

# **Installations- und Bedienungsanleitung für das KKM-Cryptokit**

Version: 1.2

Status: final

**Dokumenteninformationen**

<b>Installations- und Bedienungsanleitung für das KKM-Cryptokit</b>	
Sächsische Anstalt für kommunale Datenverarbeitung	
Version	1.2
Status	final
Datum der letzten Änderung	26.01.2009
Autoren und Ansprechpartner	Sten Kokel

**Änderungsübersicht**

Lfd. Nr.	Datum	Versi- on	Änderungen / Kapitel	Durchgeführt von
1	21.05.07	0.1	Neuanlage des Dokuments	Kokel
2	01.06.07	0.2	Review	Drechsler
3	14.06.07	0.3	Änderungen im Zusammenhang mit der Umbenennung des Scripts	Kokel
4	14.06.07	1.0	Freigabe der Version 1.0	Kokel
5	26.01.09	1.2	Austausch des PGP-Keys in der Anwendung	Kokel

**Inhalt**

**1 VORAUSSETZUNGEN .....3**

**2 KURZANLEITUNG .....3**

**3 AUSFÜHRLICHE ANLEITUNG .....4**

**3.1 Installation .....4**

3.1.1 Bestimmung des Installationsortes .....4

3.1.2 Installation bei Verwendung von kkm-cryptokit.zip .....6

3.1.3 Installation bei Verwendung von kkm-cryptokit.exe .....7

**3.2 Erstellen einer komprimierten und verschlüsselten Datenlieferung .....8**

**3.3 Deinstallation des KKM-Cryptokit .....11**

**4 AUFBAU DES KKM-CRYPTOKIT .....11**

**4.1 Zum Einsatz kommende Softwarekomponenten .....12**

## 1 Voraussetzungen

Von der SAKD wird Ihnen ein Softwarepaket (KKM-Cryptokit) für Microsoft Windows Betriebssysteme zur Verfügung gestellt, welches alle für die Erstellung einer komprimierten und verschlüsselten Datenlieferung erforderlichen Komponenten enthält. Dieses Softwarepaket wurde unter den folgenden Betriebssystemen erfolgreich getestet:

- Microsoft Windows 98/ME
- Microsoft Windows NT 4.0
- Microsoft Windows 2000
- Microsoft Windows 2003
- Microsoft Windows XP
- Microsoft Windows Vista

Wichtigste Voraussetzung, um das KKM-Cryptokit verwenden zu können, ist ausreichend freier Speicherplatz auf der Festplatte. Benötigt werden mindestens:

- Ca. 2,5 MB für das entpackte KKM-Cryptokit
- N MB für die unverschlüsselten und unkomprimierten MeldIT XML-Dateien mit den zu liefernden Daten. Der benötigte Speicherplatz ist vom Umfang der Datenlieferung abhängig.
- Zusätzlich ca. 15 % des für die unverschlüsselten und unkomprimierten MeldIT XML-Dateien benötigten Speicherplatzes ( $N * 0,15$  MB) für temporäre Dateien und die fertig komprimierte und verschlüsselte Datenlieferung

## 2 Kurzanleitung

Für eine ausführliche Anleitung zur Installation und Bedienung lesen Sie bitte Kapitel 3.

Installation:

1. Für Windows-Betriebssysteme mit vorhandenem ZIP-Programm verwenden Sie „kkm-cryptokit.zip“. Für ältere Windows-Systeme, auf denen keine ZIP-Software verfügbar ist, wird ein selbstentpackendes ZIP-Archiv „kkm-cryptokit.exe“ zur Verfügung gestellt. Sie können das KKM-Cryptokit auf schriftlichen Antrag bei der SAKD oder über das Internet von der Seite <http://www.kkm-sachsen.de> beziehen.
2. Wählen Sie ein lokales Laufwerk aus, auf dem genügend freier Speicher für das KKM-Cryptokit, die unverschlüsselte und unkomprimierte Datenlieferung sowie die komprimierten und verschlüsselten Dateien verfügbar ist. Der benötigte Speicherbedarf bestimmt sich nach der Formel:  $2,5 \text{ MB} + \langle \text{Größe Datenlieferung} \rangle + (\langle \text{Größe Datenlieferung} \rangle * 0,15)$
3. Entpacken Sie das KKM-Cryptokit an beliebiger Stelle auf dem ausgewählten Laufwerk. Es entsteht ein Ordner „kkm-cryptokit“ mit weiteren Unterordnern und der Datei „start-crypt.bat“.

