Intevation GmbH

i-mpuls JMD

Web-Anwendungs-Server für computergestützte Fallakten

Anleitung Gruppenzertifikat

Stand: Version 1.0, 09.10.2013

Bundesministerium für Familie, Senioren, Frauen und Jugend

JUGEND STÄRKEN

JMD JUGEND MIGRATIONSDIENST

Projektbezeichnung	mpuls	
Projektleiter (AG)	Frank Tönnissen, Dr. Olga Burkova (PT-DLR, Bonn)	
Projektleiter (AN)	Frank Koormann (Intevation)	
Verantwortlich	Frank Koormann, Katharina Schütze Intevation GmbH, Neuer Graben 17, 49074 Osnabrück	
Erstellt am	04.12.2008	
Zuletzt geändert	09.10.2013	
Bearbeitungszustand		in Bearbeitung
		vorgelegt
	X	fertig gestellt
Dokumentablage	mpuls_Gruppenzertifikate_JMD.odt	

Änderungsverzeichnis

Änderung			Geänderte Kapitel	Beschreibung der Änderung	Autor	Zustand
Nr.	Datum	Version				
1	04.12.08	0	Alle	Initiale Produkterstellung, abgeleitet von WASKA Gruppen-zertifikate	Koormann	i.B.
2	04.12.08	0	7	Überblick über Zertifkatsantrag	Koormann	i.B.
3	14.7.09			Grafik zum Prozess eingefügt	Ks	i.B.
4	2.11.09		Alle	Logo/Achtung-Zeichen ange-passt	ks	
5	08.07.10		Alle	Ergänzung von Hinweisen zum Verfahren (Fristen, Speicherung)	Koormann	i.B.
6	20.10.10	1.0	Alle	Screenshots aktualisiert, Mini-mal-Korrekturen	ks	i.B.
7	27.10.10		0	Aktualisuerung der Dokumenten-information	Koormann	vorgelegt
8	01.11.10				Tönnissen	freigegeben
9	10.11.10		3.1	Austausch Bildschirmfoto der An-tragstellung auf Bitte Trustcenter	Koormann	
10	26.11.10		3.1	Verweis auf Dokument „Tipps und Tricks“ der Citkomm	Koormann	
11	07.06.12		Alle	Allgemeine Überarbeitung, Er-weiterungen Erstinstallation und FAQ	bg	i.B.
12	21.06.12		2,2, 4,1	Ergänzung Zertifikats-Policy	bg	freigegeben
13	26.08.13		3.3.1	Layoutkorrektur	bg	freigegeben
14	09.10.13		4	Aktualisierung FF	bg	i.B.

Inhaltsverzeichnis

Abkürzungen:

BSI	Bundesamt für Sicherheit in der Informationstechnik
CA	Certification Authority, auch Trustcenter oder Zertifizierungsstelle
CP	Certificate Policy
ggf.	gegebenenfalls
IE	Internet Explorer
Citkomm	Kommunale Datenverarbeitungs-Zentrale Citkomm, Betreiber der für mpuls eingesetzten CA unter der V-PKI.
PKI	Public Key Infrastruktur, ein System zur Ausstellung, Verteilung und Prüfung digitaler Zertifikate. JMD nutzt ein System unter der V-PKI (Verwaltungs-PKI) des BSI.

PW	Passwort
FF	Mozilla Firefox

1 Wichtiges vorab

Bitte führen Sie den kompletten Antragsprozess zeitnah ohne große Unterbrechungen durch! Der Prozess ist erst **nach dem erfolgreichen Import** des Zertifikats abgeschlossen (vgl. Abschnitt 4.2.2), nicht schon nach dem Absenden des Antrags oder dem Herunterladen der Signaturdatei[1] vom Trustcenter! Bis zum **Abschluss** des Antragsprozesses dürfen am **Benutzerprofil auf dem Arbeitsplatzrechner des Antragstellers keine Veränderungen** vorgenommen werden. Dazu zählen z.B. auch Passwortänderungen und die Installation von Software, insbesondere Updates des Microsoft Internet Explorers bzw. des Mozilla Firefox.

Hintergrund: Das Zertifikat besteht aus zwei verschiedenen Komponenten:

- **Öffentlicher Schlüssel**, der Ihnen vom Trustcenter signiert wird
- **Privater Schlüssel**, der beim Zertifikatsantrag erstellt und verborgen auf dem Antragsrechner verbleibt. Der private Schlüssel kann nicht explizit aufgerufen werden. Durch Veränderungen am Benutzerprofil auf Ihrem PC kann der private Schlüssel beschädigt werden bzw. verloren gehen.

Nur zusammen funktionieren beide Teile als Zertifikat. Daher ist es besonders wichtig den Prozess zeitnah zu beenden und abschließend den erfolgreichen Import zu überprüfen. Lesen Sie hierzu bitte das Kapitel 4.2.1, S. 17.

Kurzportrait Gruppenzertifikat	
Gültigkeits-dauer	3 Jahre Bei Wechsel der Förderperiode, des Standorts oder des Zertifi-katsverantwortlichen kann ein gültiges Zertifikat weiter benutzt werden. Eine Neubeantragung ist nicht zwingend notwendig.
Aussteller	Trustcenter der Citkomm in Iserlohn
Verantwort-lichkeit	Eine Person pro Einrichtung
Browser	Beantragung und Erst-Installation des Zertifikates sind mit dem Microsoft Internet Explorer und Mozilla Firefox möglich, die Ver-wendung ist auch mit Opera, Safari u.a. Browsern möglich.
Speicher	Automatisch unter Eigene/Ihre Zertifikate im jeweiligen Zertifi-

1 Die Signaturdatei heißt userCertifcate.p7b

	katsmanager.

2 Einleitung

2.1 Allgemeines

mpuls ist eine Web-Anwendung, bei der die Case Managerinnen bzw. Case Manager verschlüsselt über das Internet mit dem Server kommunizieren. Um die Echtheit der Kommunikationspartner zu gewährleisten, werden an beiden Enden der Datenverbindung Zertifikate eingesetzt. Die Web-Anwendung akzeptiert nur Verbindungen von Stellen, die ihr als **vertrauenswürdig** bekannt sind. Im Gegenzug ist auch für die Einrichtungen sichergestellt, dass sie direkt und über eine gesicherte Verbindung mit mpuls kommunizieren. Zertifikate für einzelne Einrichtungen werden als Gruppenzertifikate (X.509) vergeben. Die Zertifikatverwaltung wird vom Trustcenter der Citkomm betrieben.

Insgesamt wird ein dreistufiges Verfahren implementiert: Zunächst wird über das **Serverzertifikat** das mpuls-System gegenüber der Anwenderin bzw. dem Anwender authentifiziert. Durch das **Gruppenzertifikat** wird der Anwender als Mitarbeiterin bzw. Mitarbeiter einer Einrichtung authentifiziert. Im letzten Schritt authentifiziert sich die Mitarbeiterin bzw. der Mitarbeiter durch **Benutzername und Passwort** persönlich.

Die Gruppenzertifikate basieren auf einer Public-Key-Infrastruktur. Neben öffentlichen Schlüsseln (Public-Key), die vom Trustcenter digital signiert werden (und damit Zertifikate werden), gehört dazu auch der private Schlüssel einer jeden Einrichtung. Ohne diese beiden Teile ist eine Benutzung der Zertifikate zur Authentifizierung nicht möglich. Die Zertifikate sind maximal **drei Jahre gültig**.

2.2 Dokumentation

Diese Anleitung beschreibt die **Antragsstellung** und **Installation** der Gruppenzertifikate sowie den **Import** zugehöriger Zertifikate von Zertifizierungsstellen, um eine vollständige Vertrauenskette aufzubauen.

Für die **korrekte Anwendung** der Gruppenzertifikate stellt die Citkomm außerdem folgende Dokumente bereit:

- Antragstellerhandbuch (http://cas.citkomm.de/dokument/Antragstellerhandbuch.pdf)

- Certificate Policy (CP) für die zertifikatsbasierte Schlüsselinfrastruktur (Public Key Infrastructure – PKI) des Trustcenters der Citkomm. Dieses finden Sie unter: http://cas.citkomm.de/dokument/CertificatePolicy_aktuell.pdf.

Beide Dokumente sind in der jeweils gültigen Fassung von der Web-Seite des Trustcenters: http://cas.citkomm.de unter den Stichworten „Benutzerhandbuch“ bzw. „Sicherheitsleitlinien“ herunter ladbar.

Weitere Hinweise sind unter dem Stichwort „**Tipps+Tricks**“ auf der gleichen Seite verfügbar.

