



Dateiverschlüsselung

- Vertrauliche Dateien (z.B. Dokumente) werden durch Verschlüsselung geschützt.
- Auf eine verschlüsselte Datei können nur jene Personen zugreifen, für welche die Datei auch verschlüsselt wurde.



Sollen Dateien vor dem Zugriff unbefugter Personen geschützt werden, so müssen diese verschlüsselt werden.



CCE - Citizen Card Encrypted

- CCE ist ein Tool, welches das Verschlüsseln / Entschlüsseln von Dateien über die Bürgerkarte ermöglicht.
- Unter: https://demo.a-sit.at/buergerkarte/cce2_tool/index.html stellt A-SIT ein Werkzeug zur Verschlüsselung von Daten in einem speicherbaren oder versendbaren Container unter Verwendung der Bürgerkarte frei zur Verfügung.
- Dateien können mit Hilfe des CCE Managers oder über das Kontextmenü 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.
- CCE unterstützt das sichere Löschen von Dateien. Damit ist garantiert, dass keine Reste von unverschlüsselten Daten nach der Verschlüsselung übrig bleiben.



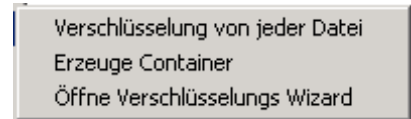
Verschlüsselungszertifikate

- Eine Datei kann für verschiedene Personen verschlüsselt werden. Dies geschieht mit Hilfe der Verschlüsselungszertifikate der gewünschten Personen.
- CCE bietet mehrere Möglichkeiten, zu den Verschlüsselungszertifikaten von Personen zu gelangen:
 - Zertifikate können von der Bürgerkarte, von Dateien und von LDAP-Servern importiert werden.
 - Verzeichnisdienste wie LDAP-Server speichern alle Zertifikate ihrer Kunden. So werden auf den Verzeichnisdiensten von a-trust oder des Hauptverbands der österreichischen Sozialversicherungsträger die Zertifikate der Personen gehalten, die ihre Bankomatkarte bzw. e-card als Bürgerkarte aktiviert haben.
 - Die LDAP-Server sind bei CCE bereits vorkonfiguriert und können durch Angabe von Daten der gewünschten Person durchsucht werden.
- CCE verwaltet Verschlüsselungszertifikate im Zertifikatspeicher. Es ist möglich Gruppen anzulegen, die mehrere Verschlüsselungszertifikate beinhalten.



Verschlüsselung von Dateien

- Über das Explorer Kontextmenü: Nach dem Markieren der Dateien können diese über das Kontextmenü des Explorers (wird durch das Drücken der rechten Maustaste geöffnet) verschlüsselt werden. Sind mehrere Dateien markiert, so kann jede Datei einzeln verschlüsselt werden (Verschlüsselung von jeder Datei) oder alle markierten Dateien in einem verschlüsselten Container abgelegt werden (Erzeuge Container).



- Über das Programm CCE-Manager: Dieses Programm wird über das Windows Start Menü gestartet. Dateien können im Reiter „Datei Verschlüsselung“ hinzugefügt und verschlüsselt werden.

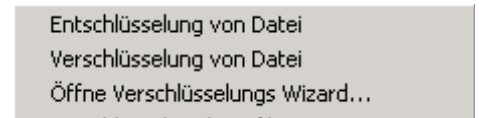


Bei den Standardeinstellungen von CCE werden die Klartextdateien nach der erfolgreichen Verschlüsselung sicher gelöscht. Dies verhindert die Wiederherstellung dieser Dateien von der Festplatte.



Entschlüsselung von Dateien

- CCE kann Dateien mit der Bürgerkarte oder mit einem Softwareschlüssel entschlüsseln. Beim Entschlüsseln wird der Benutzer nach dem PIN-Code der Bürgerkarte oder nach dem Passwort des Schlüsselspeichers gefragt.
- Über das Explorer Kontextmenü: Nach dem Markieren von verschlüsselten Dateien können diese über das Kontextmenü des Explorers entschlüsselt werden.