Bedienung:

1. Kopieren Sie die von Ihrem EWO-Verfahren erstellte unkomprimierte und unverschlüsselte Datenlieferung für alle Gemeinden, für die Ihre Meldebehörde zuständig ist, vollständig in das Verzeichnis „kkm-cryptokit\eingang“.
2. Starten Sie den Kompressions- und Verschlüsselungsvorgang durch Doppelklick auf „start-crypt.bat“ im Verzeichnis „kkm-cryptokit“.
3. Kontrollieren Sie die im sich öffnenden Fenster durchlaufenden Meldungen auf eventuelle Fehlermeldungen. Das Script durchläuft insgesamt sechs Schritte.
4. Nach Beendigung des Schrittes 6 enthält der Ordner „kkm-cryptokit\ausgang“ mindestens eine Datei mit dem Namen „Lieferung.7z.\*.gpg“ und die Datei „signaturen.txt“. Die Datei(en)

mit der Endung .gpg enthalten den Inhalt des Ordners „kkm-cryptokit\eingang“ in komprimierter und verschlüsselter Form. MD5-Prüfsummen aller Dateien des Ordners „kkm-cryptokit\eingang“ sind in der Datei „signaturen.txt“ gespeichert. Übertragen Sie nun den gesamten Inhalt des Ordners „kkm-cryptokit\ausgang“ auf einen von der SAKD zugelassenen Datenträger.

Bewahren Sie die vom EWO-Verfahren erstellte unverschlüsselte und unkomprimierte Datenlieferung noch solange auf, bis Sie von der SAKD eine Bestätigung der erfolgreichen Verarbeitung Ihrer Datenlieferung erhalten haben. Im Falle eines Fehlers beim Komprimieren der Daten bzw. bei der Verschlüsselung muss der Vorgang mit den Originaldaten wiederholt werden können.

Deinstallation:

1. Löschen Sie den Ordner „kkm-cryptokit“ mit seinem gesamten Inhalt.

### 3 Ausführliche Anleitung

#### 3.1 Installation

Das KKM-Cryptokit wird als ZIP-Archiv bereitgestellt. Eine Installation im herkömmlichen Sinne, bei der Eintragungen in die Windows-Registry vorgenommen werden und Softwarekomponenten in Form von dll-Libraries in Windows Systemorder kopiert werden, ist beim KKM-Cryptokit nicht erforderlich. Es ist ausreichend, das ZIP-Archiv an geeigneter Stelle auf dem Computer zu entpacken, um die Einsatzbereitschaft herzustellen.

Bereitgestellt wird das KKM-Cryptokit aufgrund der unterschiedlichen Ausstattung der zu unterstützenden Betriebssysteme in zwei Varianten, als ZIP-Archiv mit dem Namen „kkm-cryptokit.zip“ und als selbstentpackendes ZIP-Archiv mit dem Namen „kkm-cryptokit.exe“.

Betriebssystem	Empfohlene Variante
Microsoft Windows 98/ME	Selbstentpackendes ZIP-Archiv ( <b>kkm-cryptokit.exe</b> )
Microsoft Windows NT 4.0	
Microsoft Windows 2000	
Microsoft Windows 2003	ZIP-Archiv ( <b>kkm-cryptokit.zip</b> )
Microsoft Windows XP	
Microsoft Windows Vista	

##### 3.1.1 Bestimmung des Installationsortes

Bei der Bestimmung des Installationsortes (Laufwerk) für das KKM-Cryptokit sind zwei Voraussetzungen zu beachten:

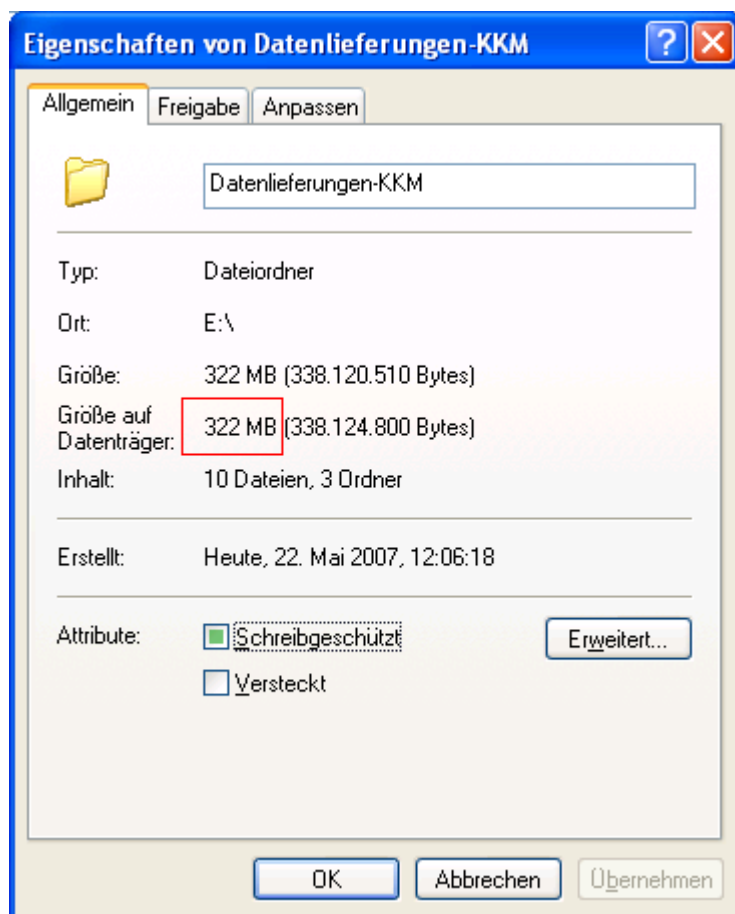
1. Das Laufwerk muss genügend freien Speicher haben, um das gesamte KKM-Cryptokit inklusive der unverschlüsselten und unkomprimierten MeldIT XML-Dateien und der temporären sowie komprimierten und verschlüsselten Dateien aufzunehmen (vgl. Voraussetzungen in Kapitel 1). Eine Verteilung auf unterschiedliche Laufwerke ist nicht möglich.
2. Das Laufwerk sollte aus Gründen der Performance und Sicherheit ein lokales Festplattenlaufwerk sein (z. B. Laufwerk D: oder C:)

Um das Vorliegen dieser Voraussetzungen zu prüfen, gehen Sie wie folgt vor.

### 1. Bestimmung der Größe der unkomprimierten und unverschlüsselten Datenlieferung:

Öffnen Sie durch Doppelklick auf das Arbeitsplatz-Symbol den Windows-Explorer. Navigieren Sie zu dem Ordner, in dem sich die MeldIT-Dateien befinden. Dieser Ordner sollte für jede von der Meldebehörde vertretene Gemeinde einen Unterordner besitzen, der als Namen den AGS der jeweiligen Gemeinde trägt und die Datenlieferung als XML-Dateien für die Gemeinde enthält.

Bestimmen Sie die Größe der gesamten Datenlieferung dadurch, dass Sie mit der rechten Maustaste auf den Namen des Ordners klicken und aus dem Menü den Punkt Eigenschaften auswählen. Sie können nun den Speicherplatzbedarf der Datenlieferung ablesen. Im gezeigten Beispiel 322 MB.



### 2. Berechnung des insgesamt benötigten Speicherplatzbedarfs

Gemäß der Angaben zu den Voraussetzungen in Kapitel 1 berechnet sich der erforderliche Speicherplatz nach folgender Formel:

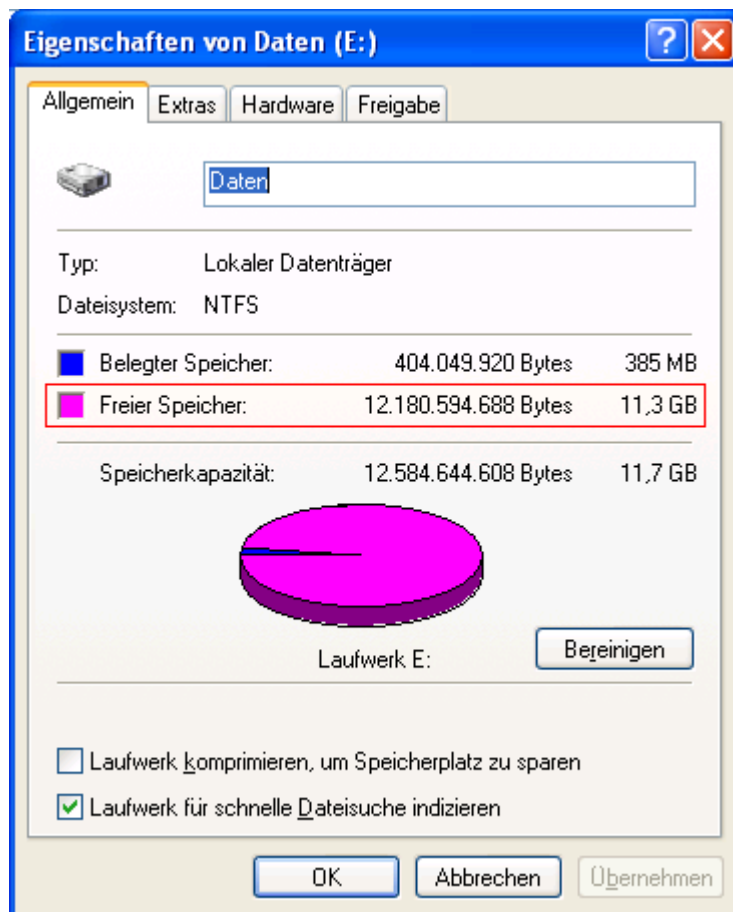
$$2,5 \text{ MB} + N + ( N * 0,15 )$$

Für das Beispiel ergibt sich ein Bedarf an freiem Festplattenspeicher am Installationsort des KKM-Cryptokit von:

$$2,5 \text{ MB} + 322 \text{ MB} + ( 322 \text{ MB} * 0,15 ) = \mathbf{372,8 \text{ MB}} \text{ ( entspricht ca. } 391.000.000 \text{ Bytes bzw. } 0,38 \text{ GB )}$$

### 3. Auswahl des geeigneten Laufwerks für die Installation

Klicken Sie im Start-Menü bzw. auf dem Desktop auf „Arbeitsplatz“. Es erscheint eine Auflistung der verfügbaren Laufwerke. Wählen Sie nacheinander die lokalen Laufwerke aus, klicken Sie mit der rechten Maustaste auf den Namen des Laufwerkes und wählen Sie aus dem erscheinenden Menü den Punkt „Eigenschaften“. Es öffnet sich ein Fenster, in dem Informationen zum Grad der Belegung des Laufwerks angezeigt werden.



Im Beispiel ist ersichtlich, dass das Laufwerk E: 11,3 GB freien Speicher hat (ca. 0,38 GB werden benötigt) und somit als Installationsort für das KKM-Cryptokit bestens geeignet ist.

#### 3.1.2 Installation bei Verwendung von kkm-cryptokit.zip

Die aktuellen Betriebssysteme von Microsoft werden von Haus aus mit einer Software zum Entpacken von ZIP-Archiven ausgeliefert. Aus diesem Grund ist die Verwendung selbstentpackender ZIP-Archive nicht mehr erforderlich.

Erzeugen Sie auf dem für die Installation ausgewählten Laufwerk einen neuen Ordner „kkm“ und kopieren Sie die Datei „kkm-cryptokit.zip“ in diesen Ordner (im Beispiel E:\kkm). Klicken Sie mit der rechten Maustaste auf den Namen des ZIP-Archivs und wählen Sie im erscheinenden Menü den Punkt „Alle extrahieren ...“. Es erscheinen nacheinander zwei Fenster, die Sie um eine Bestätigung bitten. Ändern Sie bei Bedarf das Verzeichnis, in das extrahiert werden soll und klicken Sie auf „Weiter“.

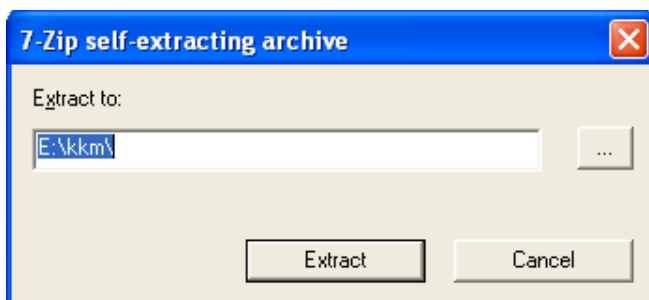


Klicken Sie auf „Fertigstellen“. Meist öffnet sich darauf hin ein Explorer-Fenster, das den Inhalt des nun entpackten KKM-Cryptokits zeigt.

