Zentrum für sichere Informationstechnologie – Austria
Secure Information Technology Center – Austria
A-1030 Wien, Seidlgasse 22 / 9 — A-8010 Graz, Inffeldgasse 16a
Tel.: (+43 1) 503 19 63–0 — Tel.: (+43 316) 873-5514
Fax: (+43 1) 503 19 63–66 — Fax: (+43 316) 873-5520
http://www.a-sit.at
E-Mail: office@a-sit.at
DVR: 1035461 — ZVR: 948166612 — UID: ATU60778947

CCE3 DOKUMENTATION (VERSION 3.3.2, JUNI 2017)

Peter Teufl – peter.teufl@iaik.tugraz.at
Bojan Suzic – bojan.suzic@iaik.tugraz.at
Johannes Feichtner – johannes.feichtner@iaik.tugraz.at

Zusammenfassung: CCE ist ein Tool, welches das Verschlüsseln / Entschlüsseln von Dateien über die Bürgerkarte ermöglicht. Dateien können mit Hilfe des CCE Managers oder über das Kontextmenu des Windows Explorers verschlüsselt / entschlüsselt werden. CCE verwendet für die Verschlüsselung das Format S/MIME. Damit ist die Kompatibilität zu E-Mail-Clients wie Outlook, Thunderbird oder Evolution garantiert. Aufgrund der Verwendung von S/MIME als Dateiformat kann CCE auch E-Mails, die mit diesem Standard verschlüsselt wurden, entschlüsseln. Ab Version 3.2 wird das Umschlüsseln von Dateien im Batch-Betrieb unterstützt. Damit können etwa bei einem Kartenwechsel verschlüsselte Dateien mit der alten Karte entschlüsselt und für die neue Karte verschlüsselt werden.

Beachten Sie besonders die Hinweise in Abschnitt I, um Datenverlust bei Defekt oder Verlust Ihrer Karte zu vermeiden – etwa über Anlegen eines Backup-Schlüssels.

Inhaltsverzeichnis

Abschnitt I: Wichtige Hinweise

Diese MÜSSEN unbedingt vor der Verwendung von CCE3 gelesen werden, um Datenverluste zu vermeiden!

1. Verschlüsselung/Entschlüsselung

CCE3 basiert auf asymmetrischen Kryptographieverfahren, die für die Verschlüsselung und Entschlüsselung von Daten verwendet werden. Eine vereinfachte Darstellung dieser Verfahren zeigt, dass es zwei zentrale Komponenten gibt, die für die Verschlüsselung und Entschlüsselung von Daten eine Rolle spielen:

- **Zertifikate** (diese werden in CCE3 und in diesem Dokument auch als „Empfänger" bezeichnet): Zertifikate werden für die Verschlüsselung von Daten verwendet und können bzw. sollen öffentlich verfügbar sein. Wenn Sie möchten, dass eine Person Daten für Sie verschlüsselt, müssen Sie dieser Person Ihr Zertifikat übermitteln. Die Zertifikate können **NUR** für die Verschlüsselung eingesetzt werden. Es ist nicht möglich, Daten damit zu entschlüsseln.
- **Schlüssel**: Zu jedem Zertifikat gehört ein Schlüssel, der für die Entschlüsselung der Daten verwendet wird. Dieser **MUSS** geheim gehalten werden, da damit der Zugriff auf die mit dem zugehörigen Zertifikat verschlüsselten Daten möglich gemacht wird. Dabei gibt es prinzipiell zwei Möglichkeiten, Schlüssel zu speichern:
    - **Smartcard (z.B. Bürgerkarte)**: Der Schlüssel befindet sich auf der Smartcard. Aufgrund der Smartcard-Technologie ist es nicht möglich, diesen Schlüssel auszulesen und zu kopieren[1]. Alle Operationen, die für die Entschlüsselung mit diesem Schlüssel durchgeführt werden, werden direkt auf der Smartcard ausgeführt. Die Operationen werden durch einen PIN Code geschützt. **ACHTUNG: Da von diesen Schlüsseln keine Kopie gemacht werden kann[1], geht der Schlüssel bei der Beschädigung oder beim Verlust der Smartcard verloren. Auf Daten, die mit diesem Schlüssel verschlüsselt wurden, kann danach NICHT mehr zugegriffen werden. Sie sind unwiederbringlich verloren (außer die Daten wurden auch noch für andere Empfänger verschlüsselt, die über die zugehörigen Schlüssel verfügen).**
    - **Datenträger**: Der Schlüssel befindet sich auf einem Datenträger (z.B.: Festplatte). In diesem Fall können Kopien erstellt werden. Dies hat den Vorteil, dass Backups erstellt werden können auf die im Falle des Verlusts

[1] *Anmerkung: Bei der österreichischen Bürgerkarte besteht für A-Trust Karten die Möglichkeit eines Schlüssel-Backups für das von CCE3 verwendete „Geheimhaltungszertifikat". Damit kann bei Verlust oder Tausch der Karte derselbe Schlüssel auf die Karte aufgebracht werden. Die Entschlüsselung damit ist dann theoretisch technisch möglich, CCE3 unterstützt dies aber nicht, da es die Zuordnung des neuen Zertifikats zum alten Schlüssel nicht durchführen kann.*

oder bei Beschädigung des Datenträgers zugegriffen werden kann. **ACHTUNG: Dadurch ist es aber leichter auch möglich, dass der Schlüssel in die Hände von unbefugten Drittpersonen gelangt, die somit Zugriff auf die Daten haben, die mit diesem Schlüssel verschlüsselt wurden.**

Es wird dringend empfohlen, den **Fehler! Verweisquelle konnte nicht gefunden werden.** dieses Dokuments zu lesen, der weitere Auskünfte zur richtigen Schlüsselverwendung gibt.

2. Backup Schlüssel

Bevor CCE3 verwendet wird, wird eindringlich empfohlen, einen Backup Schlüssel zu erstellen. Die Gründe dafür sind:

- **Verwendung von Smartcards:** Schlüssel die auf einer Smartcard gesichert sind, können nicht kopiert werden. D.h. im Falle des Verlusts oder der Beschädigung der Smartcard kann nicht mehr auf den Schlüssel zugegriffen werden. Daten die mit dem dazugehörigen Empfänger verschlüsselt wurden, können **NICHT** mehr entschlüsselt werden[2].
- **Verwenden von Software-Schlüsseln (gespeichert auf einem Datenträger):** Diese Schlüssel können im Gegensatz zu Schlüsseln auf Smartcards auf Datenträger kopiert werden, sind aber aufgrund der leichteren Angreifbarkeit durch Passwörter gesichert. Bei Verlust des Passworts oder bei Beschädigung eines Software Schlüssel-Speichers (z.B. der Speicher ***Meine Schlüssel*** in CCE3) können Daten, die mit dem zugehörigen Zertifikat verschlüsselt wurden, **NICHT** mehr entschlüsselt werden.
- **Kein Zugriff auf die Schlüssel einer Person**: Werden Daten von einer Person ohne Backup Schlüssel verschlüsselt und scheidet diese Person aus dem Dienstverhältnis aus, so kann vom Dienstgeber nicht mehr auf die Daten zugegriffen werden.

Für weitere Informationen zur Erstellung und Handhabung von Backup Schlüsseln wird auf Abschnitt IV:1 verwiesen.

3. Datenreste und Sicheres Löschen

Es wird generell empfohlen, CCE3 im Zusammenhang mit einem verschlüsselten Dateisystem zu verwenden. Details und Gründe dafür werden in diesem Abschnitt beschrieben.
Für das Löschen von Dateien aus dem Dateisystem gilt folgendes:

---

[2] *A-Tust Karten siehe auch Fussnote 1 zu Backup der Geheimhaltungsschlüssel durch A-Trust. Die damit technisch mögliche Entschlüsselung nach Verlust oder Defekt einer Karte kann allerdings nicht mit CCE3 durchgeführt werden, sondern müsste von Fachleuten gesondert umgesetzt werden. Diehe dazu auch Abschnitt II, 1.2 letzter Absatz.*

- **Daten auf einem unverschlüsselten Dateisystem:** Beim Löschen von Daten bleiben Reste zurück, die eine Wiederherstellung der Daten wahrscheinlich machen. Ein Angreifer, der Zugriff auf einen Datenträger hat, kann somit Zugriff auf bereits gelöschte Daten bekommen. Dies gilt für alle unverschlüsselten Dateisysteme die unter Windows, OS X und Linux verwendet werden, wenn die Standardlöschfunktion des Betriebssystems verwendet wird.
- **Daten auf einem verschlüsselten Dateisystem (Bitlocker, Filevault etc.):** In diesem Fall entfällt diese Problematik, da der Angreifer auch bei Zugriff auf den Datenträger keinen Zugriff auf die Daten erhält, da diese verschlüsselt am Datenträger gespeichert werden (basierend auf der Annahme dass der Angreifer keinen Zugriff auf den Schlüssel hat).

Nun ist es auch auf unverschlüsselten Dateisystemen möglich, Daten so zu löschen, dass keine Datenreste übrigbleiben. Dabei wird beim Löschen nicht nur die Referenz auf die Daten entfernt, sondern die Daten so überschrieben, dass eine Wiederherstellung nicht möglich ist. Die unterschiedlichen Betriebssysteme bieten dabei unterschiedliche Tools, die das sichere Löschen von Daten ermöglichen.

- **Windows**: Bei Windows wird kein Tool mitgeliefert. Es gibt aber externe Programme, die diese Funktionalität implementieren.
- **Linux**: Unter Linux gibt es das ***srm*** Kommando, das nachinstalliert werden kann. Dateien die über ***srm*** statt ***rm*** gelöscht werden, werden sicher gelöscht
- **OS X**: Jede OS X Variante bietet die Möglichkeit den Papierkorb sicher zu löschen. Zusätzlich wird mit jeder Installation das ***srm*** Tool mitgeliefert (analog zum ***srm*** Tool unter Linux).

Für CCE3 gelten folgende Punkte, die beim Löschen von Daten beachtet werden müssen:

- **Sicheres Löschen - Allgemein**: CCE3 versucht Daten immer sicher zu löschen, wenn das Betriebssystem die Funktionalität bietet. Ist diese Funktionalität nicht gegeben, so wird beim Start eine Warnung ausgegeben (Dateien werden dann normal gelöscht).
  Diese Abfrage ist standardmäßig deaktiviert und kann in der Konfiguration von CCE3 aktiviert werden (siehe Abschnitt V:3.1.1). Die Funktionalität hängt vom verwendeten Betriebssystem ab:
  - **Windows**: Microsoft bietet das Tool ***sdelete.exe***[3] an, das das sichere Löschen von Daten ermöglicht. Aufgrund der Lizenzbedingungen kann dieses Tool aber nicht mit CCE3 mitgeliefert werden. Ist aber die Überprüfung der "Sicheres Löschen Funktionalität" in der Konfiguration aktiviert, wird CCE3 darauf hinweisen, dass das Tool heruntergeladen werden kann. Nach dem

[3] http://technet.microsoft.com/en-us/sysinternals/bb897443.aspx

Bestätigen der Lizenzbedingungen von Microsoft, integriert CCE3 das Tool und verwendet es in Zukunft für das sichere Löschen von Dateien.

  - **OS X**: Da ***srm*** auf jeder OS X Installation vorhanden ist, wird ***srm*** automatisch beim Löschen von Daten eingesetzt. Bei etwaigen Problemen mit ***srm*** zeigt CCE3 nur eine Fehlermeldung wenn die Überprüfung der "Sicheres Löschen Funktionalität" in der Konfiguration aktiviert ist.
  - **Linux**: ***srm*** ist typischerweise nicht installiert, kann aber bei jeder Linux Distribution nachinstalliert werden. CCE3 zeigt nur eine Fehlermeldung, wenn die Überprüfung der "Sicheres Löschen Funktionalität" in der Konfiguration aktiviert ist.

- **Verschlüsseln**: CCE3 bietet beim Verschlüsseln die Möglichkeit, die Quelldateien nach der Verschlüsselung zu löschen.
- **Bearbeiten von Containern**: Um Dateien in einem Container bearbeiten zu können (siehe Abschnitt IV:4), muss CCE3 diese Dateien zuerst in einen temporären Ordner entschlüsseln (siehe Abschnitt III:1). Dieser temporäre Ordner wird nach der Verwendung wieder gelöscht.

Selbst wenn CCE3 Dateien über die ***Sicheres Löschen Funktionalität*** löschen kann, sind folgende Punkte zu beachten:

- **Temporäre Dateien**: CCE3 löscht alle Dateien, die vom Programm temporär erstellt werden. Allerdings kann CCE3 keine Dateien löschen, die von externen Programmen erstellt werden. Als Beispiel wird hier das Bearbeiten einer Word Datei in einem Container beschrieben:
  1. CCE3 entschlüsselt die Datei in einen temporären Ordner (siehe Abschnitt III:1)
  2. CCE3 öffnet die Datei mit Word
  3. Word erstellt selbst temporäre Dateien und löscht diese nach der Bearbeitung. Hier liegt das Problem: Diese temporären Dateien werden von Word nicht sicher gelöscht und CCE3 hat keine Informationen darüber wo diese Dateien angelegt werden.
  4. CCE3 löscht die temporäre Word Datei nach der Bearbeitung sicher. Allerdings liegen aufgrund der von Word selbst erstellten und gelöschten temporären Dateien immer noch Datenreste auf dem Datenträger, die von einem Angreifer wiederhergestellt werden können.
- **Beenden von CCE**: Falls sich beim Beenden von CCE3 noch temporäre Dateien im temporären Verzeichnis befinden, werden diese von CCE3 vor dem Schließen gelöscht. Wird CCE3 aber über den Taskmanager beendet oder kommt es zu einem Programmabsturz, bleiben diese Dateien bestehen und werden erst bei der nächsten Verwendung von CCE3 entfernt.

ACHTUNG: Aufgrund dieser Punkte wird es empfohlen, CCE3 auf einem verschlüsselten Dateisystem zu verwenden, da damit die Problematik der Datenreste entfällt.

Abschnitt II: Installation und Anforderungen

Dieser Abschnitt beschreibt die CCE3 Installation und die Anforderungen an das verwendeten Betriebssystem. Für weitere Details über CCE3 und die verwendeten Dateien und Ordner wird auch auf Abschnitt III verwiesen.

CCE3 ist in Java[4] programmiert und verwendet für das GUI das SWT Toolkit[5]. SWT wird über Java angesteuert, verwendet aber für die Darstellung des GUIs die APIs des eingesetzten Betriebssystems (win32 unter Windows, GTK unter Linux, COCOA unter OS X).

Die für CCE3 benötigte Java 1.6 Installation wird bei Windows und Linux mitgeliefert. Bei OS X wird die auf jedem OS X installierte Java Version verwendet. CCE3 wird dabei in einer 32bit und einer 64bit Variante ausgeliefert. Die beiden Varianten unterscheiden sich nur durch die mitgelieferte Java VM.

1. Anforderungen

1.1. Kartenleser

Es wird ein PCSC fähiger Smartcard Leser benötigt. CT-API wird von CCE3 nicht unterstützt.

1.2. Bürgerkarte/Smartcard

Im Gegensatz zu den Vorgängerversionen CCE1/2 benötigt CCE3 **KEINE** Bürgerkartenumgebung (BKU) mehr, um auf die Smartcard zuzugreifen. CCE3 liefert selbst alle für den Zugriff benötigten Komponenten mit.

