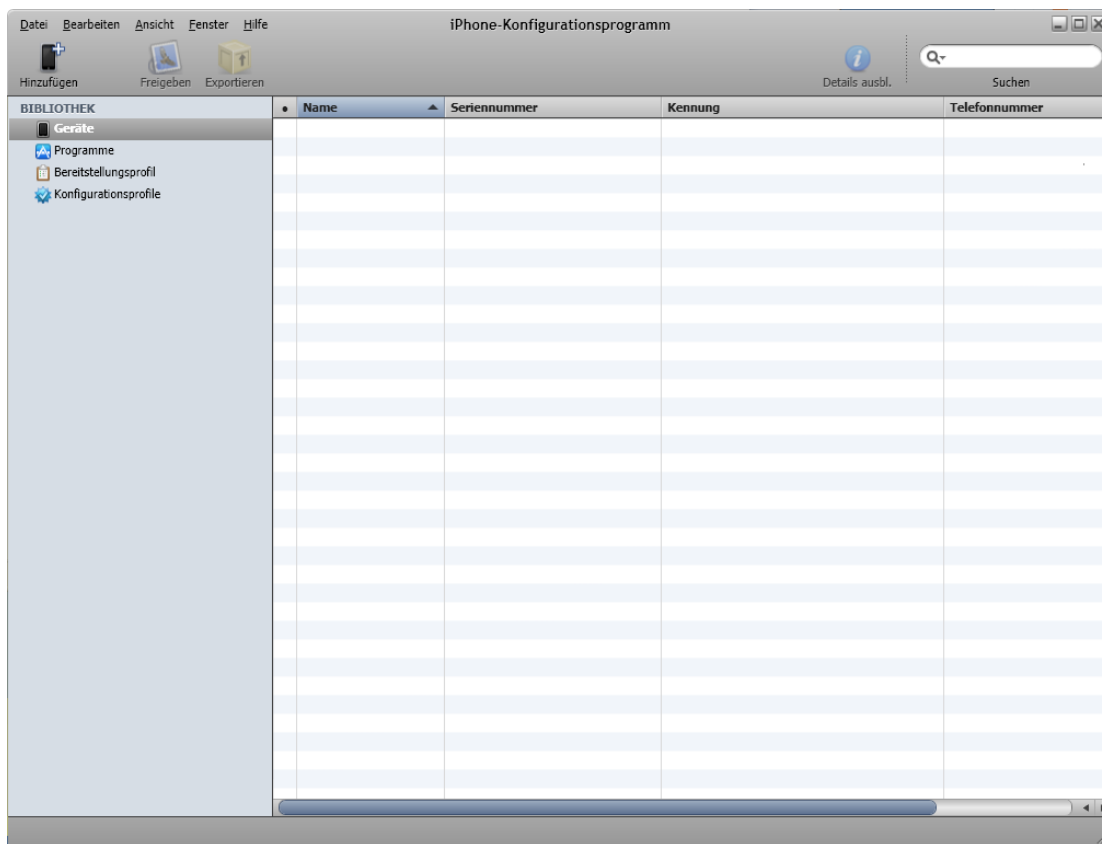
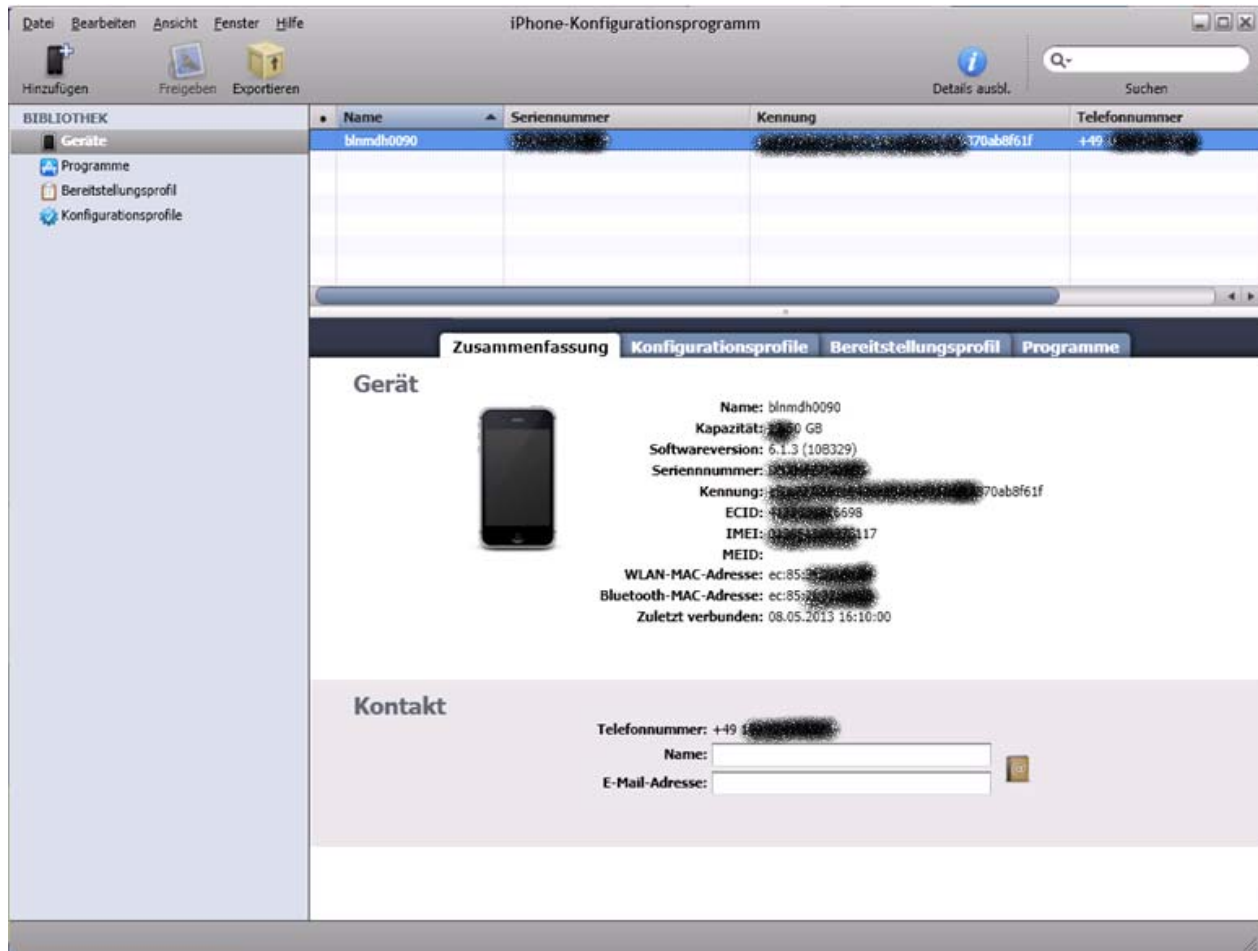


