
Bedienungsanleitung

Fremd-bPK-CA

Dipl.-Ing. Mario Ivkovic

Graz, am 24. November 2006

Inhaltsverzeichnis:

1	Allgemeines.....	2
2	Initialisierung	2
3	Zertifikatserzeugung.....	4

Abbildungsverzeichnis:

Abb. 2.1: Initialisierung.....	2
Abb. 2.2: Ausdruck vom PCA-Zertifikat.....	3
Abb. 2.3: Ausdruck vom CA-Zertifikat	4
Abb. 2.4: Passwort-Dialog.....	4
Abb. 3.1: Zertifikatserzeugung	5
Abb. 3.2: E-Gov-BerAbgrV	6
Abb. 3.3: Ausdruck vom erzeugten Fremd-bPK-Zertifikat.....	6
Abb. 3.4: Zertifikatserstellungs-Information.....	7
Abb. 3.5: Zertifikatsversand	7

1 Allgemeines

Das hier beschriebene Werkzeug, *Fremd-bPK-CA Tool*, dient zum Erstellen von Zertifikaten, mit denen Fremd-bPKs verschlüsselt werden. Diese Dokumentation setzt ein grundsätzliches Verständnis von *bereichsspezifischen Personen-Kennzeichen* und Zertifikaten voraus.

Wenn das Tool das erste Mal nach der Installation gestartet wird, muss dieses einmalig initialisiert werden, bevor damit Zertifikate erstellt werden können. Dieser Initialisierungs-Prozeß wird im nächsten Abschnitt beschrieben.

2 Initialisierung

Abb. 2.1 zeigt die Eingabemaske mit den jeweiligen Feldern zur Initialisierung des CA-Tools. Die Felder „VKZ“, „Organisation“ und „Gültig bis“ müssen ausgefüllt werden, um eine Initialisierung durchführen zu können. Das Feld „Gültig bis“, welches die Gültigkeitsdauer des Wurzel- und des Intermediate-Zertifikates kennzeichnet, wird standardmäßig auf den gegenwärtigen Tag in 5 Jahren vor-ausgefüllt, und sollte nur im Sonderfall geändert werden. Das Feld „Organisationseinheit“ kann je nach Bedarf ausgefüllt oder leer gelassen werden.

Mit den beiden Feldern „Passwort“ und „Wiederholung“ wird jenes Passwort festgelegt, mit dem die beiden bei der Initialisierung erstellten CA-Zertifikate mit den dazugehörigen privaten Schlüsseln, in einem PKCS#12 File verschlüsselt werden.

Erzeugung von Verschlüsselungszertifikaten für Fremd-pBKs v1.1

Initialisierung

VKZ: BKA

Organisation: Bundeskanzleramt

Organisationseinheit:

Gültig bis: 23 . 11 . 2011

Passwort: ***** Wiederholung: *****

Dieses Werkzeug erstellt Zertifikate mit denen Fremd-bPKs verschlüsselt werden.

A-SIT

Start Zurücksetzen Exit

Abb. 2.1: Initialisierung

Wenn alle benötigten Felder korrekt ausgefüllt sind, wird mit dem Start-Button der Initialisierungsprozeß angestoßen. Dabei wird ein Wurzel-Zertifikat, auch PCA-Zertifikat genannt, und ein Intermediate-Zertifikat, im weiteren CA-Zertifikat genannt, erstellt und sowohl als PKCS#12-Dateien mit privaten Schlüsseln und als PKCS#7-Dateien gespeichert. Die beiden PKCS#12-Dateien werden ausgehend vom Installationsverzeichnis, im „initialization“ Unterverzeichnis abgelegt. Die beiden PKCS#7-Dateien (enthalten nur die Zertifikate ohne private Schlüssel) werden wiederum ausgehend vom Installationsverzeichnis im „cert/cacerts“ Unterverzeichnis gespeichert.

Die beiden Abbildungen, Abb. 2.2 und Abb. 2.3, zeigen die beiden Dialogfenster welche nach der oben beschriebenen Erstellung der beiden Zertifikate erscheinen und die Details des jeweiligen Zertifikates und des dazugehörigen privaten Schlüssels enthalten. Mit Hilfe dieser beiden Dialoge können diese Details ausgedruckt werden und für den Fall eines Verlustes der privaten Schlüssel oder der Zertifikate, für eine spätere Zertifikats- und Schlüsselrekonstruktion genutzt werden. Diese Ausdrücke müssen unbedingt an einem sicheren Ort geheim aufbewahrt werden.

