coco:health

Krankenkassen-Kommunikations-System (KKS)

Das bewährte Kommunikationssystem

FAQ zur Softwareversion 9 und höher

19.11.2024

CoCoNet Computer-Communication Networks GmbH

www.coconet.de

coco:health

Krankenkassen-Kommunikations-System (KKS)

FAQ zur Softwareversion 9 und höher

CoCoNet Computer-Communication Networks GmbH, Parsevalstr. 9b, D-40468 Düsseldorf, Deutschland
Telefon: +49 (0) 2 11 / 2 49 02 - 0
Internet: www.coconet.de
E-Mail: info@coconet.de

Hinweis zur Protokollierung

Alle relevanten vom Benutzer oder vom System initiierten Aktionen werden protokolliert, sofern die Aktionen in dem vorgegebenen Rahmen ausgeführt werden. Bei Bedienungsfehlern oder Manipulationen ist die Protokollierung der Aktionen nicht gewährleistet.

Zu dieser FAQ

Diese FAQ beschreibt häufige Fragen bezüglich der Installation, Konfiguration und Bedienung des Produkts KKS Version 9.0 -13.0.

Für die TCP/IP Anbindung des FTAM Connectors gibt es eine separate FAQ „FAQ zum FTAM TCPIP Connector“.

Für die E-Mail Anbindung des MAIL Connectors gibt es eine separate FAQ „FAQ zum E-Mail Connector“.

Zielgruppe

Die FAQ richtet sich an die Anwender eines KKS-Systems.

Es wird vorausgesetzt, dass Sie mit der Bedienung des KKS Clients und des verwendeten Betriebssystems vertraut sind.

Hotline

Wenn Sie Fragen oder Schwierigkeiten im Umgang mit dem Produkt KKS haben, setzen Sie sich bitte mit der Hotline in Verbindung.

Bei Rückfragen zu bestehenden Anfragen erreichen Sie die CoCoNet Hotline unter:

Telefon: 02 11 / 249 02-555
Fax: 02 11 / 249 02-200

E-Mail : hotline@coconet.de

Inhaltsverzeichnis

1. KKS Client X.0 Installation

1.1. Allgemeine Hinweise

Die Installation des KKS Clients muss von einem lokalen Laufwerk aus erfolgen.

Für die neue Security wird JAVA 32-Bit benötigt. Bitte lesen Sie dazu die Hinweise im Punkt „Installation/Upgrade“.

Der installierte KKS Client sollte vor einem Wechsel auf die aktuelle Version gesichert werden. Bitte gehen Sie dazu wie im Kapitel Sicherung des KKS Clients beschrieben vor.

Bei einer neuen Installation muss die setup.exe ausgeführt werden und der neue KKS Client muss in ein neues Installationsverzeichnis installiert werden. Er darf nicht in das Installationsverzeichnis einer vorherigen Installation KKS Client installiert werden.

Bei einem Upgrade muss die Upgrade_X.0.0.x.exe in das KKS Client Installationsverzeichnis kopiert und dort ausgeführt werden.

Das Betriebssystem, auf dem der KKS Client installiert werden soll, muss eine deutsche Version sein, da es sonst bei der Installation des SQL Servers zu Problemen kommt.

Die Installation des KKS Clients auf reinen 64-Bit Betriebssystemen (ohne 32-Bit Unterstützung) ist nicht möglich, da der KKS Client eine 32-Bit Anwendung ist. Die Unterstützung von 32-Bit Applikationen muss gewährleistet sein.

Nach einem Rechnerwechsel werden die in der Datenbank hinterlegten „alten“ Pfade für die Journaldateien und die Eingabe- und Ausgabeverzeichnisse angezeigt. Diese müssen im Zuge der Installationsnachbearbeitung manuell angepasst bzw. angelegt werden. Zudem ist ggf. auch die Übernahme der Zertifikate (Trustcenter und Stammzertifizierungsstelle) in den Windows Zertifikatsspeicher des neuen KKS Rechners erforderlich (s. Punkt Nachbearbeitung).

In der KKS Client Version 9.x und höher ist die Unterstützung der vom Bundesamt für Sicherheit in der Informationstechnik (BSI) empfohlenen und in der Security Schnittstellenspezifikation der GKV festgelegten 4K Schlüssel und angepassten Sicherheitsverfahren (Paddingalgorithmen) umgesetzt worden.

Für den Betrieb der KKS Anwendung wird das Microsoft NET-Framework 4.0/4.8 benötigt. Das .NET-Framework ist Bestandteil der Windows Installation.

- ➔ Kunden der Firma AGFA HealthCare erhalten separat eine Dokumentation bezüglich des Lizenzhandlings bei der Installation des KKS Clients V.X. Bitte fordern Sie diese Dokumentation ggf. bei der Firma AGFA HealthCare an.
- ➔ Die Installation des KKS Clients muss durch einen Benutzer erfolgen, der mindestens über lokale Administratorrechte verfügt.

2. Installationsvorbereitung

Die folgenden Punkte gelten für eine Neu-Installation, nicht für ein Upgrade, da bei einem Upgrade von einem produktiven KKS Client ausgegangen wird.

2.1. Windows 10, Windows 11, Windows Server 2016/2019/2022

Die Unterstützung von 8.3 Namen muss vor der Installation aktiviert sein. Die generelle Unterstützung kann als Administrator in einer DOS-Box wie folgt geprüft werden:

fsutil 8dot3name query C:

(wobei C: für das Laufwerk steht, auf dem der KKS Client installiert werden soll).

Ist die 8.3 Notation nicht möglich wir eine Installation ohne Leerzeichen im Pfadnamens empfohlen Beispiel C:\Coconet\KKSClient\

Falls das .NET-Framework in der Version 4.5 bereits auf dem neuen Rechner vorinstalliert ist, muss diese Version temporär deinstalliert werden, da sich sonst die Version 4.0 nicht installieren lässt. Die Version 4.5 kann im Anschluss an die KKS Installation wieder über die regulären Windows Updates installiert werden.

