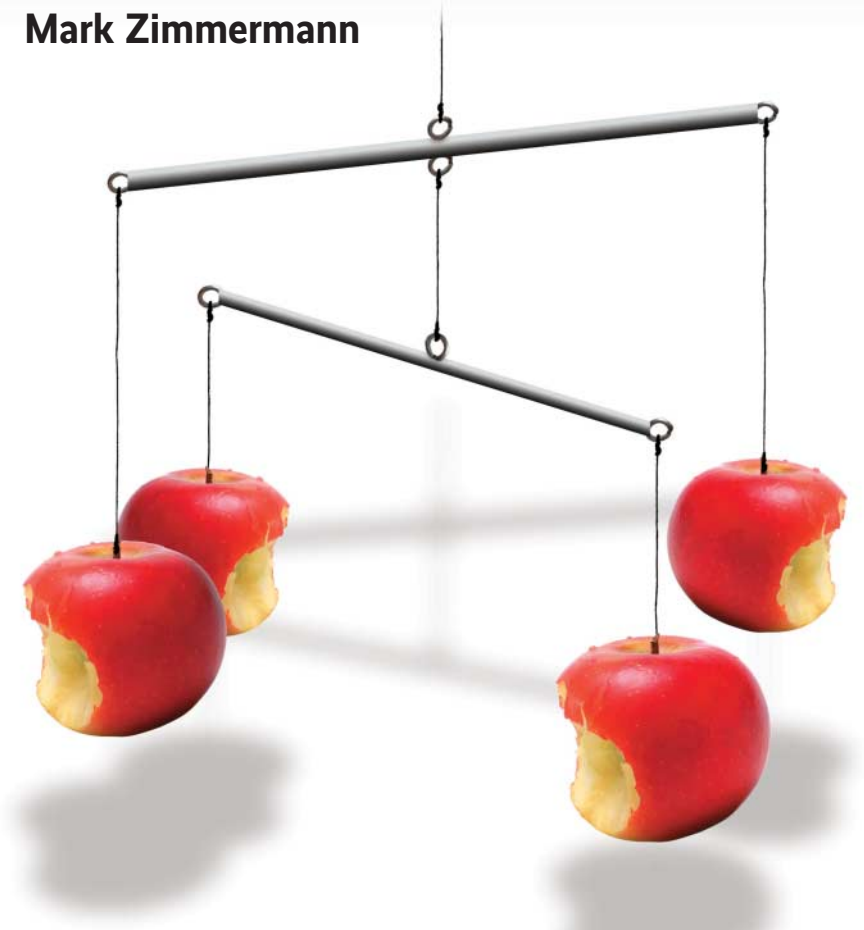
iOS-Geräte und Apps mit DEP, VPP und MDM verwalten

Volle Kontrolle

Mark Zimmermann



Apples Bereitstellungsprogramme sollen Geräteverwaltung und Lizenzierung vereinfachen. Das Device Enrollment Program (DEP) hilft, neue Geräte schnell zu konfigurieren, während das Volume Purchase Program (VPP) der einfachste Weg ist, Apps in größeren Stückzahlen für die Firma zu erwerben.

Geräteverteilung und -verwaltung ohne entsprechende Tools ist pflege-, zeit- und fehleranfällig. Durch seine Bereitstellungsprogramme will Apple das Handling von iOS- und macOS-Geräten in Kombination mit MDM-Systemen (Mobile Device Management) signifikant erleichtern. Es handelt sich dabei um:

– DEP (Device Enrollment Program) zur automatisierten Verwaltung der Verknüpfungen von iOS-Geräten mit einem MDM-System;

– VPP (Volume Purchase Program) zum Kaufen und Verteilen von Apps und Büchern in großen Stückzahlen und ihre Verwaltung in einem MDM-System (Bücher derzeit noch nicht in Deutschland).

Die Programme funktionieren unabhängig voneinander, jedes kann separat beantragt und betrieben werden.

Vor der Nutzung müssen VPP und DEP aktiviert und eingerichtet werden, und zwar beide getrennt auf der Website deploy.apple.com. Neben den üblichen Daten für eine neue Apple-ID muss man die internationale Firmennummer aus dem Data Universal Numbering System (D-U-N-S) kennen (abfragen oder beantragen unter www.upik.de) und die DEP-Nummer des Gerätelieferanten oder die eigene Kundennummer bei Apple wissen. Außerdem muss der Browser passen (Safari ab 6.0.3, Internet Explorer ab 9.0.8 oder Google Chrome 27.0.1), iOS-Browser funktionieren nicht.