3 Der Zertifizierungsprozess

Die **Beantragung** eines Zertifikats ist über einen **Internet-Explorer ab Version 7.0 oder über Firefox ab Version 16 möglich**. Andere Browser (z. B. Chrome oder Opera) werden bisher bei der Beantragung leider nicht unterstützt. Bereits erstellte Zertifikate können dann jedoch auch mit anderen Browsern benutzt werden.

Der Prozess für ein Gruppenzertifikat teilt sich in mehrere Schritte:

1. Antragsstellung (nur mit IE oder FF möglich)
2. Authentisierung durch PostIdent-Verfahren
3. Herunterladen und Erst-Installation des Zertifikates
4. Export/Import des Zertifikates (Verteilung an CM, alle Browser)

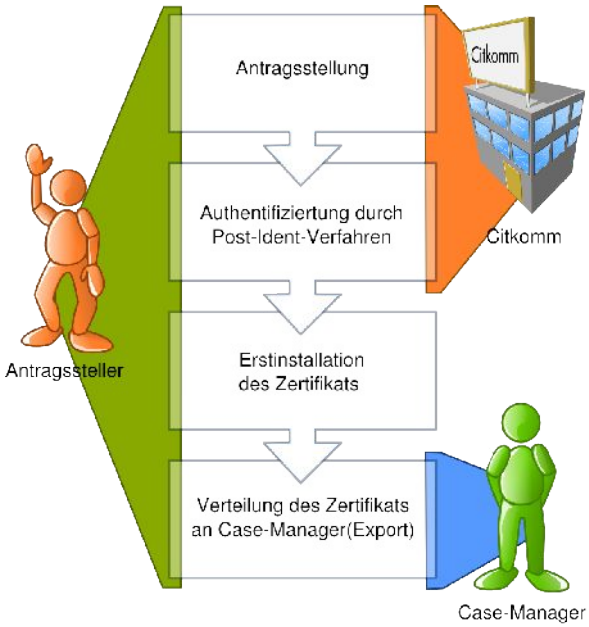


Abbildung 1: Zertifizierungsprozess im Überblick (kompakt)

Für den Zertifizierungsprozess wird in jeder Einrichtung eine Verantwortliche bzw. ein **Verantwortlicher** festgelegt. Die Schritte bis zum Verteilen des Zertifikates an die einzelnen Mitarbeiterinnen und Mitarbeiter der Einrichtungen finden auf **einem Rechner unter dem Nutzerkonto der verantwortlichen Person** statt.

3.1 Die Antragsstellung

Im Schritt der Antragsstellung wird ein Schlüsselpaar erstellt. Dieses Paar besteht aus einem öffentlichem und privatem Schlüssel. Der öffentliche Teil wird an das Trustcenter der Citkomm zur Signatur übermittelt. Zusammen fungiert das Schlüsselpaar später dann als „Gruppenzertifikat“.

Gehen Sie bitte wie folgt bei der Antragstellung vor:

1. Öffnen Sie mit dem **Microsoft Internet Explorer** Version 7 oder höher bzw. mit dem **Mozilla Firefox** Version 16 oder höher (andere Browser werden zur Zeit leider nicht unterstützt) die Seite

   https://cas.citkomm.de

   Bitte beachten Sie, dass die Bearbeitung des Antrags auf dieser Internetseite zeitlich begrenzt ist (siehe dazu Seitenende „Sitzung verfällt um xx.xx“).

2. Wählen Sie aus dem linken Menü „Beantragen Benutzerzertifikat" aus. Es werden nun schrittweise die notwendigen Angaben zum öffentlichen Schlüssel abgefragt:

a) Räumliche Ordnung: Wählen Sie „Citkomm".

b) Organisationseinheit I: Wählen Sie „**JMD**“

c) Organisationseinheit II: Wählen Sie hier den Namen Ihrer Einrichtung.

d) Es öffnet sich ein Dialog mit zwei Eingabeelementen:

- **Kennung**: Geben Sie hier bitte den vierstelligen Ziffernblock der Förderkennziffer an (z.B. 1234). Über diese Angabe wird später Ihre Einrichtung identifiziert.
- **E-Mail-Adresse**: Geben Sie hier bitte Ihre E-Mail-Adresse ein, diese ist für den weiteren Ablauf der Zertifikatsvergabe notwendig!
- Abschließend akzeptieren Sie bitte die Sicherheitsleitlinien. Diese sind verlinkt und können nachgelesen werden.

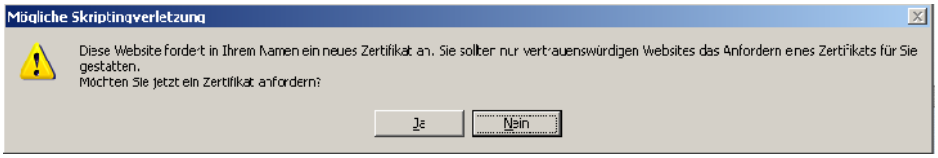
- Klicken Sie auf „beantragen".

3. Prüfen Sie die getroffenen Angaben im folgenden Dialog und bestätigen Sie diese - oder gehen Sie zurück, um die Angaben zu korrigieren.

4. Nach der Bestätigung kann es zu einer Warnmeldung kommen: *„Objekt unterstützt diese Eigenschaft oder Methode nicht“*. Es fehlt meist eine für die Schlüsselerstellung notwendige Funktion die sich jedoch leicht aktivieren lässt. Dazu verweisen wir hier auf das Dokument „Tipps und Tricks“[2] der Citkomm, Seite 19 folgende. Nach Lösung des Problems muss die Eingabe wie in 2 d) beschrieben wiederholt werden.

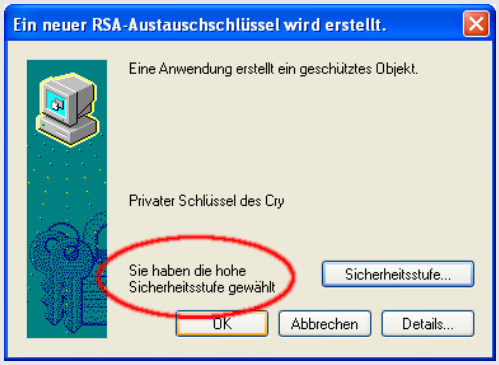
2 http://cas.citkomm.de/dokument/TippsundTricks.pdf

5. Es folgt eine Sicherheitsabfrage („Mögliche Skriptingverletzung“), die Sie bitte mit „Ja“ bestätigen. Sind die Daten der Eingabe korrekt, erfolgt eine Mircrosoft Sicherheitsabfrage, die mit **Ja** zu bestätigen ist.



6. In den folgenden Dialogen werden weitere Einstellungen für das Schlüsselpaar abgefragt:

   - Standardmäßig ist lediglich eine *mittlere Sicherheitsstufe* eingestellt. Stellen Sie sicher, dass der private Schlüssel auf **hoher Sicherheitsstufe** geschützt ist (Ändern mit Klick auf „Sicherheitsstufe“)!



   - Nach dem Bestätigen auf „OK“ werden Sie nach einem Passwort (**PW1 –** vgl. Abb. 2, S. 26) gefragt, das im Schritt 3 und 4 des Zertifizierungsprozess bei jeder Verwendung des privaten Schlüssels erforderlich ist.

     → Stellen Sie sicher, dass Sie sich für diese späteren Schritte an das Passwort (**PW1**) erinnern können.

   - Bestätigen Sie die folgenden Dialoge mit „OK“.

7. Das Schlüsselpaar wird erstellt und der öffentliche Teil an das Trustcenter übermittelt.

   Hinweis: Durch eventuelle Veränderungen am Benutzerprofil auf dem Antragsrechner könnte der **private Schlüssel** vor Abschluss des Zertifizierungsprozess **unbenutzbar** werden. Daher sollten Sie den Prozess bis einschließlich „Verteilung des Zertifikates“ (4.2.2, S. 17) zeitnah abschließen.

8. Anschließend erfolgt eine Bestätigung und die Aufforderung, den Zertifi-

katsantrag zu drucken; spätestens mit dieser Aufforderung sollte der angeschlossene Drucker betriebsbereit sein:

Drucken Sie den Zertifikatsantrag aus, er wird im weiteren Verfahren benötigt. Ohne diesen Ausdruck kann kein Zertifikat erstellt werden! Setzen Sie sich bei Problemen ggf. mit der Hotline in Verbindung – der Antrag muss bei versäumten Ausdruck nicht erneut gestellt werden.

