



## **Whitepaper**

### **Over-the-Air-Konfiguration**

und

### **Registrierung von neuen iPhones**

im

### **Enterprise-Markt**

Copyright © 2010 ICB GmbH

Alle Rechte vorbehalten. Die Weitergabe und Vervielfältigung dieses Dokumentes oder von Teilen davon ist – gleich auf welche Art und Weise – nur mit schriftlicher Genehmigung der ICB Internet Consulting for Business GmbH gestattet.

Telefon (0811) 541 77-0 • Telefax (0811) 541 77-11 • [www.icb-gmbh.de](http://www.icb-gmbh.de)  
ICB Internet Consulting for Business GmbH • Am Söldnermoos 17 • 85399 Hallbergmoos  
Amtsgericht München HRB 143316 • USt-IdNr. DE223985413  
Geschäftsführer Dipl.-Ing. Manuel Baum, Thomas Denk



---

## **1 Einleitung**

Mit der wachsenden Anzahl von iPhones in Unternehmen stellt sich die Frage, wie die Geräte konfiguriert werden können. Eine nahtlose Einbindung in die Unternehmensstruktur verlangt die Einrichtung von Diensten wie Microsoft Exchange ActiveSync, WPA2-Verschlüsselungsparameter für das WLAN und die Konfiguration der VPN-Verbindungen in die Unternehmensinfrastruktur. Apple bietet für diese Einstellungen ein Konfigurationswerkzeug, das lokal auf dem Rechner ausgeführt wird, und ein angeschlossenes iPhone konfiguriert. Mag diese Konfiguration für einzelne Geräte (meistens die der Geschäftsführer und Vorstandsmitglieder) noch gehen, so ist eine skalierbare Konfiguration von mehreren Hundert oder gar Tausenden Geräten auf diesem Weg nicht realisierbar. Stattdessen sollte die Konfiguration automatisiert erfolgen und den Nutzer des Geräts im Gedanken eines Self-Services einbinden. Ausgangspunkt des Konfigurationsprozesses ist die Authentifizierung von Geräten und Nutzern durch die Ausstellung und Verteilung digitaler Zertifikate. Diese digitalen Zertifikate werden dann für die Nutzung der Dienste verwendet.

Neben der Verwendung des Over-the-Air-Dienstes, um die Zertifikate für die öffentlichen Schlüssel der Unternehmens-PKI-Infrastruktur zu verteilen, werden auch die Konfigurationsprofile der Geräte aktualisiert. Dadurch wird sichergestellt, dass nur bestimmte Geräte mit festgelegten Konfigurationen, die den IT-Richtlinien entsprechen, verwendet werden können. Da die Konfigurationsprofile verschlüsselt sind und dadurch nicht verändert werden können, müssen alle Firmenanwender die definierten Einstellungen verwenden. Dadurch verhindert man, dass die Einstellungen nach Belieben verändert, auf fremde Endgeräte übertragen oder entfernt werden können.

Dabei kann die Konfiguration der Geräte entweder über den Over-the-Air-Prozess erfolgen, aber auch für Testzwecke manuell über den Verwaltungs-Computer mit angeschlossenen iPhones erfolgen.

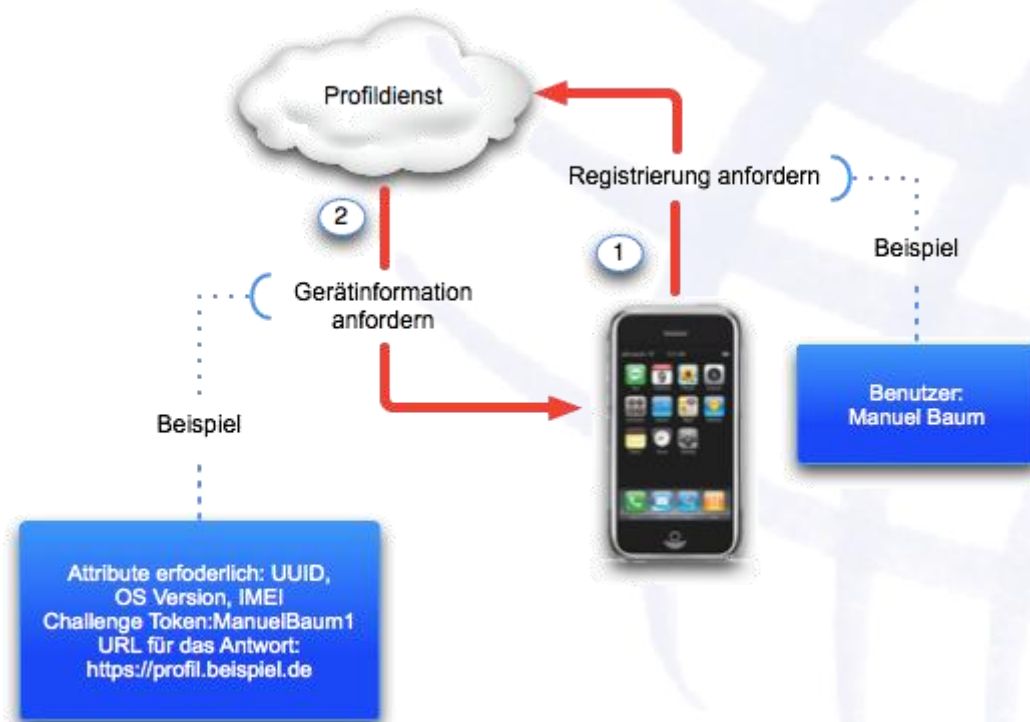
Um die Over-the-Air-Konfiguration vornehmen zu können müssen die vorhandenen Authentifizierungs-, Verzeichnis- und Zertifikatdienste im Unternehmen eingebunden und modifiziert werden. Der fertige Service kann dann über Standard-Webserver bereitgestellt und als grundsätzlicher Konfigurationsprozess definiert werden. Im Folgenden soll auf die Realisierungsmöglichkeiten für den Over-the-Air-Prozess detaillierter eingegangen werden.

