



Zentrum für sichere Informationstechnologie - Austria (A-SIT)

---

Dokumentation

# **Toolkit zur Generierung von Anwenderzertifikaten**

**(CA-Toolkit 1.2)**

Thomas Rössler

`thomas.roessler@iaik.at`

24. Februar 2003

# Inhaltsverzeichnis

<b>1</b>	<b>Einleitung</b>	<b>3</b>
<b>2</b>	<b>e-Mail-Verschlüsselungszertifikate</b>	<b>4</b>
2.1	Erststart - Initialisierung . . . . .	4
2.1.1	Hintergrund . . . . .	5
2.1.2	Bedienung . . . . .	10
2.2	Generierung von Anwenderzertifikaten zur e-Mail-Verschlüsselung . . . .	13
2.2.1	Initialisierung des Tools . . . . .	13
2.2.2	Erzeugen von Einzelzertifikaten . . . . .	14
2.2.3	Expertenmodus . . . . .	19
<b>3</b>	<b>EFS-Anwenderzertifikaten</b>	<b>25</b>
3.1	Erststart - Intialisierung . . . . .	25
3.1.1	Bedienung . . . . .	27
3.2	Generierung von EFS - Anwenderzertifikaten . . . . .	27
3.2.1	Bedienung . . . . .	29
3.2.2	Expertenmodus . . . . .	30

# 1 Einleitung

Das vorliegende CA-Toolkit stellt ein umfassendes Werkzeug dar, mit dessen Hilfe Anwenderzertifikate für verschiedene Zwecke erzeugt werden können. Die aktuelle Version ermöglicht das Erstellen von:

- e-Mail-Verschlüsselungszertifikaten
- Zertifikate für das Encrypted File System (EFS)

Erweiterungen zur Erstellung anderer Anwenderzertifikate sind selbstverständlich möglich. Allen erzeugbaren Zertifikaten ist gemeinsam, dass sie vom ein und dem selben selbstsignierten Wurzelzertifikat abstammen. Weiters verwenden alle Anwenderzertifikate das gleiche Schlüsselpaar (Anwenderzertifikate für EFS- und e-Mail-Verschlüsselung natürliche jeweils ein eigenes). Dadurch wird die Zertifikats- und Schlüsselverwaltung sehr vereinfacht. Auf der anderen Seite ist die Anwendbarkeit dieser Zertifikate dadurch nur auf einen internen Gebrauch beschränkt.

Die beiden Module des Toolkits sind weitestgehend getrennt verwendbar. Je nachdem, welche Start-Datei aufgerufen wird, wird einmal das Tool zur Erzeugung von e-Mail-Verschlüsselungs- oder EFS-Zertifikaten gestartet. Egal welches der beiden Tools zuerst aufgerufen wird, beim Erststart muss das Toolkit initialisiert werden (Erzeugung des Wurzelzertifikates, etc.). Ist dies einmalig erfolgt, so können die verschiedenen Anwenderzertifikate, aufbauend auf den Ergebnissen der Initialisierungsphase, generiert werden.

Im nachfolgenden Abschnitt wird zunächst die Komponente zum Erstellen der e-Mail-Verschlüsselungszertifikate im Detail beschrieben. In diesem Zuge wird auch die Initialisierungsphase genauer beleuchtet. Der zweite Abschnitt widmet sich dem Modul zur Generierung von EFS-Zertifikaten. Die Bedienung und der Ablauf im Hintergrund ist dabei weitestgehend identisch wie jene bei der Komponente zur Erzeugung von e-Mail-Verschlüsselungszertifikaten. Deshalb werden hier nur die wesentlichsten Unterschiede hervorgehoben.

## 2 e-Mail-Verschlüsselungszertifikate

Dieses Tool, stellt ein einfaches Werkzeug dar, welches e-Mail-Verschlüsselungszertifikate erstellt. Gestartet wird diese Komponente des CA-Toolkits durch die Startdatei „VCA start.bat“. Je nachdem, ob das CA-Toolkit zum ersten Mal gestartet worden ist oder nicht unterscheidet sich der Programmablauf. Im Zuge des Erststartes werden Konfigurationsmaßnahmen und Initialisierungsschritte durchgeführt. Bei jeder weiteren Verwendung des Tools wird dieser Vorgang übersprungen und stattdessen das Tool sofort im Standardmodus gestartet.

Diese Dokumentation gliedert sich demnach in zwei Teile. Der erste Teil geht auf die Vorgänge im Zusammenhang mit der Initialisierung im Zuge des Erststartes ein. Im zweiten Teil wird der Standard- und der Expertenmodus beschrieben, in denen die Verschlüsselungszertifikate für Endanwender erzeugt werden können. Diese beiden Kapitel gliedern sich jeweils in zwei weitere Abschnitte. Zu Beginn jeden Kapitels werden die technischen Hintergründe und die Details der Vorgänge erläutert. Im Anschluss daran wird ausschließlich auf die Bedienung und auf die Möglichkeiten aus Sicht des Anwenders eingegangen.

### 2.1 Erststart - Initialisierung

Dieser Schritt ist notwendig, um das Tool einmalig zu Initialisieren. Da das Programm Zertifikate generiert und es somit als Zertifizierungsstelle (Certificate Authority CA) fungiert, werden in diesem Schritt die CA-Zertifikate und die notwendigen Schlüsselpaare erzeugt. Im Detail werden folgende Schritte durchlaufen:

- Festlegung von Organisationsnamen, Adresse, Gültigkeitsdauer der CA-Zertifikate
- Eingabe der Maildomäne
- Generieren der Schlüsselpaare für die CA-Zertifikate
- Generieren des Schlüsselpaares für alle nachfolgenden Anwenderzertifikate

## 2.1.1 Hintergrund

### Konfiguration

Einige notwendige Konfigurationseinstellungen sind in einer **properties**-Datei zusammengefasst. Die Datei **configuration.properties** muss von vorne herein die folgenden Einträge beinhalten:

- **cert.caroot=Verzeichnis** ... Der Verzeichnisname gibt an, wohin die CA-Zertifikate geschrieben werden sollen. Falls das Verzeichnis nicht existiert wird es erzeugt.
- **cert.userroot=Verzeichnis** ... Dieser Verzeichnisname gibt an, wohin die Anwender-Zertifikate zur e-Mail-Verschlüsselung in weiterer Folge geschrieben werden sollen. Falls das Verzeichnis nicht existiert wird es erzeugt.
- **cert.efsroot=Verzeichnis** ... Dieser Verzeichnisname gibt an, wohin die Anwender-Zertifikate für EFS geschrieben werden sollen. Falls das Verzeichnis nicht existiert wird es erzeugt.
- **cert.keylength=Länge** ... Damit wird die Länge (in Bits) der zu generierenden Schlüssel festgelegt. Eine Länge von mindestens 1024 ist zu empfehlen.
- **setting.initialization=Verzeichnisname** ... Durch diesen Eintrag wird der Name des Verzeichnisses festgelegt, in dem die Initialisierungsdaten (z.B.: Schlüssel-daten) abgelegt werden. Dieses Verzeichnis wird neu angelegt.
- **logfile=Datei** ... Dieser Eintrag legt den Namen der standardmäßig zu verwendenden LOG-Datei an.

Diese **properties**-Datei mit den oben beschriebenen Einträgen muss existieren bevor das CA-Toolkit zum Ersten Mal gestartet wird. Sie ist mit Standardwerten versehen im Basisverzeichnis des Toolkits zu finden. Die Verzeichnis- und Dateiangaben können selbstverständlich abgeändert werden. Der Name und der Speicherort dieser **configuration.properties** Datei darf nicht verändert werden. Ansonsten kann das CA-Toolkit die Konfigurationsdaten nicht laden und bricht während des Startvorganges mit einer entsprechenden Fehlermeldung ab.

### Initialisierung

Beim Erststart einer Komponente des CA-Toolkits wird die **properties**-Datei geöffnet und mit der Initialisierung begonnen. Daraufhin erscheint das Konfigurationsfenster. Anfangs ist das Fenster noch inaktiv, da noch einige notwendige Objekte instanziiert und initialisiert werden. Der Fortschritt kann anhand der Fortschrittsanzeige (Progress Bar) im rechten unteren Bereich des Fensters beobachtet werden. Nach wenigen Sekunden werden die Eingabefelder editierbar und der **Start**-Button aktivierbar. Abbildung 2.1 zeigt das Konfigurationsfenster.

Während dieses Konfigurationsprozesses sind folgende Eingaben vorzunehmen:

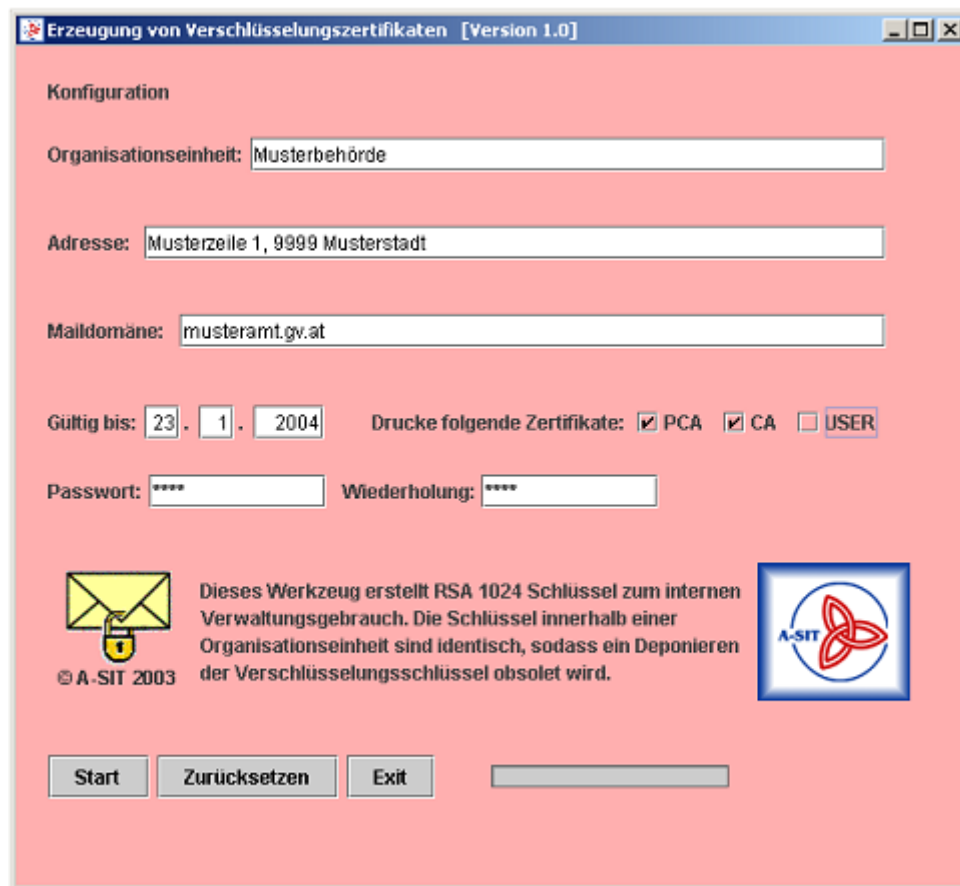


Abbildung 2.1: Konfigurationsfenster während der Initialisierungsphase - am Beispiel Komponente für die e-Mail-Verschlüsselungszertifikate

- Eingabe des Namens der Organisation (zum Beispiel: Musterbehörde)
- Eingabe der Adresse der Organisation (zum Beispiel: Musterzeile1, 9999 Musterstadt)
- Festlegen der Maildomäne (zum Beispiel: musteramt.gv.at)
- Angabe der Gültigkeitsdauer des CA-Zertifikates (standardmässig 1 Jahr)

Darüberhinaus ist die Angabe eines Passwortes notwendig, das die während der Initialisierungsphase erzeugten Zertifikate sichert. Ausserdem wird dieses Passwort bei jedem weiteren Start des Tools zu Beginn abgefragt. Dieses Passwort muss, wie auch durch andere Anwendungen gewohnt, wiederholt fehlerfrei angegeben werden. Um die während der Initialisierung erstellten Zertifikate und Schlüsselpaare auch dauerhaft und auf nicht-elektronischem Wege sichern zu können, stellt der Konfigurationsbildschirm optional die Möglichkeit zur Verfügung, die initial erzeugten Zertifikate (PCA, CA, USER) anzuzeigen und auszudrucken. Dazu stehen drei optionale Auswahlfelder zur Verfügung. Mehr

dazu in der detaillierten Bedienungserläuterung (2.1.2).

