Inhalt

PKI & CEPCES

Eine Windows PKI kann durch ihre ausgestellten Zertifikate in vielen Bereichen die Sicherheit verbessern. Dennoch hat sie aus historischen Gründen ein eigenes Problem: Clients kommunizieren via DCOM-RPC mit den Zertifizierungsstellen. Der Datenstrom selber ist zwar abgesichert, aber er arbeitet mit dynamischen Ports! Diese werden je Verbindung neu ausgehandelt und decken die gesamte obere Port-Range ab! Port-basierte Firewalls müssten daher extrem geöffnet werden.

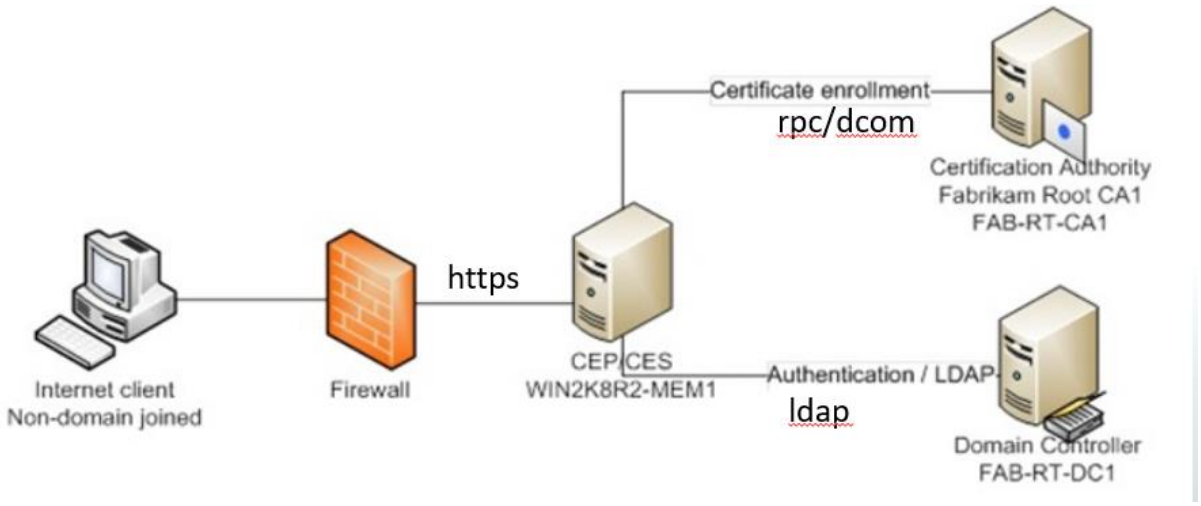
Moderne Netzwerke basieren auf verschiedenen Segmenten und zwischen diesen wird der Datenstrom mit Firewalls und IPS gefiltert und überwacht. Natürlich können professionelle Next Generation Firewalls den ausgehandelten, dynamischen Port erkennen und explizit für die Verbindung eine dynamische Ausnahme erstellen. Aber einfache Systeme können das nicht.

CEPCES ist eine Erweiterung in der PKI, mit welcher das Problem gelöst werden kann. Diese besteht aus 2 Komponenten:

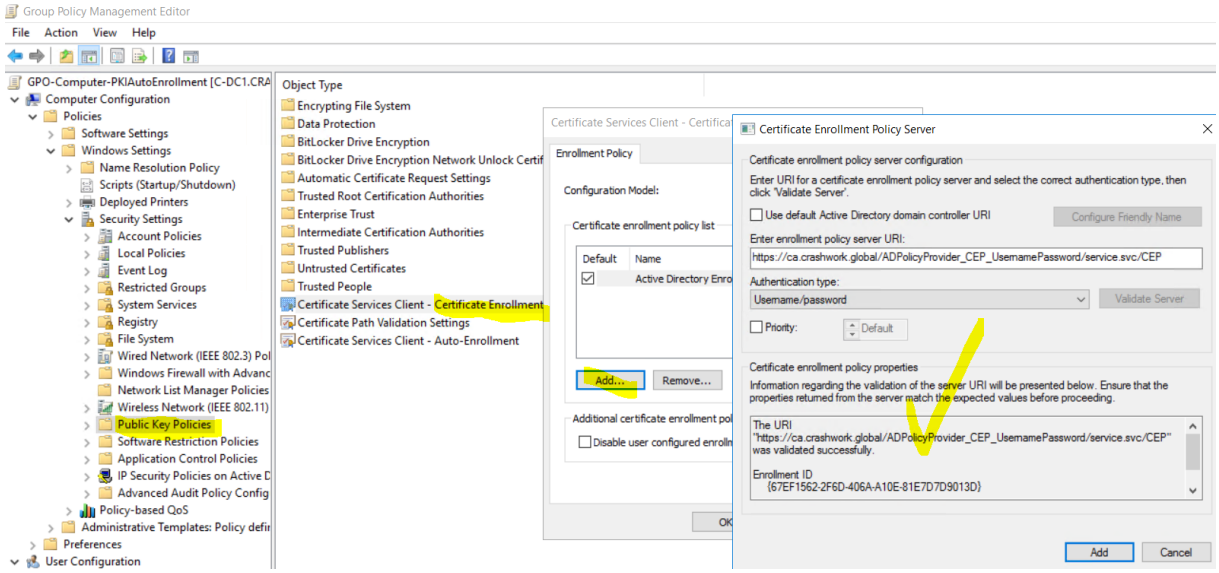
- dem **C**ertificate **E**nrollment **P**olicy web service (CEP)
- und dem **C**ertificate **E**nrollment web **S**ervice (CES)

Beide agieren als eine Art Reverse Proxy – also als ein Frontend. Während die Kommunikation mit dem Backend (also der Zertifizierungsstelle) immer noch via DCOM RPC abgebildet wird, kommunizieren die Clients nun mit dem Frontend (CEPCES) via https. Dafür ist nur ein Port erforderlich – und das ist auch mit einfachen Firewalls machbar.

So schaut das Konstrukt aus:



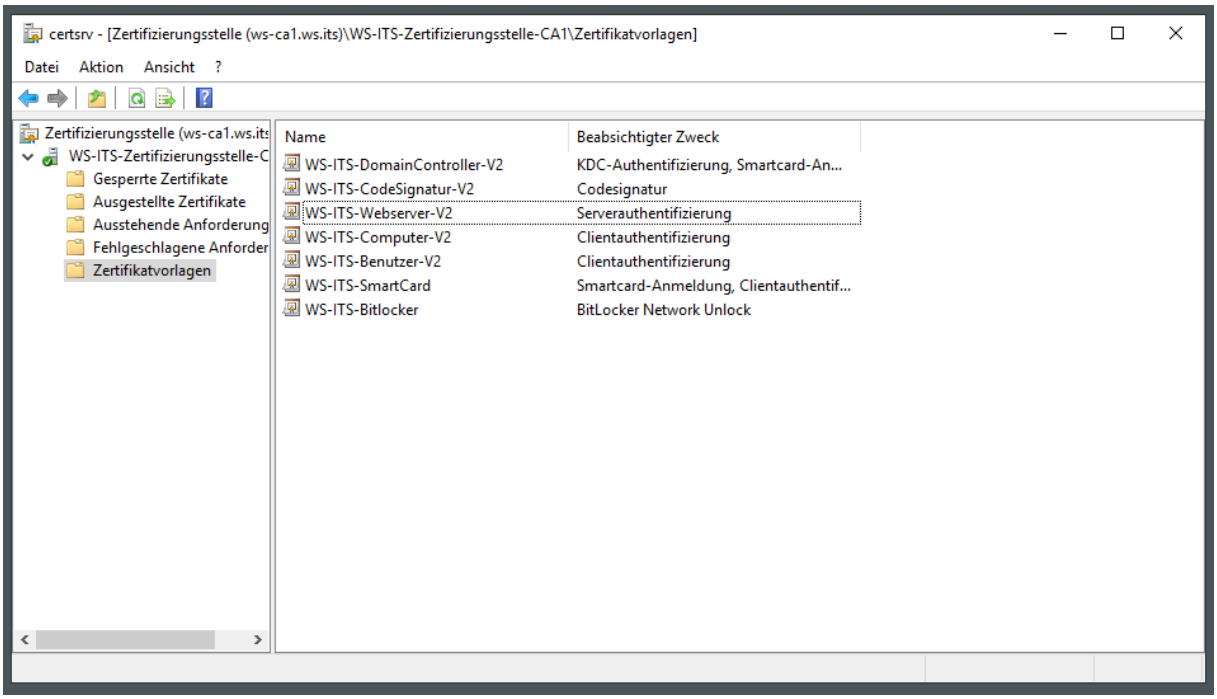
Den Clients kann über eine GPO der neue Zugriffspunkt veröffentlicht werden:



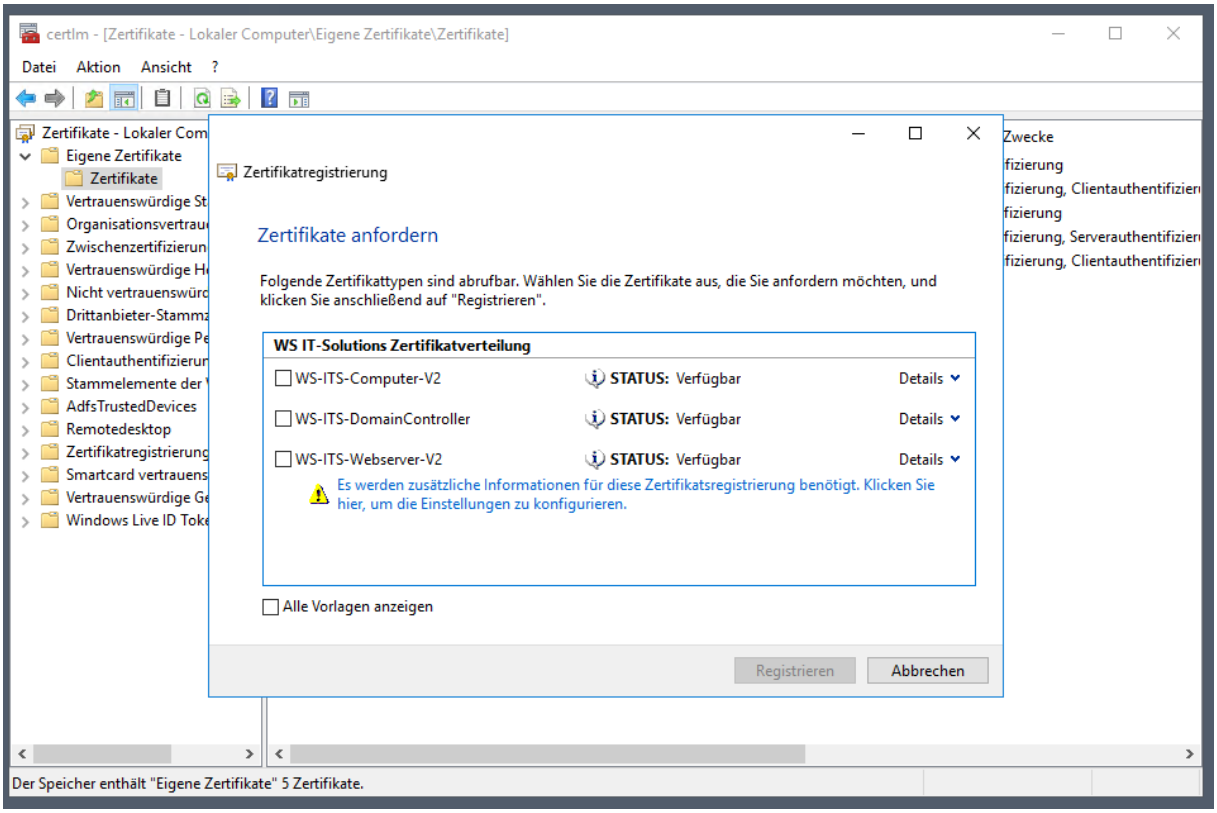
CEPCES gibt es seit Windows Server 2008R2 und ist auch im aktuellen Windows Server 2019 unverändert am Start.