2.2. Installation/Upgrade/Rechnerwechsel

Oracle JAVA 32-Bit muss auf dem Rechner installiert werden, um die neue Security nutzen zu können. Die Einrichtung der JAVA Umgebung ist hier beschrieben, s. "Vorbereitung" im Kapitel Upgrade KKS Client V.X

Das automatische JAVA Update muss ausgeschaltet werden, da sich bei einem Update der JAVA Installationspfad ändert und dann der in der Systemvariablen PATH eingetragene Pfad nicht mehr stimmt. Diese Angabe gilt nicht für KKS Client Versionen neuer als 12.0

Wenn die JAVA VM nicht gefunden werden kann, können keine Aufträge mehr verarbeitet werden, kein Schlüssel generiert werden oder Sammeldateien verarbeitet werden. Es wird folgender Fehler gemeldet:

„Die DLL: PKCS7Key.dll‘: Das angegebene Modul wurde nicht gefunden.“

Im Folgenden sind die Vorgehensweisen für die verschiedenen Installations- und Datenübernahmeszenarien beschrieben:

2.2.1. Upgrade KKS Client V.X -> V.12

Bei einem Upgrade wird eine produktive KKS Client Version x vorausgesetzt. Gehen Sie dann wie folgt vor:

Vorbereitung:

- Bevor Sie mit dem Upgrade des KKS Clients beginnen, stellen Sie bitte sicher, dass Java 8 32-Bit auf dem KKS Clientrechner installiert wurde und der vollständige Pfad zur JAVA JVM in der Systemumgebungsvariablen PATH enthalten ist.
- Laden Sie JAVA 8 JRE (Java Runtime Environment) von der Oracle Homepage herunter und installieren Sie JAVA. Wechseln Sie anschließend im Windows Explorer in das JAVA Installationsverzeichnis, dann in das Unterverzeichnis „bin“ und anschließend nach „client“ (dort liegt die Datei jvm.dll), z.B. C:\Program Files (x86)\Java\jre1.8.0_241\bin\client.
- Kopieren Sie den in der Adressleiste des Windows Explorers angezeigten Pfad und klicken auf die Windows-Taste. Suchen Sie nach „Systemumgebungsvariablen bearbeiten“ -> Umgebungsvariablen -> Systemvariablen -> PATH und fügen dort den zuvor kopierten Pfad ein (danach muss ggf. ein Semikolon als Trenner zu den bereits bestehenden Pfadangaben folgen).
- Deaktivieren Sie dann die JAVA Updates in den JAVA Einstellungen.

Upgrade:

- Öffnen Sie die KKS Administrationsoberfläche und klicken oben im Menü auf das „?“ und dort dann ganz unten auf „Installationsordner öffnen“.
- Schließen Sie die KKS Administrationsoberfläche und stoppen die KKS Dienste.
- Kopieren Sie die Datei Upgrade_X.0.0.X.exe in den zuvor im Windows Explorer geöffneten **Installationsordner**.
- Prüfen Sie über die rechte Maustaste -> Eigenschaften -> Karteikarte „Allgemein“, ob die Datei von Windows gesperrt wurde, weil sie von einem anderen Computer stammt. Ggf. gibt es unterhalb des Bereichs „Attribute“ noch den Bereich „Sicherheit“; dort muss dann auf „Zulassen“ geklickt werden.
- Führen Sie die Upgrade_X.0.0.X.exe als lokaler Administrator aus.

Nachbereitung:

- Wechseln Sie im Windows Explorer in das Verzeichnis Secret.Key.PKCS7.SHA256 -> <IK-Nummer>.ACT und prüfen, ob der Dateiname der .p7c Datei dem Dateinamen der .p10-Datei entspricht. Vor der Dateinamenserweiterung (.p7c) darf nur die 9stellige IK-Nummer stehen; ggf. ist die 9. Stelle zu ergänzen und nachfolgende Zeichen zu löschen.

Wenn Sie o.g. Schritte ausgeführt haben, muss der Rechner neu gestartet werden.

- Holen Sie anschließend die Sammeldatei **annahme-rsa4096.key vom Trustcenter ab und lassen Sie im KKS Client verarbeiten.**

2.2.2. Installation KKS Client V.12

- Kopieren Sie den Inhalt der CD in ein temporäres Verzeichnis auf dem Rechner auf dem der KKS Client installiert werden soll.
- Beenden Sie vor der Installation alle laufenden Anwendungen.
- Installieren Sie Oracle JAVA 8 32-Bit und nehmen den Pfad zur jvm.dll in die Systemumgebungsvariable PATH auf, s. Einrichten der JAVA Umgebung
- Starten Sie die setup.exe in dem temporären Verzeichnis.
- Das KKS Setup installiert nun alle noch fehlenden Komponenten
- .NET-Framework 4.0 (falls erforderlich)
- SQL Server 2017 Express
- Nach dem Start der Administrationsoberfläche hilft Ihnen ein Einrichtungsassistent bei der Neueinrichtung des KKS Clients.

2.2.3. Installation KKS Client V.13

- Kopieren Sie den Inhalt der CD in ein temporäres Verzeichnis auf dem Rechner auf dem der KKS Client installiert werden soll.
- Beenden Sie vor der Installation alle laufenden Anwendungen.
- Installieren Sie JAVA 32-Bits
- Starten Sie die setup.exe in dem temporären Verzeichnis.
- Das KKS Setup installiert nun alle noch fehlenden Komponenten
- .NET-Framework 4.8 (falls erforderlich)
- SQL Server 2022 Express
- Nach dem Start der Administrationsoberfläche hilft Ihnen ein Einrichtungsassistent bei der Neueinrichtung des KKS Clients.

2.3. Datenübernahme

Beachten Sie bitte, dass bei einer Datenübernahme nur die KKS Programmdaten übernommen werden. Nach der Datenübernahme müssen daher noch u.a. die Übergabeverzeichnisse, sowie die Zertifikate, die im Windows Zertifikatsspeicher des „alten“ Rechners abgelegt sind, übernommen werden, s. Punkt „Nachbearbeitung“.

2.3.1. Rechnerwechsel mit Datenübernahme

- Installieren Sie die bestehende KKS Clientversion auf dem neuen Rechner und starten anschließend den KKS Client, um den Erfolg der Installation zu überprüfen.
- Schließen Sie den KKS Client dann wieder, stoppen die KKS Dienste und die SQL Serverdienste.
- Wechseln Sie bitte zum den alten Rechner.

- Stoppen Sie die KKS Dienste und den SQL Server und sichern Sie folgende Dateien/Verzeichnisse in Ihrem KKS Client Verzeichnis.

```
Data
Data_orig
Journal
Secret.Key.PKCS7
Secret.Key.PKCS7.SHA256
Secret.Key.PKCS7.SHA256.4K
Public.Key.PKCS7
Public.Key.PKCS7.SHA256
Public.Key.PKCS7.SHA256.4K
Templates
KKSApplication.config
```

- Wechseln Sie zurück auf den neuen Rechner in das Installationsverzeichnis des KKS Clients und ersetzen die gleichnamigen Ordner mit den soeben gesicherten Ordnern.
- Ersetzen Sie anschließend die Datei KKSApplication.config.
- Importieren Sie die Datenbank mit Hilfe das Tools DBdump.exe (Informationen entnehmen Sie bitte den ReleaseNotes und dem Handbuch
- Abschließend muss der Rechner neu gestartet werden.