In der CCE3 Version 3.3.1 werden folgende Smartcards unterstützt:

- Alle Generationen der ECARD (STARCOS OS)
- Alle Generation der A-TRUST Karten (ACOS OS)

Die Unterstützung von weiteren nicht-österreichischen Karten ist für zukünftige Versionen geplant.

Wichtiger Hinweis im Zusammenhang mit der Bürgerkarte: Für das Verschlüsseln und Entschlüsseln von Daten werden die Zertifikate und die dazugehörigen Schlüssel der Bürgerkarte benötigt. **Beim Austausch der Karte (z.B. Ablaufen der E-CARD) erhält die neue Karte auch andere Schlüssel. Ein Zugriff auf die alten Daten ist somit NICHT**

[4] *http://www.oracle.com/technetwork/java/index.html*

[5] *http://www.eclipse.org/swt/*

mehr möglich. Dies ist nur bei anderen Bürgerkartenanwendungen möglich die auf der Personenbindung basieren (alle Webanwendungen: z.B. FinanzOnline). Diese kann aber nicht für das Ver-/Entschlüsseln verwendet werden. Daher gibt es bei CCE3 eine Abhängigkeit zur verwendeten Karte.
Das bei A-Trust Karten mögliche Schlüssel-Backup wird von CCE3 nicht unterstützt, da die Zuordnung einer neuen Karte zum alten Zertifikat nicht gefunden wird. Ein Entschlüsseln durch Fachleute ist möglich, wenn:

- Eine CMS (PKCS#7) Bibliothek verfügbar ist, über die der verwendete Schlüssel (die neue Smartcard mit dem Backup-Schlüssel) erzwungen werden kann; oder
- Mit CCE3, indem man in die CMS Datenstruktur eingreift und das neue Zertifikat zu den Empfängern (als recipientInfo der Enveloped Data) hinzufügt. Dazu
    - aus den S/MIME Daten eine BER-Datei erstellen (base64 dekodieren)
    - mit einem ASN.1 Editor das neue Zertifikate als neue recipientInfo hinzufügen oder eine bestehende editieren (Issuer-Daten und Seriennummer)
    - Das Resultat wieder in die S/MIME Struktur oacken

1.3. Netzwerk

CCE3 benötigt für die Widerrufsprüfung, die Empfängersuche über LDAP und den Zugriff auf HTTP(S) Speicher Zugriff auf folgende Ports (bei der Verwendung von Standardports):

- ***Widerrufsprüfung***: LDAP (TCP 389), OCSP über HTTP (TCP 80)
- ***LDAP Server Suche***: LDAP (TCP 389)
- ***Externer HTTP(S) Speicher***: HTTP (TCP 80) oder HTTPS (TCP 443)

2. Installation

2.1. Windows

Es werden Windows XP, Vista und Windows 7 in den 32/64bit Versionen unterstützt. Die Installation von CCE3 erfolgt dabei über die MSI Pakete, die in einer 32bit und in einer 64bit Version zur Verfügung stehen. Die Pakete sind multilingual und unterstützen die Sprachen Englisch und Deutsch.

CCE3 verwendet beim Starten die Systemsprache, kann aber auch manuell auf Deutsch oder Englisch gesetzt werden (siehe Abschnitt V:3.1.1 für weitere Details).

2.2. OS X

Es wird nur ab 10.6.x (10.6.x Snow Leopard, 10.7.x. Lion) unterstützt. Ältere Versionen von OS X verfügen nicht über die 32bit Version von Java 1.6, die für den Smartcard Zugriff benötigt wird[6].
Um die starken Verschlüsselungsalgorithmen von CCE3 unter Java verwenden zu können, müssen unter OS X entsprechende Policy Patches installiert werden.

CCE3 überprüft beim Starten ob diese Patches vorhanden sind und liefert ein Script mit dem die Installation dieser Patches durchgeführt wird. Diese manuelle Installation ist bei Linux und Windows nicht notwendig, da bei diesen Paketen eine bereits mit den Policy Patches konfigurierte Java VM mitgeliefert wird.

2.3. Linux

Im Prinzip kann CCE3 auf jeder 32/64bit Linux Version verwendet werden die über die GTK Bibliotheken für die GUI Elemente verfügt. Der Smartcard-Zugriff erfolgt über den PCSC Daemon der unter Linux zur Verfügung steht. Z.B.: Unter Ubuntu müssen dabei folgende PCSC Komponenten installiert werden:

```
sudo apt-get install libpcsclite-dev pcscd
```

[6] *OS X 10.5.x (Leopard) liefert Java 1.6 nur in einer 64bit Version mit. Aufgrund von Problemen mit dem PCSC Daemon unter OS X, kann die 64bit Java Version nicht auf die Smartcard zugreifen. Das gleiche Problem tritt bei OS X 10.6 (Snow Leopard) auf. Dort wird aber Java 1.6 in der 32bit Version mitgeliefert, die für CCE3 verwendet wird.*

Abschnitt III: Details (Container Format, Algorithmen)

1. CCE3 Dateien und Ordner

Folgende Ordner und Dateien werden von CCE3 verwendet:

- **Installationsverzeichnis:**
  - **Windows**: Im Programme-Verzeichnis wird die Installation unter den Ordnern A-SIT/CCE3 durchgeführt
  - **OS X**: Typischerweise erfolgt die Installation über Drag and Drop der CCE3.app Datei in den Applikationsordner von OS X.
  - **Linux**: CCE3 wird durch das Entpacken in das gewünschte Verzeichnis installiert
- **CCE3 Daten:** Alle CCE3 Daten (z.B.: Empfänger) werden in dem .CCE2 Verzeichnis abgelegt, das sich im Home Verzeichnis des Benutzers befindet. Dieses wird bei der Deinstallation von CCE3 **NICHT** entfernt.
  - **Windows Vista/7/8**: C:/Benutzer/BENUTZERNAME/.CCE2
  - **Windows XP**: C:/Dokumente und Einstellungen /BENUTZERNAME/.CCE2
  - **OS X**: /Users/BENUTZERNAME/.CCE2
  - **Linux**: /home/BENTUZERNAME/.CCE2
- **Temporäre Dateien**: Diese werden unter .CCE2/temp abgelegt. Siehe dazu (Abschnitt V:3.1.1).

Log Dateien: Wenn die Logging Funktionalität aktiviert ist, werden die Logs unter .CCE2/logs abgelegt (siehe **Fehler! Verweisquelle konnte nicht gefunden werden.**).

2. Container Format

Es wird der S/MIME Standard[7] für das Container Format verwendet. CCE3 verwendet dabei die Dateiendung .cce.

3. Algorithmen

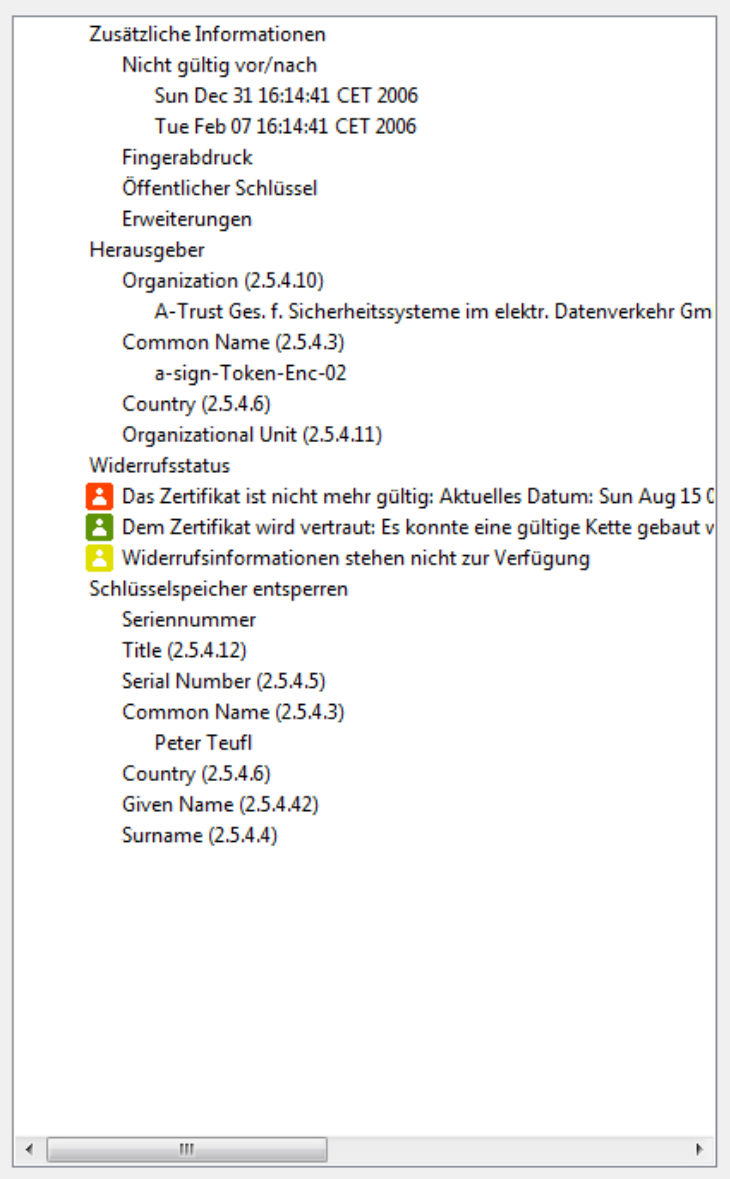
Die Daten im S/MIME Container werden mit einem symmetrischen Schlüssel verschlüsselt. Dabei wird der AES Algorithmus mit 256bit Schlüssellänge eingesetzt. Dieser Schlüssel wird dann für den jeweiligen Empfänger mit dem öffentlichen Schlüssel des Empfängerzertifikats verschlüsselt. Der dort eingesetzte Algorithmus hängt vom verwendeten Zertifikat ab.
CCE3 unterstützt dabei Zertifikate basierend auf RSA Schlüsseln und Zertifikate die auf elliptischen Kurven basieren.

[7] *http://www.imc.org/smime-pgpmime.html*

4. Widerrufsprüfung

Zertifikate (Empfänger) die in CCE3 verwendet werden, werden von CCE3 auf ihre Gültigkeit geprüft. Ein Empfänger wird dann als gültig erkannt (grün markiert), wenn alle der folgenden Punkte erfüllt sind:

- **Es wird dem Aussteller des Zertifikats vertraut.** CCE3 liefert alle Aussteller der A-TRUST Karten und der E-CARDS mit. Der Vertrauensstatus für diese Karten ist somit gegeben. Details zur Verwaltung der Aussteller werden in **Fehler! Verweisquelle konnte nicht gefunden werden.** beschrieben.
- **Das Zertifikat ist noch/schon gültig:** Das Zertifikat ist zum aktuellen Zeitpunkt gültig (abhängig von den von/bis Zeitpunkten im Zertifikat).



- Das Zertifikat ist nicht widerrufen: Bei den Widerrufspunkten (OCSP oder CRL) liegen keine Widerrufsinformationen zum überprüften Zertifikat vor.
- **Es können die Widerrufsinformationen gefunden werden:** Die angegeben Widerrufspunkte können abgerufen werden bzw. sind überhaupt vorhanden.

Sobald eine dieser Bedingung nicht erfüllt ist, wird der Empfänger als rot markiert. Detaillierte Informationen, warum der Empfänger als nicht gültig eingestuft wird, können in der Detail-Ansicht des Empfängers angezeigt werden (CCE3 Hauptmenü: ***Empfänger und Schlüssel/Empfänger***, markieren des gewünschten Empfängers).

Sobald mit nicht gültigen Empfängern verschlüsselt wird, warnt CCE3, dass diese Empfänger nicht verwendet werden sollten. Es kann jedoch in bestimmten Fällen Sinn machen diesen ungültigen Empfängern trotzdem zu vertrauen:

- **Vertrauenswürdige Quelle**: Der Empfänger wurde von einer vertrauenswürdigen Quelle erstellt, verfügt aber über keine Widerrufsinformationen. Dies trifft z.B. zu, wenn Empfänger und Schlüssel im CCE3 Speicher ***Meine Schlüssel*** erstellt werden.
- **Vertrauenswürdige Aussteller:** Der Aussteller des Empfängers ist nicht bei den vertrauenswürdigen Stammzertifizierungsstellen gespeichert (siehe **Fehler! Verweisquelle konnte nicht gefunden werden.**). Man möchte aber diesem einen Empfänger aber trotzdem vertrauen.
- **Weiterverwendung von Karten:** Eine Smartcard kann auch über den zeitlichen Ablauf des Zertifikats hinausgehend als technisch sicher sein, sodass der Verschlüsselung dafür weiter vertraut wird. Das kann etwa für im Safe verwahrte Backup-Karten sinnvoll sein, die bis zur technischen Sicherheitsgrenze weiter verwendet werden soll.

In diesen Fällen bietet CCE3 die Möglichkeit, entweder einfach trotz Warnung die Verschlüsselung durchzuführen oder (um weitere Warnungen zu unterdrücken), den Vertrauensstatus explizit zu setzen (bzw. auch wieder zu entfernen). Für weitere Details dazu wird auf **Fehler! Verweisquelle konnte nicht gefunden werden.** verwiesen.

ACTHUNG: Für die Widerrufsprüfung wird ein Zugang zum Internet benötigt. Ist dieser nicht gegeben, können die Zertifikate nicht überprüft werden und sind somit als rot markiert.

Abschnitt IV: Howtos

Dieser Abschnitt beschreibt typische CCE3 Abläufe.

1. Schlüsselhandhabung und Verwendung von Backup Schlüsseln

Mit Version 3.3.1 steht noch kein Wizard zur Verfügung, der die Installation eines Backup Schlüssels durchführt. Es werden daher hier die manuellen Schritte beschrieben. Es wird dabei von zwei Anwendungsszenarien ausgegangen - die private Anwendung von CCE3 und die Anwendung von CCE3 im Unternehmen.

1.1 Private Verwendung

Es wird von folgenden Punkten ausgegangen:

- Der Benutzer verfügt über eine Bürgerkarte (siehe dabei die Hinweise in Abschnitt II:1.2).
- Der Benutzer möchte CCE3 für die Datenverschlüsselung einsetzen und sicher gehen, dass beim Verlust, bei der Beschädigung der Karte oder beim Austausch der Karte (siehe Abschnitt II:1.2) weiterhin der Zugriff auf die verschlüsselten Daten möglich bleibt.

Der Benutzer geht dabei wie folgt vor. Details zu den Befehlen werden dabei in den Abschnitten **Fehler! Verweisquelle konnte nicht gefunden werden.** und **Fehler! Verweisquelle konnte nicht gefunden werden.** beschrieben.