9. Damit ist der erste Schritt der Antragsstellung abgeschlossen. Sie erhalten noch eine Bestätigung als E-Mail. Den Browser können Sie jetzt wieder schließen. Sie erhalten eine E-Mail, welche Sie bestätigen sollen, diese enthält als Anhang eine PDF-Datei. Die PDF-Datei ist ein Brief des Trustcenters der Citkomm. Drucken Sie ihn aus und schneiden Sie den Coupon ab. Diesen Coupon brauchen Sie für das PostIdent-Verfahren:

3.2 PostIdent-Verfahren

Die Prüfung eines Antrags und das damit verbundene persönliche Erscheinen des Antragstellenden (Authentisierung) sind in jedem Fall notwendig. Diese kann in einer beliebigen Filiale der Deutschen Post AG vorgenommen werden. Das Trustcenter der Citkomm bietet dafür das PostIdent-Verfahren an. Dieser zertifizierte Dienst der Deutschen Post AG übernimmt dann Teilaufgaben der Überprüfung.

Auf dem Hintergrund der **persönlichen Authentisierung** ist es notwendig, **Änderungen in der Zuständigkeit** für die Zertifikatsbeantragung mit einem formlosen Schreiben dem Servicebüro JMD schriftlich mitzuteilen.

Sie erhalten nach der Antragsstellung ein Schreiben des Trust-Centers mit einem Coupon für das PostIdent-Verfahren. Weitere notwendige Dokumente:

- Das ausgedruckte und vollständig ausgefüllte Namensvergabedokument für Endbenutzerzertifikate aus dem vorangegangenen Schritt „Antragsstellung“ faxen Sie bitte an das Trustcenter, die Nr. wird Ihnen per Brief mitgeteilt.
- Ihren Personalausweis oder Reisepass, für die Identifikation bei der Post.

Gehen Sie mit Ihrem gewählten Ausweisdokument und dem Coupon persönlich zu

einer Filiale der Deutschen Post AG. Die weiteren Schritte werden am Schalter durchgeführt.

4 Herunterladen und Installation[3] des Zertifikates

Nach erfolgreicher Durchführung des PostIdent-Verfahrens **signiert** das Trustcenter der Citkomm Ihren **öffentlichen Schlüssel** und stellt ein Zertifikat zur Verfügung. Die Antragstellerin bzw. der Antragsteller erhält automatisch eine entsprechende E-Mail an die im Zertifikatsantrag angegebene Adresse.

Wichtig: Es ist zwingend notwendig das Zertifikat am **Antragsrechner** in den für die Antragstellung verwendeten Internet-Browser einzuspielen. Erst in diesem Schritt werden der private und jetzt **signierte** öffentliche Schlüssel wieder zusammen gefügt, so dass diese als „Gruppenzertifikat“ fungieren können.

4.1 Mozilla Firefox

Bitte benutzen Sie für die Installation, die Überprüfung des Imports und die Sicherung des Zertifikates mit dem Mozilla Firefox die Anleitung der Citkomm unter:

http://cas.citkomm.de/dokument/TippsundTricks.pdf Seite 29ff.

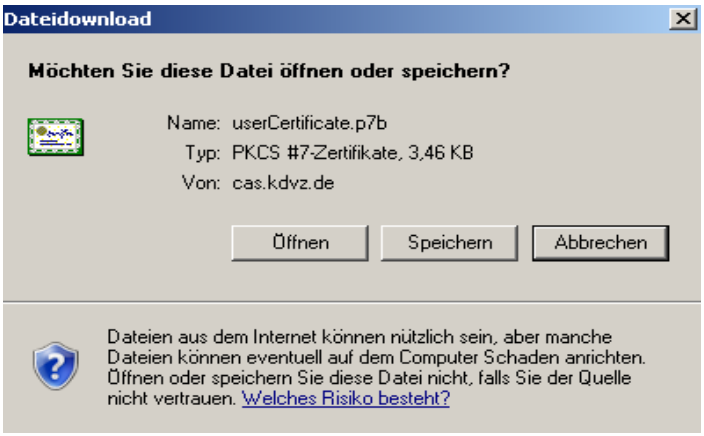
4.2 Internet-Explorer

Die folgenden Schritte sind wieder an dem Rechner auszuführen, an dem auch der Zertifikatsantrag gestellt wurde. Sie benötigen erneut den Microsoft **Internet-Explorer**:

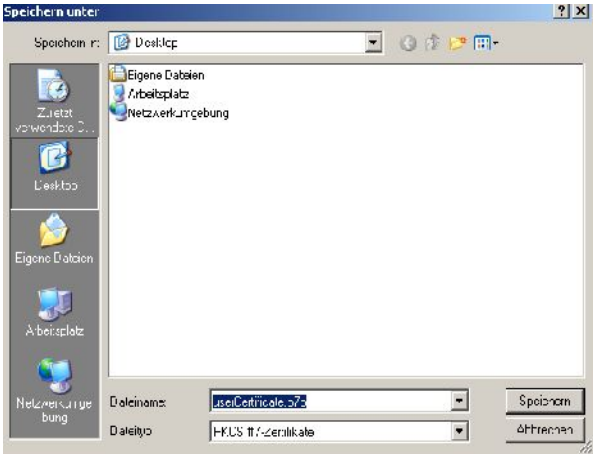
1. Benutzen Sie den in der E-Mail enthaltenen Link[4], um eine Datei mit der Endung *.p7b* herunterzuladen. Die Datei kann mit Klick auf den **„Speichern-Knopf“** auf dem lokalen Rechner in einem beliebigen Verzeichnis gespeichert werden:

3 In der Regel sind für die Installation von Zertifikaten keine besonderen Administrationsrechte notwendig.

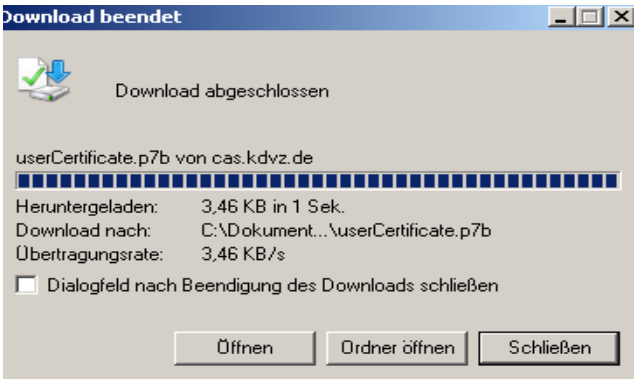
4 Einige E-Mail-Programme haben Probleme mit dem enthaltenen Link, das Dokument „Tipps+Tricks“ enthält Hinweise zur Konfiguration. Alternativ können Sie das Zertifikat von der Web-Seite des Trust-Centers (http://cas.citkomm.de) im Abschnitt „Benutzerzertifikat“ suchen und herunterladen (Vgl. Abschnitt „Zentraler Verzeichnisdienst LDAP“ im Antragstellerhandbuch).



a) Speichern Sie die Transport-Datei userCertifcate.p7b auf dem Desktop ab.



b) Nach dem Ende des Downloads können Sie das Fenster schließen. Auf dem Desktop, bzw. dem entsprechen gewählten Verzeichnis finden Sie die Datei „userCertificate.p7b“.



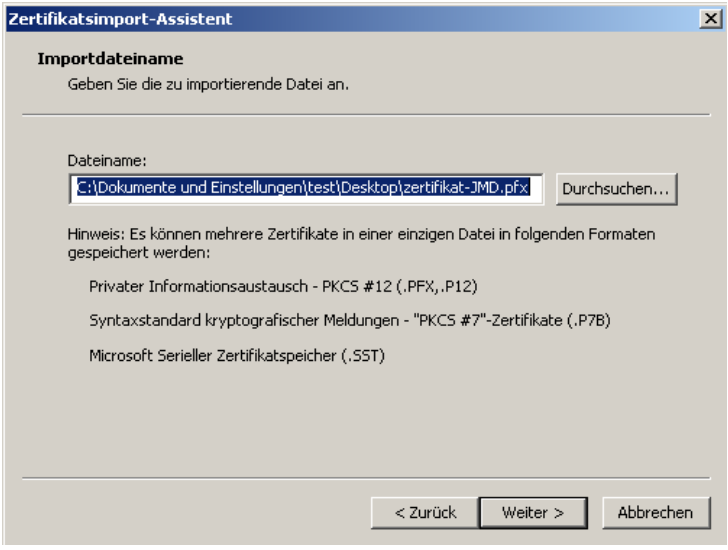
2. Klicken Sie anschließend die Datei mit der rechten Maustaste an und rufen

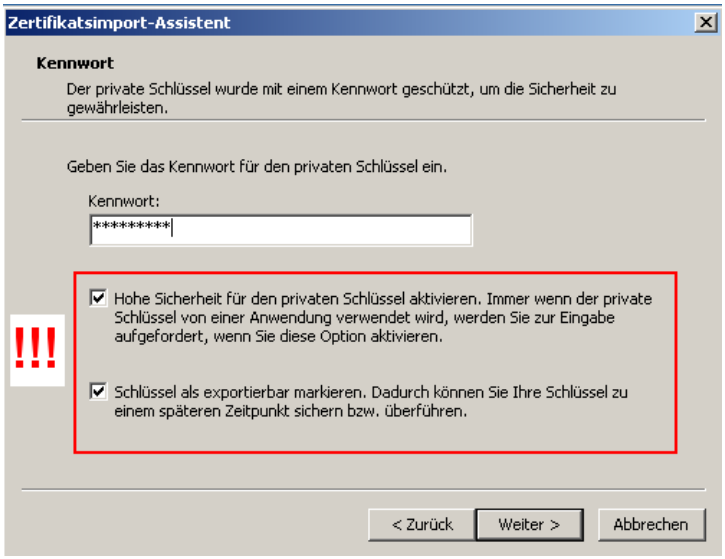
den Installationsassistenten mit einem Klick auf „Zertifikat installieren“ auf.