1. Vorbereitung:
 - Download der Cacert Zertifikate (Class1 und Class3) im PEM-Format als *.cer (<http://www.cacert.org/index.php?id=3>)
 - Download und Installation des iPhone Konfigurationsprogramm auf einen PC / MAC (Windows : <http://support.apple.com/kb/DL1466>) (MAC : <http://support.apple.com/kb/DL1465>)
 - iOS Endgerät mit Sync-Kabel in Reichweite
2. Löscht bitte alle vorhanden Zertifikate betreffend CAcert auf Eurem Device (Phone/Pad).
3. Startet das iPhone Konfigurationsprogramm auf Eurem Desktop. Sollte dieses unter Windows nicht wollen, löscht oder Benennt folgendes Verzeichniss um:
%USERPROFILE%\AppData\Local\Apple Computer\MobileDevice**Device**

a. Folgende Anwendungsoberfläche zeigt sich nun:

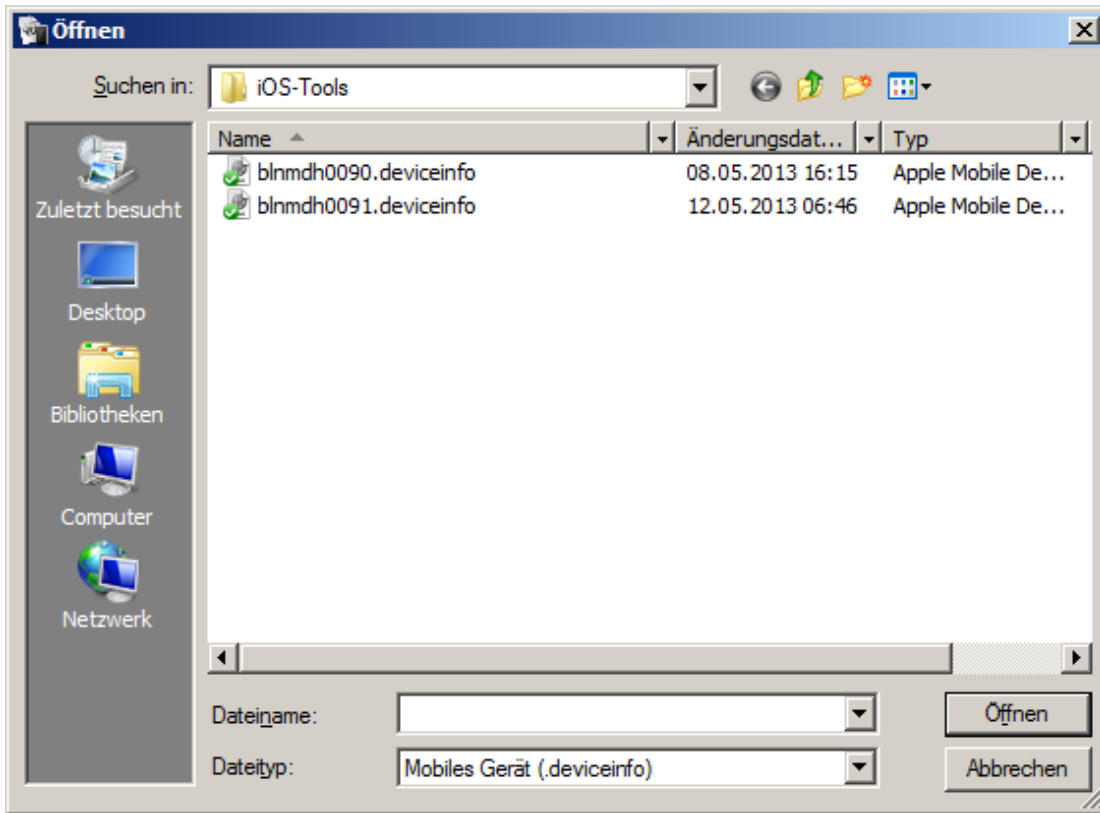


- b. Nach Anschließen des iOS-Endgerätes erscheint dieses in der Liste unter dem Reiter Geräte. Die Profile die erstellt werden, sind immer nur für das jeweils ausgewählte Endgerät gültig. Pro Endgerät wird später eine .mobileconfig erstellt, die auch nur auf diesem als Trusted bzw. Überprüft angesehen wird. Wenn Ihr viele Endgeräte zu Konfigurieren habt, wird die Nutzung eines richtigen Mobile-Device-Management ([MDM](#)) Systems bestimmt einfacher.



Für die spätere Wiederverwendung solltet Ihr das Geräteprofil gleich Exportieren ...
Eine solche Sicherung ist jedoch nur für zwei Jahre Gültig !