1. Der Benutzer erstellt einen Schlüssel im Schlüsselspeicher ***Meine Schlüssel*** (über den Befehl ***Erzeuge Schlüssel und Empfänger...***). Falls der Schlüsselspeicher noch nicht initialisiert ist, muss dieser über den Befehl ***Initialisiere den Schlüsselspeicher...*** initialisiert werden.
2. Der Benutzer exportiert diesen Schlüssel in eine PKCS12 Datei, die auf einen Backup Datenträger kopiert wird (über den Befehl ***Exportiere Schlüssel...***). Der Datenträger (oder mehrere Backup Kopien davon) und die Passwörter für die PKSC12 Dateien werden an sicheren Orten aufbewahrt.
3. Der Benutzer fügt das Zertifikat (den Empfänger) des erstellten Schlüssels zur ***default*** Gruppe des Empfängerspeichers ***Meine Empfänger*** hinzu (über Drag and Drop wie in Abschnitt V:1 beschrieben). Es macht Sinn, den Vertrauensstatus des Backup Empfängers explizit zu setzen, da dafür keine Widerrufsinformationen vorhanden sind (über den Befehl ***Diesem Empfänger explizit vertrauen***).
4. Der Benutzer fügt das Zertifikat (den Empfänger) seiner Bürgerkarte (zu finden unter ***Meine Smartcard***) zur ***default*** Gruppe des Empfängerspeichers ***Meine Empfänger*** hinzu (über Drag and Drop wie in Abschnitt V:1 beschrieben).
5. Jeder Container, der vom Benutzer erstellt wird, ist nun für diese beiden Empfänger verschlüsselt. Im Falle des Verlusts der Bürgerkarte können die Daten immer noch über

den Backup Schlüssel im Schlüsselspeicher ***Meine Schlüssel*** entschlüsselt werden. Geht zusätzlich auch noch der Schlüsselspeicher ***Meine Schlüssel*** verloren (z.B. durch einen Systemabsturz oder eine beschädigte Festplatte), kann dieser auf einer neuen CCE3 Installation wieder über die gesicherte PKCS12 Datei mit dem korrekten Schlüssel befüllt werden (über die Befehle ***Initialisiere den Schlüsselspeicher...*** und ***Füge Schlüssel von PKCS12 Datei hinzu...***)

1.2 Verwendung im Unternehmen

Es wird von folgenden Punkten ausgegangen:

- Daten sollen für Personen innerhalb einer Abteilung/Gruppe verschlüsselt werden.
- Jeder Benutzer verfügt über eine Bürgerkarte (siehe Abschnitt II:1.2).
- Es soll gewährleistet werden, dass beim Verlust von Bürgerkarten oder beim Ausscheiden von Personen die Abteilungsleitung Zugriff auf die Daten hat.

Vorgehensweise:

1. Es wird ein vorhandener Backup Schlüssel (PKCS12 Datei) in den Schlüssel Speicher ***Meine Schlüssel***[8] importiert (über den Befehl ***Füge Schlüssel von PKCS12 Datei hinzu...***). Ist noch kein Backup Schlüssel vorhanden, so kann dieser im Schlüsselspeicher ***Meine Schlüssel*** erstellt werden (über den Befehl ***Erzeuge Schlüssel und Empfänger...***) und in einer PKCS12 Datei exportiert werden (über den Befehl ***Exportiere Schlüssel...***). In beiden Fällen muss die PKCS12 Datei und das Passwort an einem sicheren Ort aufbewahrt werden (z.B. in einem Safe).
2. Alle zu verschlüsselnden Daten sollen nun mit den jeweiligen Empfängern und dem erzeugten Backup Schlüssel verschlüsselt werden. Zuvor macht es Sinn, den Vertrauensstatus des Backup Empfängers explizit zu setzen, da dafür keine Widerrufsinformationen vorhanden sind (über den Befehl ***Diesem Empfänger explizit vertrauen***). Es gibt unterschiedliche Möglichkeiten, wie der Backup Empfänger zur Verfügung gestellt werden kann:

   - **Manuell**: Das Backup Zertifikat wird in das Dateisystem exportiert (über den Befehl ***Exportiere Schlüssel***... (nicht als PKCS12 Datei)) und an alle Benutzer weitergeleitet. Diese können den Backup Empfänger zu der ***default*** Gruppe des Empfängerspeichers ***Meine Empfänger*** hinzufügen (über den Befehl ***Füge Empfänger hinzu...***).

   - **HTTP(S) Speicher:** Es kann ein zentraler HTTP(S) Speicher verwendet werden, der in der Abteilung zentral verwaltet wird (siehe **Fehler! Verweisquelle konnte nicht gefunden werden.** und **Fehler! Verweisquelle konnte nicht gefunden werden.**). Jede CCE3 Installation, die auf diesen Speicher zugreift, hat somit immer die aktuellen Empfänger (z.B. bei personellen Änderungen). Der Backup Empfänger muss nur mehr

[8] *Falls noch nicht initialisiert, wird dieser über den Befehl **Initialisiere den Schlüsselspeicher...** bereitgestellt.*

über Drag and Drop zu der ***default*** Gruppe des Empfängerspeichers ***Meine Empfänger*** hinzugefügt werden

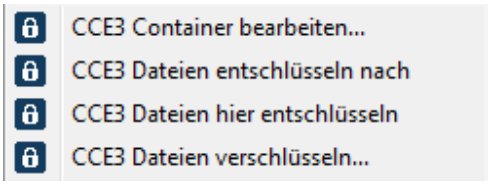
3. Jeder Container der von den Benutzern erstellt wird, verfügt nun über die ausgewählten Empfänger und den Backup Empfänger. Kommt es zum Verlust oder zur Beschädigung der verwendeten Bürgerkarten bzw. zu personellen Änderungen, ist gewährleistet, dass der Zugriff auf verschlüsselte Daten aufgrund des Backup Schlüssels möglich ist (siehe Punkt 5 der privaten Verwendung für weitere Details).

2. Daten verschlüsseln

Es werden hier die unterschiedlichen Methoden beschrieben, die bei der Datenverschlüsselung eingesetzt werden. Alle Methoden basieren auf einem zentralen Verschlüsselungswizard (siehe Abschnitt IV:2.4) und führen zum gleichen Ergebnis. Bei jeder Methode werden in der Überschrift die Betriebssysteme genannt bei denen diese Vorgehensweise eingesetzt werden kann.

2.1. Daten verschlüsseln - Über den Windows Explorer (Windows)

Dateien und Ordner können im Windows Explorer über den ***Senden an*** Ordner im Kontextmenu verschlüsselt werden. Dabei stehen 4 Operationen zur Verfügung wobei für das Verschlüsseln nur ***CCE3 Dateien verschlüsseln...*** eine Rolle spielt.



1. Markieren Sie die zu verschlüsselnden Dateien und Ordner im Windows Explorer
2. Öffnen sie das Kontextmenü durch Klicken mit der rechten Maustaste auf die markierten Dateien
3. Wählen Sie den Befehl ***CCE3 Dateien verschlüsseln...*** im ***Senden an*** Ordner
4. Es wird nun der Verschlüsselungswizard aufgerufen. Der weitere Ablauf wird in Abschnitt IV:2.4 beschrieben.

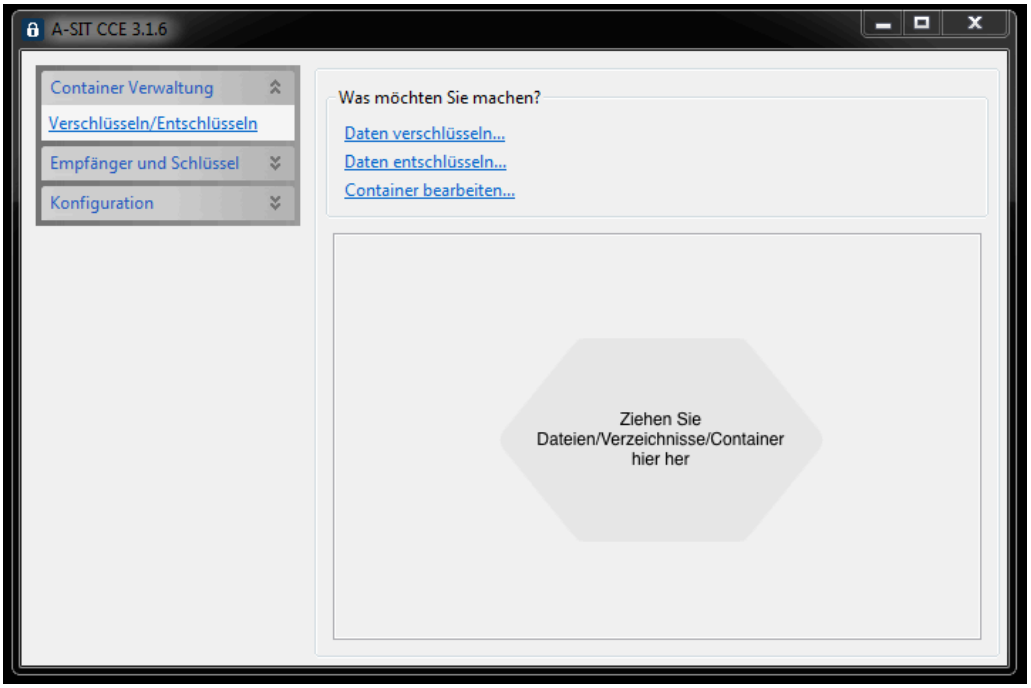
2.2. Daten verschlüsseln - Über Drag and Drop auf die CCE3 Applikation (Windows, OS X, Linux)

Dateien oder Ordner, die verschlüsselt werden sollen, können auf die CCE3-32/CCE3-64 EXE Datei gezogen werden. Es wird dann der Verschlüsselungswizard gestartet. Für den weiteren Ablauf wird auf Abschnitt IV: 2.4 verwiesen.

2.3. Daten verschlüsseln - Über die CCE3 Applikation (Windows, OS X, Linux)

Dateien oder Ordner können aus der CCE3 Applikation verschlüsselt werden.

1. Starten Sie CCE3 über das Startmenü A-SIT/CCE3/CCE3-{32/64}
2. Öffnen Sie das Menü ***Container Verwaltung*** und danach den Befehl ***Verschlüsseln/Entschlüsseln***



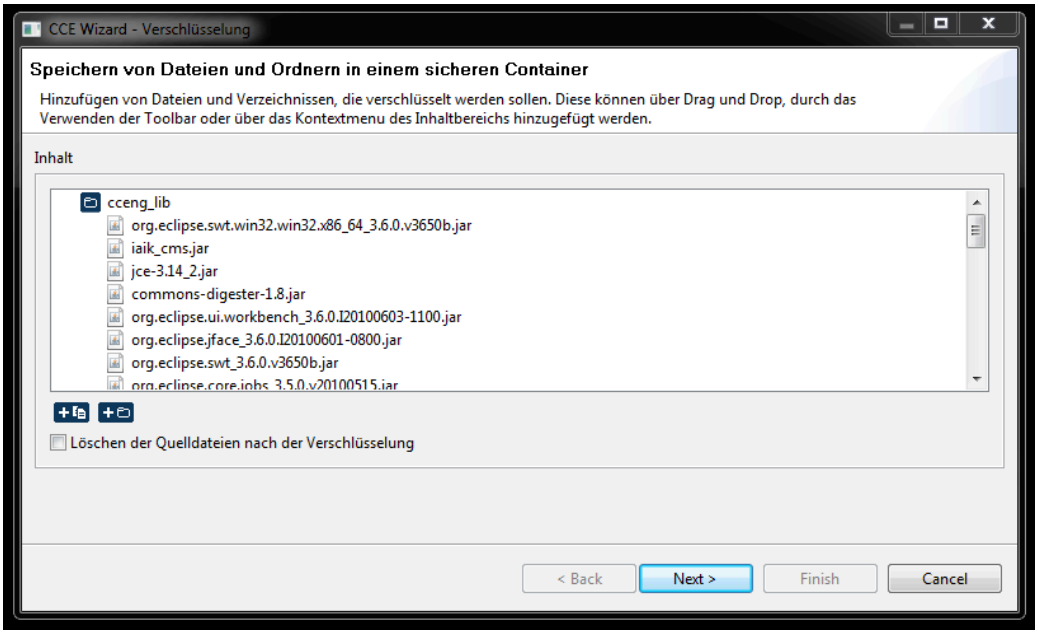
   a. Ziehen Sie die zu verschlüsselten Ordner oder Dateien auf das Feld ***Ziehen Sie die Dateien/Verzeichnisse/Container hier her***
   b. Wählen Sie den Befehl ***Daten verschlüsseln...***
3. Es wird nun der Verschlüsselungswizard geöffnet. Im Fall von 2a sehen Sie dort bereits die ausgewählten Dateien. Im Fall von 2b müssen Sie die zu verschlüsselnden Dateien/Ordner hinzufügen. Für die weitere Vorgehensweise wird auf Abschnitt IV:2.4 verwiesen.

2.4. Verschlüsselungswizard

Hier wird der Verschlüsselungswizard beschrieben, der bei jeder Datenverschlüsselung eingesetzt wird.

1. Wurden bereits Dateien in den vorherigen Schritten ausgewählt, so werden diese im Bereich ***Inhalt*** angezeigt. Wenn Sie Empfänger in der ***default*** Gruppe des CCE3 Empfängerspeichers ***Meine Empfänger*** gespeichert haben, und nur für diese die ausgewählten Daten verschlüsseln möchten, können Sie den Container bereits hier durch das Drücken von ***Finish*** erstellen.

Sind keine Empfänger in der ***default*** Gruppe oder möchten Sie noch weitere hinzufügen dann drücken Sie bitte ***Next/Weiter***.



Folgende weitere Operationen stehen zur Verfügung:

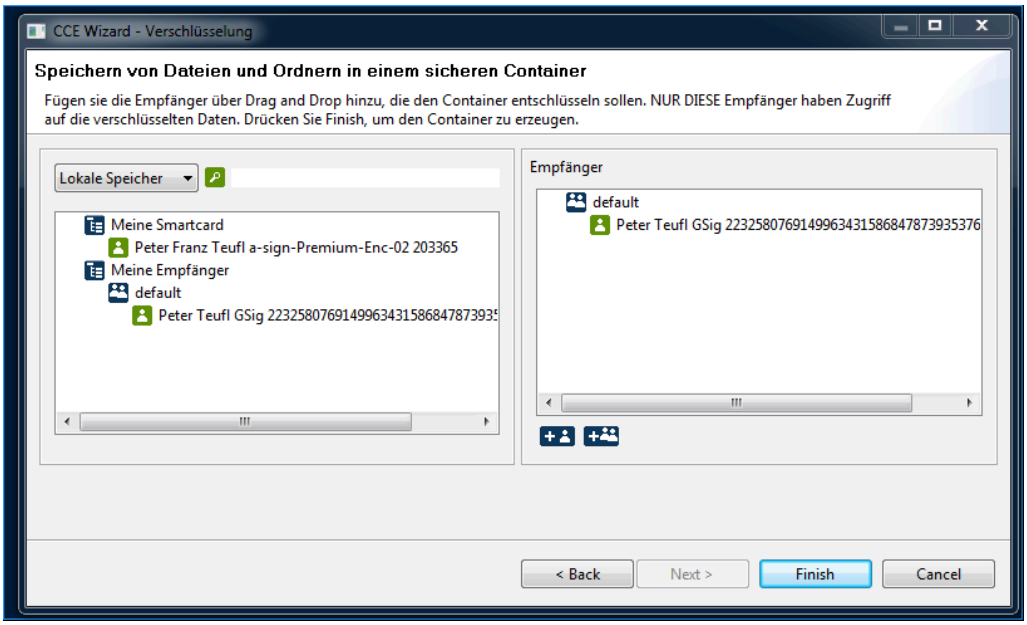
- **Löschen der Quelldateien nach der Verschlüsselung:** Beim Aktivieren dieser Option werden die Quelldateien nach der Verschlüsselung gelöscht. Bitte lesen Sie dazu unbedingt die weiteren Ausführungen in Abschnitt I:3.
- **Hinzufügen von Dateien und Verzeichnissen** über Drag and Drop aus dem Dateisystem.
- **Befehle:** Die folgende Befehle können über das Kontextmenu und über die Toolbar ausgeführt werden. Welche Befehle zur Verfügung stehen, hängt von den markierten Elementen ab.