### 3.1.3 Installation bei Verwendung von kkm-cryptokit.exe

Diese Installation ist für Betriebssysteme vorgesehen, die nicht von Haus aus mit einer Software zum Entpacken von ZIP-Archiven ausgeliefert werden. Dazu zählen insbesondere Windows 98/ME, Windows NT 4.0 und Windows 2000. Für diese Fälle wird ein selbstentpackendes ZIP-Archiv bereitgestellt.

Erzeugen Sie auf dem für die Installation ausgewählten Laufwerk einen neuen Ordner „kkm“ und kopieren Sie die Datei „kkm-cryptokit.exe“ in diesen Ordner (im Beispiel E:\kkm). Starten Sie durch Doppelklick auf „kkm-cryptokit.exe“ den Dekompressionsprozess. Es erscheint ein Fenster, in dem Sie den Installationsort durch klicken auf „Extract“ bestätigen.



Anschließend befindet sich im Ordner „kkm“ ein Unterordner „kkm-cryptokit“, der wiederum fünf Unterordner und das Start-Script „start-crypt.bat“ enthält. Sie können die Datei mit dem selbstentpackenden ZIP-Archiv (kkm-cryptokit.exe) jetzt wieder löschen.

### 3.2 Erstellen einer komprimierten und verschlüsselten Datenlieferung

Die Bedienung des KKM-Cryptokits ist sehr einfach. In nur drei Schritten können die unkomprimierten und unverschlüsselten XML-Dateien, die das EWO-Verfahren erzeugt hat, gepackt und verschlüsselt werden.

#### 1. Eingangsordner befüllen:

Kopieren Sie das komplette Verzeichnis mit allen Datenlieferungen für die Gemeinden, für die Ihre Meldebehörde zuständig ist, in das Verzeichnis „engang“. Im verwendeten Beispiel wäre das das Verzeichnis „E:\Datenlieferungen-KKM“. Der Ordner „engang“ hat danach im verwendeten Beispiel den folgenden Inhalt:

#### engang

##### Datenlieferungen-KKM

###### 14456789

*erstlieferung--144567890-1.xml*  
*erstlieferung--144567890-2.xml*

###### 14478901

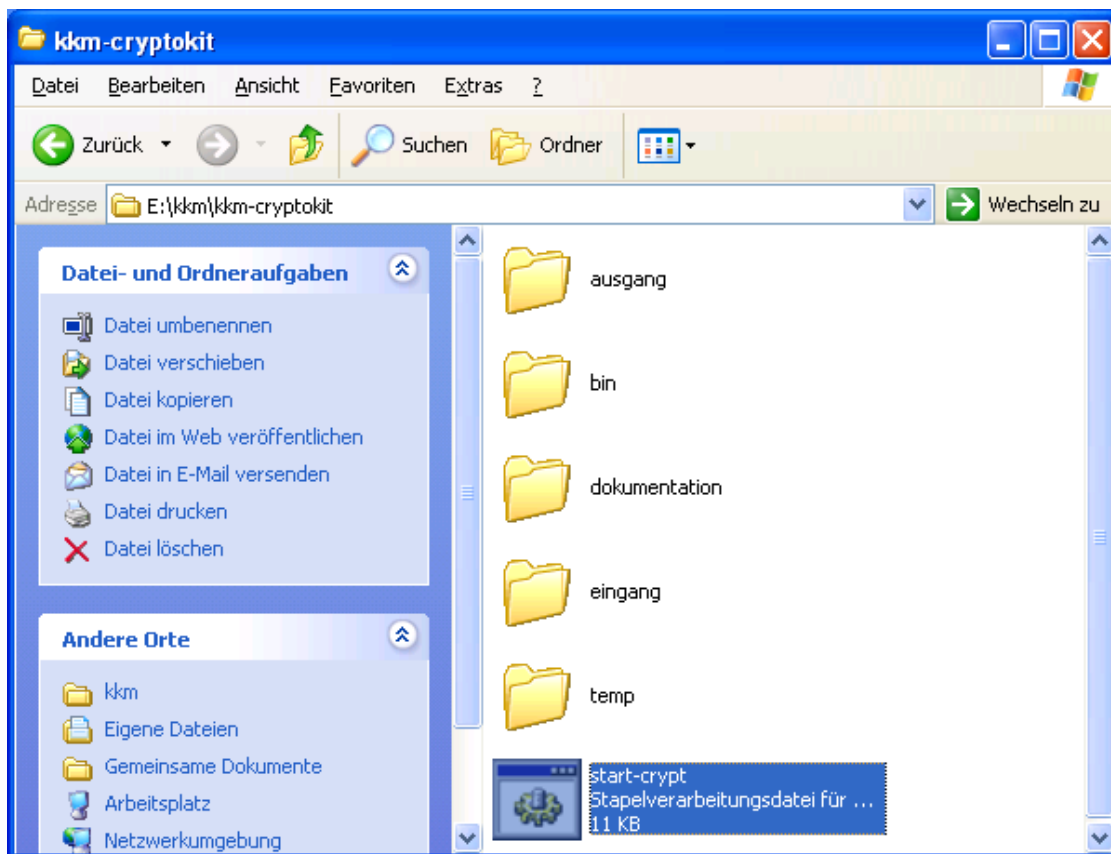
*erstlieferung--144567890-1.xml*  
*erstlieferung--144567890-2.xml*  
*erstlieferung--144567890-3.xml*  
*erstlieferung--144567890-4.xml*  
*erstlieferung--144567890-5.xml*

