

802.11ax - Lohnt sich der Umstieg?

von Florian Hojnacki

Wie Dr. Wetzlar in der Mai-Ausgabe des Netzwerk Insiders berichtete, stehen uns bereits erste 11ax-fähige Produkte zum Test zur Verfügung. In meinem ersten Artikel für den Netzwerk Insider stelle ich Ihnen die Erkenntnisse aus meiner kürzlich abgeschlossenen Masterthesis zum Thema 802.11ax vor und hoffe, Sie auch zukünftig mit interessanten Themen auf dem Laufenden halten zu können.

Die Wi-Fi Alliance hat vor kurzem ein neues Namensschema für die WLAN-Zertifizierungen eingeführt. Somit macht sich Wi-Fi 6 bereit, Wi-Fi 4 (IEEE 802.11n) und Wi-Fi 5 (IEEE 802.11ac) langfristig abzulösen. Für Unternehmen gilt es jetzt zu klären, ob und wann ein Umstieg als sinnvoll zu erachten ist.



Bevor diese Fragen jedoch beantwortet werden können, ist ein grundlegendes Verständnis der technischen Neuerungen von 802.11ax erforderlich. Neben einer Einführung in den neuen WLAN-Standard erläutere ich, an welchen Stellen der WLAN-Nutzung aktuell Optimierungspotential besteht. Außerdem beleuchte ich einige interessante und eher unbekanntere Fakten zum neuen WLAN-Standard.

Wussten Sie zum Beispiel, dass 802.11ax genau genommen nicht ETSI-konform ist?

weiter auf Seite 7

Blick in die Zukunft: Ein neuer Registrierungsmodus in iOS13 für BYOD wirft seinen Schatten voraus!

von Mark Zimmermann

MDM-Administratoren konnten bisher eine Reihe von recht aufdringlichen Konfigurationen, Befehlen und Abfragen, mit denen viele Benutzer nicht vertraut sind bzw. waren, an unternehmenseigene Apple-Geräte senden. Dazu zählte auch das Auflisten aller auf dem Gerät installierten Apps oder die Möglichkeit, ein Gerät aus der Ferne zu sper-

ren und alle Inhalte zu löschen (Lock & Wipe). Für den Einsatz in BYOD-Szenarien waren und sind solche Features ein Alptraum für Anwender, Datenschützer und Administratoren.

Auf der Worldwide Developer Conference (WWDC) 2019 kündigte Apple einen neuen Registrierungsmodus (User Enrollment =

Benutzerregistrierung) für die Registrierung von BYOD-Geräten (Bring Your Own Device) an einem MDM-System an.

Warum brauchen BYOD-Geräte diesen neuen Registrierungsmodus?

weiter auf Seite 20

Geleit

Wireless: Die große Welle steht uns noch bevor

auf Seite 2

Standpunkt

Moderne Videokonferenzsysteme: Killerapplikationen für die Informationssicherheit

auf Seite 18

Neues Seminar

Betriebs- und Infrastruktur-Anforderungen an Softwarelösungen aus der Cloud

auf Seite 16

Aktuelle ComConsult-Kongresse

ComConsult Technologie-Tage

ComConsult Wireless Forum

auf Seite 4 und Seite 15

Geleit

Wireless: Die große Welle steht uns noch bevor

Die rasante Entwicklung der drahtlosen Technologien betrachten wir für alle Organisationen als so wichtig, dass wir – nicht zum ersten Mal – Wireless zu einem der Schwerpunkte im Netzwerk Insider gemacht haben.

Welche Entwicklungen sind gemeint? Hier nur ein Auszug:

- Produkte gemäß dem neuen WLAN-Standard IEEE 802.11ax stehen vor der Tür. Wir haben erste getestet. Kollege Hojnacki berichtet in dieser Ausgabe darüber. Er hat Inkompatibilitäten und Probleme festgestellt, die zu beachten sind. Und er hat durch eigene Messungen die Durchsatzversprechen von 11ax auf den Prüfstand gestellt.
- Die Versteigerung der 5G-Frequenzen in Deutschland ist abgeschlossen. Die vier überregionalen Provider haben Frequenzen zugewiesen bekommen. Nun sind sie am Zug.
- Es tut sich auch einiges bei anderen Funktechniken. Ob sich für die hohe Anzahl von Sensoren Bluetooth Low Energy (BLE) oder ein anderes Verfahren durchsetzt, ist zweitrangig. Sehr wahrscheinlich wird es eine Vielfalt von Funkverfahren geben. Die vielen kleinen Dinge, die funken, werden kommen. Neue Firmengebäude werden davon geprägt sein.
- Auch wenn man bei Wireless zunächst an klassische Datenübertragung denkt, ist jetzt schon klar, dass wir vor der Einführung vielfältiger Funkanwendungen stehen. Mein Kollege Dr. Dams hat schon mal im Insider über Ortung geschrieben. Neueste Forschung und Entwicklung geht aber über einfache Ortung von Wireless-Geräten hinaus. Schon jetzt gibt es Prototypen für Produkte und Lösungen, die preiswerte Wireless-Technologie zum Beispiel in der Medizin einsetzen. Stellvertretend für eine ganze Reihe von Pionieren sei hier nur der Startup Emerald (emerald-inno.com) genannt. Der Nachweis ist erbracht, dass Herzfrequenz und andere Vitalfunktionen drahtlos überwacht werden können, ohne dass an Menschen Sensoren angebracht werden müssen. Die Idee ist einfach: wenn man mit WLAN & Co. orten kann, kann man mit ein bisschen mehr Sensorik und künstlicher Intelligenz anhand von Reflexionen Bewegungen, auch winzige wie die des Brustkorbs bei der Atmung, messen.



Es geht also nicht nur darum, wie ich das neue Gigabyte-schwere Update auf mein Smartphone bekomme. Aber auch darum geht es. Unsere Projekterfahrungen zeigen: Organisationen, die noch vor einigen Jahren WLAN als unzuverlässige Spielerei abgetan haben, befassen sich jetzt mit flächendeckender WLAN-Einführung. IT ist nun mal dabei, im Bereich der Endgeräte hauptsächlich zu mobiler IT zu werden. Viele neue Anwendungen werden nur noch für mobile Endgeräte entwickelt. Und kaum jemand denkt bei einem iPhone an Kabel. Sollte man lieber das Schild „Smartphones müssen draußen bleiben“ am Gebäudeeingang aufstellen? (Lachen Sie bitte nicht; es gibt noch Gebäude, vor deren Betreten ich mein Mobiltelefon abgeben muss.) Ein solches Schild wird jedoch nicht lange da sein. Zu groß ist die Welt, der wir uns damit verschließen würden. Einige Fluggesellschaften lassen Online-Check-In und Sitzplatzauswahl nur noch mit Apps auf mobilen Geräten zu.

Entwicklungen im Verbrauchermarkt werden früher oder später auch die Berufswelt erfassen. Deshalb führt an mobilen Endgeräten und damit an Wireless auch in Unternehmen kein Weg mehr vorbei.

Man könnte sich auf den Standpunkt stellen, die Vernetzung mobiler Endgeräte sei Aufgabe der kommerziellen Anbieter, die jetzt auch die 5G-Frequenzen ersteigert haben und zur Funkversorgung verpflichtet sind.

So einfach ist es aber leider nicht:

- Erstens gibt es genügend Szenarien, in denen Menschen kommerziellen Mobilfunk nicht nutzen wollen. Ich bin regelmäßig in den USA und sehe nicht ein, warum ich die hohen Roaming-Gebüh-

ren bezahlen muss. Anderes Beispiel: Ein Betriebssystem-Update über Mobilfunk verschlingt einen Großteil des Datenkontingents der meisten Mobilfunkkonten.

- Zweitens schirmen viele Gebäude elektromagnetische Wellen so stark ab, dass im betreffenden Haus eine Mobilfunknutzung unmöglich oder sehr eingeschränkt ist. Die als Abhilfe geltende In-house-Versorgung durch Provider macht entweder abhängig oder arm (je nachdem, ob sie nur für einen oder mehrere Provider gemacht wird).
- Drittens haben sich die überregionalen Provider bei der bisherigen Funkversorgung nicht gerade mit Ruhm bekleckert. Ärgernis über Funklöcher gehört zum Alltag. Bei 5G ist noch Schlimmeres zu befürchten, denn dafür werden mehr Basisstationen benötigt.
- Viertens schweben speziell die 5G-Projekte der überregionalen Provider gewissermaßen in einiger Unsicherheit. Bis der Rechtsstreit über das nationale Roaming in letzter Instanz ausgefochten ist, können Jahre vergehen. Provider, die gegen die Pflicht zum nationalen Roaming geklagt haben, können nämlich auf die Idee kommen, vor größeren Investitionen die letztinstanzliche Rechtsprechung abzuwarten oder das anhängliche juristische Verfahren als Vorwand für die eigene Unfähigkeit zum Netzausbau vorzuschieben.

