Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Verteidigung,
Bevölkerungsschutz und Sport VBS

**Schweizer Armee**
Führungsunterstützungsbasis FUB

Bern, 31. Oktober 2014

# Kurzanleitung Umschlüsselungstool

## 1 Wann braucht es eine Umschlüsselung?

### Vor der Erneuerung einer Smartcard, die alte Chiffrierschlüssel enthält[1]

X.509-Chiffrate werden durch Verwendung eines X.509-Zertifikats erzeugt. Zum Dechiffrieren eines X.509-Chiffrats wird eine Smartcard mit dem zum Zertifikat passenden privaten Schlüssel benötigt. Wegen der regelmässigen Erneuerung der Smartcard arbeitet ein Benutzer im Verlaufe der Zeit mit immer wieder neuen X.509-Zertifikaten. Ohne Umschlüsselung müssten deshalb immer mehr Chiffrierschlüssel auf der Smartcard vorhanden sein, damit ein Benutzer all seine chiffrierten Dokumente noch entschlüsseln kann. Bei der Erneuerung der Smartcard können aber aus Speicherplatzgründen nicht beliebig viele ältere Schlüssel auf der Smartcard belassen werden. Unter Umständen werden deshalb jeweils die ältesten Schlüssel gelöscht. Es ist deshalb wichtig, vor einer Erneuerung alle Dokumente, die mit älteren Chiffrierschlüsseln chiffriert sind, auf den aktuellen Chiffrierschlüssel umzuschlüsseln. Dieser wird bei der Erneuerung jeweils auf der Smartcard belassen. Die umgeschlüsselten Dokumente sind so auch nach der Erneuerung noch dechiffrierbar.

### Nach der Migration zu einer anderen PKI

Bei der Migration zu einer anderen PKI wird in der Regel eine ganz neue Smartcard ausgestellt. Damit X.509-Chiffrate, die mit der Smartcard der alten PKI chiffriert wurden, mit der neuen Smartcard geöffnet werden können, müssen sie mit Hilfe der alten Smarcard auf den neuen Chiffierschlüssel umgeschlüsselt werden (siehe 2.4 „Erweiterte Schlüsselwahl“).

## 2 Wie arbeite ich mit dem Umschlüsselungstool?

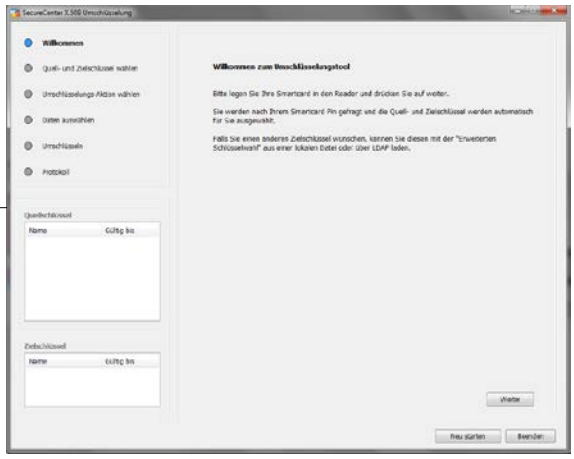
Damit die Umschlüsselung reibungslos und sicher funktioniert, halten Sie sich bitte an die in den Unterkapiteln beschriebenen Prozesse. Zudem müssen auch die unter Kapitel 3 genannten Punkte beachtet werden. Falls dennoch Probleme auftreten sollten, wenden Sie sich bitte an den Helpdesk.

ACHTUNG: Chiffrate von GEHEIM klassifizierten Informationen dürfen nur auf Geräten umgeschlüsselt werden, die für GEHEIME Informationen zulässig sind. Entfernen Sie bei solchen Chiffraten bei Prozessschritt 6 unbedingt den Haken, falls das verwendete Gerät nicht für GEHEIME Informationen zulässig ist. Führen Sie die Umschlüsselung dieser Dateien anschliessend auf einem dafür zulässigen Gerät vor.

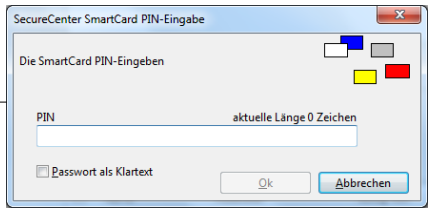
[1] Dies ist ab der zweiten Erneuerung der Fall oder auch, wenn einmal ein Key Recovery auf die Smartcard gemacht wurde.