- Über das Programm CCE-Manager: Dieses Programm wird über das Windows Start Menü gestartet. Verschlüsselte Dateien können im Reiter „Datei Entschlüsselung“ hinzugefügt und entschlüsselt werden.



Sicheres Löschen von Dateien

- Wird eine Datei „herkömmlich“ gelöscht, so bleiben die Daten physikalisch erhalten und können allenfalls wiederhergestellt werden.
- Bei sensiblen Daten ist es daher wichtig, dass die Klartextdateien nach der Verschlüsselung so gelöscht werden, dass eine Wiederherstellung nicht mehr möglich ist.
- CCE implementiert einen Algorithmus, der eine Datei mehrfach überschreibt, bevor sie gelöscht wird. So ist eine Wiederherstellung der Datei nicht mehr möglich.
- CCE ist so konfiguriert, dass Klartextdateien nach der Verschlüsselung sicher gelöscht werden.

! Klartextdateien müssen nach der Verschlüsselung sicher gelöscht werden, da sonst eine Wiederherstellung dieser Dateien möglich ist.



Hardwaretoken / Softwaretoken

- Der Aufbewahrungsort des privaten Schlüssels spielt eine große Rolle für die Sicherheit der verschlüsselten Daten. Im Prinzip unterscheidet man zwischen Hardware- und Softwaretokens.
- Hardwaretoken: Die Bürgerkarte gehört in diese Kategorie. Der private Schlüssel ist auf der Karte gespeichert und kann im Allgemeinen nicht ausgelesen werden. Alle Operationen, für die der Schlüssel benötigt wird, werden direkt auf dem Hardwaretoken ausgeführt.

- Softwaretoken: In diesem Fall wird der Schlüssel auf einem Datenträger gespeichert. Die Datei, in der der Schlüssel gespeichert ist, wird normalerweise durch ein Passwort geschützt. Bekommt ein Angreifer Zugriff auf diese Datei, so kann er versuchen, das Passwort zu kompromittieren und somit Zugriff auf den privaten Schlüssel bekommen.

- CCE unterstützt Hardware- und Softwaretoken. Softwaretoken werden in einem Schlüsselspeicher abgelegt, der mit einem Passwort gesichert ist.



Backupschlüssel

- Werden Dateien nur mit der Bürgerkarte verschlüsselt, so können diese bei Verlust oder bei der Beschädigung der Karte nicht mehr entschlüsselt werden.
- Es ist daher zu empfehlen, mindestens ein weiteres Verschlüsselungszertifikat bei der Verschlüsselung mit anzugeben.
- Bei dem zweiten Zertifikat kann es sich um ein Zertifikat von einer weiteren Bürgerkarte handeln oder um ein Zertifikat von einem Softwaretoken.
- Wird ein Softwareschlüssel als Backupschlüssel verwendet, muss unbedingt darauf geachtet werden, dass dieser nicht zusammen mit den verschlüsselten Daten aufbewahrt wird.

Es wird dringend empfohlen, neben der Bürgerkarte einen Backupschlüssel oder eine Zweitkarte für die Verschlüsselung zu verwenden.

Handelt es sich bei dem Backupschlüssel um einen Softwareschlüssel, so DARF dieser NICHT zusammen mit den verschlüsselten Daten aufbewahrt und muss sicher verwahrt werden.



Fragen

Senden Sie ein E-Mail an: technology@a-sit.at

www.a-sit.at

2010-06



CCE - Dateiverschlüsselung mit der Bürgerkarte

E-Government Flyer Nr.208

CCE - Citizen Card Encrypted - Tool zum Verschlüsseln von Dateien mit der Bürgerkarte

- Dateiverschlüsselung
- CCE - Tool
- Verschlüsselungszertifikate
- Verschlüsselung von Dateien
- Entschlüsselung von Dateien
- Sicheres Löschen von Dateien
- Hardwaretoken / Softwaretoken
- Backupschlüssel

DIGITAL  AUSTRIA