Durch Betätigung des **Start**-Buttons werden die Daten aus den Eingabefeldern übernommen und das Toolkit initialisiert. Dabei werden die folgenden drei RSA-Schlüsselpaare generiert:

1. Schlüsselpaar für ein selbstsigniertes Wurzelzertifikat
2. Schlüsselpaar für das eigentliche CA-Zertifikat der Organisationseinheit
3. Schlüsselpaar, das für alle Anwenderzertifikate (für e-Mail-Verschlüsselungszertifikate) verwendet wird

Die Länge der Schlüssel (z.B. 1024 Bit) wird aus der `configuration.properties`-Datei entnommen.

Unter Verwendung des ersten Schlüsselpaares wird ein selbstsigniertes Wurzelzertifikat für das CA-Toolkit erzeugt. Dieses selbstsignierte Wurzelzertifikat ist die Wurzel für alle mit dem Toolkit erzeugbaren Zertifikate (egal mit welchem Modul diese generiert werden). Folgenden Schlüsselverwendungen (KeyUsage) wird dabei festgelegt:

- `keyCertSign`
- `cRLSign`
- `nonRepudiation`
- `digitalSignature`

Dieses selbstsignierte Wurzelzertifikat ist die Wurzel für alle mit dem Toolkit erzeugbaren Zertifikate (egal mit welchem Modul diese generiert werden). Darüberhinaus werden die Subjekt-Eigenschaften anhand der Daten aus den Eingabefeldern wie folgt angenommen:

- `country`: AT (fix)
- `organization`: *Name der Organisationseinheit + Adresse der Organisation*
- `common name`: *Name der Organisationseinheit + [SELF SIGNED ROOT CERTIFICATE]*
- `Domain`: *Maildomäne*

Diesem Zertifikat wird der öffentliche Schlüssel des ersten Schlüsselpaares beigelegt. Unter Verwendung des privaten Schlüssels dieses Paares wird das Zertifikat signiert. Das so entstandene selbstsignierte Zertifikat stellt damit die Wurzel der Zertifikatsketten dar, die in weiterer Folge mit dem so initialisiertem CA-Toolkit erzeugt werden können. Dieses Wurzelzertifikat (ohne Beifügung des privaten Schlüssels) wird als PKCS#7 Datei (`.p7c`)

in das in der **properties**-Datei angegebene Verzeichnis der CA-Zertifikate geschrieben. Genauer gesagt wird dieses selbstsignierte Wurzelzertifikat in das Unterverzeichnis **/pca** kopiert. Der Name der Datei ist identisch mit dem der Maildomäne der Organisation. Die Dateierweiterung lautet **.pca.p7c**, um Verwechslungen mit anderen CA-Zertifikaten zu vermeiden (zum Beispiel **certs\cacerts\pca\musteramt.gv.at.pca.p7c**). Zusätzlich wird das Zertifikat auch in Form einer binären DER-Datei exportiert. Die Endung dieser Datei lautet **.pca.der**.

Auf ähnliche Weise wird das zweite CA-Zertifikat erstellt, das zum Ausstellen der e-Mail-Verschlüsselungszertifikate dient. Bei diesem wird, wie schon beim selbstsignierten Wurzelzertifikat, die Schlüsselverwendung und die Subjektinformationen wie folgt festgelegt:

Schlüsselverwendung:

- **keyCertSign**
- **cRLSign**
- **nonRepudiation**
- **digitalSignature**

Subjektinformationen:

- **country:** AT (fix)
- **organization:** *Name der Organisationseinheit + Adresse der Organisation*
- **common name:** *Name der Organisationseinheit + E-MAIL CRYPT-CA*
- **Domain:** *Maildomäne*

Dem so vorbereiteten Zertifikat wird der öffentliche Schlüssel des zweiten Schlüsselpaares beigelegt. Abschließend wird dieses Zertifikat mit dem zum selbstsignierten Wurzelzertifikat gehörenden privaten Schlüssel (des ersten Schlüsselpaares) signiert. Mit anderen Worten, es wird dieses Zertifikat unter Verwendung des selbstsignierten Wurzelzertifikates ausgestellt. Wiederum wird dieses Zertifikat ohne privatem Schlüssel als PKCS#7 Datei (**.p7c**) und als DER-Datei (**.der**) in das in der **properties**-Datei angegebene Verzeichnis der CA-Zertifikate geschrieben – diesmal in das Unterverzeichnis **/ca**. Der Name der Datei ist identisch mit dem der Maildomäne der Organisation. Die Dateierweiterung lautet **.emailcryptca.p7c**, um Verwechslungen mit dem selbstsignierten Wurzelzertifikat und mit CA-Zertifikaten der anderen Module des Toolkits (beispielsweise EFS-CA) zu vermeiden (zum Beispiel **..\cacerts\ca\musteramt.gv.at.emailcryptca.p7c**).

Die so erzeugten Zertifikate und die Schlüsselpaare werden für den späteren Gebrauch auch in Form von PKCS#12 Dateien gespeichert. Dieses Datenformat sieht



vor, dass jeweils ein Zertifikat zusammen mit dem zugehörigen Schlüsselpaar (privater und öffentlicher Schlüssel) gesichert wird. Um Missbrauch des so inkludiertem privaten Schlüssels zu verhindern, sind diese Dateien passwortgeschützt. Als Passwort wird das während des Initialisierungsprozesses angegebene Passwort herangezogen. So entstehen nach erfolgreicher Initialisierung folgende drei Dateien:

- *Maildomäne.pca.p12...* enthält das selbstsignierte Wurzelzertifikat (PCA-Zertifikat) samt zugehörigem Schlüsselpaar (erstes Schlüsselpaar)
- *Maildomäne.emailcryptca.p12...* enthält das Stammzertifikat (CA-Zertifikat) der Verschlüsselungszertifikate für die Endanwender (samt zugehörigem Schlüsselpaar - zweites Schlüsselpaar)
- *Maildomäne.emailcryptusr.p12...* diese Datei enthält ein pseudo-Anwenderzertifikat (USER-Zertifikat), wie es im Standardbetrieb auch für Endanwender erzeugt wird. In diesem Zertifikat ist somit das allen Anwenderzertifikaten gemeinsame Schlüsselpaar (drittes Schlüsselpaar) gespeichert.

Diese Dateien werden in das durch die `configuration.properties`-Datei festgelegte Initialisierungs-Verzeichnis abgelegt. Diese `p12`-Dateien sind standardisiert und somit unter Einbeziehung des angegebenen Passwortes auch in andere Zertifikatsanwendung (z.B. andere Zertifikatserstellungsprogramme) importierbar. Grundlegend werden allerdings diese Dateien nur für den internen Gebrauch innerhalb des CA-Toolkits benötigt.

Ebenfalls als Resultat dieser Initialisierung wird im `initialization`-Verzeichnis eine `init.props`-Datei und eine `groups.props`-Datei erzeugt. Die `init.props`-Datei beinhaltet nochmals den angegebenen Organisationsnamen und die weiteren Organisationsdetails (wie etwa Adresse, Maildomäne, etc.). Im Wesentlichen markiert die Existenz dieser Datei, bzw. das Vorhandensein des darin enthaltenen `initialized=true` Eintrags, dass das Tool bereits initialisiert worden ist. Die `groups.props` Datei enthält die möglichen Untergruppen der Organisation, für die Zertifikate im Rahmen des Standardbetriebs gesammelt generiert werden können. Standardmäßig wird nur eine Gruppe, nämlich die Gruppe `standard`, definiert. Im Standardbetrieb werden demnach ohne weiteres Zutun alle erzeugten Anwenderzertifikate dieser Gruppe zugeordnet und in einem gleichnamige Unterverzeichnis abgelegt. Bei der Generierung gibt es des Weiteren auch die Möglichkeit, neue Gruppen anzulegen, die existierenden Gruppen zu löschen oder diese umzuorganisieren (Näheres siehe Abschnitt 2.2).

Durch Entfernen dieses `initialization`-Verzeichnisses kann eine Reinitialisierung des gesamten CA-Toolkits erzwungen werden. Der Anwender sollte allerdings im Normalfall keine Änderungen in diesem Verzeichnis vornehmen. Das CA-Toolkit ist nunmehr initialisiert. Nachdem dieser Vorgang abgeschlossen wurde öffnet sich automatisch das Standardfenster zur Erzeugung von Anwenderzertifikaten - im speziellen Fall zur Erzeugung von e-Mail-Verschlüsselungszertifikaten.

## ANMERKUNG:

In der aktuellen Implementierung ist keine nachträgliche Änderung der während dieser Initialisierung erfolgten Einstellungen vorgesehen. Eine Neuinitialisierung ist, wie erwähnt, nur durch die Entfernung des `initialization`-Verzeichnisses möglich.

### 2.1.2 Bedienung

Wie bereits auszugsweise erwähnt, stehen in diesem Konfigurationsfenster (Abb.2.1), neben den Eingabefeldern, folgende Bedienelemente zur Verfügung:

- **Start-Button** ... aktiviert den Initialisierungsprozess
- **Zurücksetzen-Button** ... setzt sämtliche Eingabefelder zurück bzw. löscht sie
- **Exit-Button** ... beendet das CA-Toolkit
- **Auswahl-Boxen (PCA, CA, USER)** ... aktiviert zusätzliche Darstellung für den Ausdruck der Zertifikate

Darüberhinaus gibt die Fortschrittsanzeige im rechten unteren Fensterbereich Auskunft über den aktuellen Fortschritt des Initialisierungsprozesses.