3. Ein Assistent führt Sie durch die einzelnen Schritte des Imports, die Abfragen sind jeweils zu bestätigen. Sie benötigen zum Installieren das bei der Beantragung vergebene Passwort (**PW1 –** vgl. Abb. 2, S. 26).

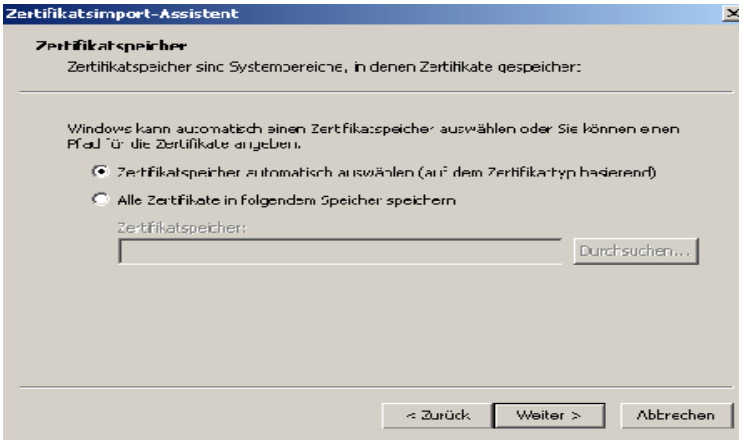
a) „Willkommen“: Bestätigen Sie mit „Weiter“.

b) „Importdateiname“: Ohne Änderung – bestätigen Sie mit „Weiter“

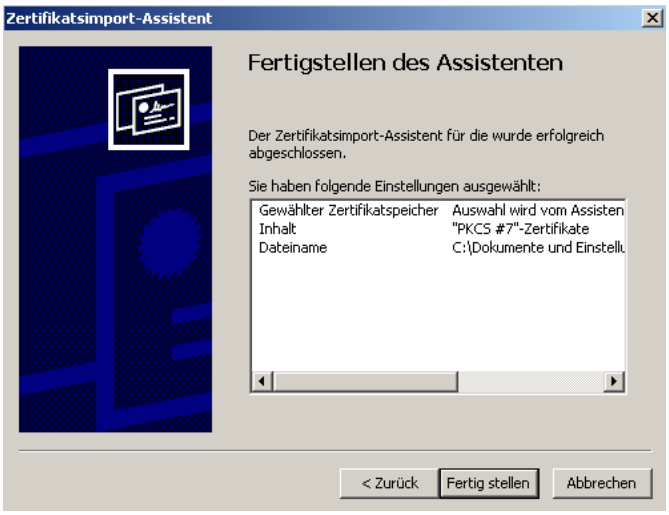




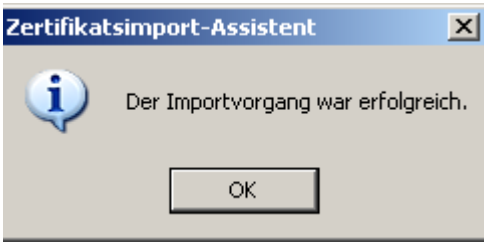
d) „Zertifikatsspeicher“: Ohne Änderung – bestätigen Sie mit „Weiter“



e) Bestätigen Sie mit Klick auf „Fertig stellen“



f) Bestätigen Sie den abschließenden Dialog mit „OK“

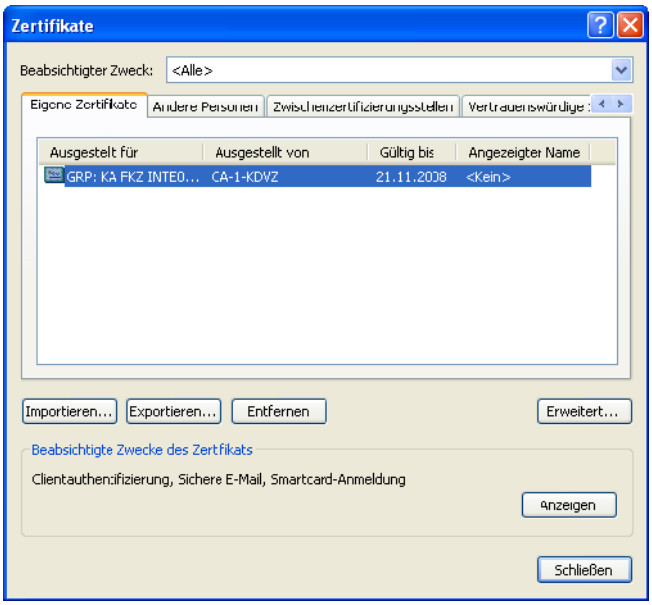


4. Es werden das eigene Zertifikat, das Zertifikat der Citkomm und das Zertifikat der Wurzelzertifizierungsstelle des BSI (Bundesamt für Sicherheit in der IT) im Zertifikatspeicher unter **Eigene Zertifikate** installiert. Dabei erfolgt ggf. eine Sicherheitsabfrage bezüglich des Wurzelzertifikats/Stammzertifikats PCA-1-Verwaltung-09. Sie können sich das Zertifikat anzeigen lassen und die Korrektheit anhand des Fingerabdrucks überprüfen (Groß-/Kleinschreibung und Füllzeichen wie Doppelpunkte sind dabei nicht relevant):
   57 B7 64 24 98 33 FC 20 D0 AB 85 01 2E 83 F3 5C 3F A4 91 57

   Stimmt der Fingerabdruck mit diesem Wert überein, so handelt es sich um das korrekte Zertifikat. Sie können dem Zertifikat vertrauen und es daher entsprechend weiter installieren.

   Stimmt der Fingerabdruck nicht überein, kontaktieren Sie bitte die Hotline.

5. Bitte überprüfen Sie abschließend den erfolgreichen Import des Zertifikats.



4.2.1 Import überprüfen

Der erfolgreiche Import sollte in jedem Fall überprüft werden. Insbesondere wenn Sie noch ein gültiges Zertifikat installiert haben und somit erst nach dessen Auslaufen feststellen, ob der Import tatsächlich erfolgreich war, ist dieser Schritt um so wichtiger.

Öffnen Sie hierzu bitte den **Zertifikatsmanager des Internet-Explorer:**

> Menü „Extras“

> „Internetoptionen“

> „Inhalte“

> „Zertifikate“

> „**Eigene Zertifikate**“ anzeigen

Der Reiter Eigene/Ihre Zertifikate zeigt nach einem erfolgreichen Import das neue Zertifikat, mit max. drei Jahren Gültigkeitsdauer.

Ist dies **nicht der Fall**, ist der Import **nicht erfolgreich gewesen**. Wenn das Zertifikat anstatt unter „Eigene/Ihre“ im Reiter „Personen“ gespeichert wurde, scheint es Probleme mit Ihrem privaten Schlüssel zu geben.

Erste Ansätze zur Problembehebung beim Import finden Sie im Kapitel 5.2, S. 23.

Hinweis: Nach Abschluss des Imports sollte eine Sicherungskopie des Zertifikates (öffentlicher **und** privater Schlüssel) erstellt werden. Die Schritte dazu sind identisch mit den ersten Schritten zur Verteilung des Zertifikates an die Case Managerinnen und Case Manager (vgl. Kapitel 4.2.2, S. 17).