Icon	Name	Beschreibung
	***Füge Dateien hinzu...***	Über ein Auswahlfenster können weitere Dateien zum markierten Ordner hinzugefügt werden.
	***Füge Verzeichnisse hinzu...***	Über ein Auswahlfenster können weitere Ordner und deren Inhalt zum markierten Ordner hinzugefügt werden.
	***Entferne***	Die markierten Dateien/Ordner werden entfernt.

2. Drücken Sie ***Weiter/Next***, um zur Empfängerauswahl zu gelangen. In der linken Hälfte werden alle verfügbaren Empfängerspeicher angezeigt. Die rechte Hälfte zeigt die Empfänger, für die der Container verschlüsselt werden soll.

   Empfänger oder Empfängergruppen, die in der ***default*** Gruppe des CCE3 internen Schlüsselspeichers ***Meine Empfänger*** gespeichert sind, werden automatisch hinzugefügt. Weitere Empfänger oder Empfängergruppen können über Drag and Drop von links nach rechts gezogen werden.

   ACHTUNG: Nur jene Empfänger, die hier hinzugefügt werden, können Zugriff auf die Daten im Container enthalten. Es gibt keine andere Möglichkeit einen Container zu entschlüsseln.
   Es wird hier eindringlichst auf Abschnitt I:2 verwiesen. Dort werden wichtige Hinweise zum Verschlüsseln von Daten und dem richtigen Schlüsselmanagement gegeben.



   Folgende weitere Operationen stehen zur Verfügung:

   - ***Suche nach Empfängern:*** Es können hier die gleichen Operationen, wie in Abschnitt V:1 beschrieben, angewendet werden.
   - ***Befehle:*** Die folgende Befehle können über das Kontextmenu und über die Toolbar ausgeführt werden. Welche Befehle zur Verfügung stehen, hängt von den markierten Elementen ab.

Icon	Name	Beschreibung
	***Füge Gruppe hinzu...***	Mit diesem Befehl wird eine neue Gruppe mit den Namen ***Neue Gruppe*** erstellt. Der Name kann durch Markieren und durch einen

		weiteren Mausklick bearbeitet werden (analog zum Umbenennen von Dateien im Windows Explorer).
	***Füge Empfänger hinzu...***	Über ein Auswahlfenster können weitere Empfänger aus dem Dateisystem hinzugefügt werden. Es werden dabei Zertifikate im CER/DER, PEM, PKCS7 oder CCE3 Format unterstützt.
	***Entferne***	Die markierten Empfänger/Empfängergruppen werden entfernt.

3. Drücken Sie ***Finish,*** um den Container mit den ausgewählten Dateien/Ordnern zu erstellen. Nur die ausgewählten Empfänger haben Zugriff auf die im Container gespeicherten Daten. Sie werden nun nach dem Dateinamen des zu erstellenden Containers gefragt.

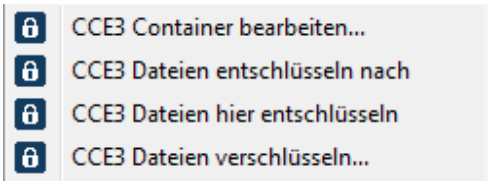
Der Container wird erstellt und der Wizard beendet. Falls Sie im Schritt 4 die Option ***Löschen der Quelldateien nach der Verschlüsselung*** ausgewählt haben löscht CCE3 die Quelldateien automatisch (siehe Abschnitt 1:3).

3. Daten entschlüsseln

Hier werden die Methoden beschrieben die für die Entschlüsselung von in einem Container gespeicherten Daten verwendet werden können. Die in diesem Abschnitt beschriebenen Methoden dienen nur zur Entschlüsselung der Daten und bieten keine Möglichkeit Daten innerhalb eines bestehenden Containers zu bearbeiten. Für diese Operationen wird auf Abschnitt IV:4 verwiesen.

3.1. Daten entschlüsseln - Über den Windows Explorer (Windows)

Daten, die in einem Container gespeichert sind, können im Windows Explorer über den ***Senden an*** Ordner im Kontextmenu entschlüsselt werden.



Folgende Operationen sind dabei von Relevanz:

- ***CCE3 Dateien entschlüsseln nach...***:
  1. Sie können einen Container nur entschlüsseln, wenn Sie dafür den passenden Schlüssel haben. Dieser kann entweder auf Ihrer Smartcard oder im CCE3 internen Schlüsselspeicher ***Meine Schlüssel*** gespeichert sein. Fügen Sie die passende Smartcard in den Kartenleser ein oder halten Sie das Passwort für den Schlüsselspeicher ***Meine Schlüssel*** bereit.
  2. Markieren Sie den zu entschlüsselnden Container im Windows Explorer.
  3. Öffnen Sie das Kontextmenü durch Klicken mit der rechten Maustaste auf den markierten Container.
  4. Wählen Sie den Befehl ***CCE3 Dateien entschlüsseln nach...*** im ***Senden an*** Ordner.
  5. Es wird nun der Entschlüsselungswizard aufgerufen. Der weitere Ablauf wird in Abschnitt IV:3.4 beschrieben.

- ***CCE3 Dateien hier entschlüsseln***:
  1. Sie können einen Container nur entschlüsseln wenn Sie dafür den passenden Schlüssel haben. Dieser kann entweder auf Ihrer Smartcard oder im CCE3 internen Schlüsselspeicher ***Meine Schlüssel*** gespeichert sein. Fügen Sie die passende Smartcard in den Kartenleser ein oder halten Sie das Passwort für den Schlüsselspeicher ***Meine Schlüssel*** bereit.
  2. Markieren Sie die zu entschlüsselnden Container im Windows Explorer.
  3. Öffnen sie das Kontextmenü durch Klicken mit der rechten Maustaste auf die markierten Container.
  4. Wählen Sie den Befehl ***CCE3 Dateien hier entschlüsseln*** im ***Senden an*** Ordner
  5. CCE3 versucht nun einen passenden Schlüssel für den Container zu finden. Ist dieser auf der eingefügten Smartcard, so werden Sie nun nach dem PIN dieser Karte gefragt. Durch eingeben des richtigen PINs wird der Container entschlüsselt.

     Wenn der Container nicht mit dem Schlüssel auf der Karte entschlüsselt werden kann oder Sie den falschen PIN eingeben haben, fragt CCE3 nach dem Passwort des Schlüsselspeichers ***Meine Schlüssel*** (nur wenn dieser auch initialisiert wurde). Kann dort der richtige Schlüssel gefunden werden, wird der Container entschlüsselt.
  6. Wenn Sie über den passenden Schlüssel und den korrekten PIN oder das korrekte Passwort verfügen, wird in dem Ordner, in dem der Container liegt, ein Ordner mit dem Namen des Containers erstellt und die Daten in diesen Ordner entschlüsselt.

     Beispiel: Ein Container mit dem Dateinamen ***Sichere Daten.cce*** wird in den Ordner ***Sichere Daten*** entschlüsselt. Ist dieser Ordner bereits vorhanden wird solange ein Index zum Basisnamen angefügt, bis ein nicht existierender Ordner

gefunden wird (z.B.: ***Sichere Daten 1***, ***Sichere Daten 2***...). Es können also bei dieser Operation **NIE** Daten unabsichtlich überschrieben werden.

7. Nach dem Entschlüsseln der Daten wird ein Explorer Fenster geöffnet, das die entschlüsselten Daten anzeigt.

3.2. Daten entschlüsseln - Über Drag and Drop auf die CCE3 Applikation (Windows, OS X, Linux)

Container die entschlüsselt werden sollen können auf die CCE3-32/CCE3-64 EXE Datei gezogen werden. Es wird dann der Entschlüsselungswizard gestartet. Für den weiteren Ablauf wird auf Abschnitt IV:3.4 verwiesen.

ACHTUNG: Wenn in der aktuellen Version (3.3.1) mehr als ein Container auf die Applikation gezogen wird, wird nur der erste Container entschlüsselt.

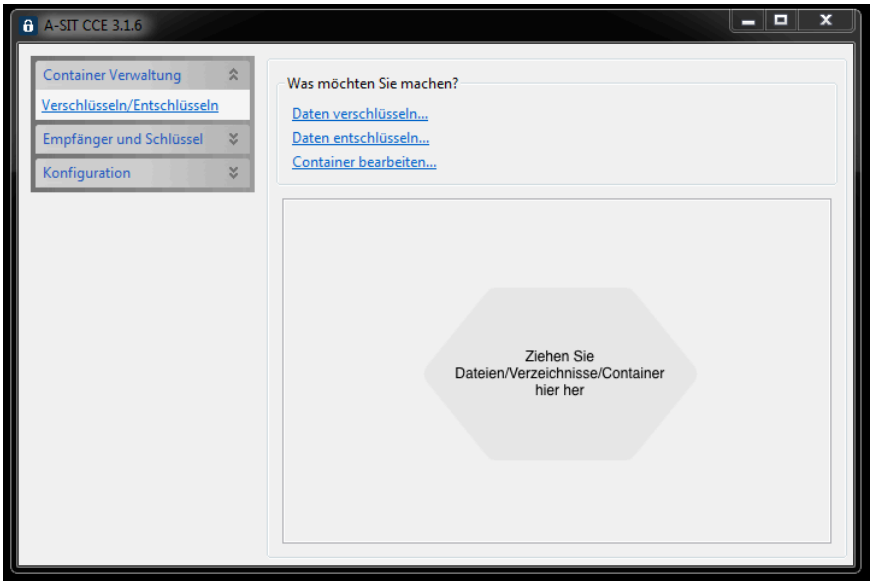
3.3. Daten verschlüsseln - Über die CCE3 Applikation (Windows, OS X, Linux)

Container können in der CCE3 Applikation entschlüsselt werden.

1. Starten Sie CCE3 über das Startmenü A-SIT/CCE3/CCE3-{32/64}
2. Öffnen Sie das Menü ***Container Verwaltung*** und danach den Befehl ***Verschlüsseln/Entschlüsseln.***

   a. Ziehen Sie den Container auf das Feld ***Ziehen Sie die Dateien/Verzeichnisse/Container hier her.***
   ACHTUNG: Wenn in der aktuellen Version (3.3.1) mehr als ein Container auf die Applikation gezogen wird, wird nur der erste Container entschlüsselt.

   b. Wählen Sie den Befehl ***Daten entschlüsseln...***

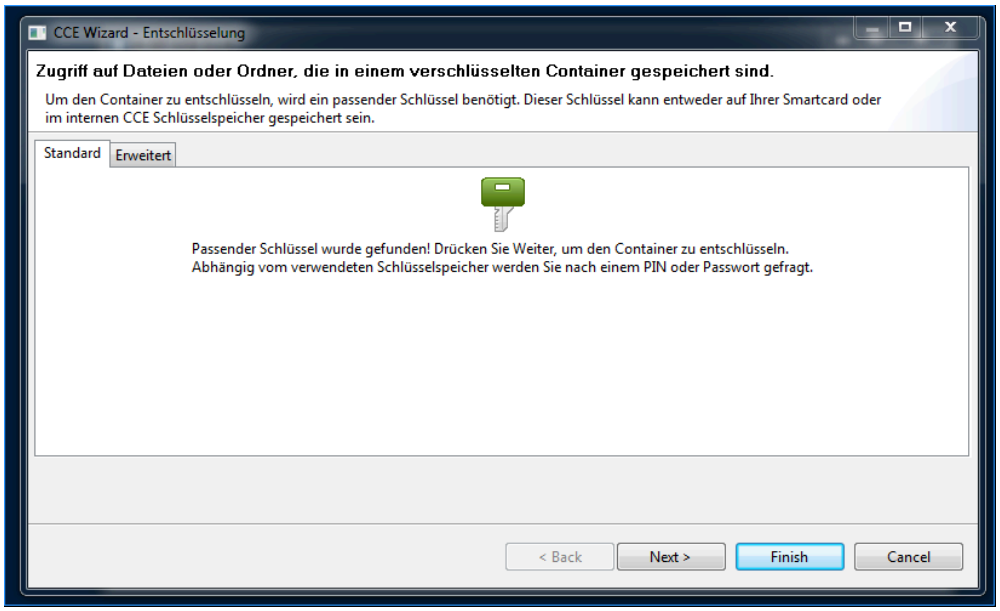


3. Es wird nun der Entschlüsselungswizard geöffnet. Im Fall von 2b werden Sie nun nach dem zu entschlüsselnden Container gefragt. Für die weitere Vorgehensweise wird auf Abschnitt IV:3.4 verwiesen.

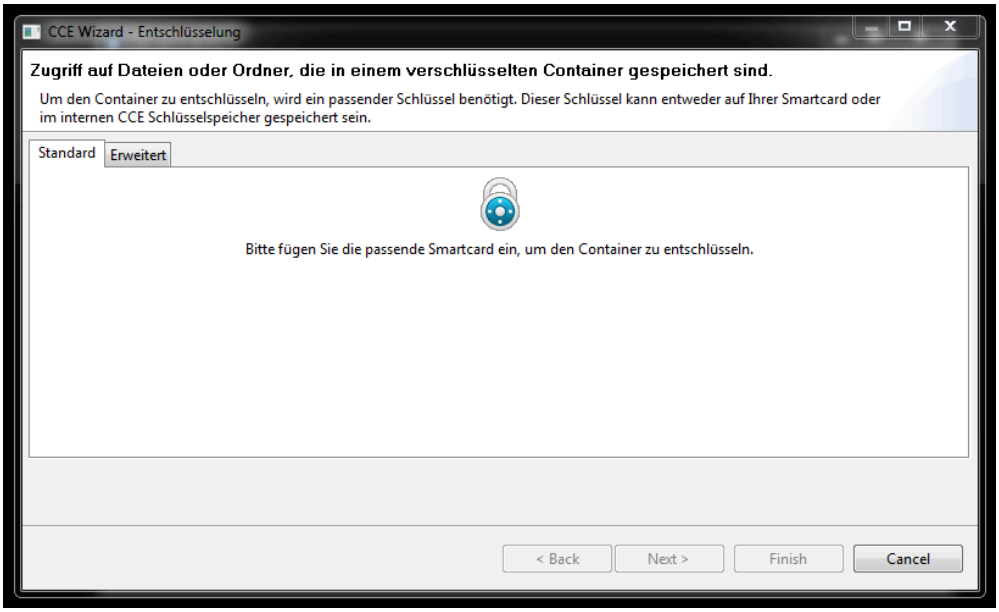
3.4. Entschlüsselungswizard

Hier wird der Entschlüsselungswizard beschrieben, der bei jeder Datenentschlüsselung eingesetzt wird.