### Schrittweises Vorgehen bei der Initialisierung:

1. Ausfüllen *aller* Eingabefelder (Name, Adresse und Maildomäne der Organisation). Alle Angaben sind erforderlich. Bei der Eingabe der Maildomäne wird diese auch auf ungültige Zeichen hin überprüft und erforderlichenfalls eine Fehlermeldung angezeigt (erlaubt sind 'A'-'Z', 'a'-'z', '0'-'9', '.', '-', ',')<sup>1</sup>.
2. Übernehmen oder Ändern des gewünschten Gültigkeitsbereiches bzw. Festlegen des Endzeitpunktes, ab dem die im Rahmen der Initialisierung generierten Wurzelzertifikate ungültig werden. Beginn des Gültigkeitsbereiches ist das aktuelle Datum. Alle weiteren, basierend auf dieser Initialisierung erzeugten Anwenderzertifikate besitzen die selbe Gültigkeitsdauer (Standardvorgabe: 1 Jahr).
3. Festlegen, ob zum Zwecke der Archivierung und Datensicherung die neu generierten Wurzelzertifikate und Schlüsselinformationen angezeigt und ggf. ausgedruckt werden sollen (siehe Abb. 2.2). Die Bedeutung der drei Auswahl-Boxen:
  - **PCA**: Ausgabe des PCA-Zertifikates (selbstsignierte Wurzelzertifikat)
  - **CA**: Ausgabe des CA-Zertifikates (Stammzertifikat der Anwenderzertifikate)

---

<sup>1</sup>gemäß RFC1034 und RFC1035

- USER: Ausgabe der allen Verschlüsselungszertifikaten gemeinsamen Schlüsselinformationen (im speziellen Informationen des Schlüssels zur e-Mail-Verschlüsselung)
4. Auswahl und wiederholtes Eingeben des Passwortes zum Schutz der Wurzelzertifikate. Dieses Passwort wird auch bei jedem weiteren Start des Toolkits abgefragt.
  5. Durch Betätigung des **Start**-Buttons wird der Initialisierungsprozess gestartet. Der Fortschritt kann anhand der Fortschrittsanzeige (Progress-Bar) beobachtet werden.



Abbildung 2.2: Ausgabe der generierten Zertifikats- und Schlüsselinformationen

Nach erfolgreicher Initialisierung werden (standardmäßig) die folgenden zwei neuen Verzeichnisse erstellt:

- **initialization...** beinhaltet Initialisierungsinformationen und die internen Dateien zum Speichern der Wurzelzertifikate (PCA,CA). Durch Entfernen dieses Verzeichnisses kann eine Reinitialisierung des Toolkits erzwungen werden.
- **certs...** beinhaltet vorerst nur die neuen Wurzelzertifikate in den jeweiligen Unterverzeichnissen `cacert\pca` und `cacert\ca`. Diese Zertifikatsdateien sind im PKCS#7 Format (ohne privatem Schlüssel) und im DER-Format gespeichert und sind für den Import in Browsern oder ähnliche Anwendungen gedacht. In weiterer Folge werden in dieses **cert**-Verzeichnis standardmäßig die Anwenderzertifikate kopiert (in Gruppen bzw. Unterverzeichnissen sortiert - Abhängig von Vorgaben in der `configuration.properties`-Datei ).

Die Verzeichnisnamen können, wie auch einige andere Eigenschaften, in der `configuration.properties`-Datei abgeändert werden. Im Normalfall sollten allerdings die Standardeinstellung ausreichen. Zum Abschluss der Initialisierung startet das Tool automatisch den Standardbetrieb, wobei auch erstmals die Passwortabfrage erscheint. Hier ist das im Konfigurationsdisplay angegebene Passwort erstmalig zu verwenden. Dadurch wird auch gleich die Korrektheit der soeben erzeugten Dateien und Zertifikate geprüft.

## 2.2 Generierung von Anwenderzertifikaten zur e-Mail-Verschlüsselung

Nachdem im Zuge des Erststartes die Initialisierung des CA-Toolkits erfolgte, erscheint automatisch bei jedem weiteren Neustart das Standardfenster zur Erzeugung von Anwenderzertifikaten (Abbildung 2.3).

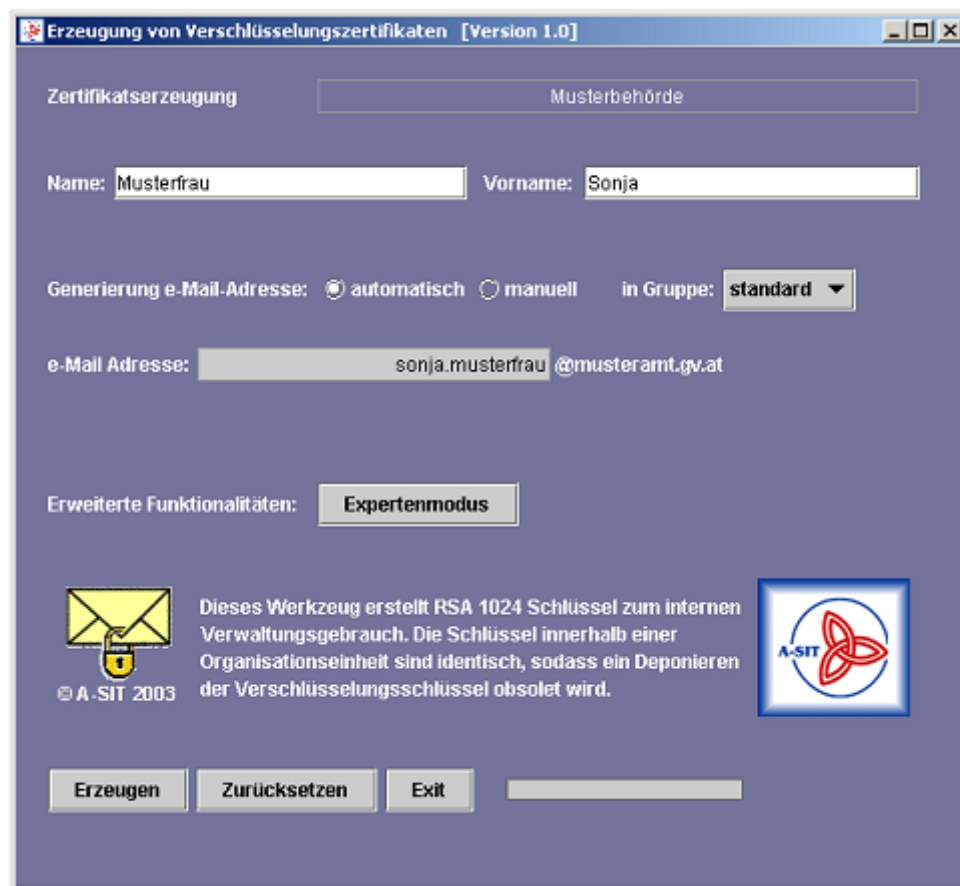


Abbildung 2.3: Standardfenster für die Erzeugung von Anwenderzertifikaten (e-Mail-Verschlüsselungszertifikaten)

### 2.2.1 Initialisierung des Tools

Durch die Existenz der `init.props`-Datei im entsprechenden `initialization`- Verzeichnis wird festgestellt, dass das Tool bereits initialisiert wurde. Somit werden nunmehr die zuvor beim Erststart generierten Wurzelzertifikate (PCA,CA,USER) und die zugehörigen Schlüsselinformationen geladen. Für das Lesen der PKCS#12-Zertifikatsdateien, die auch die benötigten Schlüsselpaare beinhalten, ist das während des Initialisierungsprozesses angegebene Passwort notwendig. Demnach wird während des Tool-

Starts der Anwender zur Eingabe dieses Passwortes aufgefordert. Dieser Vorgang benötigt einige Sekunden währenddessen die Eingabefelder des Fensters, sowie sämtliche Buttons deaktiviert bleiben. Den Fortschritt dieser Startphase kann im rechten unteren Fensterbereich anhand der Fortschrittsanzeige beobachtet werden (Progress Bar).

Sollte die Initialisierung des CA-Toolkits durch eine andere Komponente als dem Modul zur Erstellung von Verschlüsselungszertifikaten erfolgt sein, so wird erst bei dem Erststart dieser Komponente das benötigte **E-MAIL CRYPT-CA**-Zertifikat (signiert durch das bestehenden Wurzelzertifikat) erzeugt. Ausserdem wird das gemeinsame Schlüsselpaar aller Verschlüsselungszertifikate generiert. Dies geschieht für den Anwender völlig transparent. Er wird nur durch eine kleine Abfrage darauf aufmerksam gemacht, dass es zu dieser Nachinitialisierung kommt. Weiters wird durch einen Dialog gefragt, ob auch die neu generierten Schlüssel- und Zertifikatsinformationen dargestellt und ausgedruckt werden sollen (analog dem Vorgehen bei der Erstinitialisierung).

## 2.2.2 Erzeugen von Einzelzertifikaten

### Hintergrund

Zur Erzeugung von einzelnen Anwenderzertifikaten ist lediglich die Eingabe des Namen und des Vornamen (optional) des Zertifikatsbesitzers notwendig. Im einfachsten Fall wird dann anhand dessen automatisch unter Anwendung der e-Mail-Adressen-Policy die e-Mail-Adresse generiert. Diese automatische Adressgenerierung erfolgt, wenn die "Generierung der e-Mail-Adresse"-Auswahl im Standardfenster auf **automatisch** gestellt bleibt. Dann bleibt auch das Eingabefeld für die optionale e-Mail-Adresse deaktiviert.

### ANMERKUNG:

In der aktuellen Implementierung wird die e-Mail-Adresse durch eine einfache Kombination aus *Vorname.Name@Maildomäne* bzw. bei fehlendem Vornamen nur aus *Name@Maildomäne* erzeugt.

Die Auswahloption in **Gruppe** ermöglicht das Zusammenfassen von Verschlüsselungszertifikaten nach Gruppen. Als Ergebnis dieser Gruppierung werden alle Zertifikate einer Gruppe in dem gleichnamigen Verzeichnis `certs\mailcerts\Gruppe` abgelegt. Standardmäßig ist nur die Gruppe **standard** vordefiniert. Das Ändern und das Hinzufügen von neuen Gruppen kann im sogenannten *Expertenmodus* durchgeführt werden (siehe 2.2.3). Bei automatischer Ableitung der e-Mail-Adresse und bei Auswahl der Standard-Gruppe kann nach Eingabe des Namens das Zertifikat bereits erzeugt werden. Dieser Vorgang wird mit dem **Erzeugen**-Button ausgelöst.

Da diese Anwenderzertifikate im wesentlichen zur e-Mail-Verschlüsselung vorgesehen sind, wird die Einschränkung der Schlüsselverwendung wie folgt festgelegt:

- `keyEncipherment`

- `dataEncipherment`

Unter Zuhilfenahme der Organisationsdaten aus der Initialisierungsphase werden die Subjektinformationen des Anwenders folgendermassen zusammengesetzt:

- `country`: AT (fix)
- `organization`: *Name der Organisationseinheit + Adresse der Organisation*
- `common name`: *Name+Vorname*
- `emailAddress`: *Vorname.Name@Maildomaine*

Die Seriennummer des Zertifikates besteht aus zwei Teilen. Zum einen werden die vorderen 8 Byte aus dem Ablaufdatum des Zertifikates und aus dem Namen der Organisationseinheit unter Verwendung einer MD5-Hash-Funktion gebildet. Die nachfolgenden 16 Byte werden ebenfalls durch Anwendung einer MD5-Hash-Funktion aus dem Namen des Zertifikatsbesitzers (Anwender) generiert. Somit ist der erste Teil der Seriennummer bei allen Zertifikaten einer Organisation identisch (während einer Gültigkeitsperiode der CA-Zertifikate). Damit ist es möglich, durch Eingabe der identischen Daten (Name, Vorname, e-Mail-Adresse) ein Duplikat eines Zertifikates herzustellen (vorausgesetzt die Wurzelzertifikate bleiben unverändert). Dem ist aber auch bei unbeabsichtigten Namens- und Datenübereinstimmungen Rechnung zu tragen! Dem so vorbereiteten Anwenderzertifikat wird der öffentliche Schlüssel des dritten Schlüsselpaares (gemeinsames Schlüsselpaar für alle Anwenderzertifikate) beigelegt, das im Zuge des Erststartes des Tools generiert wurde. Das Anwenderzertifikat wird unter Verwendung des privaten Schlüssels des CA-Zertifikates (E-MAIL CRYPT-CA) signiert. Damit ergibt sich eine Zertifikatskette wie unter 2.4 beispielhaft dargestellt.