Das Problem

Bis hier klingt doch alles ganz gut. Dennoch gibt es ein kleines Problem, wenn neue Zertifikatvorlagen veröffentlicht werden sollen. Hier ist meine kleine PKI abgebildet. Ich habe eine neue Vorgane „WS-ITS-DomainController-V2“ erstellt. Diese soll die Vorlage „WS-ITS-DomainController“ ablösen. Die alte Vorlage habe ich aus den auszustellenden Vorlagen entfernt:



Auf meinem Domain Controller möchte ich nun die neue Vorlage für ein neues Zertifikat verwenden. Aber sie wird nicht angezeigt. Stattdessen finde ich noch die alte Vorlage gelistet:



Auch unter „alle Vorlagen anzeigen“ wird sie nicht angezeigt. Es scheint fast, als ob noch nicht alle Komponenten über die Veränderung informiert sind oder ob die angezeigten Informationen zwischengespeichert werden.

Die Lösung

Und beide Vermutungen sind richtig:

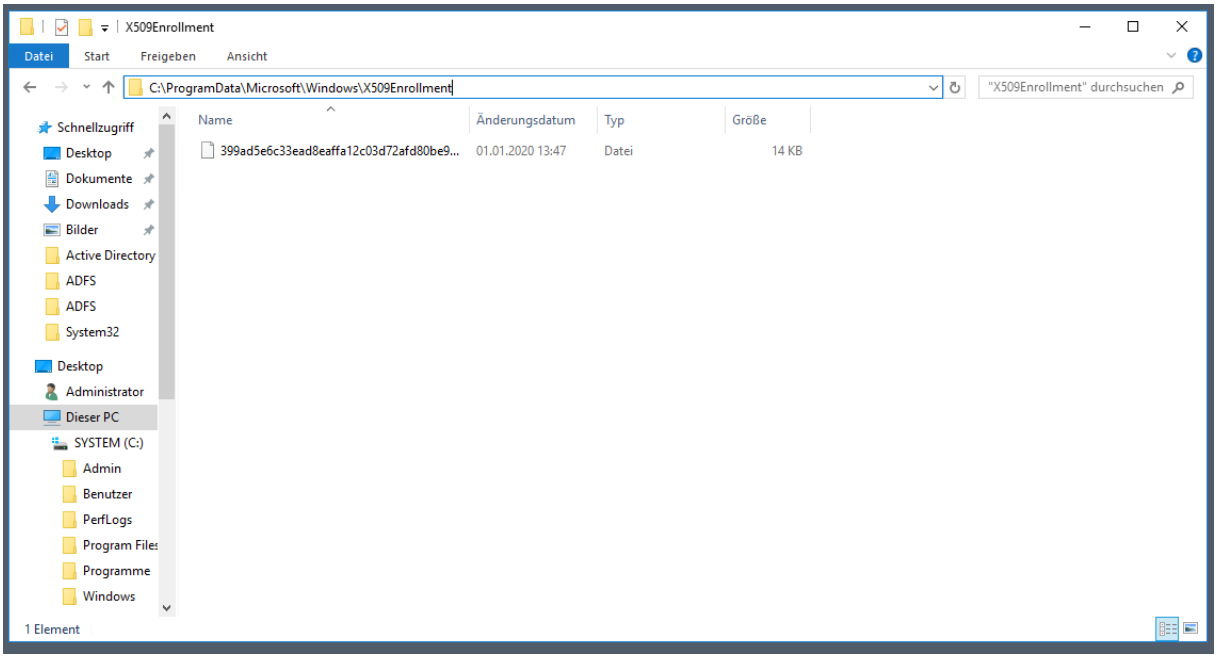
- Die Zertifizierungsstelle ist bei mir Active Directory integriert. Informationen zu Zertifikatvorlagen werden also im Active Directory gespeichert. Und Änderungen müssen erst auf alle Domain Controller repliziert werden. Das kann durchaus einen Moment Zeit in Anspruch nehmen. Werden mehrere Zertifizierungsstellenserver eingesetzt, dann müssen diese die Veränderungen erst aus dem AD laden. Auch dieser Fall wird einige Minuten dauern.
- CEPCES sind eigene Komponenten. Auch diese müssen die Veränderungen im AD erst erkennen. Erst danach werden die neuen Vorlagen angeboten. Beide Teile sind ApplicationPools im IIS. Microsoft hat hier den Standardwert von 30 Minuten für die Aktualisierung hinterlegt. Somit kann eine Veränderung schon einmal erheblich Zeit benötigen.
- Und auch der Client speichert sich die vom CEPCES geladenen Informationen zwischen. Hier beträgt die Livetime sogar 8 Stunden!

