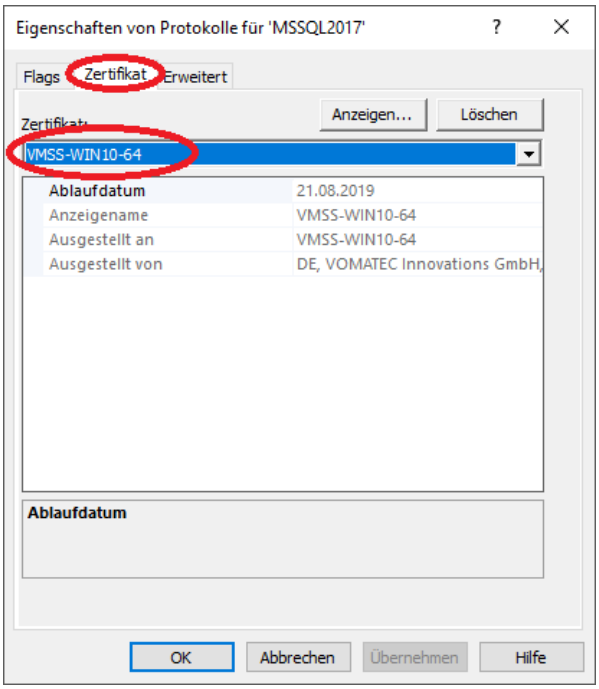


Anschließend muss das Zertifikat im Microsoft® SQL Server gewählt werden, was mit Hilfe des „Sql Server Configuration Managers“ zu tun ist.

Unter „SQL Server-Netzwerkkonfiguration“ rechts auf die betreffende Instanz klicken:



Daraufhin öffnet sich folgender Dialog, in dem auf die Karteikarte „Zertifikat“ gewechselt werden muss. Anschließend sollte das oben erstellte Zertifikat gewählt werden.



Nach dieser Änderung muss der Microsoft® SQL Server neugestartet werden.

4 Konfiguration von ARIGON® PLUS

Es gibt zwei Möglichkeiten, eine verschlüsselte Verbindung zum Microsoft® SQL Server aufzubauen:

4.1 Verschlüsselte Verbindung ohne Authentifizierung des Servers

Der Datenbankverbindungszeichenfolge wird um die folgenden beiden Einträge erweitert:

```
Encrypt=True;TrustServerCertificate=True;
```

Diese Einstellung muss zwingend in der Konfigurationsdatei des ARIGON® PLUS Servers („IMSServer.exe.config“) vorgenommen werden. Die Einstellung „Encrypt=True“ bewirkt, dass eine verschlüsselte Datenbankverbindung aufgebaut wird. Die Einstellung „TrustServerCertificate=True“ bewirkt, dass ein vom Microsoft® SQL Server während des Verbindungsaufbaus geliefertes Zertifikat nicht auf Gültigkeit geprüft wird. Es wird folglich jedes Zertifikat angenommen.

Diese Variante ist anfällig gegen Man-In-The-Middle-Angriffe, da der Microsoft® SQL Server nicht eindeutig authentifiziert wird.

4.2 Verschlüsselte Verbindung mit Authentifizierung des Servers

Der Datenbankverbindungszeichenfolge wird um den folgenden Eintrag erweitert:

```
Encrypt=True;
```

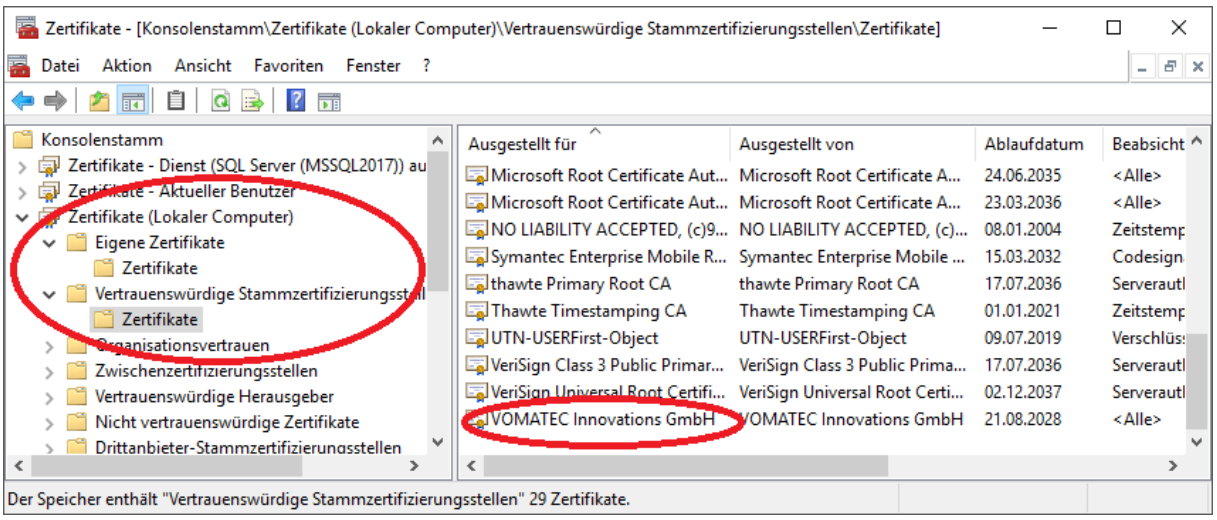
Diese Einstellung muss zwingend in der Konfigurationsdatei des ARIGON® PLUS Servers („IMSServer.exe.config“) vorgenommen werden. Die Einstellung „Encrypt=True“ bewirkt, dass eine verschlüsselte Datenbankverbindung aufgebaut wird. Die fehlende Einstellung „TrustServerCertificate=True“ bewirkt, dass ein vom Microsoft® SQL Server während des Verbindungsaufbaus geliefertes Zertifikat auf Gültigkeit geprüft wird. Es wird folglich die Identität des Microsoft® SQL Servers geprüft.