2.3.2. Nachbearbeitung

Die hier beschriebenen Prüfungen erfolgen üb die Administrationsoberfläche des KKS Clients.

Prüfen der in der Datenbank hinterlegten Pfadangaben nach einer Datenübernahme:

- Das Ablageverzeichnis des Journals (Journal -> Einstellungen) muss auf das Journal-verzeichnis im aktuellen KKS Client Installationsverzeichnis verweisen.
- Verzeichnisangaben unter Konfiguration -> Einstellungen
- Die Verzeichnisse werden nicht automatisch angelegt und müssen daher neu angelegt und zugeordnet werden. Die Verzeichnisse müssen explizit neu zugeordnet werden, auch wenn sie schon korrekt angezeigt werden.
- Falls der KKS Client auf Netzwerklaufwerke zugreift (Konfiguration -> Einstellungen) muss der Benutzer Rechte für den Betrieb des KKS Clients, für den lokalen Rechner und für die Netzlaufwerke haben. Ggf. muss beim KKS Kerneldienst und bei dem KKS FS-Connector-Dienst ein entsprechend berechtigter Benutzer konfiguriert werden (Windows -> Systemsteuerung (-> System und Sicherheit) -> Verwaltung -> Dienste – <KKS Dienst> -> Eigenschaften -> Karteikarte Anmelden).

➔ Beachten Sie bitte außerdem, dass nur UNC Pfadangaben (mit \\ beginnend) verwendet werden können. Gemappte Laufwerke (Laufwerksbuchstabe X:) können nicht verwendet werden, s. Bekannte Probleme.

➔ Hinweis: Wenn Verzeichnisangaben geändert wurden, muss der KKS FS Connector neu gestartet werden.

- Aktualisierung der Zertifikate im Windows Zertifikatsspeicher (nur bei einem Rechnerwechsel erforderlich):

- Die Vorgehensweise für die Aktualisierung der Zertifikate ist je nach Trustcenter unterschiedlich, da die Zertifikate der DKTIG nicht in den Sammeldateien mit den öffentlichen Schlüsseln der Annahmestellen enthalten sind.
    - Vorgehensweise für ITSG Kunden:
      Laden Sie die Sammeldatei mit den öffentlichen Schlüsseln der Annahmestellen von der ITSG Seite herunter und kopieren die Datei in das Eingabeverzeichnis des KKS Clients. Dadurch werden auch die Zertifikate im Windows Zertifikatsspeicher aktualisiert.

    - Vorgehensweise für DKTIG Kunden:
      Die Zertifikate können manuell aktualisiert werden (siehe Anhang „Manuelle Übernahme von Zertifikaten in den Windows Zertifikatsspeicher“). Die DKTIG bietet zusätzlich auch das Abholen der Sammeldateien über FTAM TCP/IP an.
- Die Verbindungsdaten zur DKTIG lauten:
    - IP-Adresse: 194.145.83.92
    - Port: 3280

➔ Anmerkung: Wenn die Sammeldatei über den KKS Client abgeholt wird und eine andere Sammeldatei als die angezeigte Sammeldatei ausgewählt wird, muss dies erst über den Button „OK“ bestätigt werden, um die Änderung zu speichern.
➔ Anmerkung: Wenn die CA und PCA Zertifikate nicht im Windows Zertifikatsspeicher vorhanden sind, führt dies zu folgenden Fehlern:
➔ Fehler bei der Anzeige der PKCS#7-Schlüsseldetails (Konfiguration -> Einstellungen -> Bereich Schlüsselmanagement)
➔ Fehler bei der Verarbeitung von empfangenen bzw. zu versendenden Dateien.

2.3.3. Bekannte Probleme

- Bei der Installation und dem Betrieb des KKS Clients können Probleme auftreten, wenn - die Microsoft Benutzerkontensteuerung (UAC – Einstellungen der Benutzerkonten-steuerung) aktiviert ist. Deaktivieren Sie diese ggf. in der Systemsteuerung im Menübereich Benutzer.
- Aufgrund eines Fehlers im .NET-Framework ist der Zugriff auf einen im Netzwerk freigegebenen Ordner nur über UNC Pfadangaben möglich.
- In einigen Fällen kann es vorkommen, dass sich der KKS FTAM Connector direkt nach dem Start wieder beendet (s.u. „Der KKS FTAM Connector beendet sich wieder“)
- Wenn der KKS Client auf einem Windows XP SP3 Rechner betrieben wurde und auf ein neueres Betriebssystem, wie z.B. Windows 10, gewechselt wurde, kann es Probleme mit der Zertifikatskette des privaten Schlüssels geben. In diesem Fall kommt es zu einem Fehler, wenn in der Karteikarte Konfiguration die Einstellungen aufgerufen werden. Zudem kommt es zu Verarbeitungsfehlern. Wenden Sie sich in diesem Fall bitte an die CoCoNet Hotline.

2.4. Mögliche Probleme bei der Installation

2.4.1. Probleme bei der Installation auf Windows 7/8 und Windows Server 2008

Falls das .NET-Framework 4.5 bereits auf dem Rechner installiert ist, wird die Installation des .NET-Framework 4 während des Setups übergangen. In der Folge lässt sich der KKS Client ggf. nicht starten oder es kommt im laufenden Betrieb zu Exceptions. Diese werden im Windows Ereignisanzeige (Anwendungsprotokoll) protokolliert.

Lösung: Nachträgliche Installation des .NET-Framework 4:

- Beenden Sie alle KKS-Dienste und stoppen Sie den Datenbankdienst.
- Deinstallieren Sie das.NET-Framework 4.5 und installieren Sie das .NET-Framework 4 von der Installations-CD (..\ISSetupPrerequisites\{32D7E3D1-C9DF-4FA6-9F9B4D5117AB2917} \dotNetFx40_Full_x86_x64.exe).
- Starten Sie die Dienste wieder.

➔ Anmerkung: Das .NET-Framework 4.5 kann danach über die Windows Updates wieder installiert werden.

2.4.2. Probleme bei der Installation auf Windows 7/8 und Windows Server 2008/2012

Bei der Ausführung der setup.exe wird ein Fehler bei create table gemeldet.

Dies lässt darauf schließen, dass das Setup mehrfach ausgeführt wurde.

Lösung: Bitte deinstallieren Sie den KKS Client V.9 und den SQL Server 2008 über Systemsteuerung.