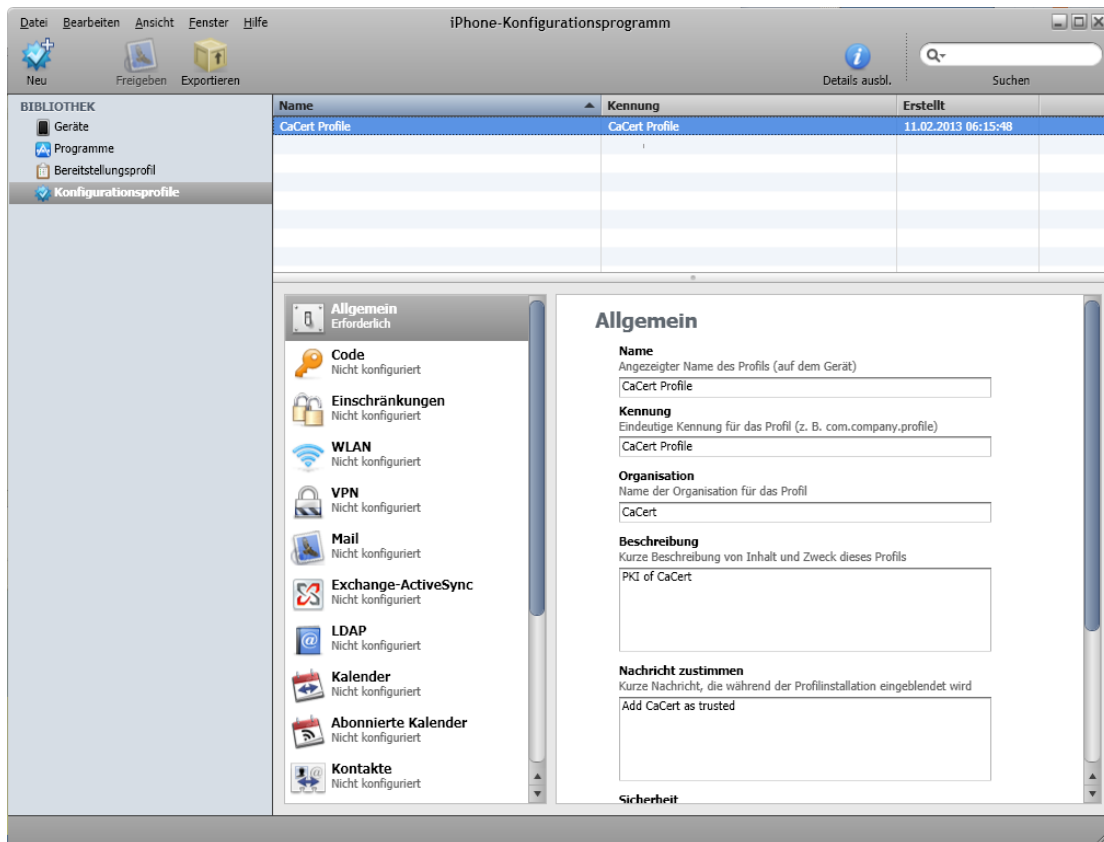
Vorhandene Geräte-Profile lasen sich per Hinzufügen Importieren ...



- Nun geht es daran, die Zertifikate einem Konfigurationsprofil hinzu zu fügen. Dies erfolgt über den Button Neu im Menü.

In dem Dialogteil der Ansicht trägt einfach alle erforderlichen Informationen zu dem Profil ein, damit sich dieses später auf dem Endgerät identifizieren lässt. Folgende Punkte sind hier noch wichtig:

Sicherheit : Diese solltet Ihr auf „Mit Authentifizierung“ ändern und ein Kennwort dafür vergeben.