###### 14498765

*erstlieferung--14498765-1.xml*  
*erstlieferung--14498765-2.xml*  
*erstlieferung--14498765-3.xml*

#### 2. Kompressions- und Verschlüsselungsvorgang starten:

Um den Kompressions- und Verschlüsselungsvorgang zu starten, wechseln Sie im Windows-Explorer in den Ordner „kkm-cryptokit“. Sie starten die Verarbeitung durch einen Doppelklick auf „start-crypt.bat“.



Das Script informiert den Nutzer über den aktuellen Bearbeitungsstand durch entsprechende Meldungen im sich öffnenden Fenster.

```

C:\WINDOWS\system32\cmd.exe

2. Schritt: Entferne alle alten Dateien aus "temp" und "eingang":
... fertig.

3. Schritt: Erzeuge eine Datei mit Prüfsummen fuer alle Dateien im Ordner
"eingang". Dieser Schritt kann je nach Groesse der Lieferung
mehrere Minuten dauern, da der gesamte Inhalt des Eingangs-
Ordners gelesen werden muss.
... fertig

4. Schritt: Komprimieren des Inhalts des Ordners "eingang":
Dieser Schritt kann je nach Groesse der Lieferung und Leistungs-
faehigkeit des PC laengere Zeit in Anspruch nehmen. Sie sehen,
nachdem Sie den Vorgang durch einen Tastendruck gestartet haben,
die Ausgaben des laufenden Kompressionsvorgangs.

7-Zip (A) 4.42 Copyright (c) 1999-2006 Igor Pavlov 2006-05-14
Scanning
Creating archive .\temp\Lieferung.7z
Compressing  eingang\Datenlieferungen-KKM\14456789\erstlieferung--144567890-1.xml
1 2%
  
```

**Schritt 1:** Es werden zunächst einige Prüfungen durchgeführt, ob in den Ordnern „ausgang“ und „temp“ neue Dateien geschrieben werden können.

**Schritt 2:** Es wird der gesamte Inhalt der Ordner „ausgang“ und „temp“ wieder gelöscht. In „ausgang“ eventuell noch vorhandene Dateien früherer Verschlüsselungsversuche gehen dabei verloren.

**Schritt 3:** Für alle Dateien des Ordners „eingang“ und dessen Unterordner wird eine krypt-

tografische Prüfsumme berechnet. Diese soll der SAKD später dazu dienen, die Unversehrtheit der entschlüsselten und dekomprimierten Dateien zu überprüfen. Die Ergebnisse dieser Prüfsummenberechnung werden in die Datei „temp\signaturen.txt“ geschrieben.

**Schritt 4:** Der Inhalt des Ordners „eingang“ wird jetzt komprimiert und in Dateien mit dem Namen „Lieferung.7z.\*“ in den Ordner „temp“ geschrieben, wobei „\*“ eine fortlaufende Nummer ist. Sollte die Lieferung sehr groß sein, wird die Lieferung auf mehrere solcher Dateien verteilt, die jeweils maximal 645 MB groß sind, so dass sie in jedem Fall auf eine CD gebrannt werden können.