## 2.1 Umschlüsselungsprozess mit automatischer Laufwerk- & Verzeichniswahl

**1. Einlogen mit alter Smartcard und öffnen Umschlüsselungstool, Dialogfenster Willkommen erscheint, mit „Weiter“ quittieren**



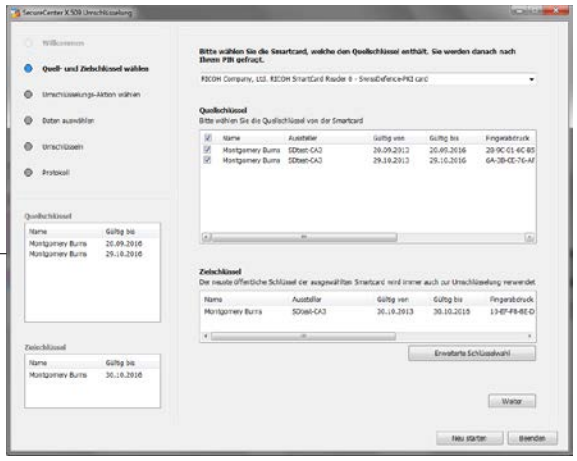
**2. Einlogen im Umschlüsselungstool mit alter Smartcard (PIN-Eingabe)**




**3. Im Dialogfenster Smartcard, welche Quellschlüssel (alter Schlüssel) enthält, auswählen**

**4. Das Dialogfenster zeigt unter Quellschlüssel den/die auf der Smartcard gespeicherten alten Schlüssel, Haken setzen falls nicht gesetzt**

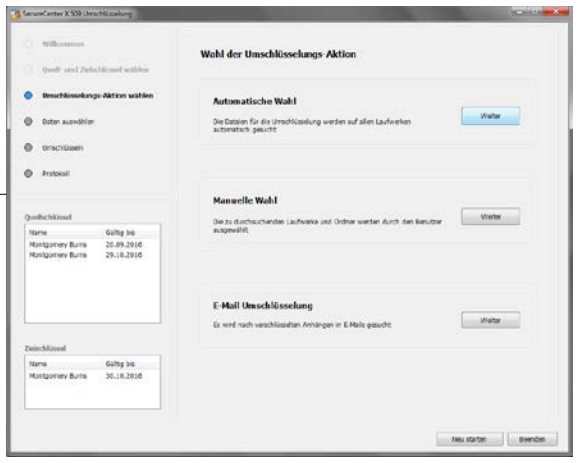
**5. Im Dialogfenster ist unter Zielschlüssel der auf der Smartcard gespeicherte neue Schlüssel ersichtlich, mit klick auf „Erweiterte Schlüsselwahl“ können zudem zusätzliche Schlüssel geladen werden (siehe Kap. 2.4)**



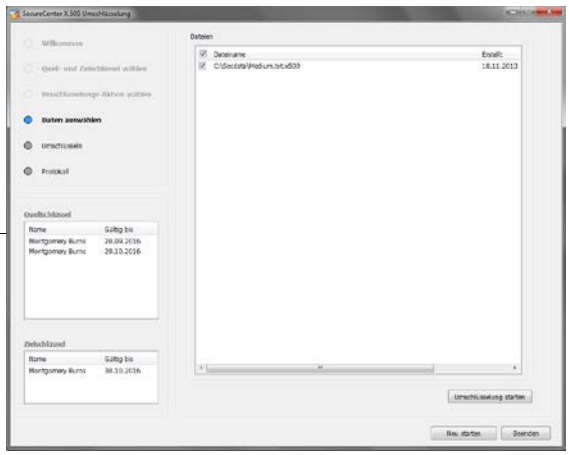
**6. Im Dialogfenster „Automatische Wahl“ durch quittieren mit „Weiter“ auswählen**

**(Automatische Wahl = automatische Durchsuchung der Laufwerke nach verschlüsselten Dateien inkl. Anwahl bei Treffer)**

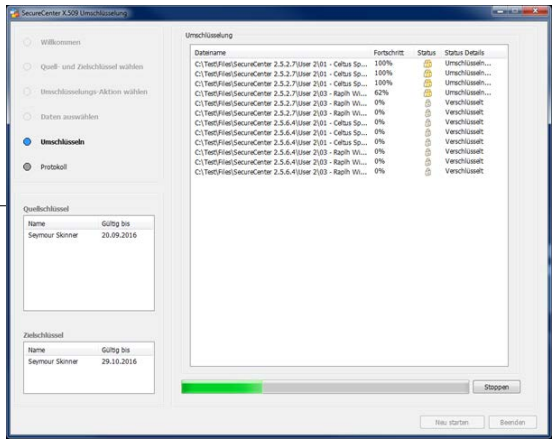
**(Man. Wahl siehe Kap. 2.2 und E-Mail Umschlüsselung siehe Kap. 2.3)**