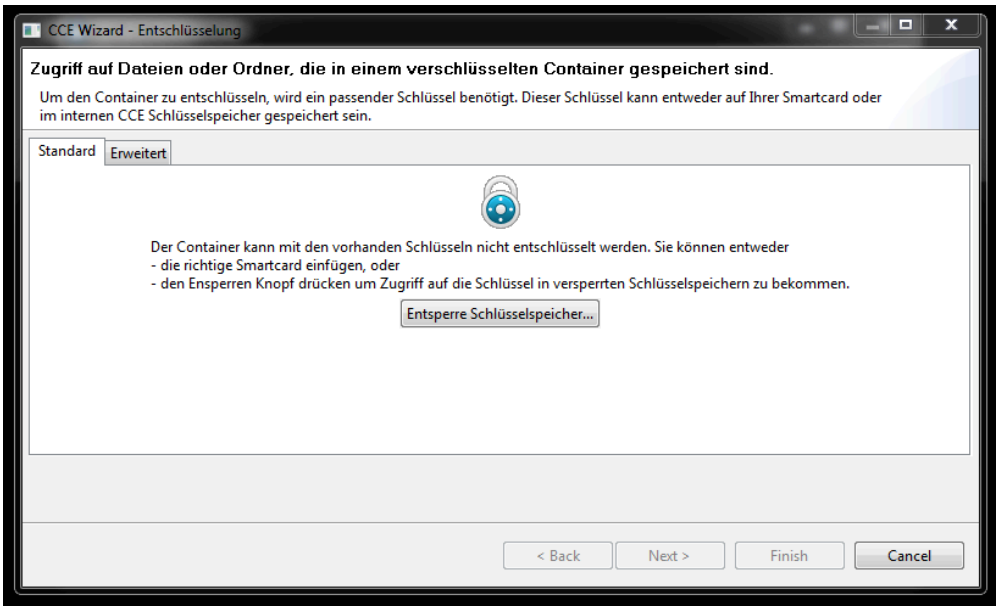
1. Bevor der Container entschlüsselt werden kann, überprüft CCE3, ob ein passender Schlüssel gefunden werden kann. Es werden dabei die Schlüssel, die auf der Smartcard und im Schlüsselspeicher ***Meine Schlüssel*** gespeichert sind, überprüft. Damit CCE3 Zugriff auf den Schlüsselspeicher hat, muss dieser entsperrt sein.
   Je nach vorhandenen Schlüsseln und dem Zustand des Schlüsselspeichers (gesperrt, entsperrt) zeigt CCE3 unterschiedliche Hinweise:



- ***Schlüssel vorhanden*** (auf Smartcard oder im entsperrten Schlüsselspeicher)
- ***Kein passender Schlüssel vorhanden*** (auf Smartcard und im entsperrten Schlüsselspeicher)

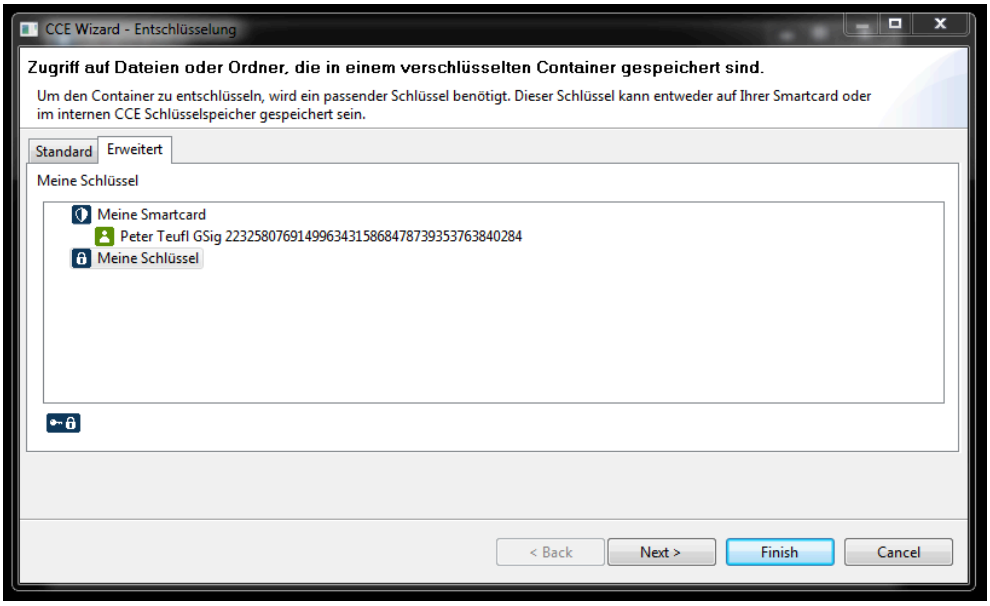


- ***Kein passender Schlüssel auf Smartcard gefunden***, der Schlüsselspeicher ist aber noch gesperrt



In diesem Fall können Sie durch das Drücken von ***Entsperre Schlüsselspeicher*** den Schlüsselspeicher ***Meine Schlüssel*** entsperren und somit Zugriff auf die dort gespeicherten Schlüssel erhalten. Kann nun ein passender Schlüssel gefunden werden, ändert sich die Anzeige auf den Screenshot, der bei ***Schlüssel vorhanden*** angezeigt wird (das blaue Schloss wechselt au einen grünen Schlüssel). Kann kein passender Schlüssel gefunden werden, ändert sich die Anzeige auf den Screenshot der bei ***Kein passender Schlüssel vorhanden*** angezeigt wird.

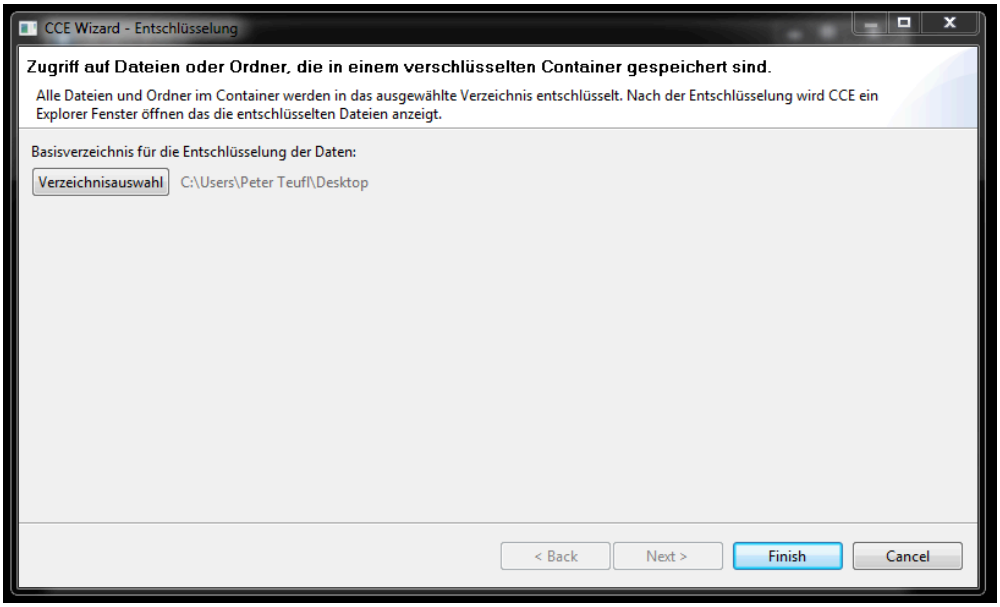
- Folgende weitere Operationen stehen zur Verfügung:



- Reiter ***Erweitert***: Hier sehen Sie alle Schlüsselspeicher, den Zustand (gesperrt/entsperrt) und die darin enthaltenen Schlüssel (nur im entsperrten Zustand).
- Befehle im Reiter ***Erweitert***:

Icon	Name	Beschreibung
	***Entsperren...***	Mit diesem Befehl wird der Schlüsselspeicher entsperrt. Sie werden nach dem Passwort des Speichers gefragt.
	***Sperren***	Mit diesem Befehl wird der Schlüsselspeicher gesperrt. CCE3 hat danach keinen Zugriff auf die im Speicher enthaltenen Schlüssel.

2. Wurde ein passender Schlüssel gefunden, kann der ***Weiter/Next*** Knopf gedrückt werden und die Entschlüsselung des Containers durchgeführt werden. Ist der Schlüssel auf der Smartcard gespeichert, muss jetzt die passende PIN eingeben werden. Ist der Schlüssel im Schlüsselspeicher ***Meine Schlüssel*** gespeichert, entfällt diese PIN Eingabe, da nach dem Entsperren CCE3 vollen Zugriff auf die darin enthaltenen Schlüssel hat.
3. Nach dem Entschlüsseln des Containers hat CCE3 Zugriff auf die darin enthaltenen Daten und Sie können das Verzeichnis auswählen, in das die Daten geschrieben werden sollen. Es wird bereits das Verzeichnis, in dem sich der Container befindet, ausgewählt.



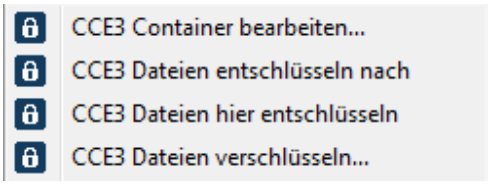
4. Drücken Sie **Finish** und die Daten werden in das ausgewählte Verzeichnis geschrieben. Nach dem Schreiben öffnet CCE3 ein Explorer Fenster, das die entschlüsselten Daten anzeigt. Für weitere Details in Bezug auf das erstellte Verzeichnis und das Überschreiben von Daten wird auf Abschnitt IV:3.1 verwiesen.

4. Container bearbeiten

Diese Funktionalität erlaubt neben dem Entschlüsseln von Daten das Bearbeiten eines bestehenden Containers. Dabei können Empfänger oder Daten im Container geändert werden.

4.1. Container bearbeiten - Über den Windows Explorer (Windows)

Ein bestehender Container, kann im Windows Explorer über den ***Senden an*** Ordner im Kontextmenu bearbeitet werden.



Der Befehl ***CCE3 Container bearbeiten...*** ermöglicht das Bearbeiten eines Containers.

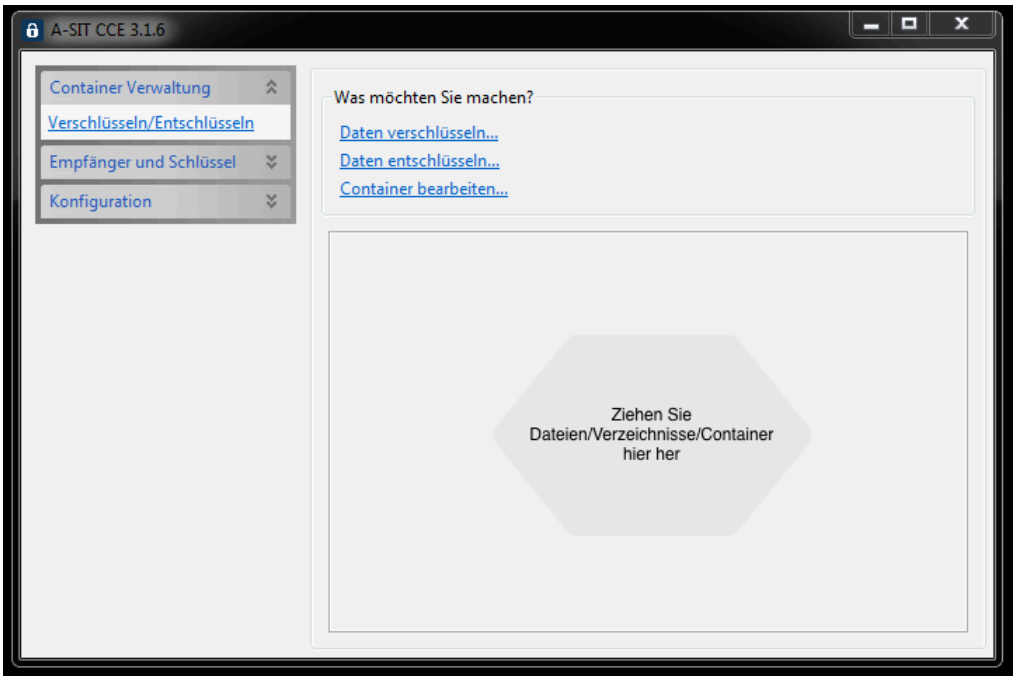
1. Markieren Sie den zu bearbeitenden Container im Windows Explorer
2. Öffnen sie das Kontextmenü durch Klicken mit der rechten Maustaste auf die markierten Container.
3. Wählen Sie den Befehl ***CCE3 Container bearbeiten...*** im ***Senden an*** Ordner

4. Sie werden nach dem zu bearbeitenden Container gefragt.
5. Nach der Auswahl des Containers wird der Bearbeitungswizard aufgerufen. Für die weiteren Schritte in diesem Wizard wird auf Abschnitt IV:4.3 verwiesen.

4.2. Container bearbeiten - Über die CCE3 Applikation (Windows, OS X, Linux)

Container können in der CCE3 Applikation bearbeitet werden.

1. Starten Sie CCE3 über das Startmenü A-SIT/CCE3/CCE3-{32/64}
2. Öffnen Sie das Menü ***Container Verwaltung*** und danach den Befehl ***Verschlüsseln/Entschlüsseln.***
3. Wählen Sie den Befehl ***Container bearbeiten...***



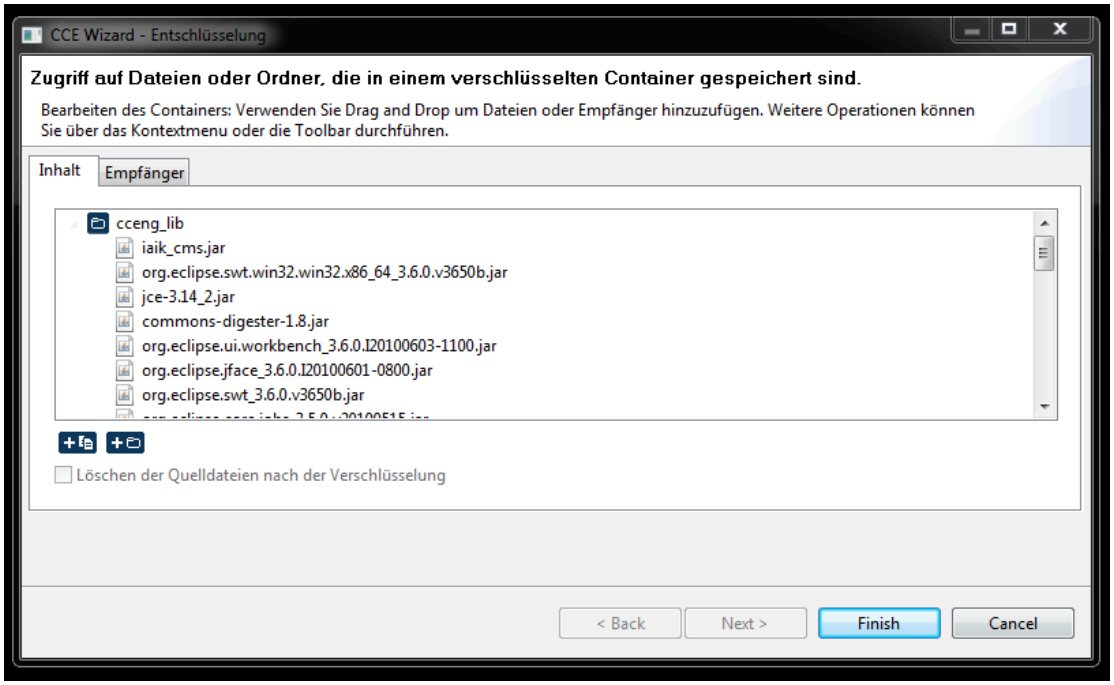
4.3. Bearbeitungswizard

Die ersten Schritte im Bearbeitungswizard entsprechen den Schritten im Entschlüsselungswizard und werden hier nicht weiter erläutert (für Details siehe Abschnitt IV:3.4). Nach dem Entschlüsseln des Containers wird dem Benutzer aber ein anderer Dialog präsentiert, der mehr Funktionalität als der Dialog im Entschlüsselungswizard bietet:

- Entschlüsseln von einzelnen/allen Dateien oder Verzeichnissen
- Hinzufügen/Entfernen von Dateien oder Verzeichnissen
- Betrachten und Bearbeiten von Dateien: Dateien können direkt im Container betrachtet und geändert werden. Geänderte Dateien werden wieder in den Container übernommen.
- Hinzufügen/Entfernen von Empfängern

Nach dem Entschlüsseln wird eine Seite mit den Reitern ***Inhalt*** und ***Empfänger*** präsentiert. Dabei werden im Reiter ***Inhalt*** die im Container enthaltenen Dateien und Verzeichnisse angezeigt. Der Reiter ***Empfänger*** zeigt die Empfänger, für die der Container verschlüsselt wurde. Wenn Sie Änderungen am Container vornehmen, wird Sie CCE3 nach dem Drücken von ***Finish*** fragen, ob diese Änderungen übernommen werden sollen. Durch das Bestätigen wird der bestehende Container mit dem neuen Container überschrieben.