Löschen Sie dann die jeweiligen Installationsverzeichnisse, starten den Rechner neu und führen dann das Setup erneut aus.

2.4.3. Probleme bei der Installation auf Windows Server 2008 R2 64-Bit

Die Installation des SQL Servers schlägt fehl.

Lösung: Bitte verwenden Sie die deutsche Version des Betriebssystems. Wenn dies sichergestellt ist, senden Sie bitte die Installations-Log-Dateien des SQL Servers an die CoCoNet Hotline (s. SQL Server 2008 Log-Dateien).

2.4.4. Probleme nach der Installation auf Windows Win7/8 bzw. Windows Server 2008/2012

Der KKS Kernel kann nicht gestartet werden.

Lösung:

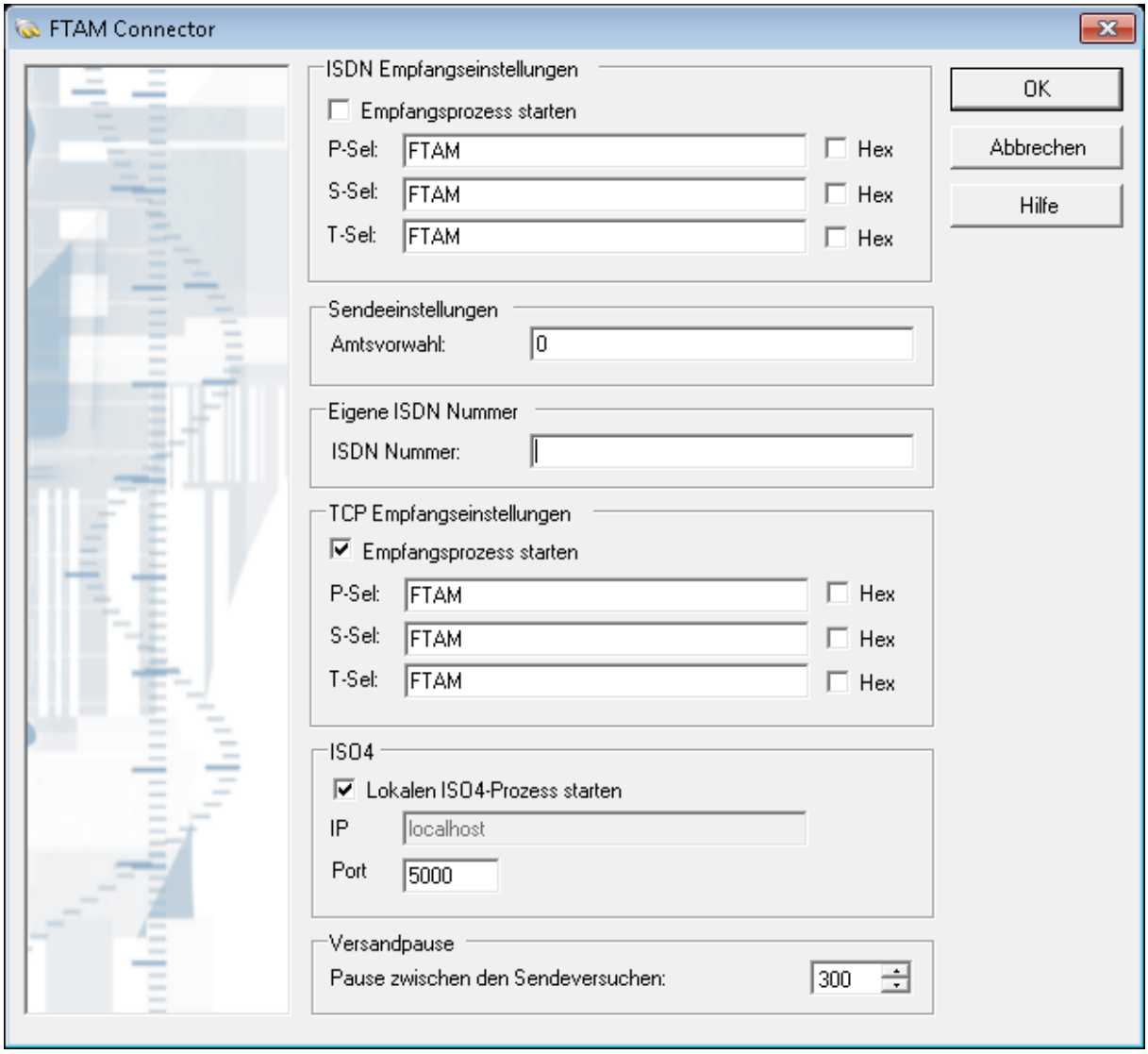
- Bitte prüfen Sie in der Windows Ereignisanzeige (Anwendungsprotokoll), ob ggf. ein Lizenzproblem gemeldet wird.
- Bitte prüfen Sie, ob die Datei `KKSApplication.config` (von der Auslieferungs-CD) im Installations-verzeichnis des KKS Clients liegt.

➔ Anmerkung:
Bei Kunden der Firma AGFA HealthCare muss zusätzlich die Datei `AGFAVersion.txt` im Installationsverzeichnis des KKS Clients liegen.

- Bitte prüfen Sie, ob die auf den Rechner übertragenen Dateien durch die Windows Sicherheit blockiert wurde, s. Programmdateien sind blockiert.
- Der KKS FTAM Connector beendet sich wieder.

Wenn die Neuinstallation auf einem System erfolgt ist, das keine ISDN Anbindung mehr hat, entfernen Sie bitte in den systemweiten Einstellungen des FTAM Connectors das Häkchen bei „Empfangsprozess starten“.

Karteikarte System -> Bereich „Dateischnittstelle und Transferverfahren“ -> FTAM



Wenn das Problem auch nach Bearbeitung der u.g. Punkte auftritt, prüfen Sie bitte auch die im Dokument „FAQ zum FTAM-TCPIP Connector“ im Kapitel „Der FTAM Connector beendet sich kurz nach dem Start“ genannten Punkte.

➔ Anmerkung zum Einspielen heruntergeladener Programmdateien:
Entpacken Sie die heruntergeladenen Dateien in ein temporäres Verzeichnis.
Stoppen Sie den KKS Kerneldienst.
Sichern Sie die bestehenden gleichnamigen Dateien im KKS Client Installations-verzeichnis, indem Sie sie in ein Sicherungsverzeichnis kopieren (bitte nicht verschieben oder umbenennen).
Kopieren Sie anschließend die entpackten Dateien in das KKS Client Installations-verzeichnis und überschreiben damit die zuvor gesicherten Dateien.
Prüfen Sie, ob die Dateien von Windows blockiert wurden, da Windows erkannt hat, dass die Daten von einem anderen System stammen. Heben Sie die Blockierung auf, s. Programmdateien sind geblockt.
Danach können die KKS Dienste wieder gestartet werden.