Grob gesagt: Wenn ich heute eine Veränderung an den auszustellenden Vorlagen vornehme, dann werden diese morgen sichtbar werden.

Falls es aber mal schneller gehen muss:

- Die Active Directory Replikation kann manuell angestoßen werden.
- Wird der IIS mit dem CEPCES neugestartet, dann wird auch die Vorlagensammlung neu vom AD synchronisiert.
- Auf dem Client kann der Cache gelöscht werden

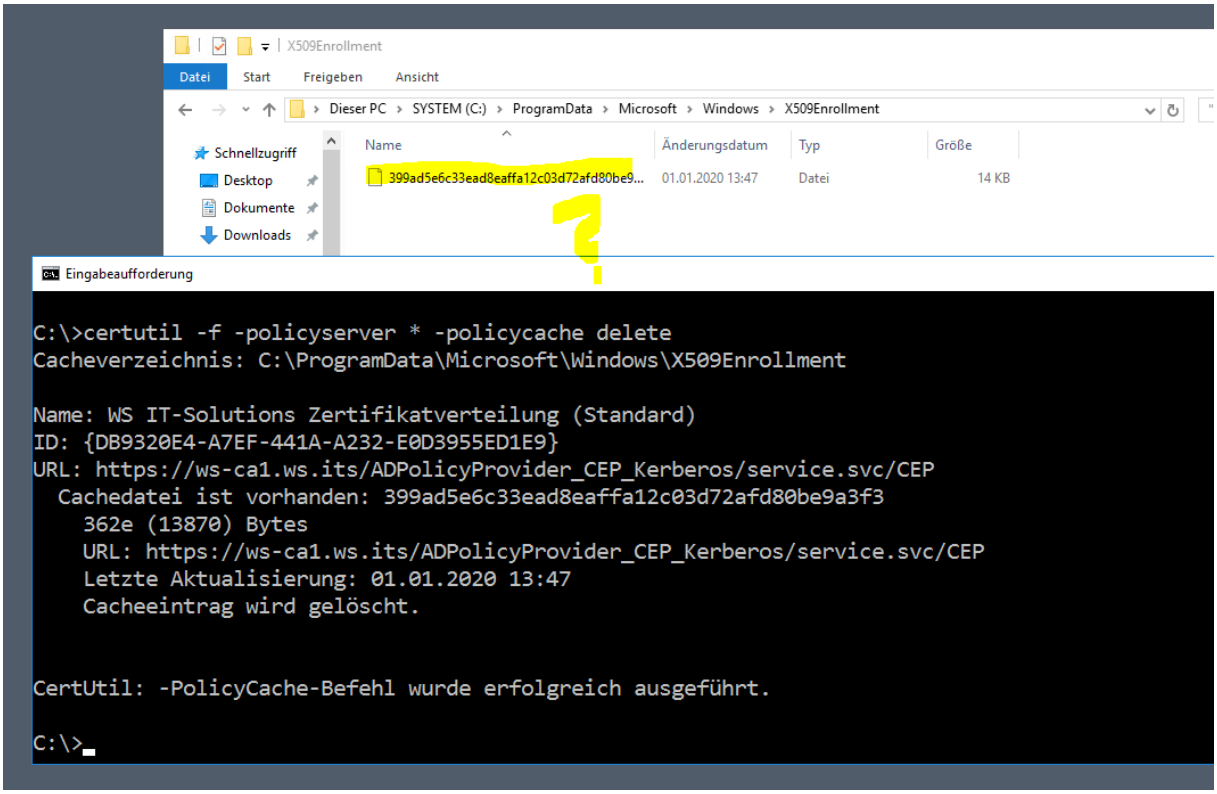
Die beiden ersten Punkte sind recht einfach zu erreichen. Bei dem Löschen des Caches hatte ich selber ein interessantes Problem. Der Cache liegt in diesem Verzeichnis:



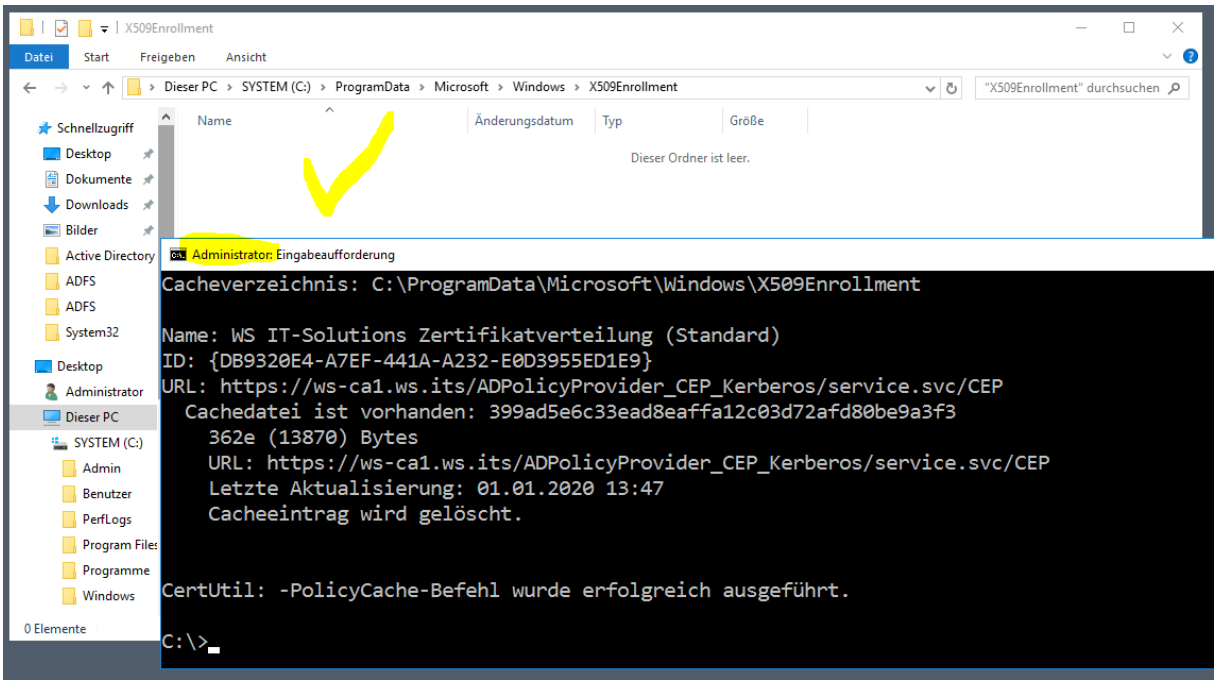
Mit einem cmd-Befehl kann der Cache gelöscht werden:

```
certutil -f -policyserver * -policycache delete
```