**7. Anwahl der Dateien mit Haken setzen sowie Fenster quittieren mit „Umschlüsselung starten“**

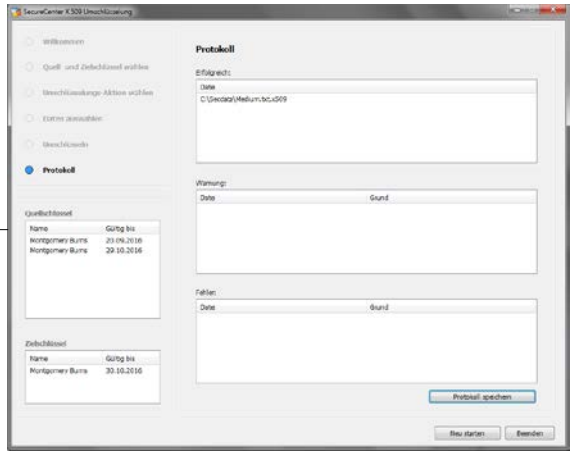


**8. Dialogfenster mit Fortschrittsanziege erscheint, der Prozesse kann jederzeit mit „Stoppen“ abgebrochen werden**



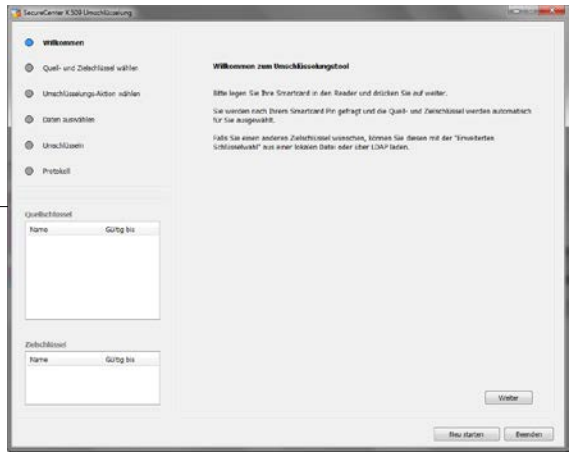
**Mit der Anzeige des Protokolls ist die Umschlüsselung abgeschlossen. Das Protokoll listet allfällige Fehler auf (weitere Informationen zu den Fehlermeldungen siehe Kap. 3.1).**

**Das Programm kann nun für eine weitere Umschlüsselung neu gestartet (Auswahl "Neu starten") oder beendet (Auswahl "Beenden") werden.**



## 2.2 Umschlüsselungsprozess mit manueller Laufwerk- & Verzeichniswahl

**1. Einloggen mit alter Smartcard und öffnen Umschlüsselungstool, Dialogfenster Willkommen erscheint, mit „Weiter“ quittieren**

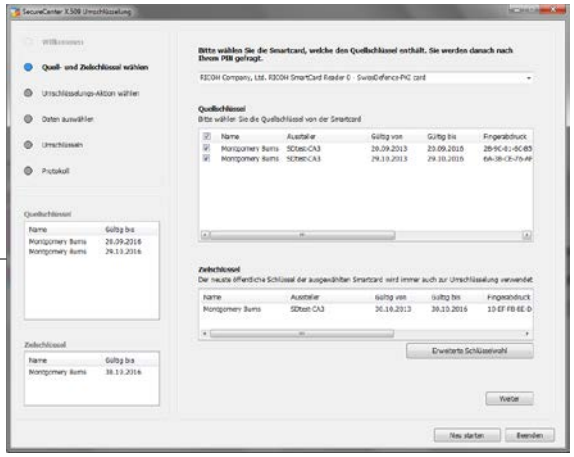



**2. Einloggen im Umschlüsselungstool mit alter Smartcard (PIN-Eingabe)**


**3. Im Dialogfenster Smartcard, welche Quellschlüssel (alter Schlüssel) enthält, auswählen**

**4. Das Dialogfenster zeigt unter Quellschlüssel den/die auf der Smartcard gespeicherten alten Schlüssel, Haken setzen falls nicht gesetzt**

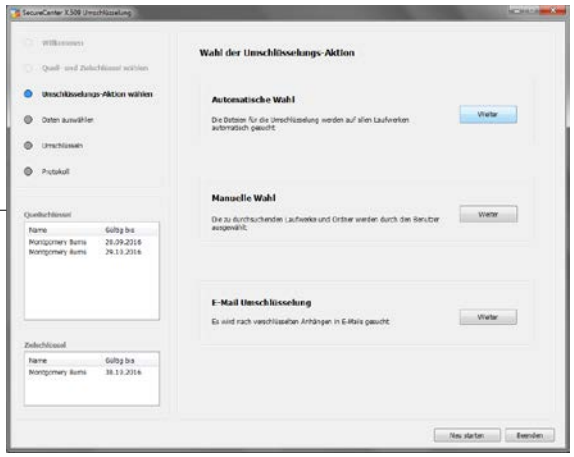
**5. Im Dialogfenster ist unter Zielschlüssel der auf der Smartcard gespeicherte neue Schlüssel ersichtlich,
mit Klick auf „Erweiterte Schlüsselwahl“ können zudem zusätzliche Schlüssel geladen werden (siehe Kap. 2.4)**