**Schritt 5:** Die erfolgreich komprimierte Datenlieferung (Dateien mit dem Namen „Lieferung.7z.\*“ im Ordner „temp“) wird nun mit Hilfe des GnuPG-Programms verschlüsselt. Dabei entstehen Dateien mit dem Namen „Lieferung.7z.\*.gpg“ im Ordner „temp“.

**Schritt 6:** Nach erfolgreicher Verschlüsselung werden alle erzeugten Dateien mit der Endung „.gpg“ und die Datei „signaturen.txt“ aus dem „temp“ in den Ordner „ausgang“ verschoben. Zusätzlich wird die Datei „CrVersion.txt“ aus dem „bin“ in den „ausgang“-Ordner kopiert. Der restliche Inhalt des „temp“-Ordners wird danach gelöscht.

### 3. Datenträger für den Versand an die SAKD erstellen:

War der Kompressions- und Verschlüsselungsvorgang erfolgreich, wird folgende Meldung ausgegeben:



```
C:\WINDOWS\system32\cmd.exe
... fertig

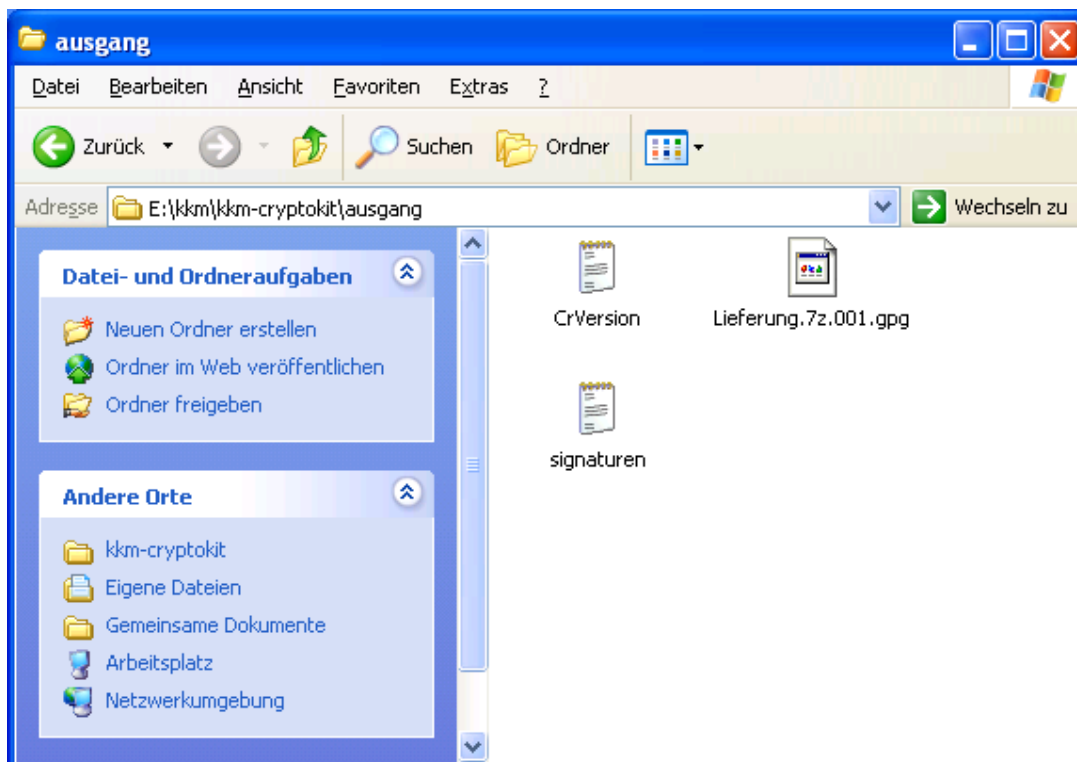
6. Schritt: Bereitstellen der verschluesselten Lieferung im Ausgangs-Ordner
Aufraeumen:
Die Dateien der verschluesselten Lieferung und die Datei mit den
Signaturen wurden erfolgreich erzeugt und im Ordner "ausgang"
bereitgestellt.
Die temporaeren Dateien im Verzeichnis "temp" wurden erfolgreich
geloescht.
... fertig

Der Inhalt des "eingang"-Verzeichnisses wurde erfolgreich komprimiert und
verschluesselt. Uebertragen Sie jetzt den GESAMTEN Inhalt des Ordners
"ausgang" auf einen fuer die Erstbelieferung des KKM von der SAKD zugelassenen
Datentraeger. Sollten nicht alle Dateien auf einen Datentraeger passen,
verteilen Sie die Dateien der Lieferung auf mehrere Datentraeger.

!!! WICHTIG !!!
Bewahren Sie in jedem Fall die Original-Dateien im Verzeichnis "eingang"
solange auf, bis der Empfang und die erfolgreiche Verarbeitung Ihrer Lieferung
durch die SAKD bestaetigt wurden. Falls die SAKD Ihre Datenlieferung nicht
lesen oder entschluesseln kann, muss der Vorgang der Verschluesselung
wiederholt werden koennen.

Druecken Sie eine beliebige Taste . . .
```