Dabei stellt das „Musterbehörde [SELF SIGNED ROOT CERTIFICATE]“-Zertifikat das selbstsignierte Wurzelzertifikat dar. Das „Musterbehörde [E-MAIL CRYPT-CA]“-Zertifikat ist das eigentliche CA-Zertifikat, welches schlussendlich für die Ausstellung des Anwenderzertifikat „Sonja Musterfrau“ verwendet worden ist. Dieses Anwenderzertifikat wird als PKCS#12 Datei mit inkludiertem privaten Schlüssel abgespeichert. Um den Schlüssel in eine Anwendung importieren zu können, ist ein Passwort erforderlich, das beim Erzeugen der PKCS#12 Datei generiert wird. Dieses 8-stellige Passwort wird während der Zertifikatsgenerierung unter Verwendung eines *Secure Pseudo Random Number Generator* errechnet und in eine Textdatei geschrieben. Sowohl das Zertifikat also auch die Passwortdatei werden in jenes Unterverzeichnis geschrieben, welches der beim Start der Erzeugung ausgewählten Gruppen entspricht. Darüberhinaus wird für jedes Zertifikat ein eigenes Unterverzeichnis angelegt. Der Name dieses Unterverzeichnisses entspricht der *e-Mail-Adresse* des Zertifikatsbesitzers (Verzeichnisname identisch mit e-Mail-Adresse ohne Domainnamen). Darin wird das Zertifikat in Form der PKCS#12-Datei (mit privatem Schlüssel - passwortgeschützt) und zusätzlich als PKCS#7-Datei (ohne privatem Schlüssel), sowie die Passwortdatei (Textdatei) abgelegt. Alle Dateien

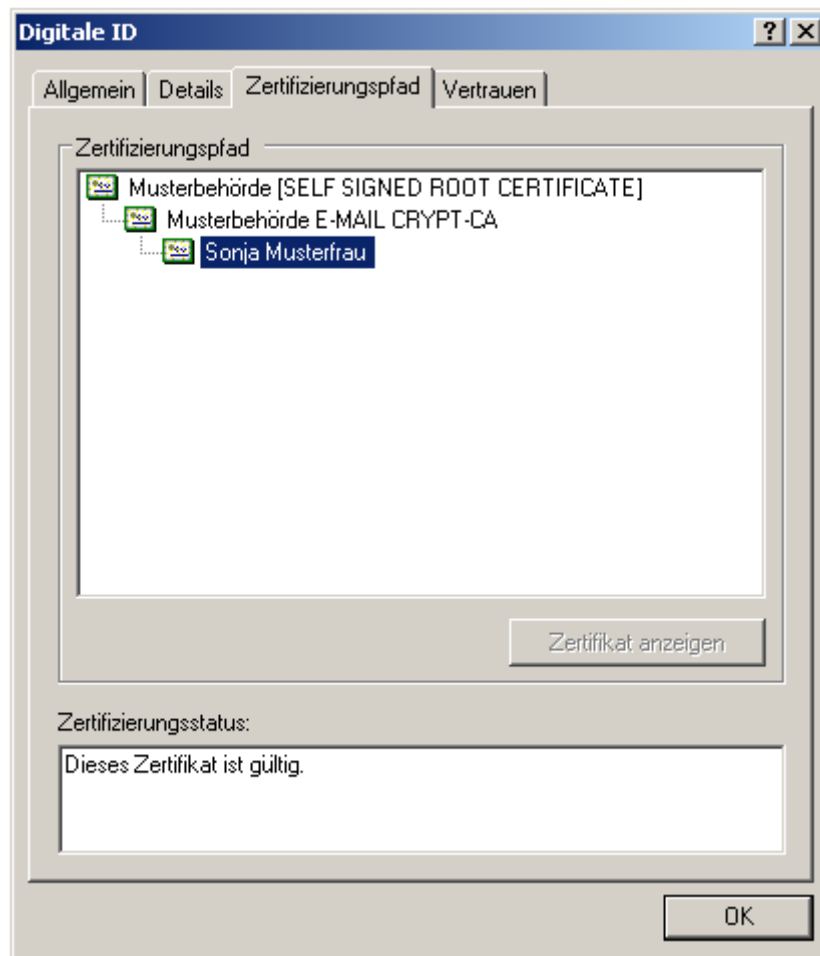


Abbildung 2.4: Beispielhafter Zertifizierungspfad

haben als Bezeichnung die *e-Mail-Adresse* des Zertifikatsbesitzers. Das Zertifikat hat je nach Format die Dateierweiterung `.p12` bzw. `.p7c`. Die Passwortdatei hat die Erweiterung `.pwd.txt`. Sollte bereits ein Unterverzeichnis und demnach ein Zertifikat gleichen Namens existieren, so wird der Anwender durch ein Dialogfenster darauf aufmerksam gemacht. Durch Abänderung der Eingabe, wobei im wesentlichen die e-Mail-Adresse manuell eingegeben werden soll, kann dieser Konflikt aufgelöst werden. Der Name des neuen Unterverzeichnisses sowie der Name der erzeugten Dateien ist demnach gleich der neuen, manuell eingegebenen e-Mail-Adresse.

Beispielsweise können sich folgende Verzeichnis- und Dateistrukturen ergeben:

- `\certs\mailcerts\Gruppe\sonja.musterfrau\`
  - `sonja.musterfrau.p7c`
  - `sonja.musterfrau.p12`



Die Gültigkeitsdauer der so generierten Anwenderzertifikate wird mit der maximal verbleibenden Gültigkeitsdauer der CA-Zertifikate festgelegt. Während der Erzeugung des Anwenderzertifikates sind alle Eingabefelder und Buttons des Standardpanels deaktiviert. Der Fortgang der Generierung kann anhand der Fortschrittsanzeige (Progress Bar) im rechten unteren Panel-Bereich verfolgt werden.

## Bedienung

Zur Bedienung stehen im Standardmodus (für Einzelzertifikate) folgende Möglichkeiten zur Verfügung:

- **Erzeuge**-Button ...startet die Erzeugung von Anwenderzertifikaten
- **Zurücksetzen**-Button ...löscht sämtliche Eingabefelder bzw. setzt sie zurück auf ihre ursprünglichen Werte
- **Exit**-Button ...beendet das Toolkit sofort
- **Expertenmodus**-Button ...wechselt in den sog. Expertenmodus mit erweiterten Funktionalitäten (siehe 2.2.3)

Weiters kann zwischen der Möglichkeit der automatischen Generierung der e-Mail-Adresse und einer manuellen Adressvorgabe gewählt werden. Dazu kann die „Generierung der e-Mail-Adresse“-Auswahl verwendet werden. Durch verändern der Auswahl auf „manuell“ kann die e-Mail-Adresse selbst vorgegeben werden. Durch das „in Gruppe“-Drop-Down-Menü kann die Gruppe und somit das zugehörige Unterverzeichnis ausgewählt werden, in welches das erzeugte Zertifikat gespeichert werden soll. Anfangs und nach Betätigen des **Zurücksetzen**-Buttons ist die Standard-Gruppe ausgewählt.

Im rechten oberen Eckbereich wird der Name der Organisation angezeigt, für die das CA-Toolkit initialisiert worden ist (zum Beispiel **Musterbehörde**). Zusätzlich wird, entsprechend der Angaben bei der Initialisierung, die Maildomäne der Organisation neben dem Textfeld der e-Mail-Adresse geführt (zum Beispiel **musteramt.gv.at**). Darüberhinaus gibt die Fortschrittsanzeige im rechten unteren Fensterbereich Auskunft über den aktuellen Fortschritt des Prozesses.

## Schrittweises Vorgehen:

1. Eingabe des Namen des Zertifikatsbesitzers. Dies wird bei Personen im Allgemeinen der Familiennamen sein. Es kann aber auch der Name einer Sub-Organisation bzw. einer Abteilung o.ä. sein. Die Eingabe des Namens ist unbedingt erforderlich.

2. Eingabe des Vornamens (optional). Wird das Zertifikat für keine Person sondern für eine Einrichtung (z.B. Abteilung) generiert, so ist ein Vorname nicht unbedingt sinnvoll und daher auch nicht zwingend notwendig. Es ergeben sich aber Unterschiede bei der automatischen Ableitung der e-Mail-Adresse.
3. Auswahl ob automatische Ableitung oder manuelle Vorgabe der e-Mail-Adresse gewünscht wird:
  - **automatisch:** Die e-Mail-Adresse wird als Kombination aus dem angegebenen Namen und dem optionalen Vornamen gebildet. Wurde nur der Name angegeben, so besteht die Adresse nur aus diesem (zum Beispiel `musterfrau@musteramt.gv.at`). Die zusätzliche Angabe eines Vornamens führt zur Adressbildung durch *vorname.name* (zum Beispiel `sonja.musterfrau@musteramt.gv.at`). Um eine Vorschau der automatischen e-Mail-Adresse zu erhalten, muss einmal auf den Auswahlknopf „automatisch“ gedrückt werden (bzw. ein Wechseln zwischen **automatisch** und **manuell** bewirkt ebenfalls eine Anzeige der automatisch erzeugbaren Adresse).
  - **manuell:** Die e-Mail-Adresse wird manuell angegeben. Dazu wird das Eingabefeld der e-Mail-Adresse aktiviert.

Bei beiden Möglichkeiten wird die resultierende Adresse auf Gültigkeit überprüft (gültige Zeichen)<sup>2</sup>. Bei eventuellen Unstimmigkeiten wird eine entsprechende Fehlermeldung angezeigt und ggf. eine korrigierte e-Mail-Adresse vorgeschlagen. Dabei erfolgt das Übersetzen von Umlauten (zum Beispiel ö auf oe) automatisch.

4. Durch die Gruppenauswahl wird festgelegt, in welches Unterverzeichnis das erzeugte Zertifikat gespeichert werden soll. Initial existiert nur die Gruppe **standard**. Weitere Gruppen können im Expertenmodus hinzugefügt bzw. bestehende Gruppen verändert werden. Ein neues Zertifikat einer gewählten Gruppe wird in das Unterverzeichnis gleichen Namens abgelegt (zum Beispiel: ausgewählt wurde Gruppe **standard**, so wird das Zertifikat unter `\usercerts\standard\sonja.musterfrau` gespeichert).
5. Die Betätigung des **Erzeuge**-Buttons startet die Erzeugung. Das Panel wird dabei deaktiviert. Bei erfolgreicher Zertifikaterzeugung wird eine kurze Bestätigung mittels Dialog angezeigt. Andernfalls erscheint eine Fehlermeldung.

Parallel zur direkten Ausgabe von Erfolgs- und Fehlermeldungen werden diese auch in einer Text-Datei mitprotokolliert. Die standardmäßige Protokolldatei befindet sich im Basisverzeichnis des CA-Toolkits. Der Name der Datei wird durch die `configuration.properties`-Datei festgelegt und lautet `Log.txt`. Der Name kann natürlich direkt in der Konfigurationsdatei verändert werden. Sie kann mit jedem beliebigen Text-Editor betrachtet werden. Abbildung 2.5 gibt einen Auszug einer beispielhaften Protokolldatei. Im Rahmen des Expertenmodus kann temporär, das heißt für die aktuelle Verwendung des CA-Toolkits, eine andere LOG-Datei ausgewählt werden.