4.2.2 Verteilung des Zertifikates

Das Sicherheitskonzept von mpuls sieht vor, dass sich jeder Nutzer als Mitarbeiterin bzw. Mitarbeiter einer bestimmten Einrichtung authentisiert. Dazu wird das erstellte Zertifikat benutzt, das als Gruppenzertifikat fungiert. Das Zertifikat muss dafür an **jedem Arbeitsplatz mit Rechner** und für jede Benutzerin bzw. jeden Benutzer installiert werden, die bzw. der mpuls benutzen soll.

Hinweis: Der Zugriff auf mpuls sollte nur von vertrauenswürdigen Rechnern aus

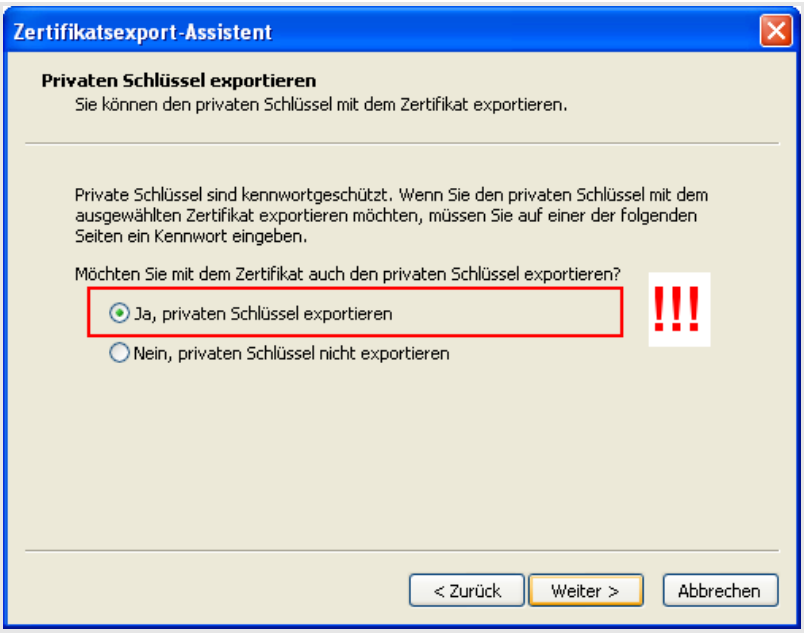
erfolgen, die hohen Sicherheitsanforderungen genügen. Rechnerpools in Schulen o. ä. erfüllen solche Anforderungen **NICHT**.

Für die Verteilung wird das Zertifikat inklusive des privaten Schlüssels zunächst aus dem Browser exportiert und dann auf den entsprechenden Rechnern wieder importiert.

4.2.3 Export

Wir beschreiben hier den Export des privaten Schlüssels und des Zertifikates über den Internet Explorer (IE). Der Zertifikatspeicher lässt sich jedoch auch mit anderen Werkzeugen verwalten, die im Antragstellerhandbuch dargestellt sind.

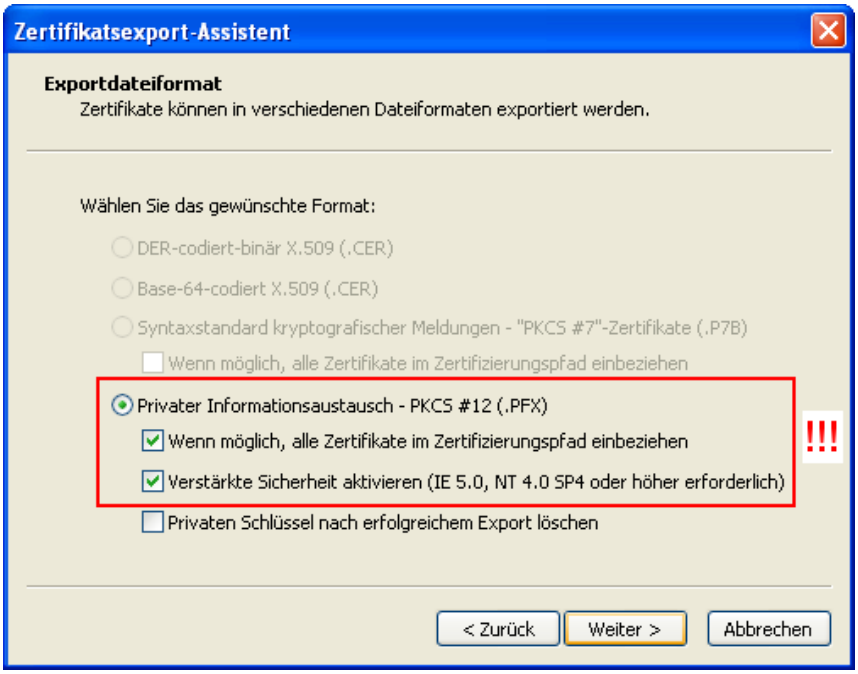
1. Wählen Sie wie oben den Zertifikatspeicher des IE:
   - > Menü „Extras“ > „Internetoptionen“ > „Inhalte“ > „Zertifikate“ > „Eigene Zertifikate“.
2. Markieren Sie das zu exportierende Zertifikat und wählen „Exportieren“, ein Assistent führt Sie durch die einzelnen Schritte des Exports:



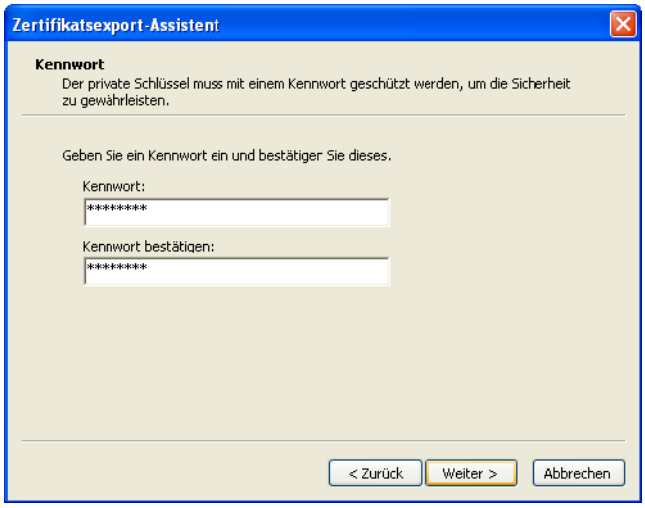
   - Stellen Sie sicher, dass Sie den **privaten Schlüssel** mit exportieren. **Ohne** den privaten Schlüssel funktioniert das Zertifikat auf anderen Rechnern **nicht!**
   - Für den Export ist das Format „PKCS #12“ vorgegeben. Wählen Sie ggf. die Option „Wenn möglich alle Zertifikate im Zertifizierungspfad einbeziehen“, um auf weiteren Rechnern nicht wieder die volle Zertifikatsket-

te einzeln importieren zu müssen. Eine unvollständige Zertifikatskette muss gemäß den Schritten unter 4.1 ergänzt werden.

- Stellen Sie sicher, dass der private Schlüssel nicht gelöscht wird, wenn Sie das Zertifikat auch auf diesem Rechner benutzen wollen!

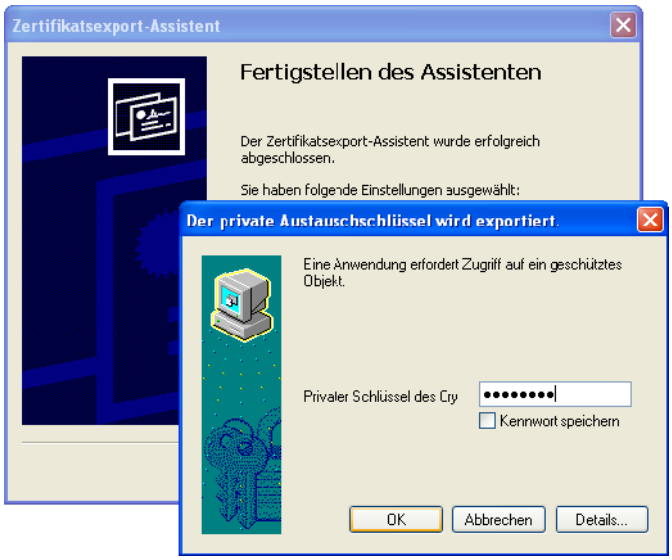


- Sie werden aufgefordert, den exportierten Schlüssel durch ein Kennwort (**PW2 –** vgl. Abb. 2, S. 26) zu schützen. Sie benötigen dieses Kennwort, um den Schlüssel und das Zertifikat auf einem anderen Rechner zu importieren.



- Wählen Sie abschließend einen Dateinamen, unter dem der exportierte Schlüssel abgelegt werden soll. Damit sind alle notwendigen Eingaben für den Assistenten getätigt.