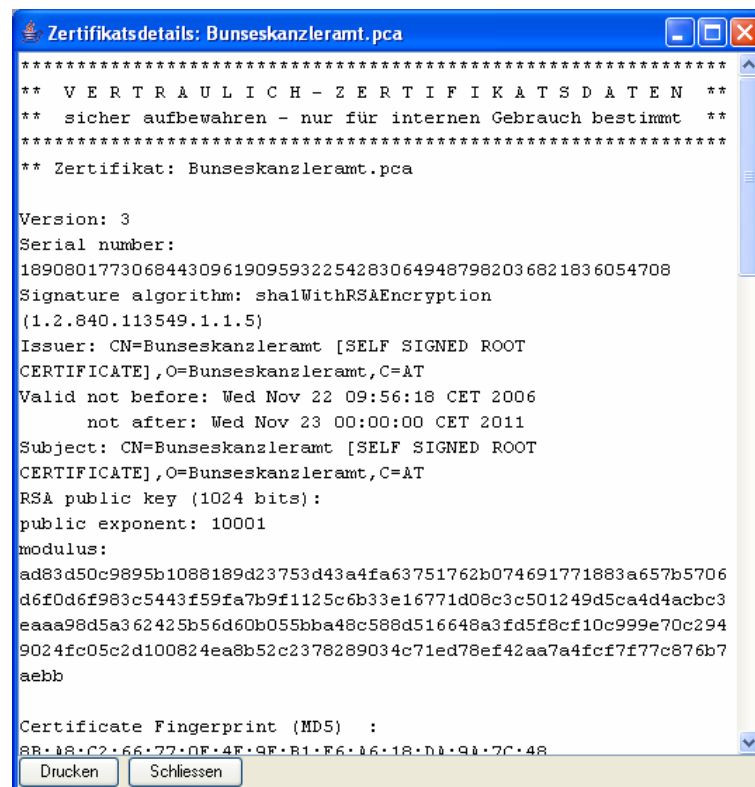


Abb. 2.2: Ausdruck vom PCA-Zertifikat

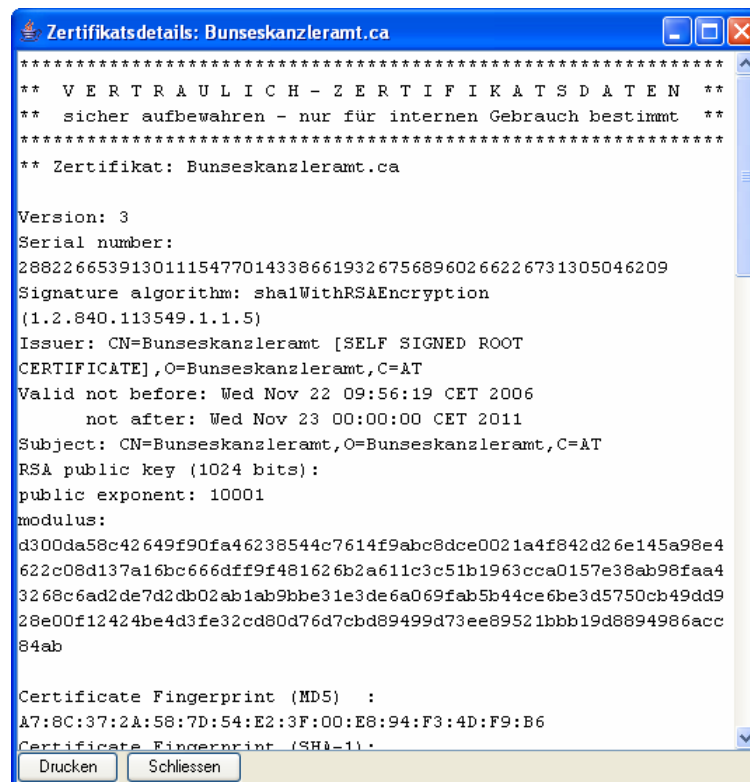


Abb. 2.3: Ausdruck vom CA-Zertifikat

Nach erfolgreicher Initialisierung erscheint der in Abb. 2.4 gezeigte Passwort-Dialog. Hier muss das während der Initialisierung festgelegte Passwort eingegeben werden. Mit Hilfe dieses Passwortes werden die beiden verschlüsselten PKCS#12-Dateien entschlüsselt und das Tool für die Zertifikatserzeugung entsprechend initialisiert.

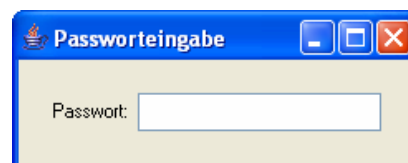


Abb. 2.4: Passwort-Dialog

3 Zertifikatserzeugung

Wenn das bereits initialisierte Tool gestartet wird, erscheint zu Beginn stets der im vorigen Abschnitt beschriebene Passwort-Dialog. Nach Eingabe des Passwortes und einer Bestätigung durch drücken der Enter-Taste lädt das Tool die benötigten privaten Schlüssel und ist für die Zertifikatserzeugung bereit.