---

<sup>2</sup>gemäß RFC1034 und RFC1035

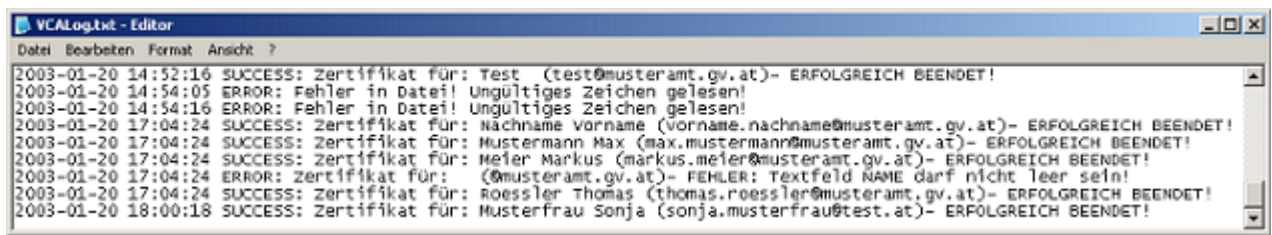


Abbildung 2.5: Auszug aus einer LOG-Datei

## 2.2.3 Expertenmodus

### Hintergrund

Der Expertenmodus ermöglicht einige erweiterte Einstellungen (LOG-Datei, Gruppeneinstellungen) sowie die Erzeugung von Massenzertifikaten basierend auf einer entsprechenden Input-Datei. Im wesentlichen bauen die Funktionalitäten des Expertenmodus auf jene des Standardmodus auf.

### Bedienung

Zur Bedienung stehen im Expertenmodus folgende Möglichkeiten zur Verfügung:

- Zurück-Button ... beendet den Expertenmodus und wechselt zurück zum Standardmodus
- Exit-Button ... beendet das CA-Toolkit sofort
- Dateiauswahl-Button ... öffnet ein Datei-Menü zur erleichterten Auswahl von Dateien (Input-Datei, LOG-Datei)

Darüberhinaus gibt es noch weitere funktionsabhängige Bedienungsmöglichkeiten, die nachfolgend im Detail beschrieben werden. Im rechten oberen Eckbereich wird der Name der Organisation angezeigt, für die das CA-Toolkit initialisiert worden ist (zum Beispiel Musterbehörde).

**Massenzertifikate** Dies ist wohl die interessanteste Zusatzmöglichkeit im Rahmen des Expertenmodus. Damit wird es möglich, eine Vielzahl von Zertifikaten auf einmal zu erzeugen. Das ist beispielsweise notwendig beim Generieren von Verschlüsselungszertifikaten für alle Mitarbeiter einer Behörde, da in diesem Falle wohl das wiederholte Erzeugen im Standardmodus zu langwierig wäre. Als Basis für diesen Prozess dient eine speziell zu formatierende Text-Datei, welche analog zum Standardmodus die Parameter aller Zertifikate beinhaltet (Name, Vorname, etc.). Wie schon aus der Beschreibung des Standardmodus bekannt, sind für jedes zu generierende Verschlüsselungszertifikat folgende Parameter erforderlich bzw. möglich:

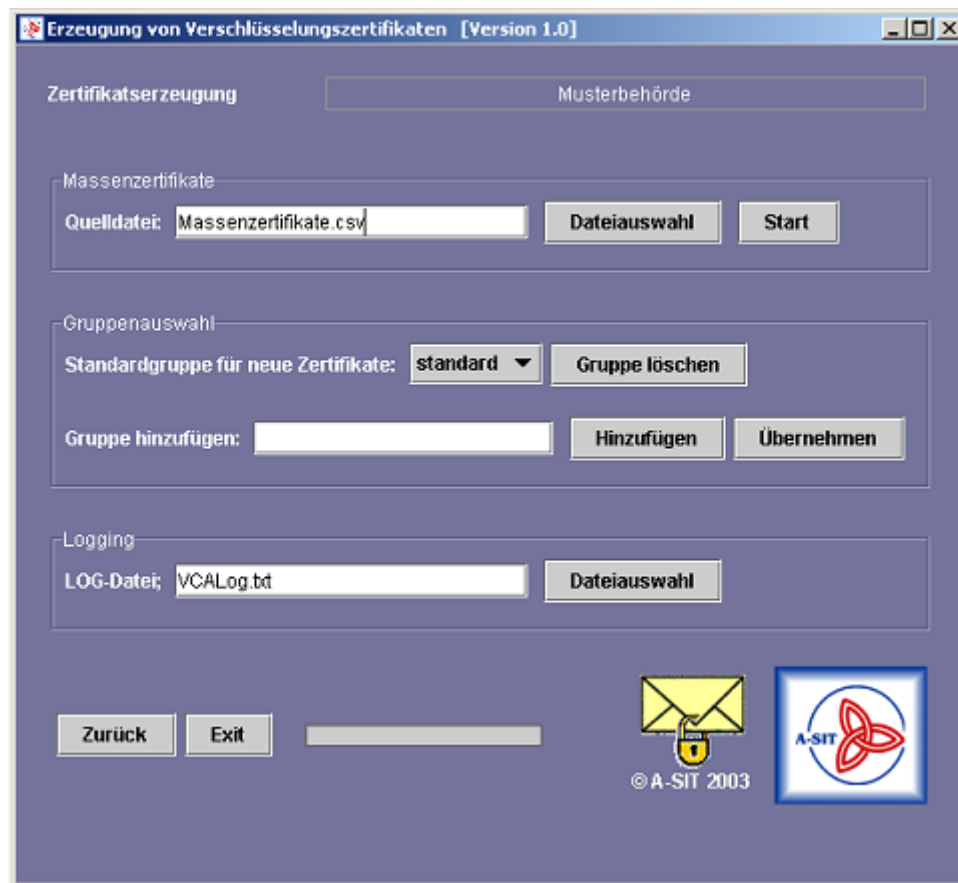


Abbildung 2.6: Expertenmodus

- Name ...unbedingt erforderlich
- Vorname ...optional
- e-Mail-Adresse ...optional
- Gruppe ...optional

Diese Parameter müssen demnach auch in der Input-Datei zu finden sein. Darüberhinaus besteht beim Generieren von Massenzertifikaten die Option ein Passwort für die Erzeugung eines e-Mail-Verschlüsselungszertifikates explizit vorzugeben. Dadurch wird es möglich, dass, beispielsweise im Zuge des Erneuerns von Zertifikaten, für eine Reihe von Mitarbeitern ihre alten Passwörter auch für die neuen Zertifikate verwendbar bleiben. Diese fünf Parameter, nämlich Name, Vorname, e-Mail-Adresse, Gruppe, Passwort, müssen für jedes einzelne Zertifikat angegeben werden. Dabei gibt es zwei unterschiedliche Formate von Input-Dateien, die derzeit unterstützt werden:

- eine Zeile pro Zertifikat und alle Parameter durch ';' getrennt

- eine Zeile pro Zertifikat und alle Parameter durch 'TAB' getrennt

Optionale Parameter, das sind alle außer der **Name**, können leer gelassen werden. Der Vorteil dieser beiden Formate ist, dass sie aus Excel-Tabellen (oder ähnlichem) standardmäßig generiert werden können. Bei Microsoft Excel gibt es die Möglichkeit, eine Tabelle als Text-Dokument entweder *Tabstopp-getrennt* oder *Trennzeichen-getrennt (CSV)* zu exportieren. Diese Beiden Formate sind als Input-Dateien zur Erzeugung von Massenzertifikaten geeignet. Abgesehen davon ist das Schreiben von derartigen Dateien unter Verwendung eines einfachen Text-Editors auch leicht möglich (hier wäre dann die Verwendung des ';' -Formates zu empfehlen). Abbildung 2.8 gibt ein Beispiel für eine Excel-Tabelle und der daraus erzeugten Input-Dateien. Zusätzlich können auch ganze Zeilen auskommentiert werden. Dies geschieht durch Einfügen des '%' -Zeichens am Zeilenanfang. Somit wird diese Zeile nicht als Vorgabe für ein neues Zertifikat gesehen, und erst der nächste Parametersatz wird dafür herangezogen. Ein '%' -Zeichen inmitten einer Zeile wird jedoch nicht als Kommentar interpretiert. Stattdessen kann es, je nach Position, als Zeichen selbst oder als falsche Eingabe ausgelegt werden (eine kompakte Definition des Dateiformates folgt im Anschluss).

Das Beispiel in Abbildung 2.7 demonstriert alle erlaubten Zeichen und das Einbinden von Kommentaren in einer gültigen Input-Datei. Man erkennt in diesem Beispiel auch, wie diese Input-Datei zeilenweise organisiert ist, und wie die optionalen Parameter auszulassen sind. Dabei ist zu beachten, dass trotzdem die erforderlichen Trennzeichen (';' oder 'TAB') notwendig sind. Wird keine e-Mail-Adresse bzw. kein Passwort angegeben, so werden diese, wie schon im Standardmodus beschrieben, automatisch angenommen. Wird das Gruppenfeld leer gelassen, so wird das betroffene Zertifikat in der Standard-Gruppe abgelegt. Werden hingegen Gruppennamen in der Input-Datei angegeben, die bislang noch nicht angelegt wurden, so werden diese in Form von Unterverzeichnissen neu angelegt.

### GÜLTIGES INPUT-DATEIFORMAT:

An dieser Stelle sei nochmals das geforderte Dateiformat für die Input-Datei zur Erzeugung von Massenzertifikaten hervorgehoben. Erlaubt sind generell nur folgende Zeichen: 'A'-'Z', 'a'-'z', '0'-'9', '-', '.', ' ', '!', ':'. Diese Einschränkung ist erforderlich, um treffsicher falsche Input-Dateien erkennen zu können. Zur Trennung der Parameter kann *entweder* ';' *oder* 'TAB' verwendet werden. Jede Zeile, beginnend ab der ersten Zeile, wird als Parametersatz interpretiert und führt grundsätzlich zur Generierung eines Zertifikates. Der Parametersatz wird mit einem Zeilenwechsel abgeschlossen, wobei die Trennzeichen für optionale Parameter nicht weggelassen werden dürfen. Wird eine Zeile mit '%' begonnen, so wird sie als Kommentar interpretiert und nicht als Vorgabe für ein neues Zertifikat herangezogen. Ein '%' -Zeichen innerhalb der Zeile wird aber *nicht* als Kommentar verstanden, sondern entweder als Zeichen genommen (z.B. im Namen-Feld) oder als falsches Zeichen (z.B. im

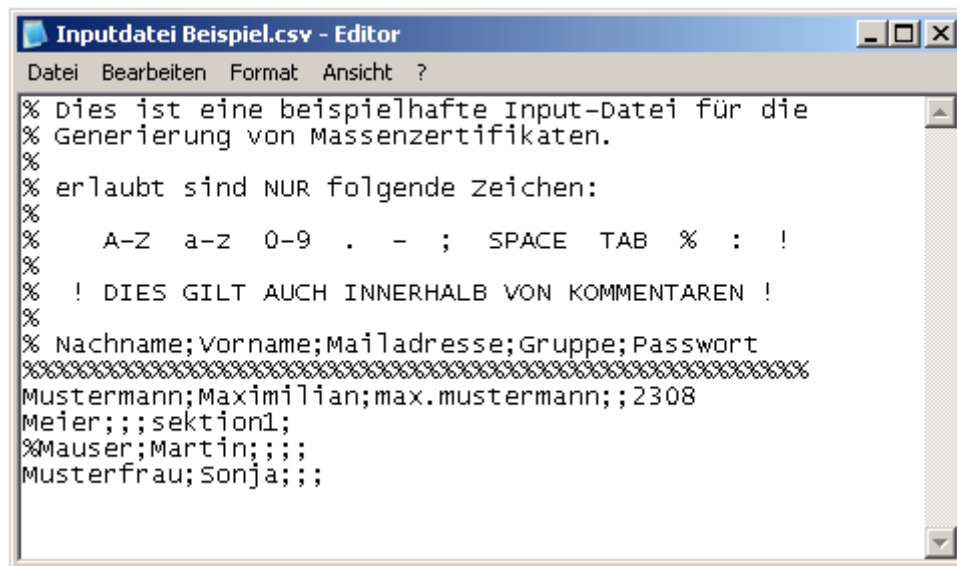


Abbildung 2.7: Gültige Input-Datei mit Kommentaren (;-Format)

Rahmen des e-Mail-Adressen- oder Gruppen-Feldes) interpretiert. Am Ende der Datei, das heißt nach dem letzten Parametersatz, darf nichts mehr angefügt werden (ausgenommen Kommentarzeilen o.ä.).