Man kann keine schon vorhandene Apple-ID für die Registrierung nutzen, aber immerhin für DEP und VPP dieselbe. Die eingetragene E-Mail-Adresse ist im Nachhinein nicht änderbar, es empfiehlt sich also eine Funktionsadresse wie appleadmin@meinefirma.de. Der Registrierungsprozess für DEP und VPP erfordert einen Prüfprozess bei Apple, der zwischen wenigen Stunden und mehreren Wochen dauern kann. In dessen Verlauf wird ein ebenfalls zu hinterlegender Zeichnungsbevollmächtigter des Unternehmens als Bestätigungskontakt telefonisch kontaktiert, um die Korrektheit der Registrierung zu bestätigen.

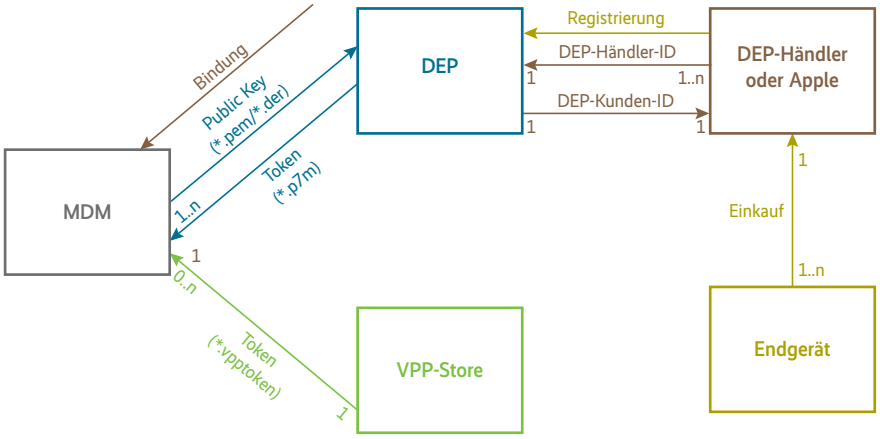
DEP-Integration in ein MDM-System

Um DEP nutzen zu können, muss mindestens ein DEP-kompatibles MDM-System in Betrieb sein. Dessen öffentlicher Schlüssel (Public Key) wird auf der DEP-Website als Zertifikatsdatei (.pem oder .der File) übergeben.

Die DEP-Site stellt wiederum ein Server-Token zum Download zur Verfügung (.p7m), das in das MDM-System eingespielt werden kann. Man kann auch mehrere MDM-Systeme autorisieren.

Neu gekaufte Geräte werden vom DEP-Händler registriert und durch den Programmverantwortlichen oder einen berechtigten Administrator mithilfe des DEP einem MDM-System zugeordnet. Ist nur ein MDM-System hinterlegt, erfolgt die Zuweisung automatisch. Ein Anmelden ist in diesem Fall nur noch nötig, wenn man einen neuen DEP-Händler hinzufügen will oder AGB-Änderungen von Apple akzeptieren muss. Gerade bei neuen iOS-Versionen ist eine AGB-Änderung ein häufiger Grund für einen gestörten Betrieb. Daher sind regelmäßige Kontrollanmeldungen beim DEP empfehlenswert.

Nach dem Einrichten sollte man in der Rubrik „Administratoren verwalten“ spezielle Administrator-Accounts für Personen einrichten, die bevollmächtigt sind, auf die Inhalte der beiden Bereitstellungssysteme zuzugreifen (das gilt gleichermaßen für DEP und VPP). Diese haben im Unterschied zum Programmverantwortlichen eingeschränkte Rech-



Sowohl Apps als auch Geräte werden über ein MDM verwaltet (Abb. 1).

te. Jeder von ihnen erhält eine Apple-ID auf Basis seiner E-Mail-Adresse, die also nicht schon für eine Apple-ID in Benutzung sein darf.

DEP automatisiert die Bindung eines direkt bei Apple oder einem teilnehmenden autorisierten Apple-Partner gekauften Geräts an ein MDM-System. Das Programm gibt es nicht nur für Unternehmen, sondern auch für Bildungseinrichtungen.

Nach dem Abschluss der technischen Einrichtung auf der DEP-Homepage bedarf es noch einer organisatorischen Maßnahme. Musste der Administrator bei der Einrichtung des DEP bereits einen autorisierten Händler als Lieferanten für Hardware benennen, muss diesem die nun erzeugte DEP-Kunden-ID des Unternehmens mitgeteilt werden.

Autorisierte Bereitstellung durch Sicherheitskette

Dies ist notwendig, um die „Letzte Meile“ in der Sicherheitskette für Apple zu schließen. Nur Geräte, die über eine durchgehende Vertrauenskette, also DEP-Händler, hinweg beschafft wurden, sind auch im DEP einsetzbar. Geräte vom Elektronikmarkt um die Ecke sind nicht DEP-fähig. Das bedeutet auch: Privateigentum lässt sich nicht nachträglich für DEP registrieren.