Abb. 3.1 zeigt die Eingabemaske welche für die Zertifikatserzeugung genutzt wird. Das Feld „VKZ“ ist mit dem während der erstmaligen Initialisierung angegebenen Wert vorgegeben und kann bzw. muss nicht mehr manuell eingetippt werden. Das Feld „Bereich“ gibt den Bereich an für den das Zertifikat ausgestellt werden soll. Unter diesem Feld befindet sich ein Button mit dem die E-

Government-Bereichsabgrenzungsverordnung (Abb. 3.2) eingesehen und so der entsprechende Bereich ausgesucht werden kann.

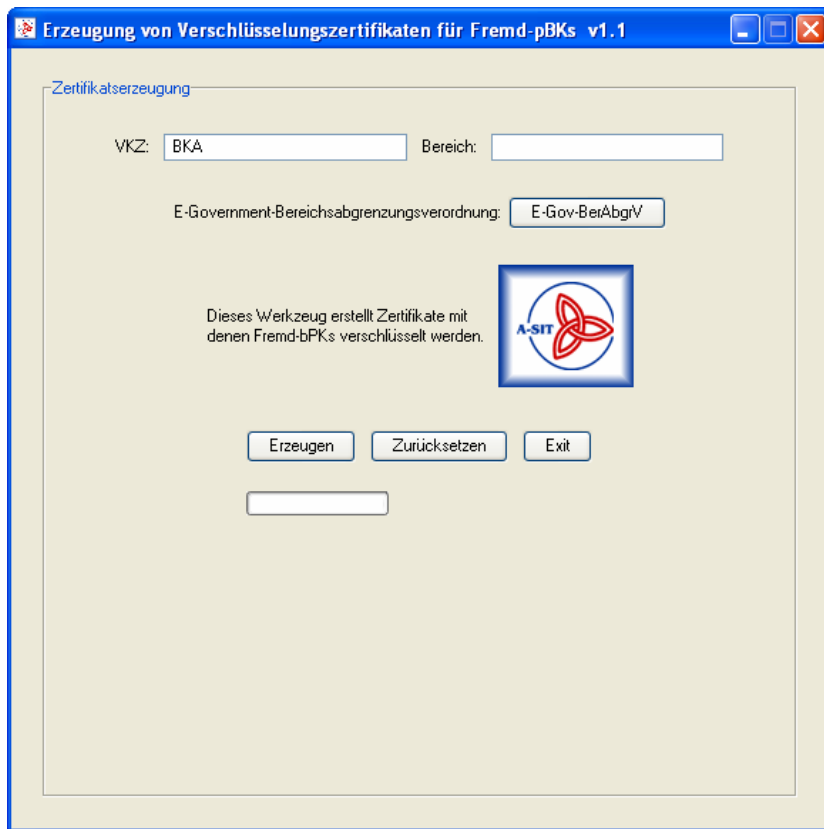


Abb. 3.1: Zertifikatserzeugung

Wenn ein Bereich eingegeben wurde, dieser kann im spezial Fall auch leer gelassen werden, wird durch drücken des „Erzeugen-Button“ ein neues Zertifikat erstellt und es erscheinen ein Dialogfenster. Dieses Fenster (Abb. 3.4) zeigt, dass die Zertifikatserstellung erfolgreich war und wo das erzeugte Zertifikat im Dateisystem abgelegt wurde. Wenn dieser Dialog bestätigt wurde erscheinen ein weiteres Dialog-Fenster und eine neue Eingabemaske. Dieses Dialog-Fenster zeigt, wie bei der Erzeugung der CA-Zertifikate während der Initialisierung, die Details zum Zertifikat (Abb. 3.3). Diese Details sollten ausgedruckt und sicher verwahrt werden, damit, für den Fall eines Verlustes des Zertifikates, dieses wieder rekonstruiert werden kann.