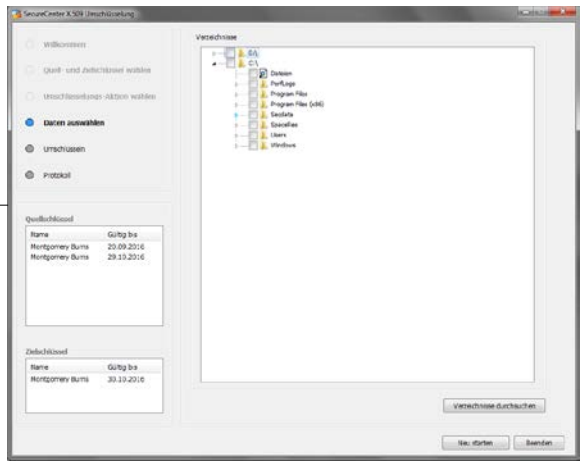

**6. Im Dialogfenster „Manuelle Wahl“ durch Quittieren mit „Weiter“ auswählen**

**(Manuelle Wahl = manuelle Anwahl der Laufwerke und verschlüsselten Dateien)**

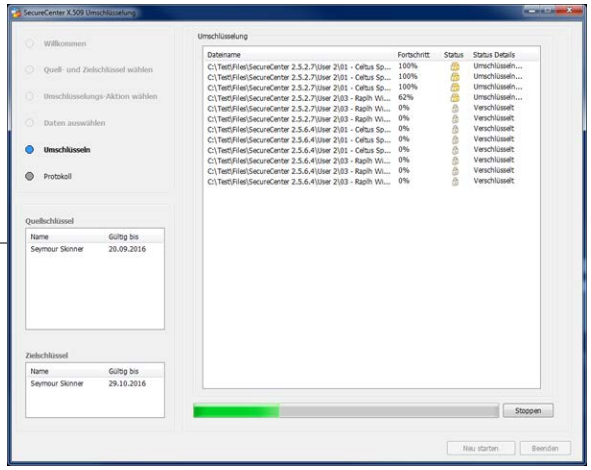
**(Auto. Wahl siehe Kap. 2.1 und E-Mail Umschlüsselung siehe Kap. 2.3)**



**7. Anwahl der Laufwerke durch Haken setzen, anschliessend auf „Verzeichnisse Durchsuchen“ klicken und Verzeichnisse durch Haken setzen auswählen, abschliessend Fenster quittieren mit „Umschlüsselung starten“**

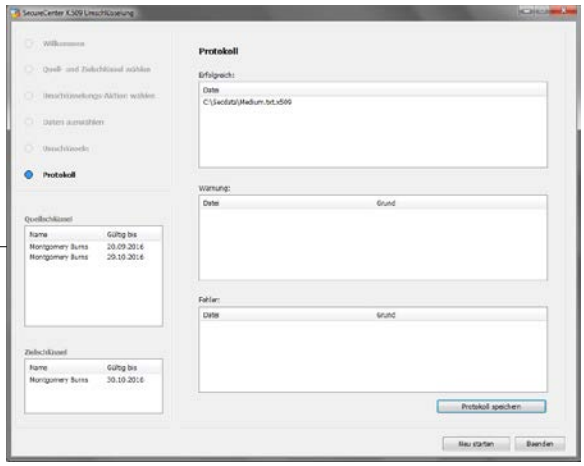


**8. Dialogfenster mit Fortschrittsanzeige erscheint, der Prozess kann jederzeit mit „Stoppen“ abgebrochen werden**



**Mit der Anzeige des Protokolls ist die Umschlüsselung abgeschlossen. Das Protokoll listet allfällige Fehler auf (weitere Informationen zu den Fehlermeldungen siehe Kap. 3.1).**

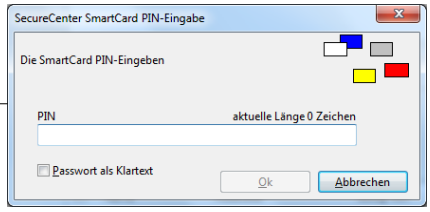
**Das Programm kann nun für eine weitere Umschlüsselung neu gestartet (Auswahl "Neu starten") oder beendet (Auswahl "Beenden") werden.**