Was lernen wir daraus?

Die Lektion ist klar: Organisationen müssen ihre Wireless-Zukunft zumindest ein Stück weit in die eigene Hand nehmen.



Abbildung 1: Verbote sind auch keine Lösung

802.11ax - Lohnt sich der Umstieg?

802.11ax - Lohnt sich der Umstieg?

Fortsetzung von Seite 1



Florian Hojnacki ist seit 2010 bei der ComConsult GmbH als Berater tätig. Im Competence Center Netze liegt sein Fokus auf der Planung und Konzeption von LAN und WLAN-Infrastrukturen im large Enterprise Umfeld. Das erlernte Wissen seiner Masterabschlüsse aus Köln und Melbourne setzt er seit 2019 erfolgreich bei Kundenprojekten ein.

Technische Einführung 802.11ax

Wie bereits in vielen anderen Publikationen zum Thema 802.11ax dargelegt wurde, liegt der Fokus im neuen Standard auf einer Steigerung der Effizienz. Orthogonal Frequency Division Multiple Access (OFDMA) beschreibt die zentrale technologische Neuerung im Hinblick auf besagte Steigerung. Mittels OFDMA bietet der Standard eine Möglichkeit, den vorhandenen Kanal mit der Breite 20 (oder 40, 80, 160) MHz in kleinere Unterkanäle (sog. Resource Units) aufzuteilen. Der Vorteil besteht darin, dass die Größe dieser RUs variabel ist und diese an mehrere Stationen gleichzeitig vergeben werden können. So bietet OFDMA die Möglichkeit, mit bis zu 9 Clients pro Spatial Stream im selben Zeitschlitz zu kommunizieren. Abbildung 1 visualisiert die vereinfachte Aufteilung dieser Unterkanäle.

Bei einem Unterträgerabstand von 78,125 kHz bietet OFDMA Unterkanäle mit Bandbreiten von 2, 4, 8 oder 20 MHz. Das in 11a/n/ac genutzte Modulationsverfahren OFDM hat zum Vergleich einen Unterträgerabstand von 312,5 kHz. Die Verkleinerung des Unterträgerabstands (bzw. Vergrößerung der Symbollänge) wirkt sich außerdem positiv auf Reichweite und Stabilität im Outdoorbereich aus. Die in diesem Kontext vergrößerte minimale Dauer des Guard Intervals (GI) auf 0,8 µs reduziert Inter-Symbol-Interference (ISI), was unter anderem zu besagter Stabilität führt.

Die durch OFDMA ermöglichte Parallelität von Übertragungen mehrerer Stationen erhöht somit die zuvor erwähnte Effizienz deutlich. Abbildung 2 stellt den theoretischen Gewinn an Airtime dar. Das gemeinsame Senden von Daten für mehrere Stationen reduziert die Anzahl benötigter Preambles sowie der notwendigen

Pausen zwischen einzelnen Übertragungen. Besonders vorteilhaft ist diese Technologie bei vielen kleinen Datenpaketen, wie sie zum Beispiel beim Telefonieren über VoIP genutzt werden.

Eine Studie von Aruba Networks in 2015 besagt, dass 80% des gesamten WLAN-Verkehrs in einem typischen Büroumfeld aus Frames mit Größen unterhalb 256 Byte bestehen [1]. Diese Aussage dürfte heute noch immer zutreffend sein.

Die Analyse einiger Wireshark-Mitschnitte untermauert diese Aussage. Abgesehen von mitgeschnittenen iPerf Sessions ist eine durchschnittliche Paketgröße von knapp 200 Byte erkennbar.