Größere Organisationen haben meist mehrere Zulieferer. Diese können dem DEP-Account durch den Programmverantwortlichen hinzugefügt werden. Der entsprechende Menüpunkt (Händler/Zulieferer hinzufügen) steht unter der Rubrik „Organisationsdetails“ zur Verfügung.

Beim Löschen eines MDM-Servers ist zu beachten, dass die zugehörigen Endgeräte vorher einem anderen MDM-Server zugewiesen werden. Sonst verlieren sie ihre Zuweisung.

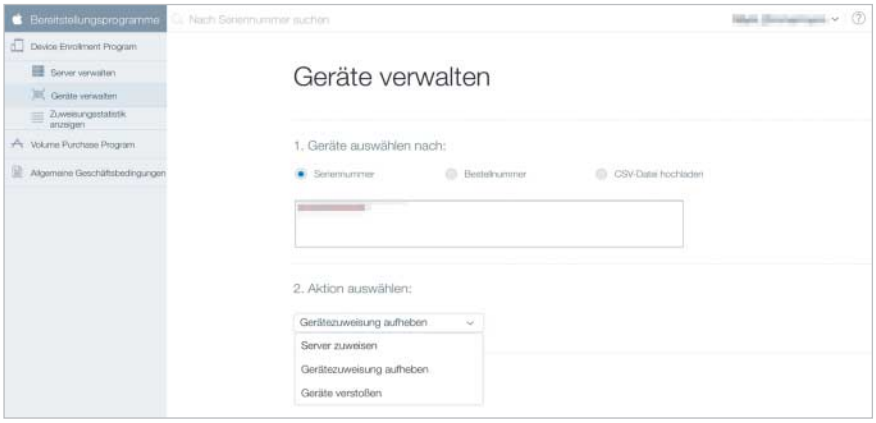
Rückwirkende Registrierung bis 2011

Neue Geräte müssen durch diese Verfahren dem Administrator nicht physisch vorliegen oder ausgepackt werden. Bestandsgeräte lassen sich bis zum 1. März 2011 rückwirkend durch DEP an ein MDM-System anbinden – wenn der damalige Lieferant Teil der Sicherheitskette ist und dies unterstützt. Nicht alle bieten dies für in der Vergangenheit erworbene Geräte an. Ein Grund dafür kann sein, dass der Zulieferer des DEP-Händlers damals nicht registriert war.

Zudem muss man sich über Service- und Bearbeitungspauschalen einigen. Apple selbst verlangt zwar kein Geld, weder von Endkunden noch von Lieferanten, doch manche Lieferanten rufen für DEP initial 5000 Euro Bearbeitungsgebühren auf, zuzüglich 5 Euro pro Gerät. Hier lohnt ein Vergleich. Hintergrund ist, dass Apple zwar keine Gebühren vom DEP-Händler erhebt, das Verfahren aber recht aufwendig ist, da das Warenwirtschaftssystem des Händlers an die Systeme von Apple angebunden werden muss.

Wenn ein Gerät ausgemustert werden soll oder verloren geht, ist es gemäß Apples AGB dauerhaft aus der Liste der verwalteten Geräte zu entfernen. Aber Achtung: Die Option „Aktive Geräte verstoßen“ sollte man nur mit äußerster Vorsicht einsetzen. Ist ein Gerät einmal aus dem DEP-Prozess „verstoßen“, kann es nicht mehr in das eigene DEP aufgenommen werden. Bei Leasing-Geräten bedarf es der Rücksprache mit dem DEP-Support oder dem Leasing-Geber.

Ein zentrales DEP-fähiges MDM-System kann über Einstellungen zur Initiali-



DEP beruht auf einer sogenannten Vertrauenskette vom Hersteller bis zum Kunden (Abb. 2).

sierung (Enrollment-Profil) festlegen, welche Eigenschaften für ein Gerät gelten, unabhängig von den Konfigurationsprofilen des MDM-Systems selbst. Dieses Enrollment-Profil speichern die MDM-Systeme bei Apple.

Zusammenspiel DEP mit dem MDM-System

Innerhalb der möglichen Einstellungen ist beispielsweise eine Kontaktperson/-telefonnummer definierbar. Diese wird im Rahmen des Einrichtungsassistenten dem Anwender gezeigt und ermöglicht es so, ihm zentrale Ansprechpartner mitzuteilen. Auf iPhones lässt sich die hinterlegte Telefonnummer direkt anrufen.

