



Zentrum für sichere Informationstechnologie – Austria Secure Information Technology Center – Austria

A-1040 Wien, Weyringergasse 35
Tel.: (+43 1) 503 19 63-0
Fax: (+43 1) 503 19 63-66

A-8010 Graz, Inffeldgasse 16a
Tel.: (+43 316) 873-5514
Fax: (+43 316) 873-5520

<http://www.a-sit.at>
E-Mail: office@a-sit.at

CCE (CITIZEN CARD ENCRYPTED)-DATEIFORMAT VERSION 1.0.0

Zusammenfassung: *Dieses Dokument beschreibt das von CCE für die Dateiverschlüsselung verwendete Format*

1 Inhaltsverzeichnis

1	Inhaltsverzeichnis	1
2	Einleitung	2
	2.1 Verschlüsselung	2
	2.2 Entschlüsselung	2
3	Details zum Dateiformat	2
	3.1 Header	2
	3.2 Aufbau einer CCE Datei	3
	3.3 Assymetrische Ver/Entschlüsselung	3
	3.4 Symmetrische Ver/Entschlüsselung	3
4	Literatur	3

2 Einleitung

Das **CCE** Dateiformat basiert auf dem S/MIMEV3 Standard und verwendet die **IAIK-CMS mit S/MIMEv3 [1]** Bibliothek.

2.1 Verschlüsselung

Mit **CCE** erstellte S/MIMEV3 Dateien werden verschlüsselt aber nicht signiert.

Zusätzlich zu den zu verschlüsselnden Daten wird noch die Datei **Recipients.p7c** hinzugefügt. Diese Datei enthält die Zertifikate der Personen, für die die Daten verschlüsselt wurden. Diese zusätzlichen Informationen werden von **CCE** benötigt, wenn ein bestehender Container modifiziert werden soll. Unter Modifikation wird das Hinzufügen/Entfernen von Benutzerzertifikaten/Dateien verstanden. Diese Operationen erfordern das Anlegen eines neuen Containers. Dazu werden Verschlüsselungsoperationen benötigt für die die öffentlichen Schlüssel der Empfänger benötigt werden. Diese Schlüssel sind in den Zertifikaten der Empfänger und somit in der Datei **Recipients.p7c** enthalten.

Für die symmetrische Verschlüsselung der Daten wird der Algorithmus **AES** mit einer Schlüssellänge von **256 bit** verwendet. Der Algorithmus ist fix eingestellt und kann vom Anwender nicht verändert werden. Es ist zu beachten, dass die momentanen Versionen von Outlook, Thunderbird, sowie einige P7M Viewer nicht mit diesem Algorithmus und/oder mit dieser Schlüssellänge umgehen können.

2.2 Entschlüsselung

CCE ist in der Lage beliebige S/MIME Nachrichten, die mit anderen Applikationen (z.B. Email Clients wie Outlook, Thunderbird) erstellt wurden, zu entschlüsseln. Zusätzlich werden Enveloped Data (P7M) [3] Dateien unterstützt. Dies ermöglicht die Entschlüsselung von S/MIME Nachrichten, wenn nur ein Webmail Zugang zu einem Mailserver vorhanden ist. Die verschlüsselten Daten sind dann im Client als **smime.p7m** Attachment zu sehen und können direkt mit **CCE** geöffnet werden. Wenn eine S/MIME Nachricht oder enveloped-data Datei mit **CCE** geöffnet wird, sucht **CCE** zuerst nach der Datei **Recipients.p7c**, die die Zertifikate der Empfänger enthält. Ist diese Datei vorhanden, stehen die Befehle für die Containermodifikation zur Verfügung. Im anderen Fall ist nur ein Entschlüsseln der im Container enthaltenen Daten möglich.

Bei der Entschlüsselung von beliebigen S/MIME Nachrichten werden alle Elemente (Multipart, Text/plain, Signed Data, application/octet-stream usw.) rekursiv ausgewertet und in einer Ebene in **CCE** dargestellt. Ist der Dateiname eines Elements gesetzt, wird dieser als Name für das Element verwendet. Wenn kein Name vorhanden ist, so verwendet **CCE** den Namen **plain** für die Daten.

3 Details zum Dateiformat

Dieser Abschnitt beschreibt die Details des **CCE** Dateiformats.

3.1 Header

Bei der Erstellung einer **CCE** Datei werden folgende Header verwendet:

```
Message-ID: <3807284.1124194795542.JavaMail.USER@HOSTNAME>
Date: Tue, 16 Aug 2005 14:19:55 +0200 (CEST)
From: CCE-CitizienCardEncrypted
To: SMIME
Subject: CCE SMimeContainer
Mime-Version: 1.0
Content-Type: application/pkcs7-mime; smime-type=enveloped-data;
             name=smime.p7m
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename=smime.p7m
```

Die erste und die zweite Zeile sind dabei variable. Die Message-ID wird bei jedem erstellten Container neu berechnet. Für **USER** und **HOSTNAME** werden die entsprechenden Werte eingetragen. In der zweiten Zeile steht der Zeitpunkt, zu dem der Container erstellt wurde.

3.2 Aufbau einer CCE Datei

Die *smime.p7m* Datei hat folgendes Format:

```
application/pkcs7-mime; smime-type=enveloped-data
  multipart/mixed
    application/octet-stream: Für Binärdaten, pro Datei ein Eintrag
    text/plain: Für reine Textdaten, pro Datei ein Eintrag
    application/octet-stream: Dieser Eintrag wird für die Speicherung der
                             Zertifikate der Empfänger verwendet und hat
                             den Namen Recipients.p7c. Der PKCS7
                             signed-data Standard [3] wird als
                             Dateiformat verwendet
```

Es muss mindestens ein **application/octet-stream** Eintrag oder ein **text/plain** Eintrag vorhanden sein. D.h. es muss mindestens eine Datei im Container vorhanden sein. Weiters gibt es noch einen weiteren **application/octet-stream** Eintrag, der den Namen *Recipients.p7c* hat und die Zertifikate der Empfänger enthält.

3.3 Assymetrische Ver/Entschlüsselung

Für die Ver/Entschlüsselung des symmetrischen Schlüssels können alle Algorithmen verwendet werden, die vom S/MIME Format unterstützt werden. Der verwendete Algorithmus wird durch das Zertifikat des Empfängers bestimmt. Für eine detaillierte Auflistung der unterstützten Algorithmen wird auf [2] verwiesen.

3.4 Symmetrische Ver/Entschlüsselung

Bei Verschlüsselung:

Bei der Verschlüsselung setzt **CCE** fix vorgegeben den Algorithmus **AES** mit einer Schlüssellänge von **256 bit** ein.

Bei Entschlüsselung:

Für die Entschlüsselung können alle Algorithmen verwendet werden, die vom S/MIME Format unterstützt werden. Für eine detaillierte Auflistung der unterstützten Algorithmen wird auf [2] verwiesen.

4 Literatur

1. **iaik-cms with s/mimev3** - http://jce.iaik.tugraz.at/products/03_cms/index.php -abgerufen aus dem WWW am 21.08.2005
2. **iaik-cms with s/mimev3 - features** - http://jce.iaik.tugraz.at/products/03_cms/features/index.php - abgerufen aus dem WWW am 21.08.2005
3. **RFC2630 – Cryptographic Message Syntax** – <http://rfc.net/rfc2630.html> - abgerufen aus dem WWW am 21.08.2005