Der Ordner „ausgang“ enthält dann die (unverschlüsselte) Datei mit den Signaturen, die Datei „CrVersion.txt“ mit Angaben zur verwendeten Version des KKM-Cryptokits und mindestens eine Datei mit dem Namen „Lieferung.7z.\*.gpg“.



Übertragen Sie **alle** Dateien aus dem Ordner „ausgang“ mit einer geeigneten Software auf einen von der SAKD zugelassenen Datenträger.

Wurden mehrere Dateien mit der Endung .gpg erzeugt, können diese bei Bedarf auf mehrere Datenträger verteilt werden. Die Dateien „CrVersion.txt“ und „signaturen.txt“ sind dann nur auf den ersten Datenträger zu kopieren.

### 3.3 Deinstallation des KKM-Cryptokit

Um das KKM-Cryptokit vollständig vom Rechner zu entfernen, genügt es, den Ordner „kkm-cryptokit“ zu löschen.

## 4 Aufbau des KKM-Cryptokit

Das KKM-Cryptokit besteht aus einem Ordner „kkm-cryptokit“, der folgende Unterstruktur aufweist:

- Unterverzeichnis „ausgang“  
Dieses Verzeichnis wird später die komprimierte und verschlüsselte Datenlieferung beinhalten.
- Unterverzeichnis „bin“  
Dieses Verzeichnis enthält die zur Erstellung der komprimierten und verschlüsselten Datenlieferung erforderlichen Programme „gpg.exe“ und „iconv.dll“, „md5.exe“ und „7za.exe“. Weiterhin ist ein Unterordner „gnupg“ vorhanden, der den zur Verschlüsselung benötigten PGP-Schlüssel enthält und die Datei „CrVersion.txt“ mit Informationen über die Version des KKM-Cryptokits.
- Unterverzeichnis „dokumentation“  
In diesem Verzeichnis sind Informationen zum KKM-Cryptokit und Copyright-Informationen der verwendeten Programme zu finden.
- Unterverzeichnis „eingang“  
Hier wird die unkomprimierte und unverschlüsselte Datenlieferung bereitgestellt, die komprimiert und verschlüsselt werden soll.

- Unterverzeichnis „temp“  
In diesem Verzeichnis werden temporäre Dateien mit Zwischenergebnissen erstellt, die später wieder gelöscht werden.
- Script „start-crypt.bat“  
Windows Shell Script, das unter Verwendung der im Verzeichnis „bin“ hinterlegten Programme die Datenlieferung aus „eingang“ analysiert, komprimiert und verschlüsselt und das Ergebnis in „ausgang“ bereitstellt.

#### 4.1 Zum Einsatz kommende Softwarekomponenten

Für das KKM-Cryptokit wurden die folgenden lizenzkostenfrei verfügbaren Open Source- und Freeware-Produkte verwendet:

bin\md5.exe	Implementierung des MD5-Digest Algorithmus zur Erzeugung kryptografischer Prüfsummen Autor: Matthias Withopf Bezug: <a href="http://www.heise.de/software/default.shtml?prg=41158">http://www.heise.de/software/default.shtml?prg=41158</a> Lizenz: Freeware
bin\7za.exe	7-Zip: Datenkompressionswerkzeug (standalone Kommandozeilenversion) Bezug: <a href="http://www.7-zip.org/de/">http://www.7-zip.org/de/</a> Lizenz: GNU LGPL
bin\gpg.exe	GnuPG: Open Source Implementierung des OpenPGP-Standards nach RFC2440 Bezug: <a href="http://www.gnupg.org/">http://www.gnupg.org/</a> Lizenz: GNU GPL