ACHTUNG: Da ein neuer symmetrischer Schlüssel erzeugt wird, ist auch garantiert dass entfernte Empfänger keinen Zugriff mehr auf den Container haben.

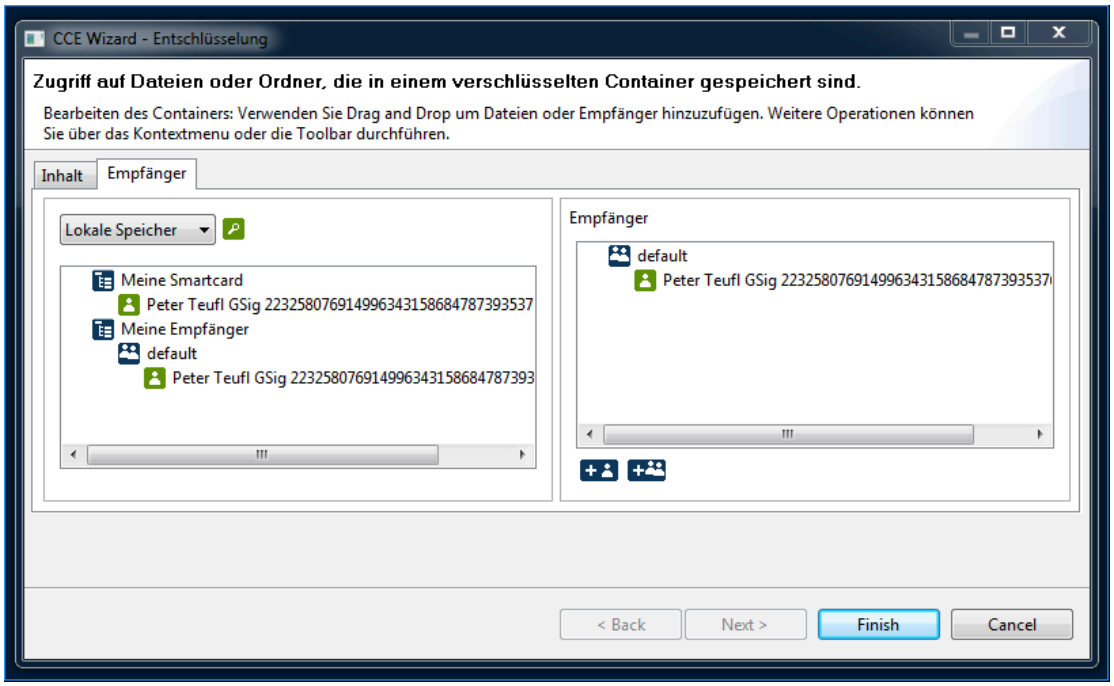


Funktionen des Reiters ***Inhalt***:

- **Löschen der Quelldateien nach der Verschlüsselung:** Beim Aktivieren dieser Option werden neu hinzugefügte Quelldateien nach der Verschlüsselung gelöscht. Bitte lesen Sie dazu unbedingt die weiteren Ausführungen in Abschnitt I:3.
- **Hinzufügen von Dateien und Verzeichnissen** über Drag and Drop aus dem Dateisystem.
- **Entschlüsseln von Dateien und Verzeichnissen** über Drag and Drop in das Dateisystem
- **Betrachten/Bearbeiten einer Datei**: Durch den Doppelklick auf eine Datei wird diese mit dem im Betriebssystem registrierten Standardprogramm geöffnet. Sie können dann Änderungen in der Datei vornehmen. CCE3 wird sie danach fragen, ob diese Änderungen in den Container übernommen werden sollen.
- **Befehle:** Die folgende Befehle können über das Kontextmenu und über die Toolbar ausgeführt werden. Welche Befehle zur Verfügung stehen, hängt von den markierten Elementen ab.

Icon	Name	Beschreibung
	***Entschlüsseln nach...***	Über ein Auswahlfenster können Sie ein Verzeichnis angeben, in das die Dateien/Verzeichnisse entschlüsselt werden.
	***Öffne/Bearbeite Datei...***	Die ausgewählte Datei wird mit dem Standardprogramm geöffnet. Im Falle von Änderungen fragt CCE3, ob diese in den Container übernommen werden sollen.
	***Füge Dateien hinzu...***	Über ein Auswahlfenster können weitere Dateien zum markierten Ordner hinzugefügt werden.
	***Füge Verzeichnisse hinzu...***	Über ein Auswahlfenster können weitere Ordner und deren Inhalt zum markierten Ordner hinzugefügt werden.
	***Entferne***	Die markierten Dateien/Ordner werden entfernt.

Funktionen des Reiters ***Empfänger***:
Es werden die gleiche Funktionen wie im Verschlüsselungswizard zur Verfügung gestellt (siehe Abschnitt IV:2.4).



5. Verwenden eines externen HTTP(S) Speichers

Ein externer Empfängerspeicher auf den über HTTP oder HTTPS zugegriffen werden kann, vereinfacht die Verwaltung von Empfänger und Gruppen, etwaiger größeren Abteilungen eines Unternehmens. Dazu wird eine bestehender Empfängerspeicher oder eine Empfängergruppe exportiert und auf einem Webserver zur Verfügung gestellt.

Die CCE3 Installationen können nun diesen Speicher einbinden und erhalten lesend Zugriff auf die darin gespeicherten Empfänger und Empfängergruppen. Änderungen von Empfängergruppen müssen daher nur mehr einmal durchgeführt werden und alle CCE3 Installation erhalten diese automatisch beim Start von CCE3.

Folgende Schritte sind für das Einrichten eines HTTP(S) Speichers notwendig:

1) Die Verwaltung des HTTP(S) Speichers wird auf einer CCE3 Installation im Empfängerspeicher ***Meine Empfänger*** durchgeführt (z.B. in einer eigenen Gruppe, oder es kann auch der gesamte Speicher verwendet werden).

2) Soll der HTTP(S) Speicher erstellt werden oder muss ein bestehender Speicher aktualisiert werden, so muss die gewünschte Empfängergruppe (oder auch der gesamte Speicher ***Meine Empfänger***) über den Befehl ***Exportiere Empfänger...*** in eine Datei exportiert werden. Beim Exportformat muss es sich um das **CCE3 Empfänger Speicher** Format handeln. Die erstellte XML Datei kann nun auf einen Webserver gelegt werden. Für die weitere Vorgehensweise wird von folgender URL ausgegangen: https://host.domain:443/empfaenger.xml

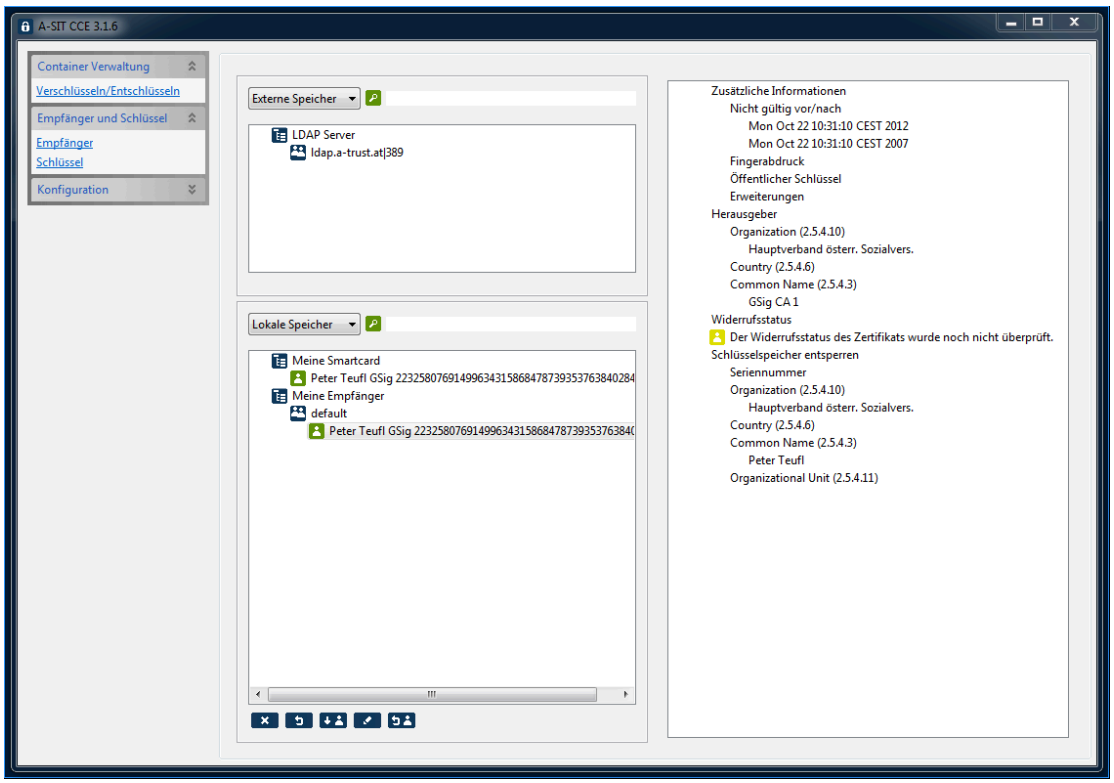
3) CCE3 Installationen, die auf diesen Empfängerspeicher zugreifen sollen, müssen einen HTTP(S) Empfängerspeicher mit der URL https://host.domain:443/empfaenger.xml hinzufügen (siehe Abschnitt V:3.1.3).

4) Der hinzugefügte HTTP(S) Empfängerspeicher ist nun in der Kategorie ***Lokale Speicher*** sichtbar und kann beim Erstellen von Containern verwendet werden.

Abschnitt V: Weitere Funktionen

1. Empfänger Verwaltung

Empfänger können im Hauptmenü der CCE3 Applikation unter ***Empfänger und Schlüssel/Empfänger*** verwaltet werden. Dabei werden folgende Ansichten gezeigt:



- Links oben - Empfängeransicht der externen Speicher
- Links unten - Empfängeransicht der internen Speicher
- Detailansicht des ausgewählten Empfängers

In den Empfängeransichten kann ausgewählt werden, ob lokale oder externe Speicher angezeigt werden sollen. Diese Ansichten unterscheiden sich wie folgt:

- **Lokale Speicher**:
  - **Meine Empfänger:** Hier handelt es sich um den internen CCE3 Empfängerspeicher. In diesem Speicher können Empfänger aus anderen Quellen (Dateisystem, Smartcard, Schlüsselspeicher, HTTP(S) Speicher, LDAP Server) hinzugefügt und in Gruppen verwaltet werden. Dabei gibt es eine Standardgruppe mit dem Namen ***default.***
    Alle Empfänger und Empfängergruppen, die in dieser Gruppe gespeichert sind, werden beim Verschlüsseln von Daten automatisch zu dem zu erstellenden Container hinzugefügt.

- **Meine Smartcard (nur lesbar):** Hier wird der Empfänger (das Zertifikat) Ihrer Smartcard angezeigt.
- **Meine Schlüssel (nur lesbar):** Hier werden die Empfänger (Zertifikate) ihrer in CCE3 erstellten oder importierten Schlüssel angezeigt (siehe auch **Fehler! Verweisquelle konnte nicht gefunden werden.**).
- **HTTP(S) Speicher (nur lesbar)**, die in der Konfiguration konfiguriert wurden (siehe **Fehler! Verweisquelle konnte nicht gefunden werden.**).

- **Externe Speicher**: Hier werden Speicher angezeigt die aufgrund der großen Anzahl der darin gespeicherten Empfänger nicht automatisch geladen werden können (z.B. das LDAP Verzeichnis eines Zertifizierungsdiensteanbieters). Diese Speicher können nur mit Hilfe der Suchfunktion durchsucht werden (siehe unten).

Folgende Funktionen stehen zur Verwaltung der Empfänger zur Verfügung:

- **Drag and Drop:** Empfänger und Empfängergruppen werden über Drag and Drop organisiert. Ein Empfänger der z.B.: im Speicher ***Meine Smartcard*** gespeichert ist kann über Drag and Drop in den CCE3 internen Speicher ***Meine Empfänger*** gezogen werden.
  ACHTUNG: Auch wenn hier die Empfänger von Schlüsselspeichern angezeigt werden und per Drag and Drop in den CCE3 internen Empfängerspeicher *Meine Empfänger* kopiert werden können, so wird NIE der in den Schlüsselspeichern gespeicherten Schlüssel kopiert (ist bei der Smartcard nicht einmal technisch möglich). Schlüssel können NUR über die Export Funktion exportiert werden (siehe dazu Abschnitt V:2).
- **Verwalten von Gruppen:** Im Speicher ***Meine Schlüssel*** können beliebige Gruppenhierarchien erstellt werden. Empfänger können somit in Empfängergruppen organisiert werden. Z.B. können damit einfach Container erzeugt werden, die nur für die Mitglieder der eigenen Abteilung zugänglich sind.
- **Importieren von Empfängern:** Empfänger können von anderen Speichern (z.B.: ***LDAP Server***, ***Meine Smartcard***) in den internen Speicher ***Meine Empfänger*** über Drag and Drop importiert werden. Empfänger die auf dem Dateisystem gespeichert sind, können durch die jeweiligen Befehle in den Speicher ***Meine Empfänger*** importiert werden (siehe unten).
- **Exportieren von Empfängern:** Empfänger und Empfängergruppen können über die entsprechende Befehle in das Dateisystem exportiert werden (siehe unten).
- **Detailansicht**: Die Detailansicht zeigt alle Details eines ausgewählten Empfängers (z.B.: Gültigkeitsdauer, detaillierte Informationen zum Widerrufsstatus).
- **Default Empfänger:** Alle Empfänger die sich in der ***default*** Gruppe des Speichers ***Meine Empfänger*** befinden, werden automatisch beim Erzeugen eines Containers zum Container hinzugefügt. Diese Funktionalität sollte für Backup Schlüssel verwendet werden. Weitere Details dazu können unter Abschnitt I:2 gefunden werden.

- **Widerrufstatus:** Die Farbe (grün, rot, gelb) des Empfänger Icons gibt Auskunft über den Widerrufsstatus des Empfängers. Weitere Details dazu können unter Abschnitt III:4 gefunden werden.
- **Suche:** Das Suchfenster ermöglicht das Filtern der anzeigten Empfänger und/oder Empfängergruppen. Die Funktionalität unterscheidet sich etwas bei den internen und externen Speichern:
    - **Interne Speicher:** Es werden nur die Empfänger/Empfängergruppen angezeigt die die im Suchfeld eingegebene Zeichenkette enthalten.
    - **Externe Speicher:** Wird eine Zeichenkette eingegeben, die länger als 4 Zeichen ist, werden die LDAP Server nach passenden Empfängern durchsucht. Die Suchergebnisse werden danach als Empfänger zur jeweiligen LDAP Server Gruppe hinzugefügt.
      Die gefunden Empfänger können mit Drag and Drop in den internen Speicher ***Meine Empfänger*** gezogen werden.