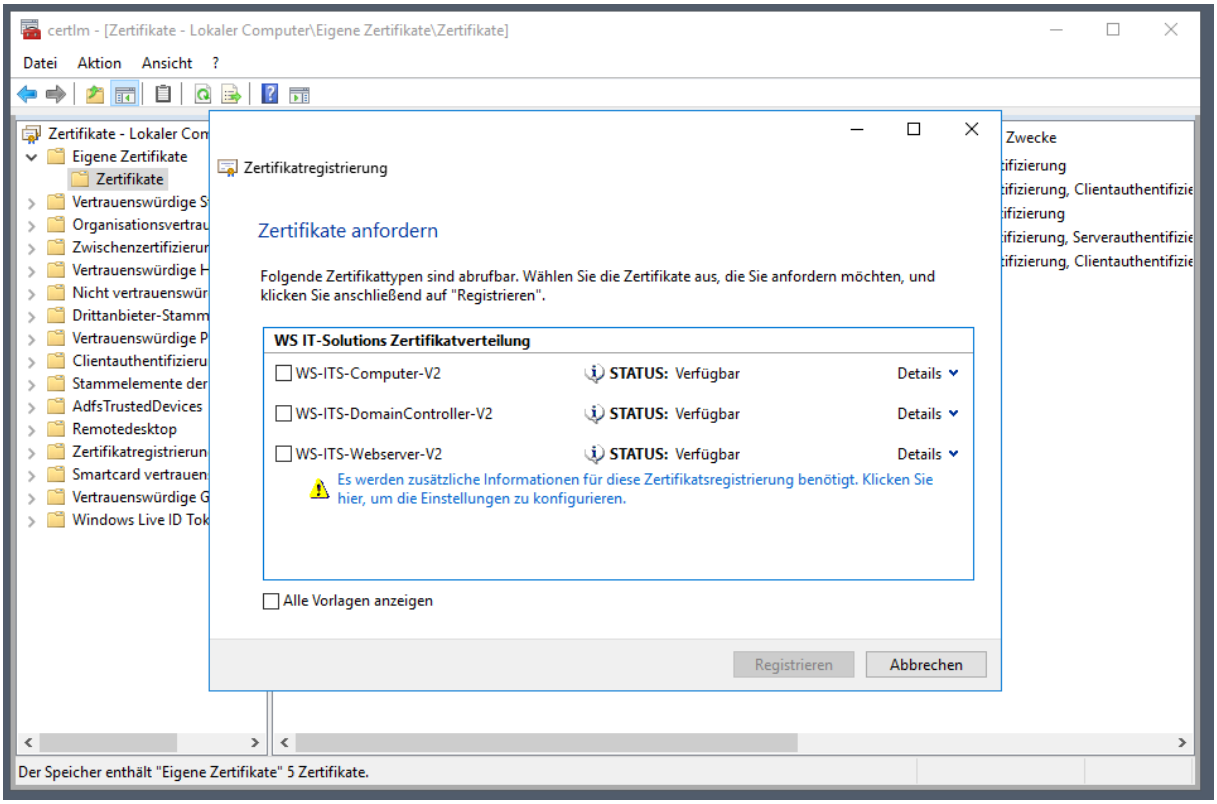
Das habe ich nach meiner Änderung auch auf meinem Domain Controller gemacht, denn hier wollte ich das neue Zertifikat haben. Aber der Cache wurde nicht bereinigt! Mir wurde aber eine Erfolgsmeldung „Cacheintrag wird gelöscht“ präsentiert:



Natürlich gab es danach immer noch keine neuen Vorlagen in der Anzeige! Nur durch eine Kontrolle der Cache-Datei und ihrem TimeStamp wusste ich, dass der Befehl fehlerhaft arbeitete. Als ich die Datei manuell löschen wollte (das geht natürlich auch), fragte die Benutzerkontensteuerung nach der administrativen Bestätigung. Und dann war die Lösung klar: der Befehl muss administrativ ausgeführt werden. Ich ließ die Datei im Verzeichnis und versuchte es in einer privilegierten cmd erneut:



Die Ausgabe des Befehls ist unverändert. Aber die Cache-Datei wurde tatsächlich bereinigt. Und so musste mein Server beim nächsten Kontakt mit CEPCES frische Informationen anfragen:



Nun konnte ich mein neues Zertifikat anfragen.