2.4.5. Probleme nach einem Upgrade

Nach dem Upgrade wird die alte KKS Client Version angezeigt:

In diesem Fall wurde die Upgrade_X.0.0.x.exe nicht aus dem KKS Client Installationsverzeichnis ausgeführt.

Lösung:

- Deinstallieren Sie das KKS Client Update wieder über die Windows Programme.
- Kopieren Sie die Upgrade_X.0.0.x.exe in das KKS Client Installationsverzeichnis und starten Sie die Upgrade_X.0.0.x.exe mit Administratorrechten.

3. FAQ

3.1. Allgemeiner Hinweis

Sollte sich Ihr Problem nicht durch die unten aufgeführten Hinweise lösen lassen, so senden Sie uns bitte über das Supportformular (zu finden auf unserer Homepage) eine genaue Fehlerbeschreibung, Screenshots von der Fehlermeldung, die Journaldateien und, sofern möglich, die „Informationen zur Fehlerbehebung“ (siehe KKS Menü -> ? -> „Informationen zur Fehlerbehebung“) zu.

- ➔ Die meisten Probleme nach einer Installation sind Folgeprobleme.
- ➔ Bitte stellen Sie sicher, dass JAVA 32-Bit installiert ist und der vollständige Pfad zur JAVA VM der Systemumgebungsvariablen PATH vorangestellt ist, s.“Einrichten der JAVA Umgebung““
- ➔ Bitte stellen Sie sicher, dass die Dateinamen in den privaten Schlüsselverzeichnissen korrekt benannt sind, s. „Prüfen Sie die Dateinamen im privaten Schlüsselverzeichnis“

3.2. Einrichten der JAVA Umgebung

Laden Sie JAVA 8 von der Oracle Homepage herunter und installieren Sie JAVA. Wechseln Sie anschließend im Windows Explorer in das JAVA Installationsverzeichnis, dann in das Unterverzeichnis „`bin`“ und dann in das Unterverzeichnis „`client`“ (dort liegt die Datei `jvm.dll`), z.B. `C:\Program Files (x86)\Java\jre1.8.0_241\bin\client`.

Kopieren Sie den in der Adressleiste des Windows Explorers angezeigten Pfad und klicken auf die Windows-Taste. Suchen Sie nach „Systemumgebungsvariablen bearbeiten“ und klicken auf den Button „Umgebungsvariablen“ -> Systemvariablen -> PATH und fügen dort den zuvor kopierten Pfad ein (danach muss ggf. ein Semikolon als Trenner zu den bereits bestehenden Pfadangaben eingefügt werden).

Deaktivieren Sie dann die JAVA Updates in den JAVA Einstellungen.

3.3. Fehler bei oder nach einem Upgrade

3.3.1. Die KKS Dienste sind nach der Deinstallation des Upgrades nicht mehr vorhanden

Die KKS Dienste können wie folgt registriert werden:

- Installieren:
  [FRAMEWORKDIR]\ v4.0.30319\InstallUtil.exe „[INSTALLDIR]\Kernel.exe"
  [FRAMEWORKDIR]\ v4.0.30319\InstallUtil.exe „[INSTALLDIR]\FSConnector.exe"
  [FRAMEWORKDIR]\ v4.0.30319\InstallUtil.exe „[INSTALLDIR]\FTAMConnector..exe"
  [FRAMEWORKDIR]\ v4.0.30319\InstallUtil.exe „[INSTALLDIR]\HTTPConnector..exe"
  [FRAMEWORKDIR]\ v4.0.30319\InstallUtil.exe „[INSTALLDIR]\MailConnector..exe"
- Deinstallieren
  [FRAMEWORKDIR]\ v4.0.30319\InstallUtil.exe /u „[INSTALLDIR]\Kernel.exe"

`FRAMEWORKDIR` entspricht dem .NET Framework Installationspfad.

Dies liegt unter c:\Windows\Microsoft.NET\Framework\

`INSTALLDIR` entspricht dem KKS Client Installationsverzeichnis.

3.3.2. Der KKS Kernel kann nicht gestartet werden

Prüfen Sie die hier genannten Punkte.

3.3.3. Fehler bei der Verarbeitung von zu versendenden Dateien

Fehlermeldung: PKCS7Cryptography: SignFile: PKCS7.dll – Could not sign

Lösung:

- Prüfen Sie die Dateinamen im privaten Schlüsselverzeichnis.
- KKS Client Menü -> „?“ -> „Installationsordner öffnen“
- <KKS Client Installationsverzeichnis>\Secret.Key.PKCS7.SHA256\<IK-Nummer>.ACT
  bzw.
  <KKS Client Installationsverzeichnis>\Secret.Key.PKCS7.SHA256.4K\<IK-Nummer>.ACT
- Bei der Zertifikatsdatei vom Trustcenter (Dateiendung .p7c) muss die IK-Nummer vollständig sein (oft fehlt die 9.Stelle bei der .p7c-Datei). **Nach der IK-/BN-Nummer darf nur noch die Dateiendung .p7c folgen**, z.B. 111222333.p7c.
- Starten Sie anschließend nochmal die Verarbeitung des fehlerhaft verarbeiteten Auftrags über die rechte Maustaste „Job erneut erzeugen“ an.
- Laden Sie die aktuelle Sammeldatei von der **ITSG** Seite herunter. Achten Sie bitte darauf, dass Sie die Sammeldateien vom Trustcenter herunterladen, welche die Zertifikate mit denselben kryptographischen Verfahren (SHA-256 oder RSA-4096) wie Ihr privater Schlüssel enthalten.

- Sollten die Schlüsseldetails nach der Verarbeitung der Sammeldatei immer noch nicht angezeigt werden können, muss die Zertifikatskette manuell in den Windows Zertifikatsspeicher übernommen werden (siehe erweiterte Lösungsvariante im Anhang: „Manuelle Übernahme von Zertifikation in den Windows Zertifikatsspeicher“.

Fehlermeldung: PKCS7Cryptography: SignFile

Es wurde versucht, im geschützten Speicher zu lesen oder zu schreiben. Dies ist häufig ein Hinweis darauf, dass anderer Speicher beschädigt ist.