Folgende weitere Funktionen stehen zur Verfügung:

- **Ändern des Namens eines Empfängers oder Empfängergruppe:** Der Name wird durch das Markieren eines Empfängers oder einer Empfängergruppe und nochmaligen Klick auf den markierten Empfänger oder die markierte Empfängerruppe bearbeitet.
- **Befehle:** Die folgende Befehle können über das Kontextmenu und über die Toolbar ausgeführt werden. Welche Befehle zur Verfügung stehen, hängt von den markierten Elementen ab.

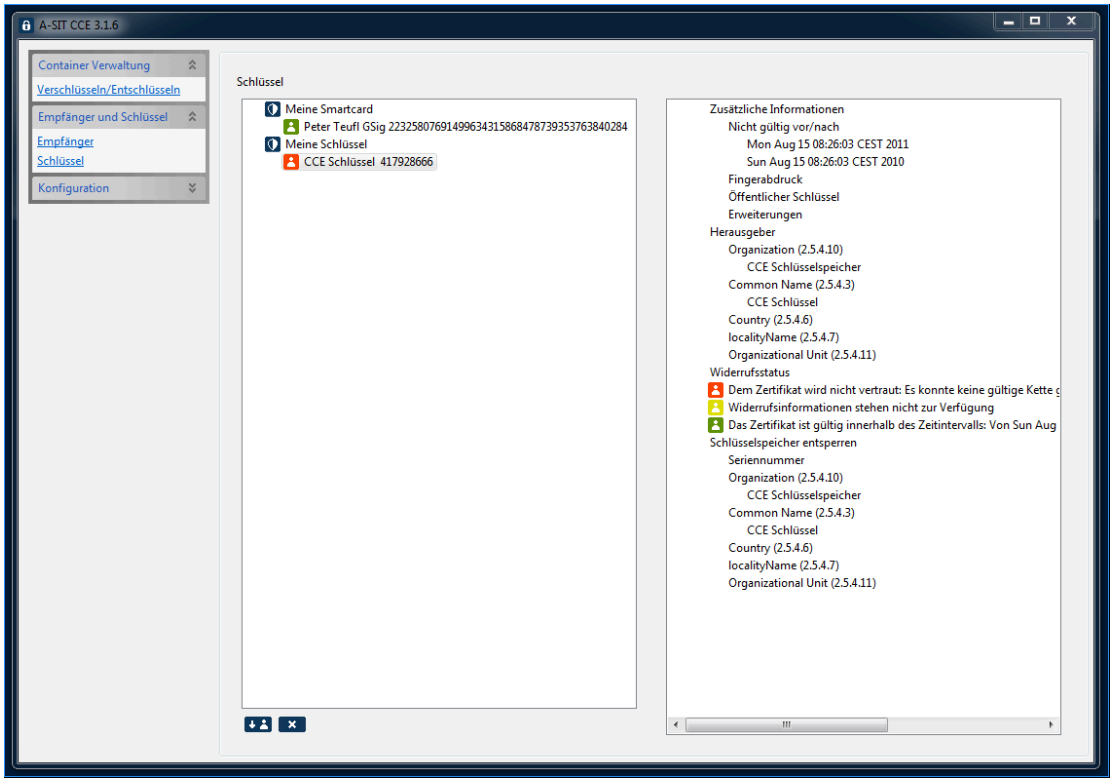
Icon	Name	Beschreibung
	***Füge Empfänger hinzu...***	Über ein Auswahlfenster können weitere Empfänger aus dem Dateisystem hinzugefügt werden. Es werden dabei Zertifikate im CER/DER, PEM, PKCS7 oder CCE3 Empfängerspeicher (xml) unterstützt.
	***Setze den Namen zurück***	Es wird der Name des Empfängers auf den Standard-Namen zurückgesetzt: Dieser ist Common Name plus Common Name des Herausgebers plus Seriennummer der Zertifikats.
	***Umbenennen...***	Es kann hier der Name des markierten Empfängers oder der Empfängergruppe geändert werden.

	***Exportiere Empfänger...***	Die markierten Empfänger oder Empfängergruppen können mit diesem Befehl in folgende Formate exportiert werden: DER/CER, PEM, PKCS7 oder CCE3 Empfängerspeicher (xml).
	***Diesem Empfänger explizit vertrauen***	Unabhängig von den festgestellten Widerrufsinformationen wird dem Empfänger vertraut. Der Empfänger wird dazu zu den vertrauenswürdigen Empfängern hinzugefügt (siehe Abschnitt III:4). Dies macht etwa bei Zertifikaten Sinn, die über keine Widerrufsinformationen verfügen, denen man aber aufgrund anderer Eigenschaften vertrauen kann (z.B. das Zertifikat wurde im CCE3 Schlüsselspeicher erstellt).
	***Explizite Vertrauensstellung aufheben***	Der explizite Vertrauensstatus der vorher mit ***Diesem Empfänger explizit vertrauen*** gesetzt wurde, kann mit diesem Befehl wieder aufgehoben werden. Der Empfänger wird dabei von den vertrauenswürdigen Empfängern entfernt (siehe Abschnitt III:4).
	***Entferne***	Die markierten Empfänger/Empfängergruppen werden entfernt.

2. Schlüssel

Schlüssel können im Hauptmenu der CCE3 Applikation unter ***Empfänger und Schlüssel/Schlüssel*** verwaltet werden. Die linke Ansicht zeigt dabei die vorhandenen Schlüsselspeicher (***Meine Smartcard*** und ***Meine Schlüssel***). Die rechte Ansicht zeigt Details zu einem Zertifikat eines markierten Schlüssels[9].

[9] *Das Zertifikat (der Empfänger) wird für die Verschlüsselung benötigt und kann öffentlich gemacht werden. Der Schlüssel wird für die Entschlüsselung verwendet und MUSS geheim gehalten werden. Siehe Abschnitt V:1 für weitere Hinweise.*



Folgende weitere Funktionen stehen zur Verfügung:

- **Befehle:** Die folgende Befehle können über das Kontextmenu und über die Toolbar ausgeführt werden. Welche Befehle zur Verfügung stehen hängt von den markierten Elementen ab.

Icon	Name	Beschreibung
	***Exportiere Schlüssel...***	Die markierten Schlüssel können mit diesem Befehl in folgende Formate exportiert werden: Nur die zu den Schlüsseln gehörigen Zertifikate: DER/CER, PEM, PKCS7 oder CCE3 Empfängerspeicher (xml) Schlüssel und Zertifikate: PKCS12
	***Schlüssel entfernen***	Die markierten Schlüssel werden entfernt. **ACHTUNG: Container die mit den entfernten Schlüsseln verschlüsselt wurden, können danach NICHT mehr entschlüsselt werden (außer der Container wurde auch mit anderen Schlüsseln verschlüsselt über die man noch verfügt)!**

	***Initialisiere den Schlüsselspeicher...***	Mit diesem Befehl wird der Schlüsselspeicher initialisiert. Sie werden dabei nach einem Passwort gefragt, das zum Entsperren des Schlüsselspeichers benötigt wird. **ACHTUNG: Ist der Schlüsselspeicher bereits initialisiert, werden alle darin enthaltenen Schlüssel gelöscht! Ein Zugriff auf Container, die mit diesen Schlüsseln verschlüsselt wurden, ist dann nicht mehr möglich (außer der Container wurde auch mit anderen Schlüsseln verschlüsselt über die man noch verfügt)!** **ACHTUNG: Das vergebene Passwort wird für den Zugriff auf den Schlüsselspeicher benötigt. Wird das Passwort vergessen, ist der Zugriff auf Container, die mit diesen Schlüsseln verschlüsselt wurden, nicht mehr möglich (außer der Container wurde auch mit anderen Schlüsseln verschlüsselt über die man noch verfügt)!**
	***Entsperren***	Sie werden nach dem Passwort des Schlüsselspeichers gefragt. Nach der Eingabe des Passworts hat CCE3 Zugriff auf die darin enthalten Schlüssel und kann diese für die Entschlüsselung von Containern verwenden.
	***Füge Schlüssel von PKCS12 Datei hinzu...***	Schlüssel können von externen PKCS12 Dateien in den Schlüsselspeicher importiert werden. Dazu müssen Sie über das Passwort der PKCS12 Datei verfügen.
	***Ändere das Passwort...***	Mit diesem Befehl wird das Passwort

		des Schlüsselspeichers geändert. **ACHTUNG: Das vergebene Passwort wird für den Zugriff auf den Schlüsselspeicher benötigt. Wird das Passwort vergessen, ist der Zugriff auf Container, die mit diesen Schlüsseln verschlüsselt wurden, nicht mehr möglich (außer der Container wurde auch mit anderen Schlüsseln verschlüsselt über die man noch verfügt)!**
	***Erzeuge Schlüssel und Zertifikat...***	Mit diesem Befehl werden ein Schlüssel und das dazu passende Zertifikat (Empfänger) erzeugt. Das Zertifikat (der Empfänger) kann dann für das Verschlüsseln eines Container verwendet werden. Zum Entschlüsseln des Containers wird der erzeugte Schlüssel verwendet.
	***Sperren***	Mit diesem Befehl wird der Schlüsselspeicher gesperrt. CCE3 hat somit keinen Zugriff mehr auf den Schlüsselspeicher. Beim Schließen von CCE3 werden entsperrte Schlüsselspeicher automatisch gesperrt.

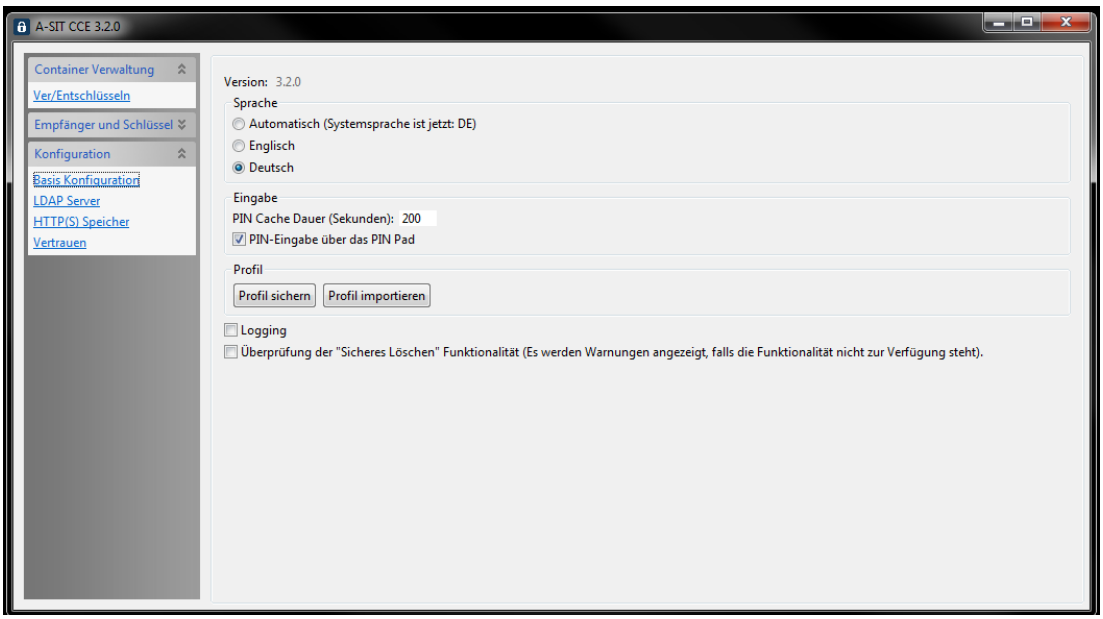
3. Konfiguration

Hier werden die unterschiedlichen Komponenten von CCE3 konfiguriert.

3.1. Basis Konfiguration

- ***Sprache***: CCE3 unterstützt Deutsch und Englisch. In der Standardkonfiguration (***Automatisch***) stellt CCE3 über die eingestellte Systemsprache fest, welche Sprache verwendet werden soll. Handelt es sich bei der Systemsprache um eine andere Sprache als Deutsch oder Englisch so wird CCE3 in Englisch präsentiert. Die Sprache kann auch manuell gewählt werden (Option ***Englisch*** oder ***Deutsch***).

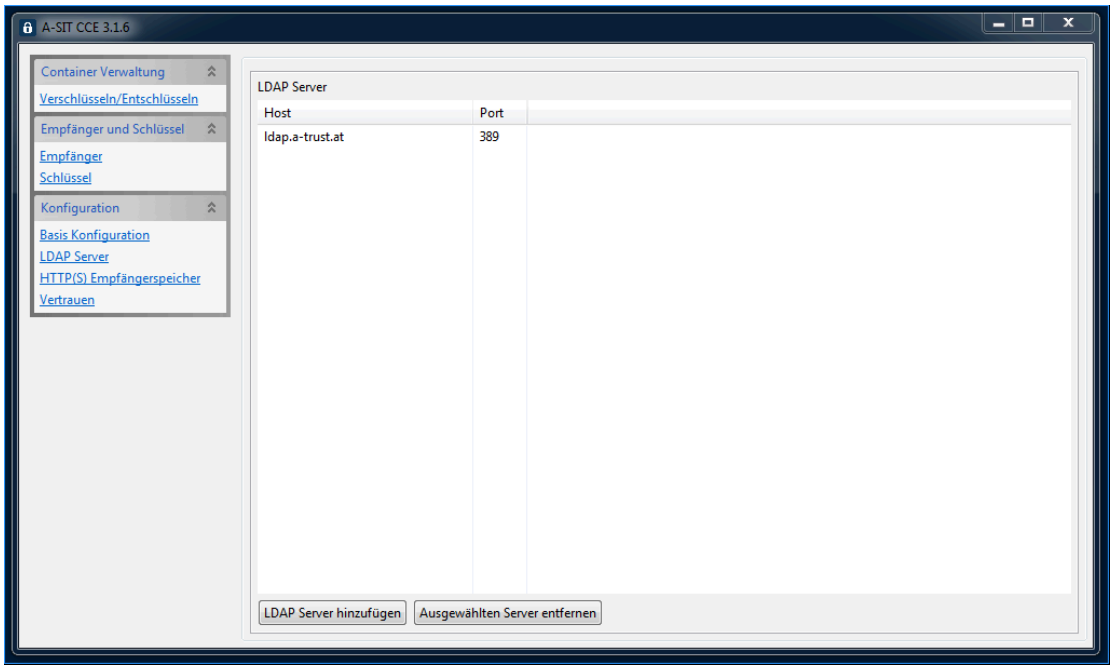
- ***PIN Cache Dauer***: bei manchen Smartcards muss der PIN-Code für jede Aktion wieder eingegeben werden (z.B. bei der Entschlüsselung). Diese Option ermöglicht eine temporäre PIN-Speicherung, solange die Applikation aktiv ist. Dieser PIN-Cache läuft für die Dauer der letzten Eingabe bzw. Anwendung von PIN-Codes. Die Dauer von dem PIN-Cache ist in Sekunden einzugeben. Der Ein Wert von 0 deaktiviert den PIN-Cache.
- ***PIN-Eingabe über das PIN-Pad:*** diese Option aktiviert/deaktiviert die Eingabe des PIN-Codes direkt am Pinpad (sofern der angeschlossene Kartenleser über ein solches verfügt). Der PIN-Cache funktioniert, nur wenn der PIN-Code über die Tastatur eingegeben wird, d.h. die Eingabe am PIN-Pad deaktiviert ist.
- ***Profil:*** Der Befehl ***Profil sichern*** erlaubt es, alle CCE3 Speicher und Einstellungen zu exportieren und bei einer anderen Installation durch den Befehl **Profil importieren** wieder zu importieren.
  ACHTUNG: Das beim Befehl *Profil importieren* ausgewählte Profil überschreibt alle CCE3 Speicher und Einstellungen. Ihre bisher gespeicherten Empfänger und Schlüssel gehen somit verloren und werden mit den Daten vom gespeicherten Profil überschrieben.