3. Wählen Sie „Fertigstellen“, um nun das Zertifikat und den privaten Schlüssel zu exportieren. Dabei werden Sie aufgefordert, das Kennwort für den privaten Schlüssel einzugeben, das Sie während der Antragsstellung vergeben haben (**PW1 –** vgl. Abb. 2, S. 26):



Der private Schlüssel und das Gruppenzertifikat sind damit exportiert und befinden sich in einer Datei mit der typischen Endung .p12 bzw. .pfx

4. Wir empfehlen die Daten auf **einem** einzigen Datenträger, z.B. einer CD, zu speichern, der zur Verteilung des Zertifikats und des privaten Schlüssels dient und abschließend als Datensicherung verwahrt werden kann. Stellen Sie dabei auch sicher, dass Sie sich an das Passwort der Exportdatei (**PW2 –** vgl. Abb. 2, S. 26) erinnern können.

Wir raten von einem Versand der Exportdatei per E-Mail ab. Dies birgt ein Sicherheitsrisiko, da Unberechtigte unbemerkt eine Kopie der Exportdatei erlangen könnten und anschließend beliebig Zeit/Versuche haben, Ihr Passwort zu raten.

4.3 Import

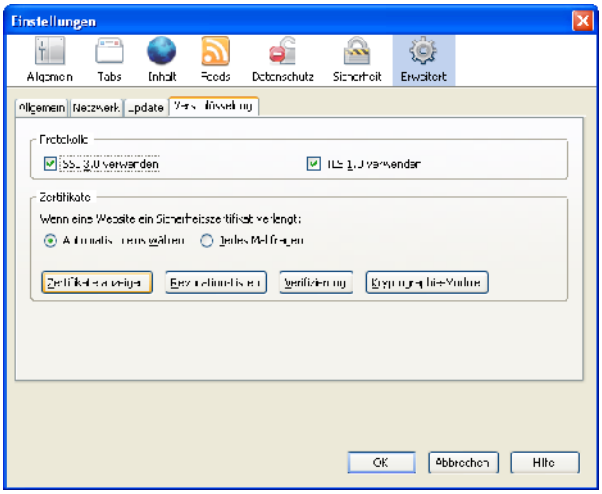
Für den Import des Gruppenzertifikates und des Schlüssels benötigen Sie die Exportdatei (z.B. auf einer CD) und das Kennwort (**PW2 –** vgl. Abb. 2, S. 26), das während des Exports vergeben wurde.

Der Import in den Internet Explorer ist den bisher beschriebenen Vorgängen sehr ähnlich: Mit einem Klick der rechten Maustaste auf das Datei-Icon einer Exportdatei öffnet sich ein Kontextmenü, hier können Sie die Option „Installieren“ wählen.

Im Folgenden stattdessen das Vorgehen mit dem Mozilla Firefox:

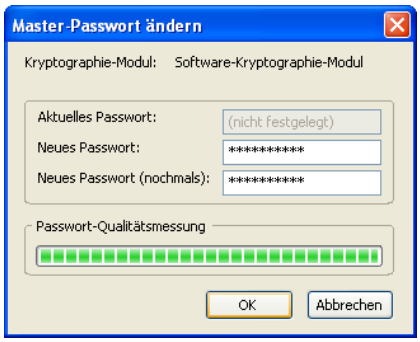
1. Starten Sie den Firefox und wählen Sie, analog zum Vorgehen im Internet Explorer, den Zertifikat-Manager:

Firefox	**Internet-Explorer**
> Menü „Extras“	> Menü „Extras“
> „Einstellungen“	> „Internetoptionen“
> „Erweitert“	> „Inhalte“
> „Verschlüsselungen“	> „Zertifikate“
> „Zertifikate anzeigen“	> „**Eigene Zertifikate**“ anzeigen
> „**Ihre** Zertifikate“ anzeigen	



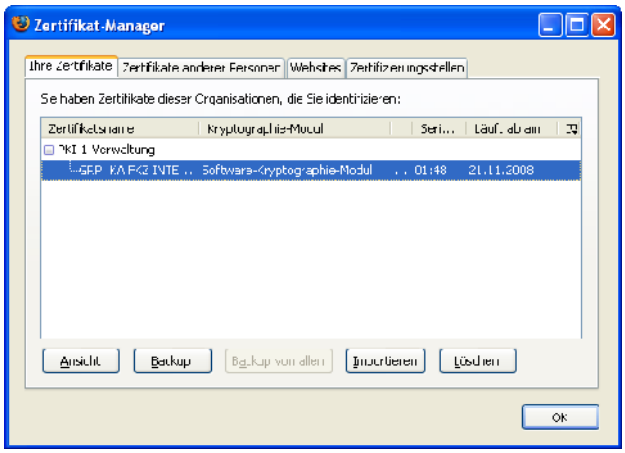
2. Klicken Sie im Zertifikat-Manager den Knopf „Importieren“, um den Import zu starten und die im vorherigen Schritt erstellte Exportdatei auszuwählen.

3. Der Firefox speichert die Schlüssel in einem „Schlüsselbund“, der durch ein Master-Passwort geschützt ist. Wenn Sie noch kein Passwort für diesen Schlüsselbund vergeben haben, werden Sie aufgefordert, dies nun zu tun. Andernfalls werden Sie aufgefordert, Ihr bestehendes Passwort einzugeben.



4. Für den Import wird nun das Passwort abgefragt, mit dem die im vorherigen Schritt erstellte Exportdatei geschützt wurde (**PW2 –** vgl. Abb. 2, S. 26)

5. Bei korrekter Eingabe des Passwortes werden der Schlüssel und alle mit exportierten Zertifikate nun importiert und der erfolgreiche Import bestätigt.
6. Abschließend ist das Gruppenzertifikat im Zertifikat-Manager aufgeführt:



7. Nach dem erfolgreichen Import von privatem Schlüssel und Zertifikaten kann auch vom entsprechenden Nutzerkonto aus auf den mpuls-Anwendungsbereich Ihrer Einrichtung zugegriffen werden.

8. Bitte stellen Sie sicher, dass der Datenträger nach der Verteilung vernichtet oder sicher verwahrt wird. Ein unbemerkter Verlust des Datenträgers gibt Unberechtigten eine Möglichkeit, mit beliebiger Zeit/Anzahl von Versuchen Ihr Sicherungspasswort zu raten.

5 Support und Hilfen

5.1 Dokumentation

Neben dieser Anleitung bietet das Trustcenter der Citkomm weitere Dokumentationen an, die von der Web-Seite http://cas.citkomm.de heruntergeladen werden können:

- Bedienungsanleitung: Dieses Antragstellerhandbuch stellt den Antragsprozess und die Handhabung von Zertifikaten umfassend dar.
- Sicherheitsleitlinien: Die Sicherheitsleitlinie (Certificate Policy, CP) ist das zentrale Dokument der PKI der Citkomm und enthält die vertragsrelevanten Informationen zur Aufbau- und Ablauforganisation der PKI. Dieses ist unter http://cas.citkomm.de/dokument/CertificatePolicy_aktuell.pdf abrufbar.

- Tipps+Tricks: Bereits häufiger aufgetretene Probleme sind hier mit Lösungsansätzen dokumentiert.

Auf den Anwenderportalen der Programme (Adressen siehe Zusatzinformationen) finden Sie eine umfangreiche Sammlung von häufig gestellten Fragen (FAQ, Frequently Asked Questions) und entsprechende Antworten. Ebenso sind dort die aktuellen Versionen der Dokumentation zu mpuls hinterlegt. Folgend ein Auszug aus der FAQ Liste.

5.2 FAQ – die häufigsten Fragen

- **Die Zuständigkeit für die Zertifikatsbeantragung hat sich geändert, was müssen wir tun?**

  → 3.2, S. 11: Eine Zuständigkeitsänderung für die Zertifikatsbeantragung sollten Sie mit einem **formlosen Schreiben** per Fax oder Post direkt an Intevation GmbH bekannt geben. Nennen Sie den vorherigen und den neuen Ansprechpartner inkl. E-Mail Adresse. Eine Beispielvorlage finden Sie im Anwenderportal.

  Die Änderung der Zuständigkeit erfordert **keine Neubeantragung**! Das bestehende Zertifikat Ihrer Einrichtung bleibt weiterhin gültig.

- **Wie oft muss das Zertifikat erneuert werden?**

  → 2.1, S. 6: Das Sicherheitskonzept von mpuls sieht vor, dass die Gruppenzertifikate, die Sie dazu berechtigen auf die entsprechenden Server und Datenbanken zuzugreifen, **alle drei Jahre erneuert** werden. Es ist notwendig den vollständigen Prozess zu durchlaufen, da es sich tatsächlich um eine NEU-Beantragung der Zertifikate handelt.