Lösung:
Aktualisieren Sie die Zertifikate im Windows Zertifikatsspeicher, s. Punkt „Nachbearbeitung“ bzw. „Manuelle Übernahme von Zertifikaten in den Windows Zertifikatsspeicher“

3.3.4. Fehler bei der Archivierung von Dateien

Fehlermeldung: „SendFile: Exception occured while sending files from job; Ein Teil des Pfades X:\ konnte nicht gefunden werden"

Bei der Verwendung von gemappten Laufwerken (X:\Freigabename) für den Zugriff auf einen Netzwerkpfad kann es durch einen Fehler im .NET-Framework zu Problemen kommen (siehe „***Bekannte Probleme***“).

Lösung:

Verwenden Sie UNC Pfade (\\Servername\Freigabename\Pfad bzw. \\IP-Adresse\ Freigabename\Pfad).

Fehlermeldung: „Datei bereits vorhanden“

Lösung:

Prüfen Sie, ob bereits eine Datei mit demselben Namen im Ausgabeverzeichnis liegt. Verschieben Sie die Datei in ein Sicherungsverzeichnis oder passen Sie unter Konfiguration -> Einstellungen das Ausgabeverzeichnis bzw. den Ausgabedateinamen für versendete Dateien an. Starten Sie dann die Verarbeitung des Auftrags nochmal über „Job erneut starten“ an.

3.3.5. Fehler bei der Verarbeitung von empfangenen Dateien

Fehlermeldung: PKCS7Cryptography: DecryptFile: PKCS7.dll - Could not decrypt

Prüfen Sie die Gültigkeit des eigenen Zertifikates, .s. Schlüsseldetails unter Konfiguration -> Einstellungen.

Sollte das Problem direkt nach einem Zertifikatswechsel auftreten, kann es sein, dass der Partner noch nicht den aktuellen Schlüssel verwendet. Fordern Sie die Daten dann erneut an.

Fehlermeldung: PKCS7Cryptography: VerifySignedFile: PKCS7.dll – Could not verify signature

Ursachen:

- Das Zertifikat des KKS-Partners ist nicht vorhanden, abgelaufen oder aus anderen Gründen ungültig, z.B. aufgrund einer ungültigen Signatur oder eines falschen Signatur-hashalgorithmus.
- Die Vorgehensweise zur Prüfung eines Zertifikates finden Sie im Anhang im Abschnitt „Prüfen der Zertifikate“.
- Löschen Sie die Schlüssel des Partners aus dem entsprechenden Public Key Verzeichnis und spielen die aktuellen öffentlichen Schlüssel ein.
- Der Partner hat einen neuen Schlüssel zertifizieren lassen und ggf. sind ältere vom Partner empfangene Daten noch mit seinem alten Schlüssel und neuere Daten dann mit dem neuen Schlüssel verarbeitet worden.
- Dann muss die Datei mit dem neuen Schlüssel vom Partner neu gesendet werden.
- In diesem Fall muss die lokale Zertifikatskette erneuert werden. Aktualisieren Sie bitte die öffentlichen Schlüssel.

Aktualisierung der öffentlichen Schlüssel der Annahmestellen:

- Stoppen Sie den KKS Kernel
- Löschen Sie den Inhalt des Verzeichnisses „Public.Key.PKCS7.SHA256.4K“
- Starten Sie den KKS Kernel und Datei Connector
- Kopieren Sie die Sammeldatei in das Jobin des KKS Clients und splitten Sie den öffentliche Schlüsseldatei erneut.
- Fehlerhafte Aufträge über das Kontextmenu auf dem einzelnen Auftrag mit **„Job erneut erzeugen“** starten.

Fehlermeldung: PKCS7Cryptography: DecryptFile: Certificate for recipient(s) specified in the EnvelopedData object cannot be found.

Beim Entschlüsseln kann das System den lokalen Empfänger, für den die Nachricht verschlüsselt wurde, nicht ermitteln.

Ursachen:

- Der eigene Schlüssel ist nicht mehr gültig.
- Prüfen des eigenen Zertifikates (Konfiguration -> Einstellungen -> PKCS#7-Schlüssel-details), s.a. „Prüfen der Zertifikate“.
- Nach einer Zertifizierung:
    - Die Zertifikatsantwort wurde noch nicht eingespielt, aber der Partner hat schon den neuen öffentlichen Schlüssel verwendet.
    - Zertifikatsantwort einspielen, Auftrag erneut verarbeiten.
    - Die Zertifikatsantwort wurde eingespielt; der alte SHA-256 Schlüssel ist nicht mehr gültig.
    - Dann wurden die Daten noch mit dem alten SHA-256 verschlüsselt. Diese Daten müssen neu von der Annahmestelle angefordert werden.

- Nach einer Doppel-Neuzertifizierung:
    - Partner verwendet nicht den aktuellsten öffentlichen Schlüssel.
    - Den Partner bitten, den Auftrag mit dem aktuellsten öffentlichen Schlüssel zu verschlüsseln und anschließend noch einmal zu senden.
    - Auftrag wurde nicht für den lokalen Empfänger verschlüsselt.
    - Partner kontaktieren.

3.3.6. Fehler beim Versand von Aufträgen

➔ Bitte stellen Sie sicher, dass der Sendepartner wie im Dokument „FAQ zum FTAM-TCPIP Connector“ in Kapitel „Konfiguration der KKS Partner für den Versand über TCP/IP“ beschrieben konfiguriert wurde.

Fehlermeldung: Versandversuch für Datei <Dateiname> gescheitert. Details: FtamConnector, CoCoNet.Kks.Client.Shared.ConnectException: No connection on lower levels LowlayerRc=-6

- Überprüfung der FTAM Sendeeinstellungen beim Partner.
- Die Sendeeinstellungen müssen ggf. nochmal mit dem Partner abgestimmt werden.
- Nach kurzer Wartezeit den Auftrag erneut senden.

Fehlermeldung: Versandversuch für Datei <Dateiname> gescheitert. Details: FtamConnector, CoCoNet.Kks.Client.Shared.ConnectException: Unknown username LowlayerRc=0

Diese Meldung erscheint, wenn der FTAM Sendeprozess nicht auf die in der Datei FTAM_ENV angegebenen Verzeichnisse zugreifen kann, weil einer (oder ggf. mehrere) der Verzeichnisnamen in den Pfadangaben nicht in der alten DOS 8.3er Dateinamenskonvention aufgelöst werden können. Die betriebssystemseitige Unterstützung der DOS 8.3. Dateinamenskonventionen gehört zu den Systemvoraussetzungen (siehe „Installationsvorbereitung“).