## 2 Überblick über den authentifizierten Einrichtungs- und Konfigurationsprozess

Zur Umsetzung des Over-the-Air-Konfigurationsdienstes muss ein eigener Profildienst erstellt werden, der HTTP-Verbindungen akzeptiert, die Benutzern authentifiziert, ein gerätespezifisches Profil erzeugt und dann dem Endgerät bereitstellt. Benötigt wird dazu die Zertifikatsstelle des Unternehmens (Certificate Authority - CA), um das Gerät mit Authentifizierungsdaten entsprechend dem Simple Certificate Enrollment Protocol (SCEP) auszustatten

Auf den folgenden Seiten werden die verschiedenen Phasen und Schritte zur Registrierung und Konfiguration beschrieben.

### 2.1 Phase 1 – Registrierung Anfang



Phase 1 - Beginn der Anmeldung:

Start des Konfigurationsprozesses ist das Öffnen der Profildienst-URL durch den Anwender unter Verwendung von Safari (Schritt 1). Dort muss sich der Benutzer mit seiner Identität authentifizieren. Dazu können entweder einfache Authentifizierungsmechanismen wie globale Passwörter, Einmal-Passwörter oder auch bestehende Verzeichnisdienste (z.B. Active Directory) verwendet werden.

In Schritt 2 sendet der Profildienst ein Konfigurations-Profil als Antwort. Dieses Profil gibt eine Liste von Anfrageattributen vor, die das iPhone in der nächsten Antwort beantworten muss. Ferner wird zur Aushandlung der Verschlüsselung ein Pre-Shared Key basierend auf den Benutzerdaten als Challenge versendet. Dadurch soll einerseits die Identität des Benutzers zusätzlich gesichert und zudem eine benutzerspezifische Sitzung aufgebaut werden. Anfrageattribute, die durch den Dienst erfasst werden können sind die iPhone OS-Version, Geräte-ID (MAC Adresse), Abfrage des Produktes (iPhone oder iPod touch), Telefon-ID (IMEI) und SIM-Informationen (ICCID).

## 2.2 Phase 2 - Geräteauthentifizierung

Phase 2 - Geräteauthentifizierung: Nachdem der Benutzer die Installation des Profils akzeptiert hat (Phase 1), sucht das Gerät die angeforderten Attribute, fügt der Verschlüsselungs-Challenge (falls vorhanden) eine Antwort bei und signiert die Antwort mit dem Gerät integrierten Identität (ein von Apple ausgestelltes Zertifikat). Die Antwort wird über HTTP-Post zurück an den Server geschickt.



### 2.3 Phase 3 - Installation des Gerätezertifikats



In Schritt 1, antwortet der Profildienst mit den Spezifikationen, die vom Gerät zur Erzeugung eines Schlüssels (RSA 1024) benötigt werden und gibt dem Endgerät an, wo die Zertifizierungsanfrage nach SCEP (Simple Certificate Enrollment Protocol) zurück geschickt werden muss.

In Schritt 2 schickt das Endgerät die SCEP Anfrage automatisch an die Zertifizierungsstelle, wobei der Challenge-Schlüssel zur Authentifizierung des SCEP Anfragepakets verwendet wird.

In Schritt 3, antwortet die Zertifizierungsstelle mit einem verschlüsselten Zertifikat für das Endgerät.

## 2.4 Phase 4 - Konfiguration des Endgeräts



In Schritt 1, antwortet das Gerät mit der Liste der Attribute, signiert mit dem Verschlüsselungszertifikat von der Zertifizierungsstelle in der vorherigen Phase.

In Schritt 2, antwortet der Profildienst mit einer verschlüsselten .mobileconfig Datei, die automatisch installiert wird. Der Profilservice signiert die .Mobileconfig (z.B. via SSL).





---

Neben den allgemeinen Einstellungen werden in diesem Konfigurationsprofil die Unternehmensrichtlinien definiert, die durchgesetzt werden sollen. Außerdem kann das Konfigurationsprofil gesperrt, damit der Benutzer es nicht mehr aus dem Gerät entfernen kann. Das Konfigurationsprofil können zusätzliche Anforderungen für die Registrierung von Identitäten via SCEP enthalten, die ausgeführt werden, wenn das Profil installiert ist.