Der Generierungsprozess wird mit dem **Start**-Button ausgelöst. Alle Eingabefelder werden daraufhin deaktiviert, und die Fortschrittsanzeige dokumentiert den Verlauf des Prozesses. Sollte es sich um keine gültige Input-Datei handeln, so wird eine Fehlermeldung angezeigt. Ansonst werden alle anderen Fehlermeldungen, die während der Zertifikatserzeugung auftreten, unterdrückt und nur in der Protokolldatei vermerkt. Demnach erscheint auch kein Dialog bei etwaigen Namensgleichheiten und der damit verbundenen Gefahr des Überschreibens von Dateien. In diesem Fall wird das betreffende Zertifikat nicht weiter bearbeitet und stattdessen ein entsprechender Protokolleintrag vorgenommen. Dadurch wird die Massenerzeugung nicht aufgrund einzelner Fehler unterbrochen. Am Ende des Prozess erscheint ein Nachricht über die fehlerfreie Erzeugung aller Zertifikate bzw. eine Fehlermeldung, wenn zumindest ein Fehler aufgetreten ist. In Verbindung mit dieser Fehlermeldung erscheint auch ein Verweis auf die LOG-Datei.

**Gruppenauswahl** In diesem Teil des Expertenmodus können bestehende Gruppen gelöscht, neue Hinzugefügt und eine andere Standard-Gruppe festgelegt werden. Wie schon mehrfach erwähnt werden alle Zertifikate einer Gruppe in einem gemeinsamen Unterverzeichnis gesammelt. Die Gruppenauswahl hat keinerlei Einfluss auf den Inhalt der Verschlüsselungszertifikate.

- *Gruppe Löschen:* Die aktuell im Gruppen-Drop-Down-Menü ausgewählte Gruppe wird durch Betätigen des **Gruppe löschen**-Buttons gelöscht. Dabei wird nicht

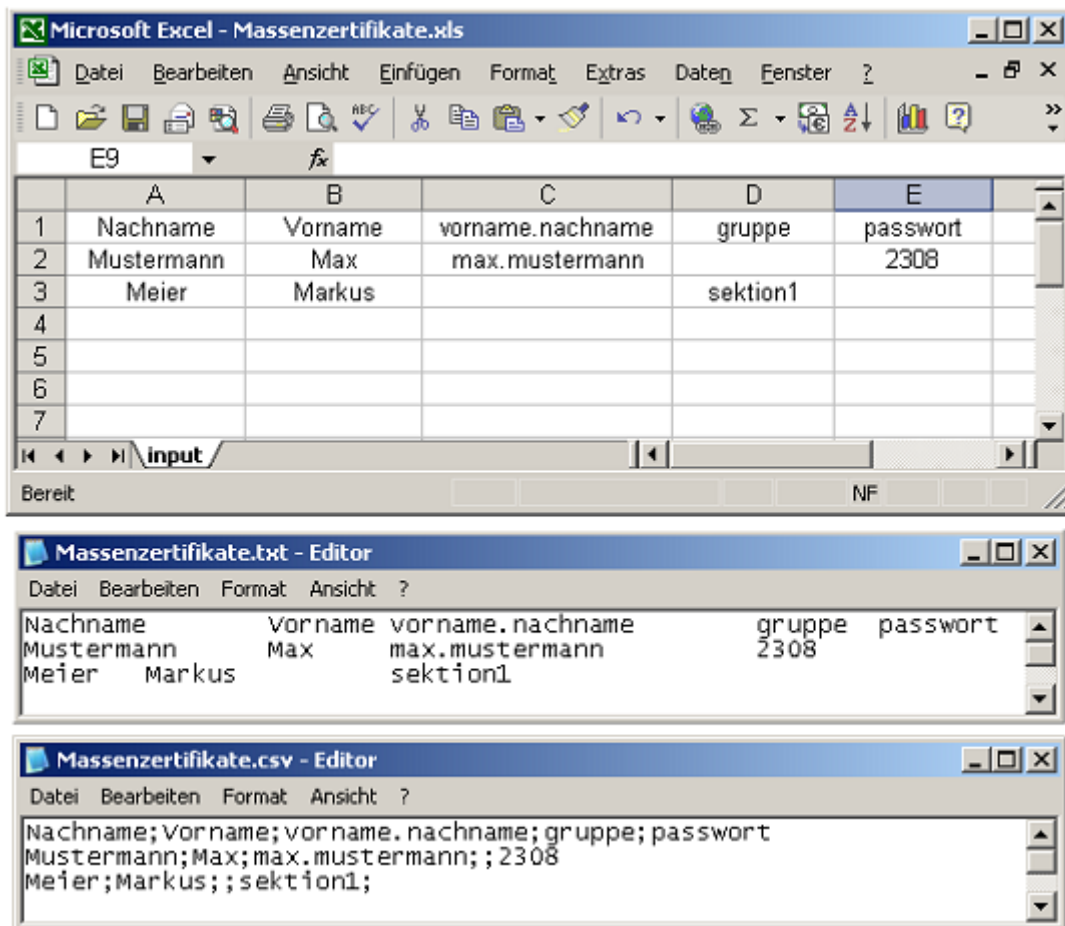


Abbildung 2.8: Excel-Tabelle und die mögliche Input-Dateien

das existierende gleichnamige Unterverzeichnis entfernt. Vielmehr wird der Eintrag der Gruppe aus der Gruppenauswahl gelöscht. Somit ist es nicht mehr möglich, beispielsweise im Standardmodus, Zertifikate für diese Gruppe auszustellen. Existiert nur mehr eine Gruppe, so kann diese nicht gelöscht werden (entsprechende Fehlermeldung macht darauf aufmerksam). Sie ist somit auch automatisch die Standard-Gruppe.

- *Gruppe hinzufügen:* Durch Eingabe eines neuen Gruppennamens im entsprechenden Textfeld und darauf folgender Betätigung des **Hinzufügen**-Buttons kann eine neue Gruppe in die Auswahl mit aufgenommen werden. Das gleichnamige Unterverzeichnis wird erst bei Bedarf, d.h. beim erstmaligen Erzeugen eines Zertifikates dieser Gruppe, angelegt.
- *Standardgruppe ändern:* Soll die Standardgruppe geändert werden, so muss die gewünschte Gruppe zuerst im Drop-Down-Menü ausgewählt werden. Durch Betätigen des **Übernehmen**-Buttons wird die ausgewählte Gruppe zur neuen

Standard-Gruppe und erscheint ab sofort als Erste in der Auswahl.

Alle Unterverzeichnisse der derart gewählten und eingerichteten Gruppen werden bei Bedarf im Verzeichnis `certs\mailcerts` angelegt (die Änderung des Standardverzeichnisses für e-Mail-Verschlüsselungszertifikaten ist in der `configuration.properties`-Datei möglich).

**LOG-Datei** Hier kann eine andere LOG-Datei ausgewählt werden. Standardmäßig wird die in der Konfigurationsdatei (`configuration.properties`) festgelegte Datei zur Mitprotokollierung verwendet. Temporär, das heißt für die Dauer einer Sitzung mit dem Toolkit, kann hier eine andere LOG-Datei ausgewählt werden. Durch den `Dateiauswahl`-Button wird dazu ein Auswahl-Dialog geöffnet. Dabei kann einerseits eine bestehende Datei selektiert oder im `Dateiname`-Eingabefeld des Auswahl-Dialoges eine noch nicht existierende Datei angegeben werden. Durch Betätigen des `Öffnen`-Buttons wird entweder diese neue Datei oder die existierende LOG-Datei ausgewählt und als aktuelle Protokolldatei festgelegt. Bei bereits existierenden Dateien wird am Ende der Datei das Protokollieren fortgesetzt. Noch nicht existierende Dateien werden bei Bedarf erzeugt. Nach dem Beenden und Neustarten des Tools wird allerdings wieder die in der Konfigurationsdatei angegebene LOG-Datei verwendet. Eine dauerhafte Änderung ist demnach nur durch Editieren der `configuration.properties`-Datei möglich. Die Idee hinter der Auswahl mehrerer verschiedener LOG-Dateien steht im Zusammenhang mit der Erzeugung von Massenzertifikaten, wobei für verschiedene Generierungsprozessen auch verschiedene LOG-Dateien (zugehörig zu den jeweilig Input-Dateien für die Massengenerierung) gewünscht sein können.



## 3 EFS-Anwenderzertifikaten

Dieses Modul des CA-Toolkits ermöglicht das Erzeugen von Anwenderzertifikaten zur Verwendung mit dem Encrypted File System (EFS). Im Wesentlichen sind die Abläufe im Hintergrund identisch mit denen bei der Komponente zur Erstellung von Verschlüsselungszertifikaten (siehe Kapitel 2). In diesem Kapitel werden demnach nur die Unterschiede näher beleuchtet.

Gestartet wird diese Komponente des CA-Toolkits durch die Startdatei „EFSCA start.bat“.