Lösung:
Die Datei `<KKS Client Installationsverzeichnis>\ftam\FTAM_ENV` enthält z.B. folgende Pfadangabe:

- FTAM_DIR C:\PROGRA~2\CoCoNet\KKSCLI~1.0\ftam\
  Auf Windows 7 (64-Bit) entspricht dies der Langform:

  C:\Program Files (x86)\CoCoNet\KKS Client X.0\ftam.

Bitte gehen Sie wie folgt vor, um die Verwendung der Kurznamen zu verifizieren:

- Ermitteln Sie den Pfad zum Installationsverzeichnis des KKS Clients: KKS Client Menü -> „?“ -> „Installationsordner öffnen“. Der Pfad wird in der Adressleiste des Browsers angezeigt.
- Öffnen Sie dann eine DOS-Box (Windows-R -> cmd) und wechseln in das Hauptverzeichnis (cd \).
- Prüfen Sie mittels dir /x, ob das erste Verzeichnis im Pfad in gekürzter Form angezeigt wird.
  Beispielausgabe:
  01.01.2018 12:31 <DIR> PROGRA~1 Program Files
  01.01.2018 13:51 <DIR> PROGRA~2 Program Files (x86)
- Wechseln Sie dann in das nächste Unterverzeichnis des Installationspfades und führen dort dieselbe Überprüfung durch.
- Wiederholen Sie dies für alle Verzeichnisse im Pfad.
- Sichern Sie die Datei FTAM_ENV, tragen dann die gekürzten Pfade an den jeweiligen Stellen ein und speichern die Änderungen.
- Starten Sie den KKS FTAM Konnektor neu.

Falls ein Verzeichnis im Pfad nicht in gekürzter Form angezeigt wird, obwohl der Name des Verzeichnisses mehr als 8 Zeichen (vor einem Punkt) hat, ist ggf. die betriebssystemseitige Unterstützung der 8.3er Notation zum Zeitpunkt der Erstellung des Verzeichnisses deaktiviert gewesen. Bitte wenden Sie sich in diesem Fall an Ihren Systemadministrator, damit die Unterstützung der Kurznamen aktiviert wird und ggf. die Verzeichnisse neu angelegt werden.

➔ Anmerkung: Die Pfadangabe der Umgebungsvariablen FTAM_ENV (Ausgabe in der DOS Box mittels des Befehls set) darf die Notation mit Langnamen haben.

Fehlermeldung: Versandversuch für Datei <Dateiname> gescheitert. Details: FtamConnector, CoCoNet.Kks.Client.Shared.ConnectException: VFS password wrong LowlayerRc=0

Lösung:

- Überprüfen Sie die Authentifizierungsdaten im FTAM Sendeprofil des Partners: Benutzername -> eigene IK, Passwort -> leer oder gem. Vorgabe durch den Kommunikations-partner (achten Sie auf Leerzeichen).

Fehlermeldung: Versandversuch für Datei <Dateiname> gescheitert. Details: FtamConnector, CoCoNet.Kks.Client.Shared.ConnectException: Partner confirms connection establishing negative LowlayerRc=0

Überprüfen der FTAM Sendekonfiguration beim Partner:

- Alle Selektoren müssen FTAM (ASCII und in Großbuchstaben) lauten.
- Bei Benutzernamen muss die eigene IK eingetragen sein.
- Passwort leer (keine Leerzeichen), außer bei Vorgabe durch den Kommunikationspartner, aber nicht am Ende des Passwortes.
- Überprüfen, ob der Kommunikationspartner den Zugang zum System erlaubt.

3.3.7. Fehler bei der Generierung der Zertifizierungsanfrage

Es wird kein Trustcenter bei „Organisation“ angezeigt und der Button „Generieren“ ist ausgegraut.

- Prüfen Sie bitte das dem Trustcenter zugewiesene Sicherheitsverfahren in den Trustcenter Einstellungen (Konfiguration -> Trustcenter -> Bearbeiten). Es muss das Sicherheitsverfahren „PKCS#7“ ausgewählt werden (**nicht PKCS#7SHA256_4K**). Bitte ändern Sie dies oder legen ggf. das Trust Center neu an und generieren dann nochmal einen neuen Schlüssel.

➔ Anmerkung: Die Zuordnung des falschen Sicherheitsverfahrens kann dazu führen, dass eine ungültige Zertifizierungsanfrage generiert wird.

3.3.8. Sonstige Fehlermeldungen

Fehlermeldung, wenn .dll-Dateien direkt aus einem Zip-Archiv in das KKS Client Installationsverzeichnis entpackt werden

Auszug aus der Meldung:

An attempt was made to load an assembly from a network location which would have caused the assembly to be sandboxed in previous versions of the .NET-Framework. This release of the .NET-Framework does not enable CAS policy by default, so this load may be dangerous. If this load is not intended to sandbox the assembly, please enable the loadFromRemoteSources switch.

Prüfen Sie die .dll-Dateien, s.a. „Programmdateien sind blockiert“.

4. Anhang

4.1. Manuelle Übernahme von Zertifikaten in den Windows Zertifikatsspeicher

Die fehlenden Zertifikate können aus dem Windows Zertifikatsspeicher (Altsystem) exportiert und dann in den Windows Zertifikatsspeicher (Neusystem) importiert werden. Der Zugriff auf den Windows Zertifikatsspeicher erfolgt über die Windows Management Konsole (mmc).

4.1.1. Export der Zertifikatsdaten aus dem Windows Zertifikatsspeicher (alter Rechner) über die Windows Management Konsole (mmc).

- Melden Sie sich bitte als lokaler Administrator auf dem alten KKS-Rechner an.
- Start -> Ausführen -> mmc eingeben und Ausführen mit „Ja“ bestätigen.
- Datei -> Snap-In hinzufügen/entfernen.
- Verfügbare Snap-Ins -> „Zertifikate“ -> Hinzufügen -> **Computerkonto** auswählen-> Weiter -> Lokalen Computer -> Fertigstellen
- Fenster „Snap-Ins hinzufügen“ über „OK" schließen.
- Konsolenstamm -> Zertifikate
- Export des Datenaustauschzertifikates:
- **Vertrauenswürdige Stammzertifizierungsstellen** -> Zertifikate -> Auswahl des entsprechenden Zertifikats („Datenaustausch im Gesundheits- und Sozialwesen“) -> Über rechte Maustaste -> Alle Aufgaben -> Exportieren -> DER-codiert-binär abspeichern.

➔ Hinweis: Es können mehrere Zertifikate existieren, die exportiert werden müssen.