## 2.3 Umschlüsselungsprozess E-Mail Anhänge

**1. Einloggen mit alter Smartcard und öffnen Umschlüsselungstool, Dialogfenster Willkommen erscheint, mit „Weiter“ quittieren**

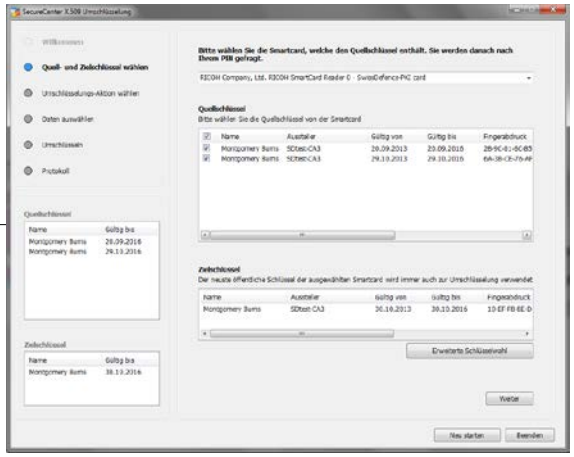
**2. Einloggen im Umschlüsselungstool mit alter Smartcard (PIN-Eingabe)**




**3. Im Dialogfenster Smartcard, welche Quellschlüssel (alter Schlüssel) enthält, auswählen**

**4. Das Dialogfenster zeigt unter Quellschlüssel den/die auf der Smartcard gespeicherten alten Schlüssel, Haken setzen falls nicht gesetzt**

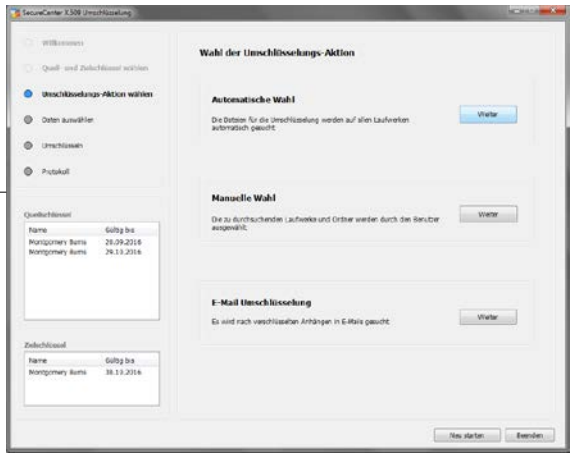
**5. Im Dialogfenster ist unter Zielschlüssel der auf der Smartcard gespeicherte neue Schlüssel ersichtlich, mit Klick auf „Erweiterte Schlüsselwahl“ können zudem zusätzliche Schlüssel geladen werden (siehe Kap. 2.4)**



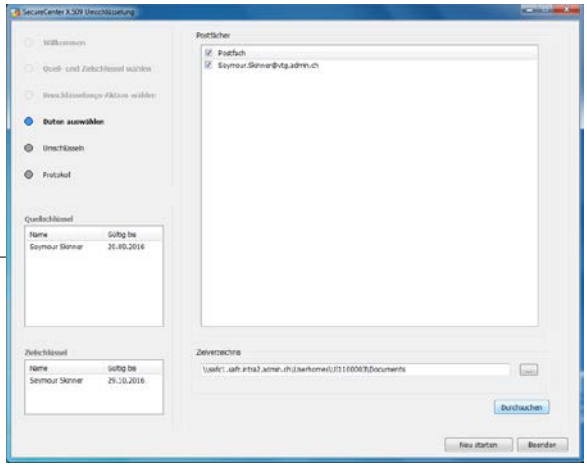
**6. Im Dialogfenster „E-Mail Umschlüsselung“ durch Quittieren mit „Weiter“ auswählen**

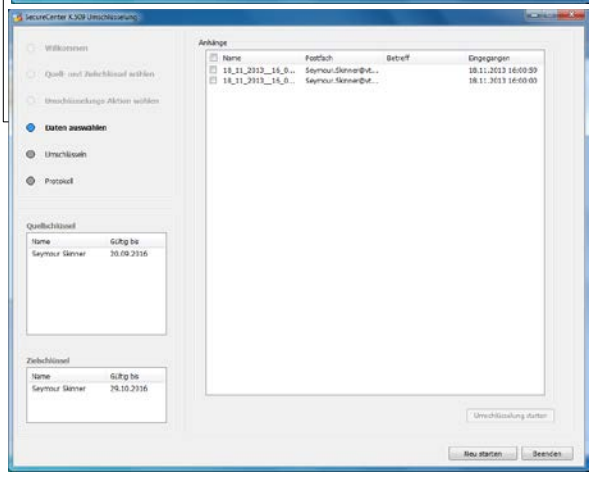
**(E-Mail Umschlüsselung = Suche nach E-Mail Anhängen in ausgewählten Postfächern)**