Diese Variante ist nicht anfällig gegen Man-In-The-Middle-Angriffe, da der Microsoft® SQL Server eindeutig authentifiziert wird.

Achtung!
Da das Zertifikat auf den FQDN des Hosts, auf dem der Microsoft® SQL Server installiert ist, ausgestellt ist und in diesem Fall auf Gültigkeit geprüft wird, muss der Servername in der Datenbankverbindungszeichenfolge vollständig mit dem FQDN übereinstimmen. Die Angabe einer IP-Adresse ist in diesem Fall nicht möglich.

Unabhängig von der Datenbankverbindungszeichenfolge muss das folgende Zertifikat auf allen Client-Rechnern (alle Rechner mit ARIGON PLUS Workstation und/oder ARIGON PLUS Interface) installiert sein:

- Zertifikat der Stammzertifizierungsstelle (CA, certificate authority) des Zertifikats für den Host des Microsoft® SQL Servers



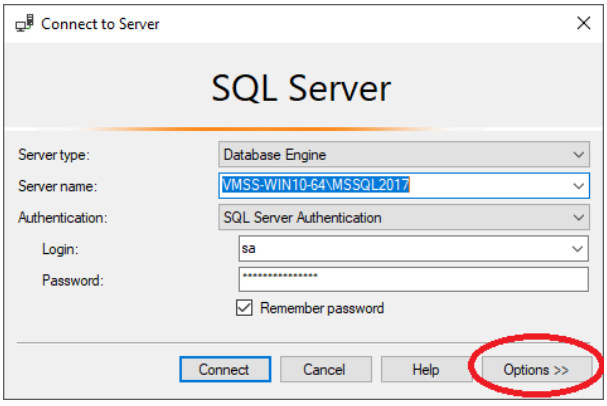
Über dieses Zertifikat wird die Gültigkeitsprüfung des vom Microsoft® SQL Server während des Verbindungaufbaus gelieferten Server-Zertifikats vorgenommen.

5 Verschlüsselte Verbindungen mit Microsoft® SQL Server Management Studio

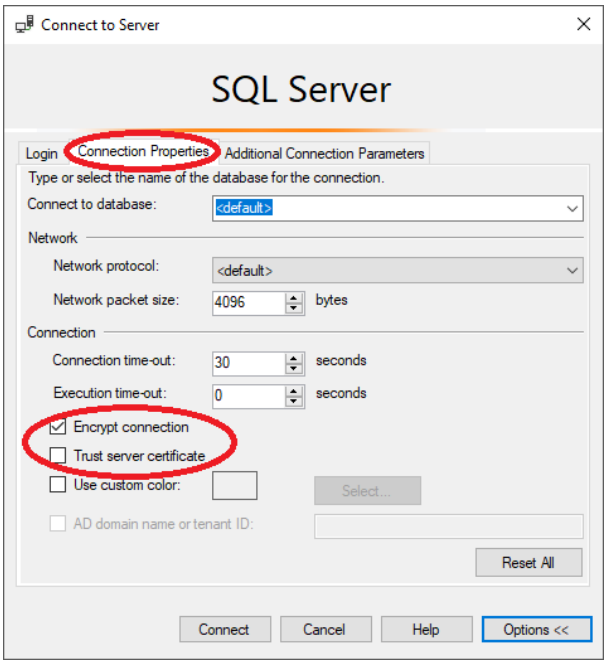
Innerhalb des Microsoft® SQL Server Management Studio sind folgende Informationen bei Einsatz von verschlüsselten Datenbankverbindungen von Belang:

5.1 Herstellen einer verschlüsselten Verbindung

Beim Herstellen der Verbindung ist der Taster „Options >>“ zu betätigen.



Daraufhin ändert der Verbindungsdialog sein Aussehen wie folgt:



Auf dem Tab „Connection Properties“ gibt es die beiden Checkboxen „Encrypt connection“ und „Trust server certificate“. Diese beiden Checkboxen haben analoge Bedeutungen wie die korrespondierenden Einstellungen in der Datenbankverbindungszeichenfolge (siehe Konfiguration von ARIGON® PLUS).

5.2 Prüfen auf bestehende, verschlüsselte Verbindungen

Mit folgendem SQL Befehl kann geprüft werden, welche bestehenden Verbindungen zum Microsoft® SQL Server verschlüsselt sind:

```
SELECT session_id,
       connect_time,
       net_transport,
       encrypt_option,
       auth_scheme,
       client_net_address
FROM sys.dm_exec_connections
```