- Export des Trustcenterzertifikates:
- **Zwischenzertifizierungsstellen** -> Zertifikate -> Auswahl des entsprechenden Zertifikats (ITSG: „ITSG TrustCenter fuer sonstige Leistungserbringer“/DKTIG: „DKTIG TrustCenter fuer Krankenhaeuser und Leistungserbringer PKC“) -> Über rechte Maustaste -> Alle Aufgaben -> Exportieren -> DER-codiert-binär abspeichern.

➔ Hinweis: Es können mehrere Zertifikate existieren, die exportiert werden müssen.

- MMC schließen, aber Konfiguration nicht abspeichern, damit ggf. erneut das Computer-konto in der Zertifikatsverwaltung ausgewählt werden kann.

4.1.2. Import der Zertifikatsdaten (neuer Rechner)

- Melden Sie sich bitte als lokaler Administrator auf dem neuen KKS-Rechner an.
- Start -> Ausführen -> MMC
- Datei -> Snap-In hinzufügen/entfernen
- Verfügbare Snap-Ins -> „Zertifikate“ -> Hinzufügen -> **Computerkonto** -> Weiter -> Lokalen Computer -> Fertigstellen
- Fenster „Snap-Ins hinzufügen“ über „OK" schließen.
- Konsolenstamm -> Zertifikate
- Import des Datenaustauschzertifikates:
- **Vertrauenswürdige Stammzertifizierungsstellen** -> Zertifikate -> Über rechte Maustaste -> Alle Aufgaben -> Importieren -> <abgespeichertes „Datenaustausch“ Zertifikat> auswählen und importieren.
- Import des Trustcenterzertifikates:
- **Zwischenzertifizierungsstellen** -> Zertifikate -> Über „Alle Aufgaben“ das Zertifikat der DKTIG/ITSG importieren.
- MMC schließen, aber Konfiguration nicht abspeichern, damit ggf. erneut das Computerkonto in der Zertifikatsverwaltung ausgewählt werden kann.
- Starten des SQL Servers, Starten der KKS Dienste, starten des KKS Clients.
- Prüfen, ob die Schlüsseldetails des privaten Schlüssels nun korrekt angezeigt werden können.

4.2. Protokollierung der Verarbeitung

In einigen Fällen kann es vorkommen, dass es trotz gültigen privaten und öffentlichen Zertifikaten zu Verarbeitungsfehlern kommt (Fehler bei der Signierung/Signaturprüfung bzw. beim Verschlüsseln/Entschlüsseln.

In solchen Fällen kann die Verarbeitung protokolliert werden.

- Fordern Sie in diesem Fall die Datei PKC7Key.ini von der CoCoNet Hotline an oder folgen Sie folgendem Link zur PKCS7Key.ini.
- Entpacken Sie die ZIP-Datei in ein temporäres Verzeichnis.
- Prüfen Sie dann in den Journaleinstellungen (Journal -> Einstellungen), ob die Protokolltiefe auf maximal steht. Wenn nicht, passen Sie dies bitte an.
- Kopieren Sie dann die entpackte Datei PKCS7Key.ini in das KKS Client Installationsverzeichnis und starten die Verarbeitung des fehlerhaften Auftrags über die rechte Maustaste -> „Job erneut starten“.
- Bitte senden Sie der CoCoNet Hotline dann die Datei PKCS7Key.Trace (liegt im KKS Client Installationsverzeichnis), die Journaldateien, sowie einen Screenshot von den Auftragsdetails.

4.3. Programmdateien sind blockiert

- Wenn die Programmdateien von einem anderen Rechner auf den KKS Rechner kopiert wurden, prüfen Sie bitte bei jeder Programmdatei über die rechte Maustaste -> Eigenschaften, ob Windows den Zugriff auf die Datei blockiert, siehe Abbildung unten. In diesem Fall muss die Datei erst zugelassen werden.
-

4.4. Erzeugung von ISO4- und FTAM-Traces

Die Erzeugung der FTAM und der ISO4 Tracen ist in der FAQ-zum-FTAM-TCPIP-Connector in Kapitel „Erzeugen von ISO4- und FTAM-Traces“ beschrieben.

4.5. Prüfen der Zertifikate

Die öffentlichen Zertifikate liegen in den Verzeichnissen:

- SHA-256 Zertifikate:
  <KKS Client Installationsverzeichnis>\Public.Key.PKCS7.SHA256
- RSA-4096 Zertifikate:
- <KKS Client Installationsverzeichnis>\Public.Key.PKCS7.SHA256.4K

Die privaten Zertifikate liegen in den Verzeichnissen:

- SHA-256 Zertifikate:
  <KKS Client Installationsverzeichnis>\ Secret.Key.PKCS7.SHA256\IK-Nummer.act
- RSA-4096 Zertifikate:
- <KKS Client Installationsverzeichnis>\ Secret.Key.PKCS7.SHA256.4K\IK-Nummer.act

Bitte gehen Sie wie folgt vor, um ein Zertifikat zu prüfen:

- Ermitteln Sie die IK-Nummer des Kommunikationspartners in der Partnerverwaltung.
- Öffnen Sie die Zertifikatsdatei des Kommunikationspartners durch Doppelklick.

- In der Zertifikatsansicht -> Allgemein -> Zertifikatsinformationen zeigt ein rotes Kreuz oder ein gelbes Ausrufezeichen ein Problem an.
- Genauere Informationen finden sich im Statustext bzw. in der Karteikarte Zertifizierungspfad. Nach Auswahl des fehlerhaften Zertifikates wird dort im Feld Zertifizierungsstatus eine genauere Fehlermeldung angezeigt.
- In der Karteikarte Details werden die Details zum Zertifikat angezeigt, z.B. der Signaturhashalgorithmus (SHA-1, SHA-256 oder RSA-4096).

➔ Anmerkung: Wenn ein SHA-256 Zertifikat im Verzeichnis für SHA-1 Zertifikate liegt, führt dies im KKS Client zu einem

➔ Fehler bei der Verarbeitung von empfangenen Dateien.

4.6. SQL Server Express Log-Dateien

Bei der Installation des SQL Servers werden Log-Dateien angelegt, die ggf. für die weitere Analyse benötigt werden.

Diese Dateien befinden sich in folgenden Verzeichnissen:

- C:\Program Files\Microsoft SQL Server\<*Installierte Serverversion*>\Setup Bootstrap\Log bzw.
- C:\Program Files (x86)\Microsoft SQL Server\<*Installierte Serverversion*>\Setup Bootstrap\Log
  Der genannte Ordner enthält u.a.
  - die Datei Summary.txt und
  - Unterordner mit Datum-Zeitstempel, z.B. 20140723_123009
    (es wird für jeden Installationsversuch ein Ordner angelegt).