**(Auto. Wahl siehe Kap. 2.1 und Manuelle Wahl siehe Kap. 2.2)**

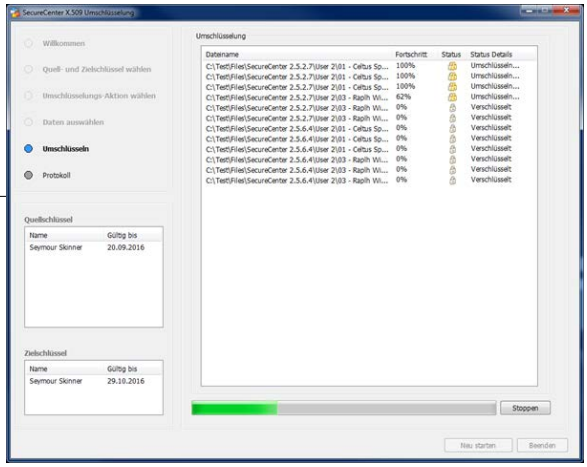


**7. Anwahl der Postfächer durch Haken setzen, anschliessend auf „Durchsuchen“ klicken und Verzeichnisse durch Haken setzen auswählen, dann Fenster quittieren mit „Umschlüsselung starten“, abschliessend Zielverzeichnis angeben und „speichern“ anwählen**



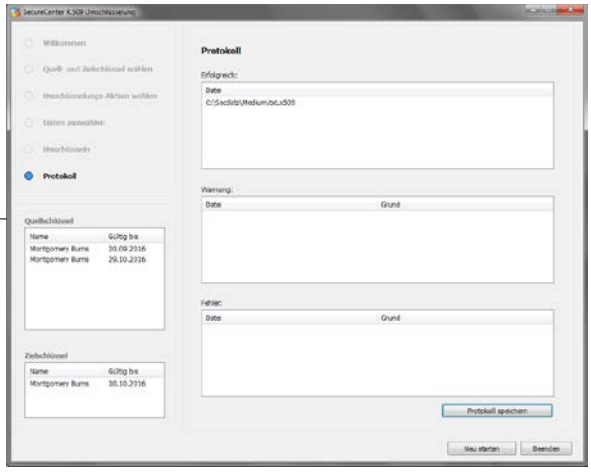


**8. Dialogfenster mit Fortschrittsanzeige erscheint, der Prozess kann jederzeit mit „Stoppen“ abgebrochen werden**



**Mit der Anzeige des Protokolls ist die Umschlüsselung abgeschlossen. Das Protokoll listet allfällige Fehler auf (weitere Informationen zu den Fehlermeldungen siehe Kap. 3.1).**

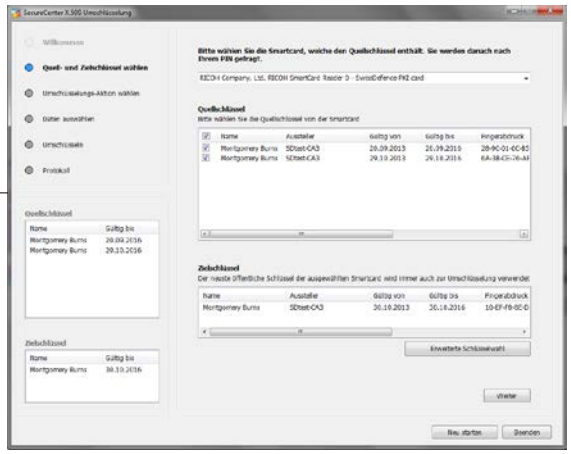
**Das Programm kann nun für eine weitere Umschlüsselung neu gestartet (Auswahl "Neu starten") oder beendet (Auswahl "Beenden") werden.**



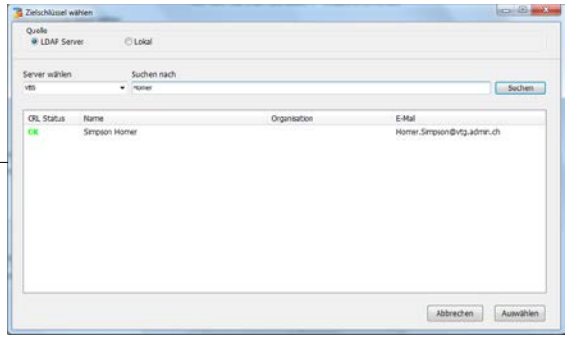
## 2.4 Erweiterte Schlüsselwahl

Wenn eine bewusste Umschlüsselung auf zusätzliche Schlüssel nötig ist, können die gewünschten Schlüssel über die „erweiterte Schlüsselwahl“ hinzugefügt werden. Informationen zum Schlüsselstatus finden sich in Kap. 3.2.