### 3.1 Erststart - Intialisierung

Wird das Toolkit zum ersten Mal gestartet, so muß eine Initialisierung erfolgen. Dies geschieht auf die selbe Weise wie schon unter Kapitel 2.1 beschrieben. Ein wesentlicher Unterschied ist, dass im Rahmen dieses Modules beim Erststart ein CA-Zertifikat für die Ausstellung von EFS-Zertifikaten generiert wird. Anstelle des E-MAIL CRYPT-CA-Zertifikates wird ein Zertifikat mit folgenden Einschränkungen erstellt:

Schlüsselverwendung:

- keyCertSign
- cRLSign
- nonRepudiation
- digitalSignature

Die Subjektinformationen werden wiederum aus den Werten der Eingabefelder des Initialisierungsfensters 3.1 angenommen:

Subjektinformationen:

- country: AT (fix)
- organization: *Name der Organisationseinheit + Adresse der Organisation*
- common name: *Name der Organisationseinheit + EFS-CA*

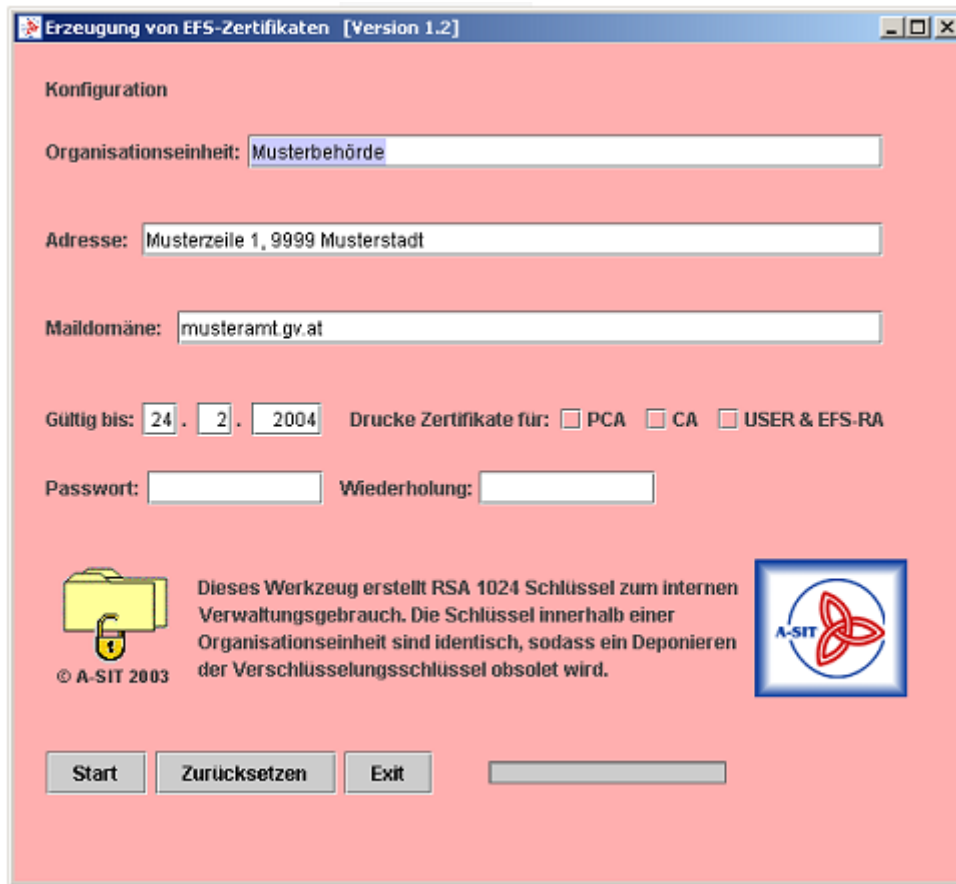


Abbildung 3.1: Konfigurationsfenster während der Initialisierungsphase - am Beispiel der Komponente für die EFS-Zertifikatserstellung

- Domain: *Maildomäne*

Dieses CA-Zertifikat wird unter Verwendung des selbstsignierten Wurzelzertifikates ausgestellt und in das Verzeichnis `certs/ca/` abgelegt (Verzeichnisname basierend auf den Vorgaben der `configuration.properties`-Datei). Der Name dieser Zertifikatsdatei entspricht dem Domain-Namen der Organisation bzw. Behörde. Um Verwechslungen mit den anderen CA-Zertifikaten zu vermeiden (etwa CA-Zertifikat der e-Mail-Verschlüsselungszertifikate) wird der Name um die Endung `.efsc` erweitert. Es werden zwei Dateien angelegt. Zum einen das Zertifikat im PKCS #7 Format (Endung `.p7c`) und zum anderen im DER-Format (Endung `.der`).

Beispielsweise: `..\cacerts\ca\musteramt.gv.at.efsc.p7c`). Ausserdem wird auch für dieses Modul im Zuge der Initialisierung ein allen EFS-Zertifikaten gemeinsames Schlüsselpaar erzeugt, welches als PKCS #12 Datei im `initialization`-Verzeichnis des CA-Toolkits abgelegt wird (`..\initialization\musteramt.gv.at.efssusr.p12`).

Beim Erststart dieses Modules wird zusätzlich zum CA-Zertifikat noch ein weiteres Zertifikat erzeugt, das in Windows für den sogenannten *EFS Recovery Agent* benötigt wird.

Mit Hilfe dieses Agent und des zugehörigen Zertifikates können verschlüsselte Daten auch ohne dem ursprünglichen, zur Verschlüsselung verwendeten, EFS-Zertifikat wieder entschlüsselt werden (für nähere Details dazu - siehe Microsoft Windows Dokumentation). Die Subjektinformationen und die Schlüsselinformationen werden dafür wie folgt festgelegt:

Subjektinformationen:

- **country:** AT (fix)
- **organization:** *Name der Organisationseinheit + Adresse der Organisation*
- **organization unit:** EFS File Encryption Certificate
- **common name:** EFS Recovery Agent
- **locality:** EFS

Schlüsselverwendung:

- **keyEncipherment**
- **dataEncipherment**
- **1.3.6.1.4.1.311.10.3.4.1** (Enhanced Key Usage)

Dieses EFS Recovery Agent Zertifikat wird in das Verzeichnis der EFS-Anwenderzertifikate (Festlegung in der `configuration.properties` Datei) sowohl im DER-Format also auch im PKCS #12 und #7-Format geschrieben. Um dieses Zertifikat nicht mit anderen EFS-Anwenderzertifikaten zu verwechseln, wird es mit der Endung `.efsRA` versehen (zum Beispiel: `..\efscerts\EFS Recovery Agent\musteramt.gv.at.efsRA.der`).

### 3.1.1 Bedienung

Die Bedienung des Initialisierungsfenster ist identisch wie im Kapitel 2.1.2 beschrieben. Einzig die Darstellung der generierten Wurzel- und CA-Zertifikate bezieht sich natürlich auf das EFS-CA-Zertifikat. Ebenso beziehen sich die darstellbaren Schlüsselinformationen für die Anwenderzertifikate auf das allen EFS-Anwenderzertifikaten gemeinsame Schlüsselpaar (Checkbox **USER & EFS-RA**). In diesem Zuge werden auch die Details des Zertifikates für den *EFS Recovery Agent* angezeigt, um diese aus Sicherheitsgründen ausdrucken zu können.

## 3.2 Generierung von EFS - Anwenderzertifikaten

Auch die Erzeugung von EFS-Anwenderzertifikaten erfolgt analog, wie es schon unter 2.2 beschrieben worden ist. Wurde das CA-Toolkit zwar schon initialisiert jedoch die

EFS-Komponente noch nie zuvor gestartet, so erfolgt auch in diesem Fall eine Nachinitialisierung, währenddessen das EFS-CA Zertifikat, das EFS-RA Zertifikat und das allen EFS-Anwenderzertifikaten gemeinsame Schlüsselpaar erzeugt wird. Dies erfolgt weitestgehend im Hintergrund. Lediglich eine Abfrage über eine optionale Darstellung und Ausgabe der soeben generierten Zertifikats- und Schlüsselinformationen macht den Anwender darauf aufmerksam.

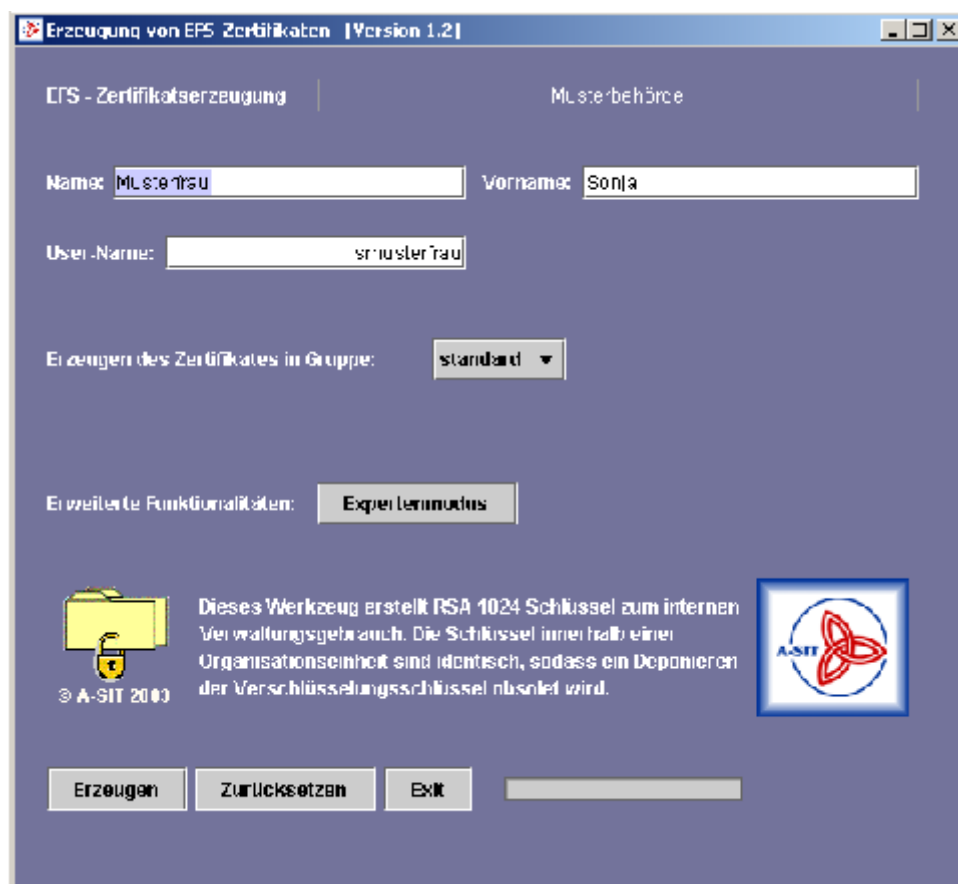


Abbildung 3.2: Standardfenster für die Erzeugung von EFS-Anwenderzertifikaten (Einzelzertifikate)

Die damit erstellbaren EFS-Anwenderzertifikate haben folgende Subjekt- und Schlüssel-daten:

Subjektinformationen:

- country: AT (fix)
- organization: *Name der Organisationseinheit + Adresse der Organisation*
- organization unit: EFS File Encryption Certificate

- **common name:** *User-Name*
- **locality:** EFS
- **given name:** *Vorname + Nachname*

Schlüsselverwendung:

- 1.3.6.1.4.1.311.10.3.4 (Enhanced Key Usage)

Die so erstellten Zertifikate werden in das Verzeichnis der EFS-Anwenderzertifikate geschrieben, das in der `configuration.properties` Datei festgelegt wird. Der Name des jeweiligen Unterverzeichnisses ist gleich dem User-Namen, welcher als Vorgabe zur Erzeugung des Zertifikates angegeben wurde. Auch das Zertifikat selbst wird so benannt. Einerseits wird das EFS-Anwenderzertifikat im PKCS #12-Format gespeichert (Endung `.p12`), wobei das zugehörige Random-Passwort in der gleichnamigen Datei mit der Endung `.pwd.txt` abgelegt wird. Ausserdem wird das EFS-Zertifikat ohne privatem Schlüssel als PKCS #7-Datei (Endung `.p7c`) zur Verfügung gestellt (zum Beispiel `..\efscerts\smusterfrau\smusterfrau.p12`). Abbildung 3.3 zeigt eine beispielhafte Zertifikatskette, die hinter einem solchen EFS-Anwenderzertifikat steht. Das selbstsignierte Wurzelzertifikat ist dabei allen Zertifikaten des CA-Toolkits gemeinsam.