Das Kennwort unbedingt notieren, zum Entfernen des Profils wird dies später benötigt!
Siehe auch Problembhebung am Ende der Dokumentation.



5. Nun wechselt Ihr im Profilmanagement in den Bereich Zertifikate. Hier werden jetzt das Class1 sowie das Class3 Zertifikat hinzugefügt, welche Ihr ja schon im Filesystem liegen habt.

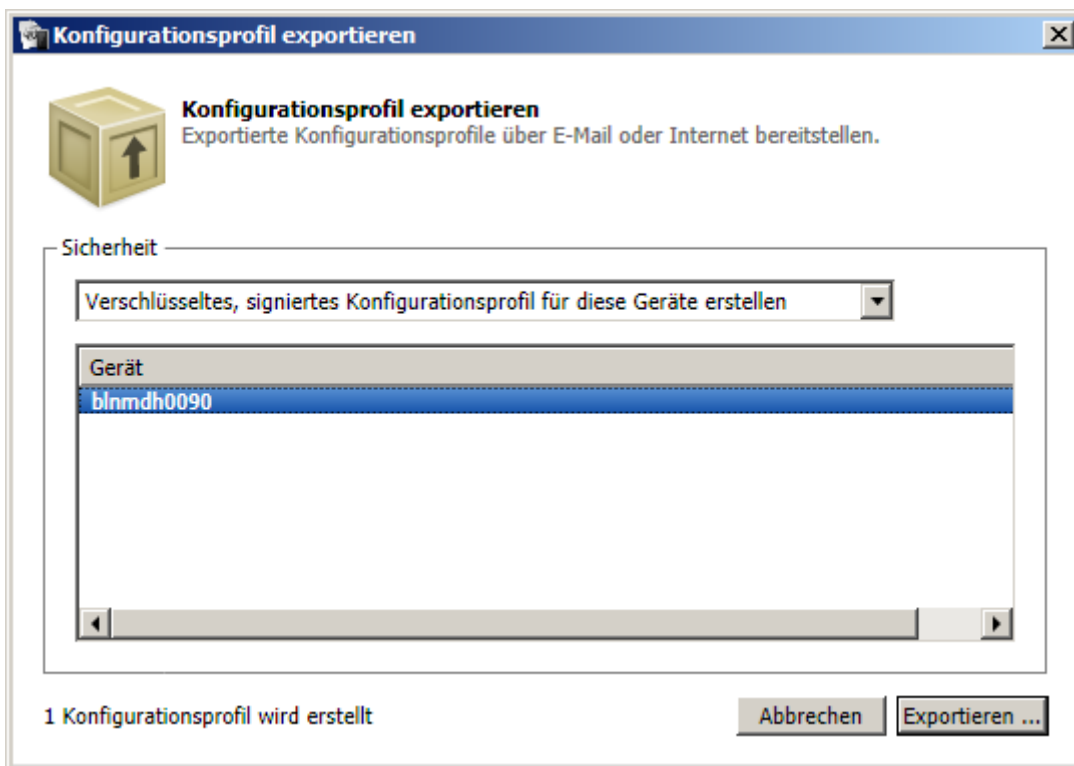
Bei Bedarf können auch noch weitere, z.B. persönliche Zertifikate (von CAcert !) für die Mailverschlüsselung, hinzugefügt werden.