- **Das importierte Zertifikat ist im Zertifikatsmanager nicht unter Eigene/Ihre Zertifikate gelistet – warum?**

  → , S. : Wenn sich das importierte Zertifikat unter einem anderen Reiter befindet, können Sie davon ausgehen, dass der private Schlüssel hier die Ursache ist. Stellen Sie sicher, dass der Erstimport tatsächlich auf dem **Antragsrechner** durchgeführt wird, da hier der originale private Schlüssel liegt. Für die anschließende Verteilung an die CM muss beim Export des Zertifikates der **private Schlüssel** mit exportiert werden.

- **Mit welchem Browser kann ich das Zertifikat nutzen?**

→ 4, S. 12: Das Zertifikat können Sie für die Arbeit mit mpuls mit jedem Browser mit SSL/TLS-Unterstützung benutzen. Wir empfehlen aktiv sicherheitsgepflegte Versionen. Lediglich die Beantragung und die Erstinstallation sind auf den Internet-Explorer bzw. Mozilla Firefox beschränkt.

- **Kann i-mpuls JMD an einem Computer mit mehreren Browsern verwendet werden?**

  Ja, Sie müssen nur das Gruppenzertifikat in jedem verwendeten Browser extra importieren.

- **Das neue Zertifikat ist installiert. Beim Aufrufen von mpuls wird aber weiterhin eine Fehlermeldung angezeigt – warum?**

  → 4.2.1, S. 17: Vermutlich ist die Vertrauenskette nicht vollständig. Mit einem manuellen Import von Wurzel- und/oder Serverzertifikat können Sie die Vertrauenskette wieder herstellen.

- **Muss ich das Zertifikat auch auf meinem Laptop installieren?**

  → 4.2.2, S. 17: Das Zertifikat dient der Authentifizierung vor dem Server und muss somit an jedem Arbeitsplatz installiert werden, wo Sie mit mpuls die Akten der Jugendlichen pflegen möchten. Wenn Ihr Laptop dazugehört, muss auch hier ein Zertifikat installiert werden.

- **Ich muss das Gruppenzertifikat neu beantragen, wo mache ich das?**

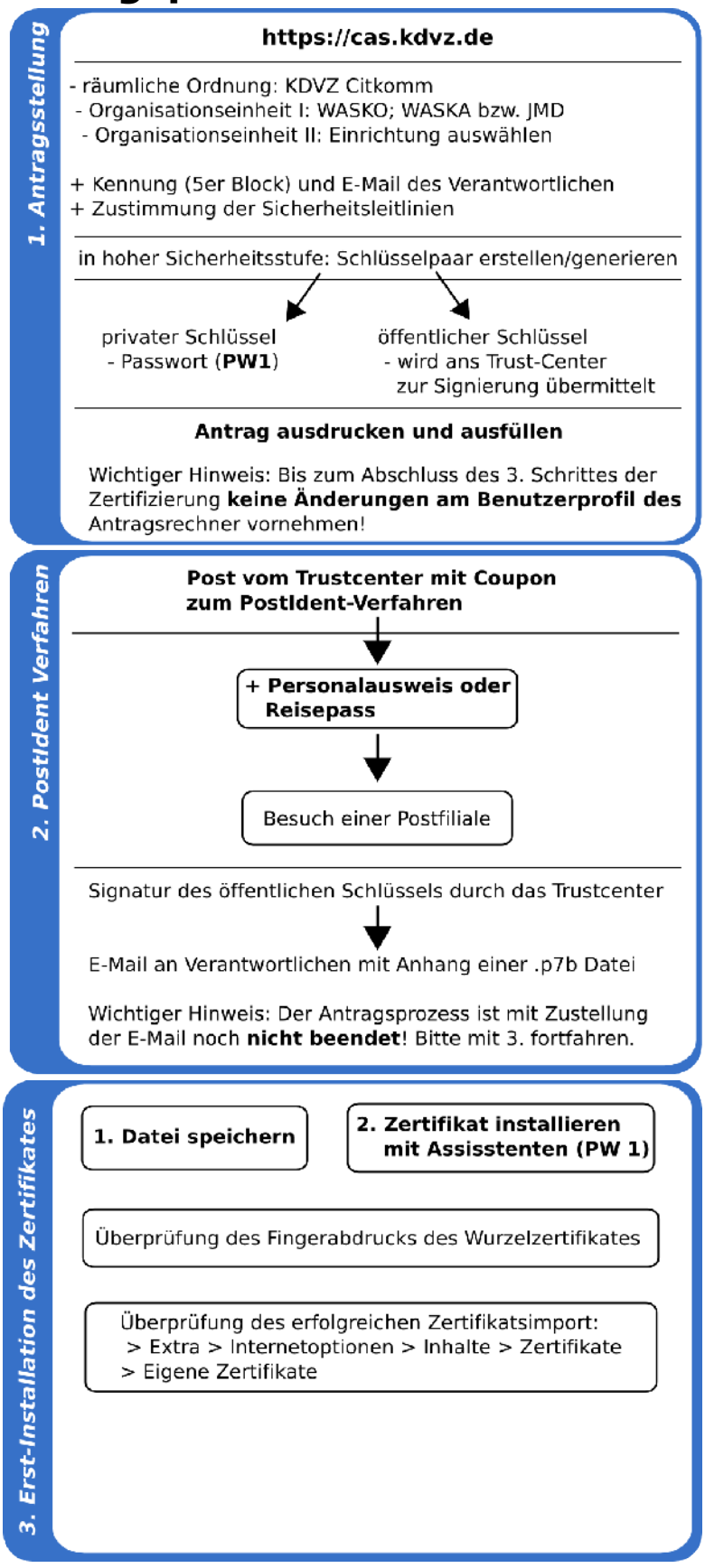
  Die Neubeantragung erfolgt wieder über das Trustcenter der Citkomm.

5.3 Individuelle Unterstützung

Sollten schwere Probleme auftreten, die sich mit der Dokumentation nicht lösen lassen, so können Sie beim Trustcenter unter der kostenpflichtigen Rufnummer 02371 – 43 96 99 66 individuelle Unterstützung anfragen.

Sie erreichen unter dieser Nummer die Berater des Trustcenters, die Ihnen Mo. – Do. von 8:00 bis 16:00 Uhr sowie Fr. von 8:00 bis 13:00 Uhr (außer an Feiertagen in Nordrhein-Westfalen) zur Verfügung stehen.