- **Logging:** Wenn diese Option aktiviert ist, erstellt CCE3 Log Dateien im Verzeichnis ***logs*** des CCE3 Konfigurationsordners (***.CCE2*** im Home Verzeichnis des Benutzers). Für weitere Details wird auf Abschnitt III:1 verwiesen.
- **Überprüfung der "Sicheres Löschen" Funktionalität:** Wenn diese Option aktiviert ist, überprüft CCE3 bei jedem Start, ob die dafür benötigen Programme am System installiert sind und verwendet werden können. Siehe Abschnitt I:3 für weitere Details.

3.2. LDAP Server

Hier können LDAP Server konfiguriert werden, auf die bei der Suche nach Empfängern in externen Speichern zugegriffen wird. Ein neuer Server kann über den Befehl ***LDAP Server hinzufügen*** hinzugefügt werden. Der Hostname und die Portnummer können dabei direkt in der Tabelle bearbeitet werden.
Dies wird durch einen Mausklick auf das jeweilige Feld durchgeführt. Durch Markieren eines LDAP Servers und der Auswahl des Befehls ***Ausgewählten Server entfernen*** kann ein bestehender LDAP Server wieder entfernt werden und wird somit bei der Suche nicht mehr berücksichtigt. Für weitere Details wird auf die Beschreibung der externen Speicher in Abschnitt V:1 verwiesen.

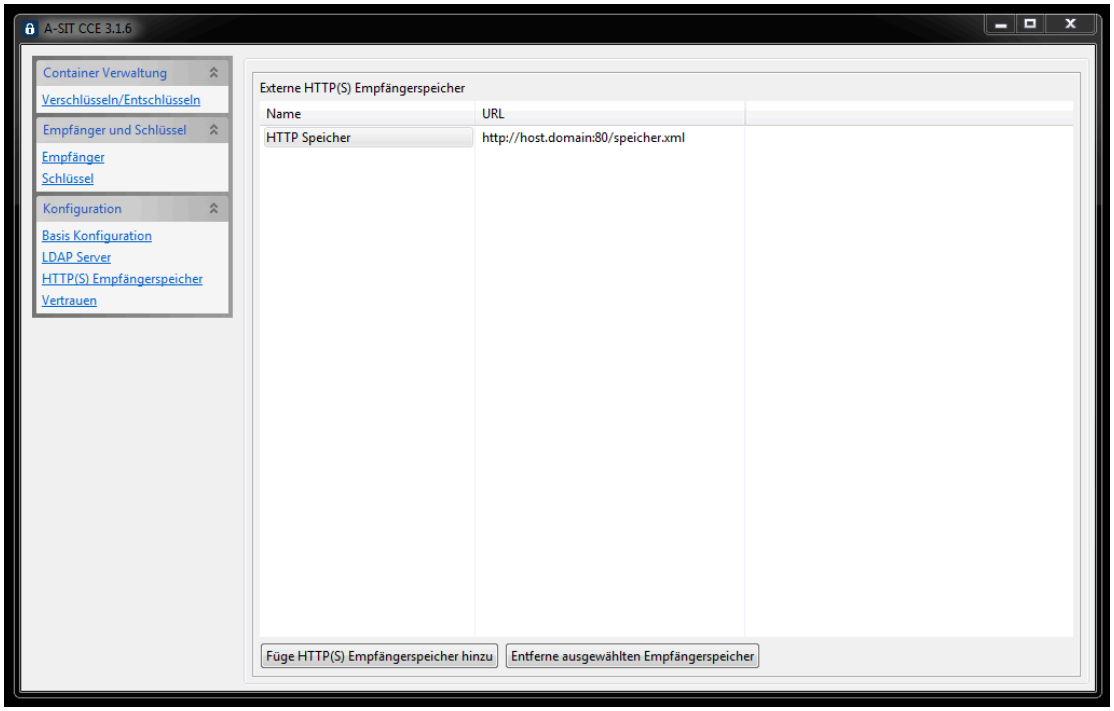


3.3. HTTP(S) Empfängerspeicher

Hier können externe Empfängerspeicher konfiguriert werden, die über das HTTP oder HTTPS Protokoll geladen werden. Dadurch kann ein Empfängerspeicher, der zentral verwaltet wird, allen CCE3 Installationen zur Verfügung gestellt werden. Die dort gespeicherten Empfänger oder Empfängergruppen werden bei CCE3 Empfängerspeichern angezeigt (siehe Abschnitt V:1).

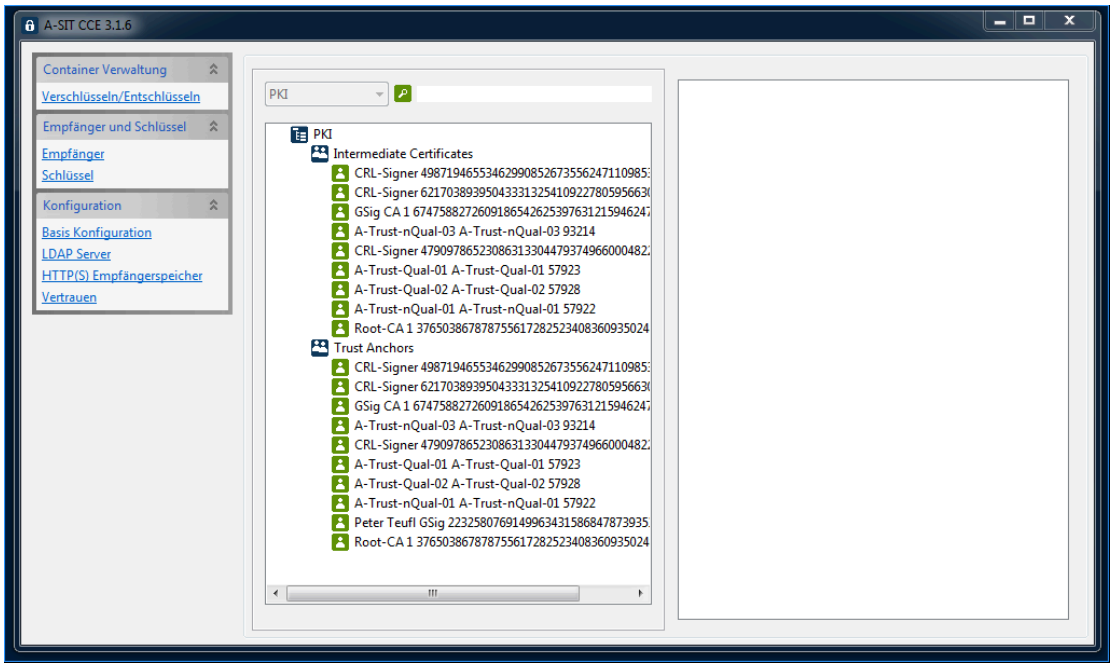
Ein neuer HTTP(S) Empfängerspeicher wird über den Befehl ***Füge HTTP(S) Empfängerspeicher*** hinzugefügt. Die Parameter werden dabei direkt in der Tabelle durch einen Mausklick auf das gewünschte Feld bearbeitet. Bestehende HTTP(S) Empfängerspeicher können durch Markieren und dem anschließenden Drücken von ***Entferne ausgewählten Empfängerspeicher*** wieder entfernt werden.

ACHTUNG: Es kann auf diese Speicher nur lesend zugegriffen werden. Details zur Wartung eines solchen Speichers werden in Abschnitt IV:5 beschrieben.



3.4. Vertrauen

Hier werden die vertrauenswürdigen Stammzertifizierungszertifikate gespeichert, die für die Widerrufsprüfung (siehe Abschnitt III:4) verwendet werden. Weiters werden hier alle Empfänger abgelegt, denen über den Befehl (***Diesem Empfänger explizit vertrauen***) explizit vertraut wird.



Die folgende Befehle können über das Kontextmenu und über die Toolbar ausgeführt werden. Welche Befehle zur Verfügung stehen hängt von den markierten Elementen ab.

Icon	Name	Beschreibung
	***Füge Empfänger hinzu...***	Über ein Auswahlfenster können weitere Empfänger aus dem Dateisystem hinzugefügt werden. Es werden dabei Zertifikate im CER/DER, PEM, PKCS7 oder CCE3 Empfängerspeicher (xml) unterstützt.
	***Setze den Namen zurück***	Es wird der Namen des Empfängers auf den Standard-Namen zurückgesetzt: Dieser ist der Common Name plus Common Name des Herausgebers plus Seriennummer der Zertifikats.
	***Umbenennen...***	Über ein Auswahlfenster können weitere Dateien zum markierten Ordner hinzugefügt werden.
	***Exportiere Empfänger...***	Die markierten Empfänger oder Empfängergruppen können mit diesem Befehl in folgende Formate exportiert werden: DER/CER, PEM, PKCS7 oder CCE3 Empfängerspeicher (xml).
	***Entferne***	Die markierten Empfänger-/Empfängergruppen werden entfernt.

Abschnitt VI: Umschlüsselung im Batch-Betrieb

Seit Version 3.2.0 unterstützt CCE optional die Umschlüsselung im Batch-Betrieb. Der Batch-Betrieb ist ausschließlich durch Verwendung des Kommandozeilen- Interfaces[10] möglich.

Die Verwendung des Interfaces wird durch folgende Maske beschrieben:

`CCE3-CMD [Modifikator] <<Option> [Parameter`]>

Mit Hilfe von Modifikatoren wird die allgemeine Ausführung von Befehlen eingestellt. Damit kann man z.B. die Auswahl von neuen Schlüsseln und Gruppen beschränken, die Eingabe von PIN-Code am Pinpad aktivieren oder diese deaktivieren (wenn möglich). Die Modifikatoren sind keine eigenen Befehle, daher können die nur neben den Befehlen (Optionen) angewandt werden.

Die Option beschreibt die Befehle, die das generelle Verhalten des Programms bestimmt. Damit wird die konkrete Aktion ausgewählt und mit Hilfe von Parametern weiteres definiert.

Grundsätzlich ist die Reihenfolge von und Modifikatoren beliebig. Manche Optionen können mehrfach angewandt werden[11].

1. Generelle Hinweise:

- Schlüssel werden aus lokalem oder externen (`--certstore`) Speicher gewählt. Diese können in Gruppen und hierarchisch organisiert sein. Es wird empfohlen, die Struktur (Gruppen/Friendly names) vor Verwendung über Aufruf mit "`CCE3-CMD --certs`" anzuzeigen.

- Dateinamen, Verzeichnisse oder Schlüsselnamen/-gruppen, die Leerzeichen enthalten, sollten in Anführungszeichen gestellten werden (z.B. "`meine Datei.cce`").

- Dateinamen und Eingabemasken (`--recursive`) mit wildcards werden in Apostroph eingegeben (z.B. `--recursive 'meine*.cce' '*_2012.cce'`).

---

[10] ***`Cce3-cmd`*** *im Windows und OS X,* ***`cce3-32`*** *und* ***`cce3-64`*** *im Linux*

[11] *Wie z.B.* ***`–file`****,* ***`--addgroup`*** *und andere.*

2. Optionen

Befehle	Beschreibung
`--help`	diese Hilfe anzeigen
`--gui`	GUI aktivieren
`--log`	Aktivitäten werden in Benutzerverzeichnis protokoliert (/.CCE2/logs/cce_cmd.log)
`--csvresults`	Aktivitäten werden in Benutzerverzeichnis protokoliert (/.CCE2/logs/cce_cmd.csv)
`--certs`	Zertifikatsliste im aktiven Zertifikatsspeicher zeigen
`--certstore`	Zertifikatsspeicher auswählen
`--file`	Datei(en) zur Verarbeitungswarteschlange hinzufügen
`--recursive`	Auswahl von Ordnern und Eingabemasken bei rekursiver Verarbeitung
`--addfkn`	Empfänger hinzufügen (friendly name)
`--addgroup`	Gruppe hinzufügen
`--rmfkn`	Empfänger entfernen
`--rmgroup`	Gruppe entfernen
`--scpin`	Smart Card PIN anwenden
`--swpin`	Software Key Store PIN anwenden
`--encrypt`	Datei(en) verschlüsseln (GUI)
`--decrypt_here`	Datei entschlüsseln im gleichen Ordner (GUI)
`--decrypt_full`	Datei entschlüsseln (GUI)
`--verbosity`	STANDARD, VERBOSE oder ERROR

3. Modifikatoren zur Schlüsselauswahl

Modifikator	Beschreibung
`--include-children`	auch die Untergruppe auswählen (standard)
`--exclude-children`	Untergruppen werden nicht ausgewählt
`--replace-keys`	alte Schlüssel werden entfernt und dann die neuen Schlüssel hinzugefügt (Sicherung empfohlen, falls Fehler auftreten)
`--enable-pinpad`	aktiviert PIN-Eingabe am PIN-Pad (falls vorhanden)
`--disable-pinpad`	deaktiviert PIN-Eingabe am PIN-Pad (falls vorhanden)

4. Beispiele

In Folge werden einige Beispiele gegeben, wie Sie Schlüssel zu bestehenden CCE-Dateien hinzufügen können (d.h. unter einem bestehenden Schlüssel entschlüsseln und mit den bisherigen und dem/den neuen Schlüssel(n) neu verschlüsseln).

- Einzelne Schlüssel aus Zertifikatsstore extern hunzufügen und entfernen bei allen .cce Dateien in aktuellem Ordner; Protokollierung aktiv:

  ```
  CCE3-CMD --file *.cce --addfkn group/fn#1 --rmfkn fn#2 --log
  --certstore extern
  ```

- Alte Schlüssel entfernen und neue Gruppe hinzufügen, wird auf eine Dateilist (file1 / file2) angewandt:

  ```
  CCE3-CMD --file file1.cce file2.cce --addgroup neutral
  --replace-keys
  ```

- Einzelne Schlüssel aus Zertifikatsstore extern bei aktuellen Ordner und Unterordnern rekursiv hinzufügen:

  ```
  CCE3-CMD --certstore extern --recursive '*.cce'
  --addfkn f_name#2 "Group 1/Max Mustermann" "friendly name #3"
  ```

- Schlüssel hinzufügen bei mehreren Gruppen und Ordnern, rekursiv:

  ```
  CCE3-CMD --recursive c:\user\folder1 c:\user\folder2
  'start*.cce' '*end.cce' --addfkn fname#1 fname#2
  ```

- Datei(en) und/oder Verzeichnis(se) verschlüsseln (GUI wird aktiviert):

  ```
  CCE3-CMD --encrypt doc1.doc lib c:\user\folder1
  ```

- Einzelne Datei entschlüsseln (GUI wird aktiviert):

  ```
  CCE3-CMD --decrypt_full container.cce
  ```

Abschnitt VII: Lizenz-Notiz

Die Teile des Pakets sind auch die folgenden Dateien, die vollständige Lizenz enthalten:

- EUPL v.1.1 - Licence.pdf
- EUPL v.1.1 - Lizenz.pdf
- NOTICE.TXT
- SIC_LICENSE.txt

Die Dateien sind im Programmverzeichnis abrufbar.