Die Einstellungen zur Initialisierung erlauben jedoch noch mehr. So ist es möglich, den sogenannten Betreuungsmodus (Supervised Modus) auf einem iOS-Gerät zu aktivieren. Funktionierte dies früher nur mit einem Mac, dem Programm AC-2 (Apple Configurator 2) und einer Kabelverbindung zu jedem einzelnen Gerät, lässt sich dieser Modus via DEP „over the air“ aktivieren. Der Betreuungsmodus erlaubt das Setzen zusätzlicher Einschränkungen wie das Stilllegen von iMessage, iTunes, AirDrop oder des Game Center, das Filtern von Webinhalten und die Einrichtung von White- und Blacklists für Apps.

Zudem ist das Gerät fest an das MDM gekoppelt. Ohne DEP kann nämlich der Anwender diese Bindung entfernen. Updates sind für Geräte mit DEP-Registrierung zentral steuerbar, im Einrichtungsassistenten lassen sich etliche Schritte überspringen, sodass unter dem Strich das iPhone oder iPad nach wenigen Minuten einsatzbereit ist. Weiterer Vorteil: Da die Bindung an das MDM-System nicht aufhebbar ist, sind die Geräte für Unbefugte nicht nutzbar.

Flexible Lizenzverwaltung und -verteilung

Das Volume Purchase Program bietet Unternehmen die Möglichkeit, Apps und Bücher in großen Stückzahlen zu kaufen und an Geräte beziehungsweise Mitarbeiter zu verteilen. Das erspart eine Reihe von Umständlichkeiten, die bei einem Privatkauf mit anschließender Abrechnung gegenüber der Firma anfallen. Der Kauf selbst erfolgt in einer iTunes-ähnlichen Umgebung: vpp.itunes.apple.com. Nach der Anmeldung beim VPP können Administratoren nach Apps oder Büchern suchen und diese in der benötigten Stückzahl erwerben.

Auch die Verbindung zwischen VPP und dem MDM-System läuft über ein Token des VPP, das in das MDM-System eingespielt wird. Im Unterschied zum DEP lässt sich ein VPP-Account nur mit einem MDM-System verbinden, ein MDM-System kann aber mehrere VPP-Accounts unterstützen. Die Token haben eine Gültigkeitsdauer von 365 Tagen oder laufen bei einem Kennwortwechsel ab. Dies gilt auch für die DEP-MDM-Kommunikation.

Der VPP-Zugang erlaubt auch den Erwerb maßgeschneiderter B2B-Apps für iOS. Externe Entwickler können spezifischen VPP-Accounts angepasste Versionen ihrer App anbieten, zu individuellen Preisen.

In Verbindung mit einem MDM-System gibt es zwei Verteilungsarten. Bei beiden bleiben die Eigentumsrechte beim Unternehmen und können jederzeit neu vergeben werden.

VPP User Assignment: Apps sind einzelnen Anwendern zugeordnet. Dazu müssen diese VPP-Teilnehmer sein, autorisiert durch ihre Apple-ID. Eine Nutzung auf mehreren Geräten durch diesen Anwender ist erlaubt.

VPP Device Assignment: Seit iOS 9 können per VPP verteilte Applikationen auch einem Gerät anhand dessen Seriennummer zugewiesen werden. Eine Apple-ID wird nicht benötigt, die App steht ausschließlich auf dem zugewiesenen Gerät zur Verfügung.

Bei beiden Verfahren lassen sich die Einstellungen nachträglich ändern, man kann zwischen ihnen wechseln. Unterschiede bestehen ebenfalls in den Update-Prozeduren – nur beim Device Assignment hat der Administrator die volle Kontrolle über die App auf dem Gerät.

Der Vollständigkeit halber sei erwähnt, dass Apps auch ohne MDM-System im VPP-Store erworben werden können, und zwar mittels Einlösecodes (VPP User Redemption). Diese sind dauerhaft mit der einlösenden Apple-ID verknüpft. So zugeordnete Apps stehen auch per Familienfreigabe den Angehörigen zur Verfügung, bei einer Verteilung über ein MDM-System ist dies nicht der Fall.

Noch mehr Komfort durch Caching-Server

Wer noch mehr tun will, kann einen Caching-Server für Apps einrichten oder die manuellen Konfigurationen im MDM-System durch die Nutzung einer API ersetzen. Den Caching-Server gibt es für 20 Euro im App-Store, und unter http://appconfig.org ist der Einstieg in die AppConfig Community zu finden. (js)

Onlinequellen

Data Universal Numbering System (D-U-N-S)
https://www.upik.de

DEP- und VPP-Registrierung
http://deploy.apple.com

MDM-APIs
http://appconfig.org

VPP-Web-Interface
http://vpp.itunes.apple.com

Mark Zimmermann

ist als Experte für mobile Lösungen tätig. Seine Expertise umfasst die Konzeption und Architektur sicherer mobiler Anwendungen.

Alle Links: www.ix.de/ix1706110