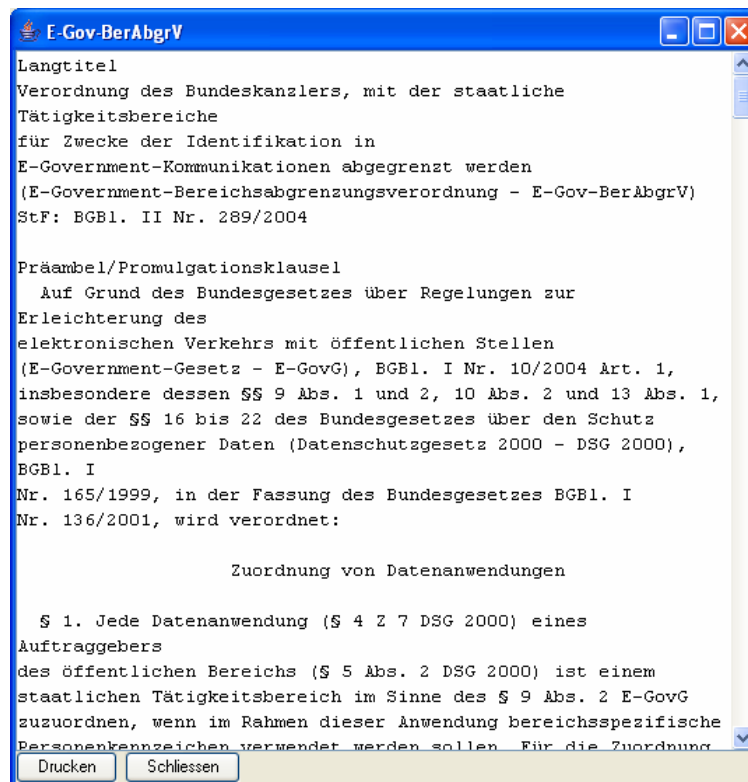


Abb. 3.2: E-Gov-BerAbgrV

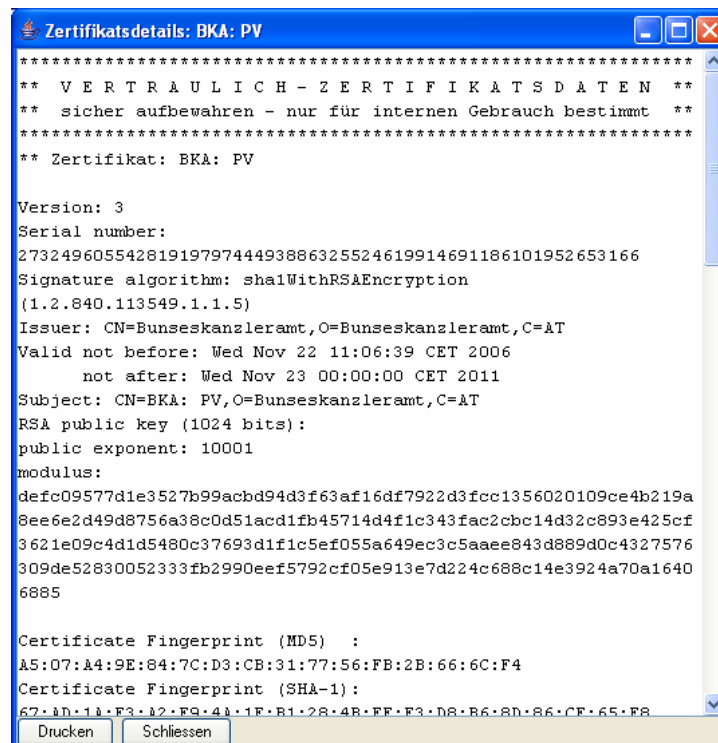


Abb. 3.3: Ausdruck vom erzeugten Fremd-bPK-Zertifikat

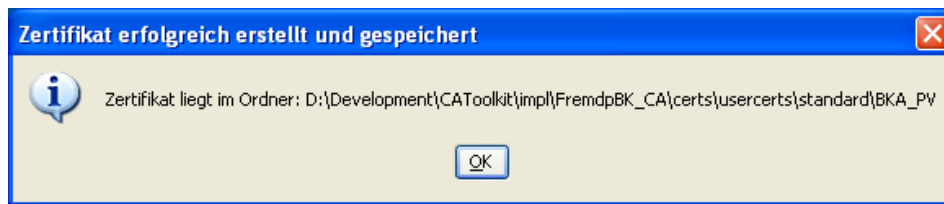


Abb. 3.4: Zertifikatserstellungs-Information

Die Eingabemaske (Abb. 3.5) dient zum automatischen E-Mail-Versand des gerade erstellten Zertifikates. Die angezeigten Felder müssen nur einmalig ausgefüllt werden und werden nach dem Versand gespeichert und für die zukünftigen Zertifikatserstellungen automatisch wieder geladen.

Falls keine E-Mail versendet werden soll, kann dies durch drücken des „Überspringen“ Button erreicht werden.

In das Feld „Server“ muss der E-Mail-Server eingetragen werden der zum Versenden verwendet werden soll. Wenn dieser Server nicht bekannt ist, sollte der System-Administrator kontaktiert werden. Gleiches gilt für das Feld „Port“, welches aber in der Regel auf 25 belassen werden kann. In das Feld „From“ muß die E-Mail-Adresse des Absenders eingetragen werden.

Abb. 3.5: Zertifikatsversand

Die Felder „Subject“ und „Message“ werden automatisch ausgefüllt, können aber selbstverständlich entsprechend angepaßt werden.

Wenn alle Felder ausgefüllt wurden, wird die E-Mail durch drücken von „E-Mail versenden“ generiert und abgeschickt. Dieser E-Mail wird das erzeugte Zertifikat automatisch angehängt.