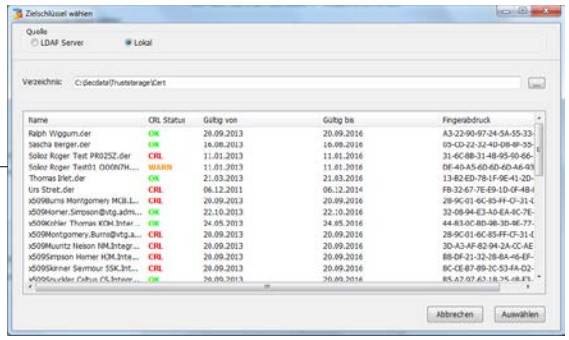
**1. Anwahl „Erweiterte Schlüsselwahl“ um weitere Schlüssel hinzuzufügen**



**2. Quelle auswählen „LDAP“ oder „Lokal“, anschliessend gewünschte Schlüssel markieren und mit „Auswählen“ übernehmen**



**Schlüssel wurden übernommen und sind im Dialogfenster „Quell- und Zielschlüsselwahl“ unter Zielschlüssel ersichtlich**



# 3 Wichtige Hinweise

## 3.1 Abschliessendes Protokoll

Das Protokoll gibt Auskunft über den Ablauf der Umschlüsselung: War die Umschlüsselung erfolgreich, sind Fehler aufgetreten, welche Fehler sind aufgetreten und für welche Schlüssel war die Umschlüsselung nicht erfolgreich.

Hier die Liste der möglichen Fehler:

| Fehlermeldung | Bedeutung | Massnahmen |
|---|---|---|
| Benötigte Schlüssel nicht vorhanden | Die benötigten Schlüssel konnten nicht von der Smartcard geladen werden. | Smartcard aus dem Leser entfernen, erneut einsetzen und Umschlüsselung neu starten. |
| Allgemeiner Fehler | Ein nicht vorhersehbarer Fehler ist aufgetreten. Dies kann durch Dateisystemfehler, beschädigte Dateien, Kryptofehler o.Ä. hervorgerufen werden. | Umschlüsselung neu starten und nicht umgeschlüsselte Dateien erneut umschlüsseln. |
| Keine Smartcard vorhanden | Die Smartcard konnte nicht gelesen werden, weil sie entfernt wurde oder ein Fehler den Zugriff verhindert hat. | Smartcard in den Leser einsetzen und Umschlüsselung neu starten. |
| Die Originaldatei ist fehlerhaft | Die Quelldatei konnte nicht entschlüsselt werden, da diese einen Fehler in der Krypto-Einheit hervorgerufen hat. Dies passiert, wenn die Quelldatei beschädigt ist. | Quelldatei überprüfen und Umschlüsselung neu starten. |
| Unbekannter Fehler | Ein unbekannter Fehler ist aufgetreten. | Umschlüsselung neu starten. |
| Schlüssellistenfehler | Die Schlüsselliste der umgeschlüsselten Datei entspricht nicht dem erwarteten Resultat. | Umschlüsselung neu starten und betroffene Datei(en) erneut umschlüsseln. |
| Dateistatusfehler | Die umgeschlüsselte Datei ist kein gültiges X.509 Chiffrat. | Umschlüsselung neu starten und betroffene Datei(en) erneut umschlüsseln. |

Der Warnhinweis „Fehlende Schlüssel: Benutzer X“ tritt dann auf, wenn die entsprechende Datei nach dem Umschlüsseln von Benutzer X nicht mehr geöffnet werden kann, weil für diesen kein Zertifikat gefunden werden konnte oder er nicht eindeutig identifizierbar war. In diesem Fall finden Sie im angegeben Pfad nun sowohl die Original-Quelldatei als auch die umgeschlüsselte Datei, welche Sie daran erkennen, dass dem Namen der Original-Quelldatei am Anfang „<Ihr Name>_“ hinzugefügt wurde.

Falls die Datei für den Benutzer X und evtl. weitere angegebene Benutzer weiterhin zugänglich sein muss, speichern Sie zuerst das Protokoll („Protokoll speichern“).