### 3.2.1 Bedienung

Die Handhabung des Modules zur Erzeugung von EFS-Anwenderzertifikaten ist identisch wie in Kapitel 2.2.2 beschrieben. Zur Bedienung stehen im Standardmodus (für Einzelzertifikate) folgende Möglichkeiten zur Verfügung (siehe Abb. 3.2):

- **Erzeuge-Button** ... startet die Erzeugung von Anwenderzertifikaten
- **Zurücksetzen-Button** ... löscht sämtliche Eingabefelder bzw. setzt sie zurück auf ihre ursprünglichen Werte
- **Exit-Button** ... beendet das Toolkit sofort
- **Expertenmodus-Button** ... wechselt in den sog. Expertenmodus mit erweiterten Funktionalitäten (siehe 2.2.3)

Das Standardfenster erfordert dabei folgende Angaben:

- **Name**
- **Vorname** (optional)
- **User-Name**
- **Gruppe** (optional)

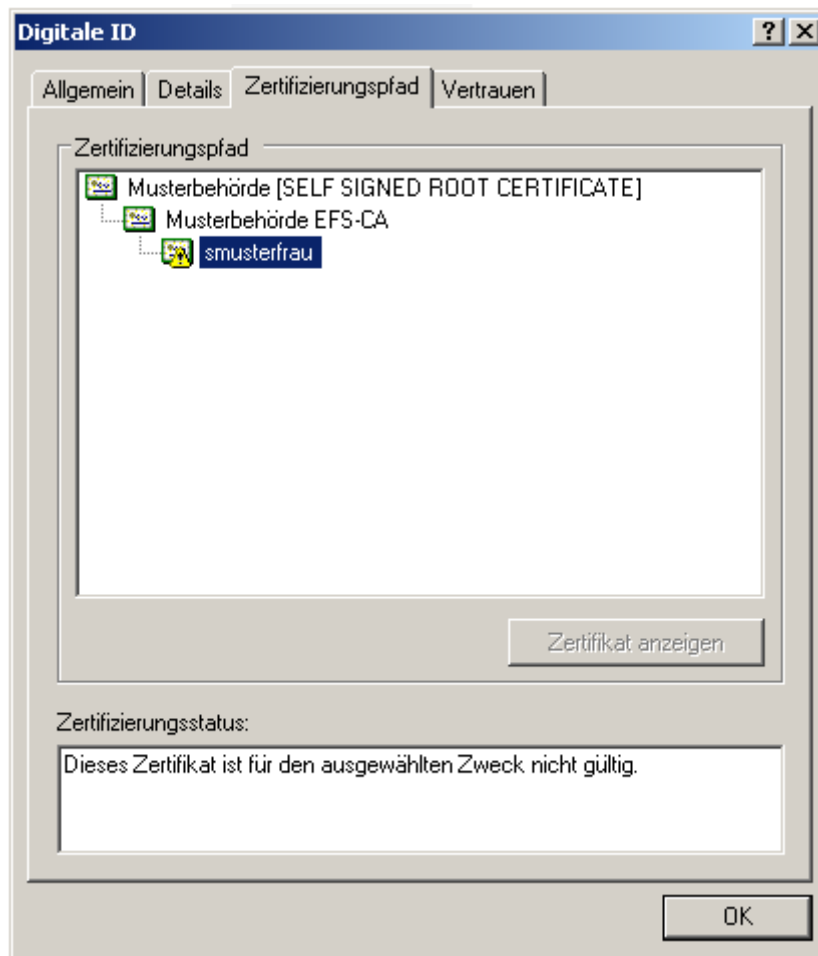


Abbildung 3.3: Beispielhafte Zertifikatskette eines EFS-Anwenderzertifikaten

Alle diese Eingaben werden auf unzulässige Zeichen hin geprüft. Weiters werden bei allfällig resultierenden Namensgleichheiten, speziell hinsichtlich der anzulegenden Unterzeichnisse, Warnungen in Form von Fehlermeldungen ausgegeben. Sind die Vorgaben vollständig und zulässig, so kann durch den **Erzeuge**-Button die Generierung gestartet werden. Ein kurzer Dialog gibt Aufschluß über den Erfolg der Zertifikatserzeugung.

Die Beschreibung der zusätzlichen Möglichkeiten, wie beispielsweise die Auswahl von Gruppen und Gruppenverzeichnissen, ist dem Kapitel 2.2.2 zu entnehmen.

### 3.2.2 Expertenmodus

Auch die Komponente zum Erstellen von EFS-Zertifikaten bietet einen Expertenmodus, mit dessen Hilfe Massenzertifikate erstellt und Gruppen- bzw. LOG-Datei-Einstellungen vorgenommen werden können. All diese Tätigkeiten laufen vollkommen gleich ab, wie bereits in den Kapiteln zur Erzeugung von e-Mail-Verschlüsselungszertifikaten beschrieben

(siehe Kapitel 2.2.3). Außer bei dem Verfassen von Inputdateien zur Massengenerierung müssen die Felder den benötigten Vorgabewerten angepaßt werden.

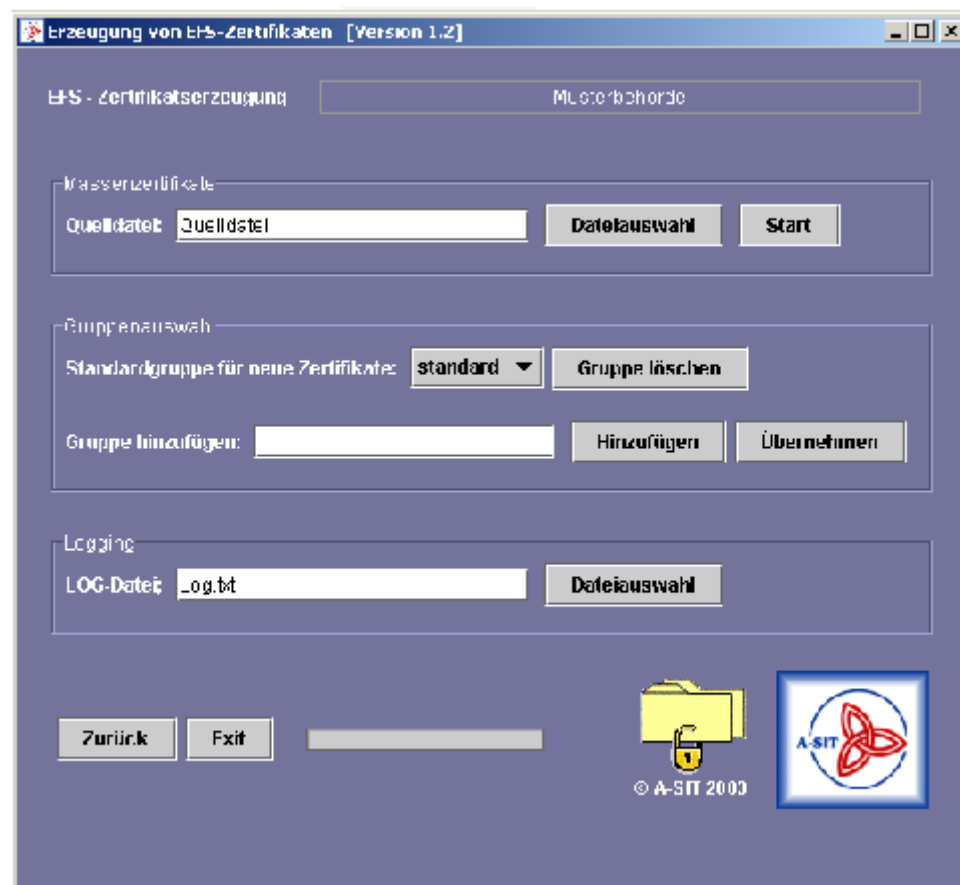


Abbildung 3.4: Expertenmodus beim Erstellen von EFS-Anwenderzertifikaten

**Massenzertifikate** Generell gelten die selben Regeln für den Aufbau der Input-Dateien, wie in Abschnitt 2.2.3 definiert. Jedoch müssen hier für jedes zu erstellende EFS-Zertifikat folgende Parameter vorgegeben werden:

- Name ... unbedingt erforderlich
- Vorname ... optional
- User-Name ... unbedingt erforderlich
- Gruppe ... optional
- Passwort ... optional

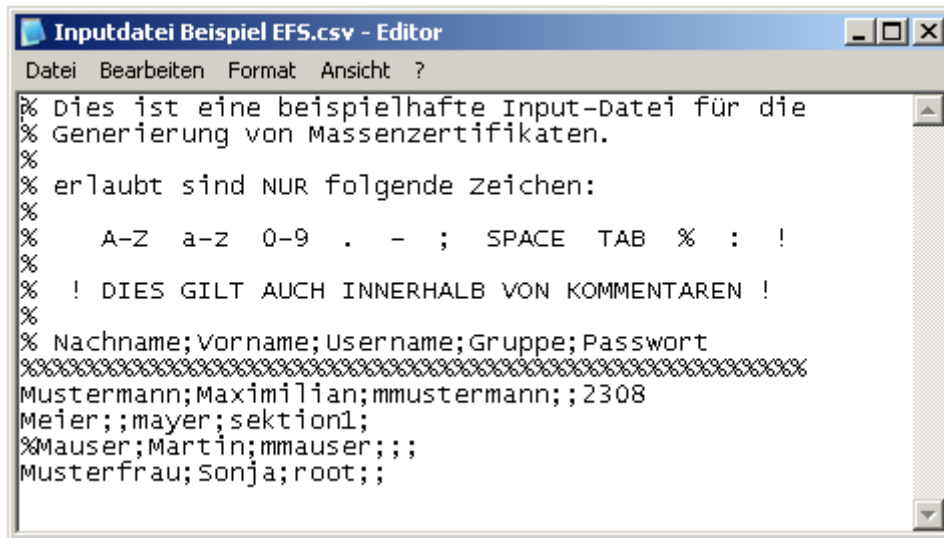


Abbildung 3.5: Beispielhafte Input-Datei zur Erzeugung von EFS-Zertifikaten

Darüberhinaus gibt es keinen Unterschied. Abbildung 3.5 gibt ein beispielhafte Input-Datei zur Generierung von EFS-Anwenderzertifikaten. Auch hier sind Kommentare zulässig.

### GÜLTIGES INPUT-DATEIFORMAT:

An dieser Stelle sei nochmals das geforderte Dateiformat für die Input-Datei zur Erzeugung von Massenzertifikaten hervorgehoben. Erlaubt sind generell nur folgende Zeichen: 'A'-'Z', 'a'-'z', '0'-'9', '-', '.', '!', ':', ';', ' ', 'TAB'. Diese Einschränkung ist erforderlich, um treffsicher falsche Input-Dateien erkennen zu können. Zur Trennung der Parameter kann *entweder* ';' *oder* 'TAB' verwendet werden. Jede Zeile, beginnend ab der ersten Zeile, wird als Parametersatz interpretiert und führt grundsätzlich zur Generierung eines Zertifikates. Der Parametersatz wird mit einem Zeilenwechsel abgeschlossen, wobei die Trennzeichen für optionale Parameter nicht weggelassen werden dürfen. Wird eine Zeile mit '%' begonnen, so wird sie als Kommentar interpretiert und nicht als Vorgabe für ein neues Zertifikat herangezogen. Ein '%'-Zeichen innerhalb der Zeile wird aber *nicht* als Kommentar verstanden, sondern entweder als Zeichen genommen (z.B. im Namen-Feld) oder als falsches Zeichen (z.B. im Rahmen des User-Namen- oder Gruppen-Feldes) interpretiert. Am Ende der Datei, das heißt nach dem letzten Parametersatz, darf nichts mehr angefügt werden (ausgenommen Kommentarzeilen o.ä.).

**Gruppenauswahl, LOG-Datei** Die Beschreibung dieser Elemente ist bitte vollständig dem vorhergegangenen Kapitel 2.2.3 zu entnehmen.