Bei vielen kleinen Frames zeigt OFDMA den höchsten Effizienzgewinn, da mit Einsatz der Resource Units sämtliche Zeitslots effizienter ausgelastet werden. Es

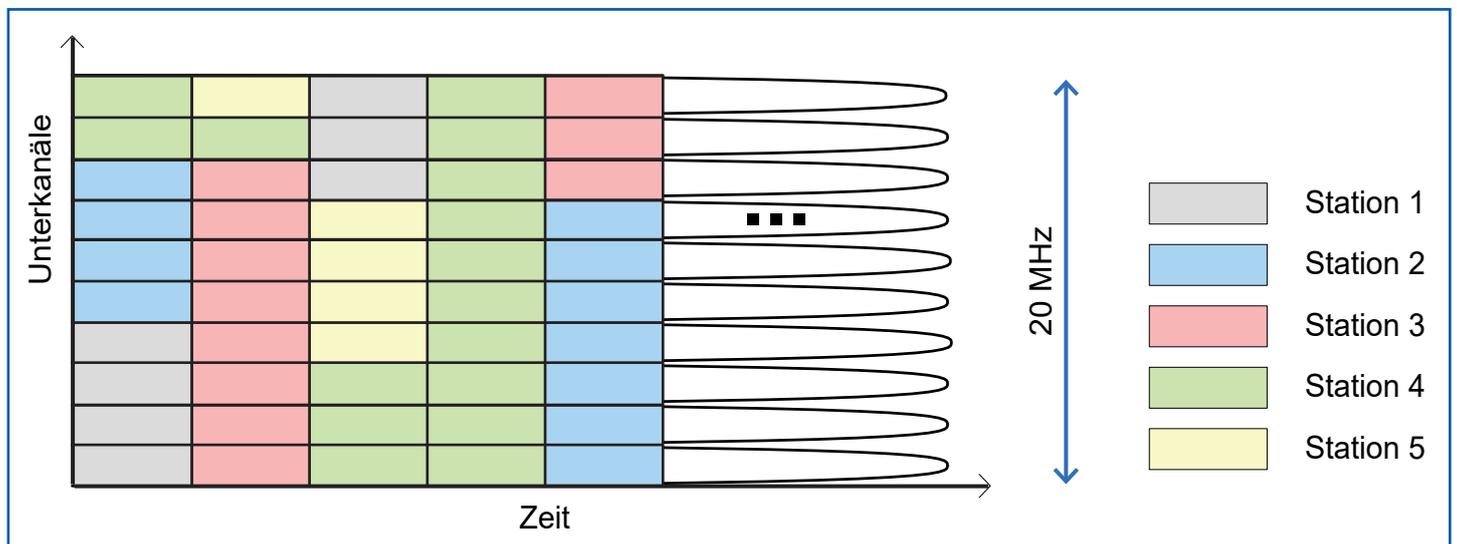


Abbildung 1: OFDMA Resource Units

802.11ax - Lohnt sich der Umstieg?