Fehlen nur wenige Benutzer, können Sie diese nun einen nach dem anderen durch erneutes Umschlüsseln wieder hinzufügen. Starten Sie dazu das Umschlüsselungstool erneut, wählen Sie im 5. Prozessschritt „Erweiterte Schlüsselwahl“ und wählen Sie den Chiffrierschlüssel des Benutzer X, welchen Sie hinzufügen möchten, als Zielschlüssel. Im 6. Prozessschritt wählen Sie „Manuelle Wahl“ und aktivieren Sie die Datei „<Ihr Name>_<Name der Original-Quelldatei>“. Führen Sie nun die Umschlüsselung durch. Weiterer Benutzer fügen Sie durch Wiederholen dieses Vorgangs hinzu.

Wenn Sie fertig sind, können Sie die Original-Quelldatei löschen und falls gewünscht die Datei „<Ihr Name>_<Name der Original-Quelldatei>“ in „<Name der Original-Quelldatei>“ umbenennen.

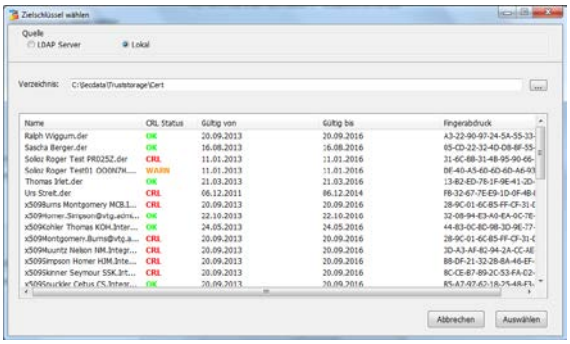
Fehlen viele Benutzer, konsultieren Sie die FAQ. Dort finden Sie eine Lösungsvariante, die in diesem Fall effizienter ist.

Der Warnhinweis „ Altes Chiffratformat oder unvollständige Schlüsselinformation“ bei einer Datei tritt dann auf, wenn die Datei ursprünglich noch für andere, aber nicht namentlich bekannte, Benutzer chiffriert war. Dateien mit diesem Warnhinweis werden für Sie umgeschlüsselt und als Datei mit Name „<Ihr Name>_<Name der Original-Quelldatei>“ gespeichert. Diese Datei kann nun von Ihnen entschlüsselt werden, nicht aber von den anderen, namentlich nicht bekannten Benutzern, für welche die Original-Quelldatei auch noch chiffriert war. Deshalb dürfen Sie die Original-Quelldatei nicht löschen, wenn sie sich an einem Speicherort befindet, auf den andere berechtigte Personen zugreifen können.

## 3.2 Status Erklärung der Schlüssel

Untenstehend finden sich die Statuserklärungen, gültig für die erweiterte Schlüsselwahl vom LDAP, wie auch einem lokalen Laufwerk. Bitte beachten Sie, dass grundsätzlich nur Schlüssel mit der grünen Kennung „OK“ verwendet werden sollten. Das Hinzufügen von Schlüsseln mit der erweiterten Schlüsselwahl wird in Kap. 2.4 erklärt.

| Status | Beschreibung |
|---|---|
| OK | Schlüssel ist gültig und nicht in der Sperrliste (CRL) |
| WARN | Schlüssel ist gültig, es ist jedoch nicht bekannt ob der Schlüssel in der Sperrliste ist weil:<br>a) keine Sperrliste vorhanden<br>b) Sperrliste veraltet |
| CRL | Schlüssel ist in der Sperrliste, egal ob gültig oder abgelaufen |




## 3.3 Arbeitsmethodik

### 3.3.1 E-Mail Anhänge

Die E-Mail Anhänge werden bei der Umschlüsselung in ein Zielverzeichnis (vom User bestimmt) kopiert und dort umgeschlüsselt. Sie stehen anschliessend in diesem Verzeichnis zur Verfügung. Es ist zu beachten, dass sich im Postfach nach wie vor die chiffrierte Originaldatei befindet, bei welcher keine Änderungen vorgenommen wurden.
Es wird daher empfohlen, die E-Mail Anhänge gemäss der gültigen Weisung des jeweiligen Amtes auf einem Laufwerk abzulegen und diese nicht im E-Mail Programm zu belassen. Die Umschlüsselung von E-Mail Anhängen wird in Kap. 2.3 erklärt.

### 3.3.2 Verhalten nach Umschlüsselung

Nach der Umschlüsselung muss zwingend der Arbeitsplatz mit SecureCenter gereinigt werden. Die Durchführung dieser Aktion ist im SecureCenter Handbuch unter „Kap. 7.4 Reinigen Arbeitsplatz“ erklärt.

## 3.4 Sicherheit Hinweis

Bitte beachten Sie, dass GEHEIM klassifizierte Dokumente nur auf für diese Klassifikations-stufe zugelassenen Geräten umgeschlüsselt werden dürfen.

# 4 FAQ

FAQ und weitere Informationen zur Umschlüsselung oder SecureCenter finden sie unter www.securecenter.ch.