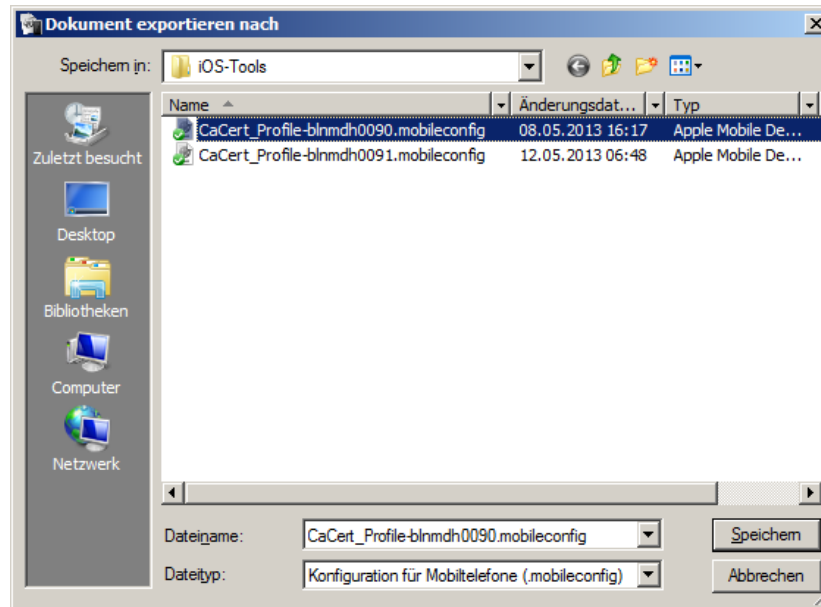
- Nach den vorhergehenden Schritten muss die Konfiguration nur noch Exportiert werden. Hierbei ist wichtig, dass der Export als verschlüsseltes und signiertes Profil für Euer Gerät erfolgt.



Wählt das oder die Geräte aus der Liste aus und dann Exportieren.
Sollte sich keine Geräteauswahl zeigen, habt Ihr bei Schritt 3.b etwas verkehrt gemacht.



Die erstellten Profile sendet dann einfach per Mail auf Euer Gerät



Aus der Mail auf dem Gerät öffnet den .mobileconfig-Anhang und folgt Einrichtungsdialog. Je nach Gerätevorgaben ist noch die System-PIN erforderlich. Danach sollten die Zertifikate als Überprüft im System vorhanden und nutzbar sein ...

Wie erkennbar, ist das Paket mit einer Signatur von iPCU mit der UUID des Gerätes als vertrauenswürdig erstellt und trägt auch dessen Signatur.



Bis auf Chrome verlassen sich seit dem alle Anwendungen auf die CA von CAcert.

Problembhebung

Wie lösche ich vorhandene Profile, wenn das Kennwort vergessen wurde?

Ohne Kenntnis des unter Punkt 4 vergebenen Kennwortes ist ein löschen des Profils nicht möglich. Um an diese zu gelangen ist ein lokales Backup durch iTunes erforderlich.

Sollten Euch nur verschlüsselte vorliegen, kann das Tool „iPhone Backup Extractor“ von Reincubate helfen.

Ihr benötigt die *.stub-Files aus dem Pfad \Home Domain\Library\ConfigurationProfiles. In diesen findet sich das Klartextkennwort unter dem Key: RemovalPassword