6 Zertifizierungsprozess im Überblick



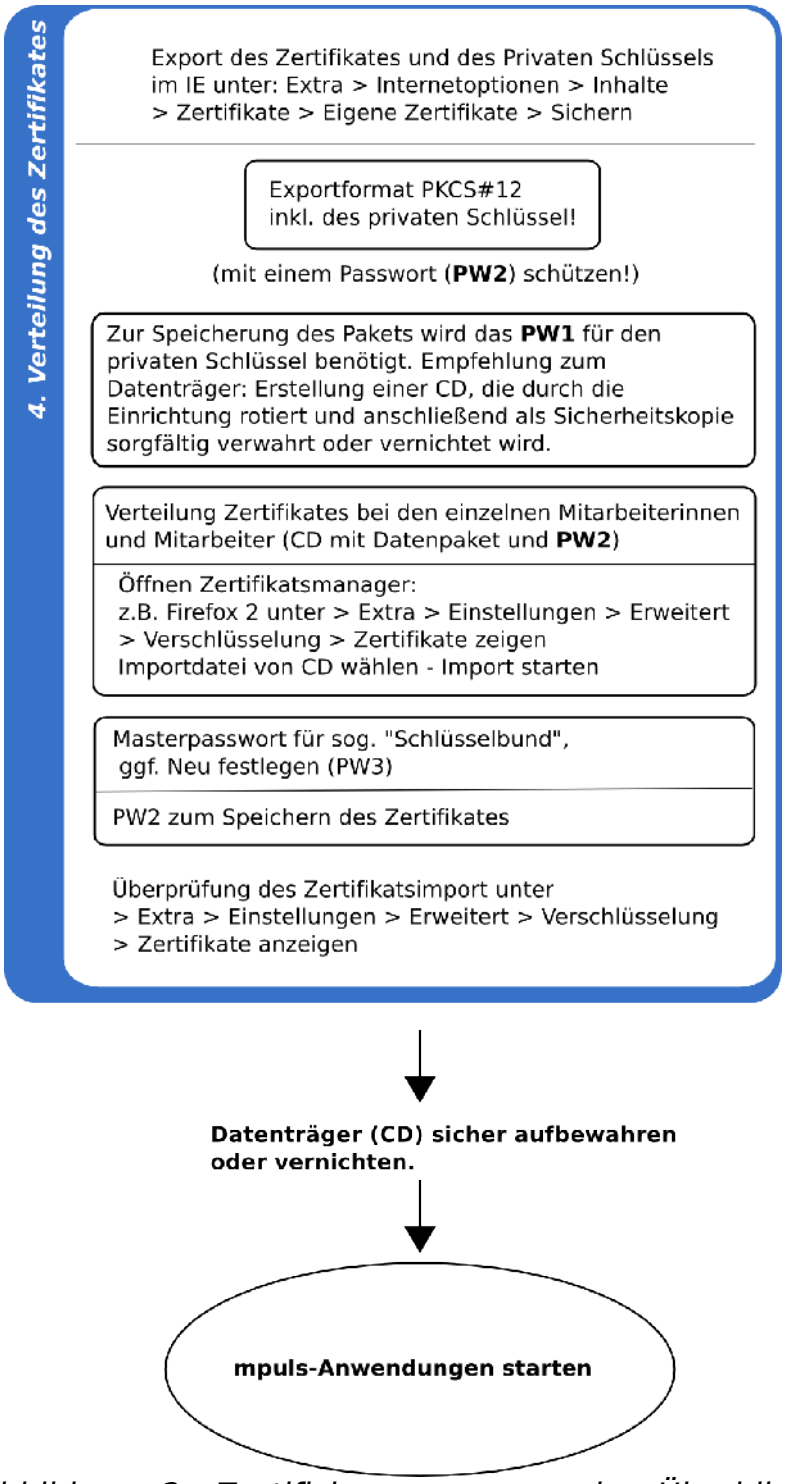
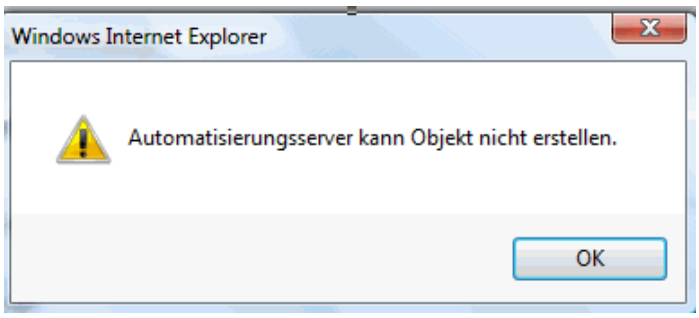


Abbildung 2: Zertifizierungsprozess im Überblick (detailliert)

7 Anhang: Die wichtigsten Tipps und Tricks

7.1 Windows 7: „Automatisierungsserver kann Objekt nicht erstellen“

Unter Windows 7 kann folgende Warnung erscheinen:



Bitte im Internet Explorer

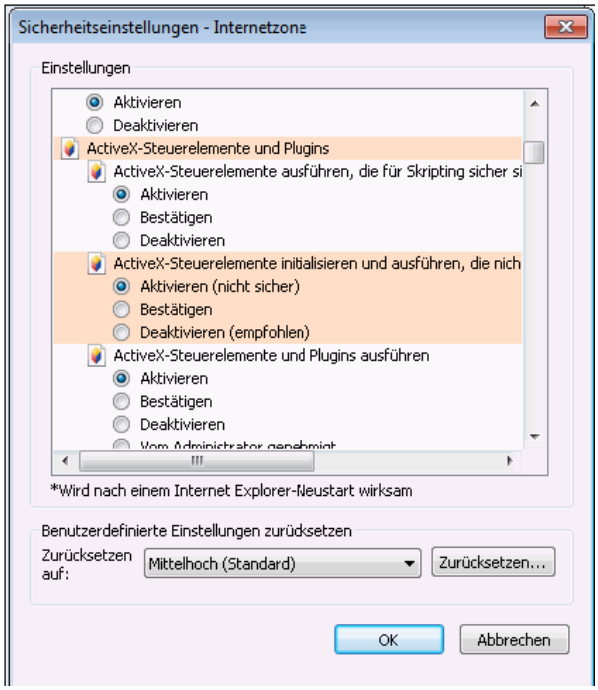
> Extras

> Internetoptionen

> Sicherheit

Hier ist auszuwählen:

Stufe anpassen



Folgende Einstellungen sind zu aktivieren:

vorher: Deaktivieren (empfohlen)

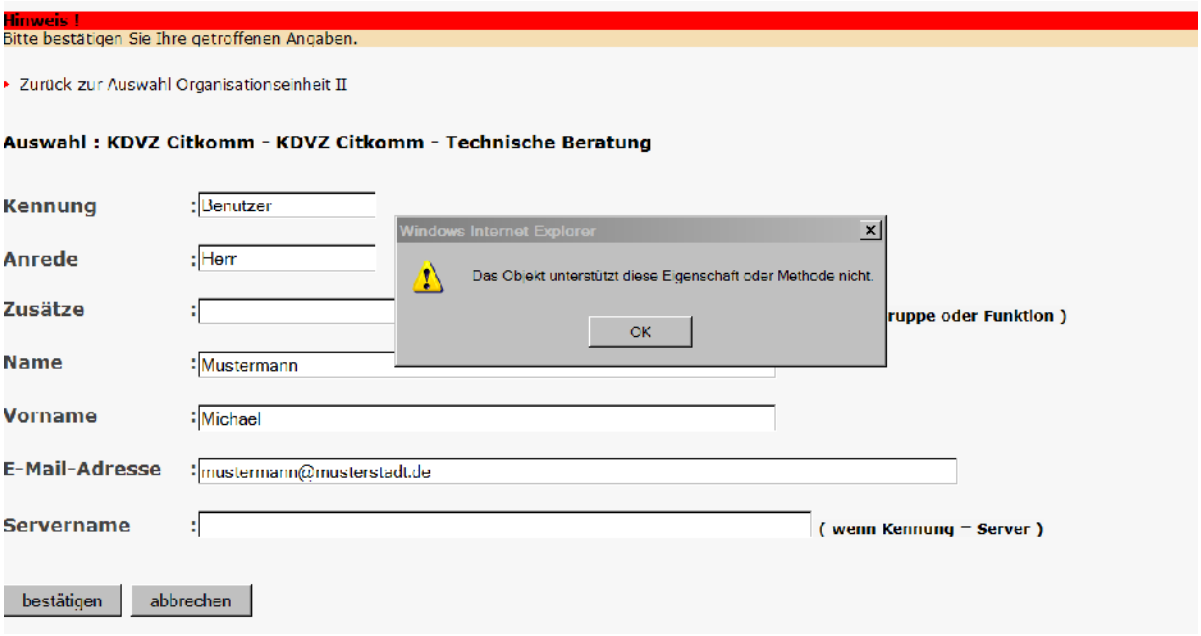
nachher**: Aktivieren (nicht sicher)**

Nachfolgenden Dialog „Webzugriffsbestätigung:

→ **mit „Ja“ bestätigen**

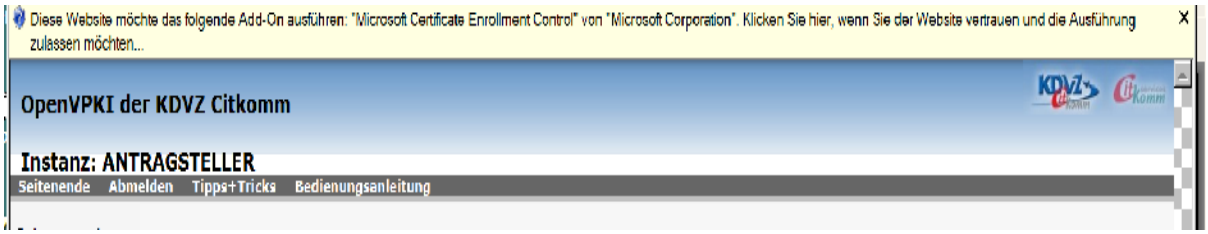
7.2 Windows XP: „Das Objekt unterstützt diese Eigenschaft oder Methode nicht“

Wenn bei der Beantragung des Zertifikats der Button „bestätigen“ gedrückt wurde, kann die Meldung kommen: „Das Objekt unterstützt diese Eigenschaft oder Methode nicht“.



Lösung:

Möglicherweise ist das ActiveX-Steuerelement „CEnroll Class“ nicht ausgeführt. Es ist das entsprechende Add-On aktivieren.



Dazu ist oberhalb der Webseite (über OpenVKI der KDVZ Citkomm) mit der rechten Maustaste „Active Steuerelement ausführen“ auszuwählen. Danach sind die Eingaben zu wiederholen.