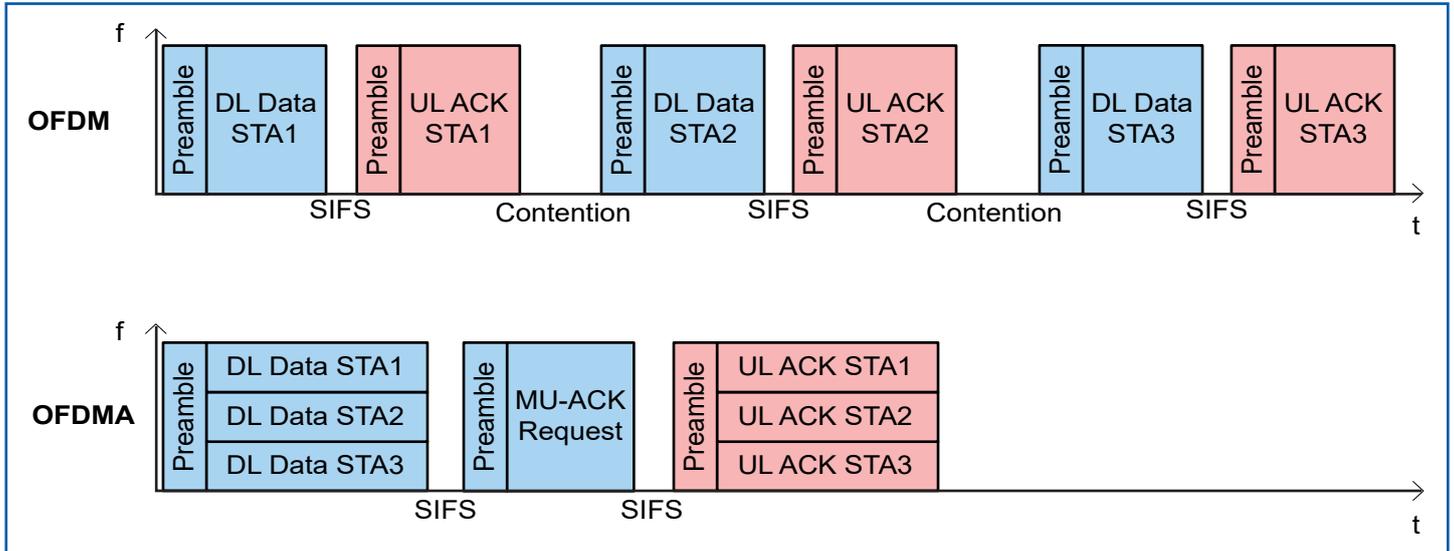


Abbildung 2: OFDM vs. OFDMA

ist zu erwarten, dass der somit erreichbare Gesamtdurchsatz einer WLAN-Zelle bei hohen Clientzahlen deutlich steigt.

Mit der Einführung eines neuen Header-Typs wird MU-MIMO nun auch in Uplink-Richtung ermöglicht. Der AP meldet seine Empfangsbereitschaft mit Trigger Frames an eine zuvor ausgehandelte Gruppe von Stationen, welche daraufhin zeitgleich ihre Daten senden.

Zur Erinnerung: MU-MIMO beschreibt die Aufteilung mehrerer Datenstreams auf unterschiedliche Nutzer. Ermöglicht wird dies durch die Erstellung einer Steering Matrix, die Informationen über die RF-Charakteristiken aller teilnehmenden Stationen enthält. Viele Access Points unterstützen derzeit vier Spatial Streams über vier Antennen (4x4:4). Unter der Annahme, dass zwei Smartphones mit jeweils einer Antenne und ein Tablet mit zwei Antennen zum

Datenempfang bereitstehen, kann ein AP dies durch Beamforming seiner zur Verfügung stehenden Antennen zeitgleich durchführen.

Die Kombination aus OFDMA und MU-MIMO ermöglicht somit Parallelität auf zeitlicher und räumlicher Ebene.

Dieser Vorteil ist in Abbildung 3 verdeutlicht. Die parallele Kommunikation mit mehreren Stationen auf Frequenzebene wird durch OFDMA ermöglicht. Mehrere Spatial Streams können dank MU-MIMO ebenfalls auf mehrere Stationen aufgeteilt werden.

Diese Flexibilität ermöglicht eine deutlich effizientere Ausnutzung der zur Verfügung stehenden (Unter-)Kanäle.

Wie hoch der tatsächliche Gewinn letztendlich sein wird, werden erste Testum-

gebungen und Pilotprojekte belegen, sobald eine größere Anzahl an Stationen 11ax unterstützen. Wir werden in naher Zukunft Tests mit einer steigenden Anzahl an 11ax-fähigen Endgeräten durchführen und über die Ergebnisse informieren. Ziel ist eine Abbildung des tatsächlichen Effizienzgewinns durch OFDMA und Spatial Reuse.

Das eben genannte Spatial Reuse ist eine weitere wichtige Neuerung. Das Ziel dieser Technologie ist die Reduzierung von Gleichkanalstörungen. Das Problem in aktuellen WLAN-Netzen besteht in der sequentiellen Kanalnutzung und dem fehlenden Bewusstsein der Zellzugehörigkeit. Empfängt eine Station Frames von fremden Zellen mit einer gewissen Signalstärke auf demselben Kanal, wartet die Station auf Beendigung dieser Fremdkommunikation, bevor mit der eigenen Kommunikation fortgefahren werden kann.

Wie in Abbildung 4 vereinfacht dargestellt muss somit Station B warten, bis die Kommunikation zwischen Station A und dem fremden Access Point abgeschlossen ist.

Optimierungspotential besteht in den Fällen, in denen eine Station während des Clear Channel Assessments (CCA) Datenverkehr aus benachbarten Zellen empfängt, die der AP jedoch nicht mehr sieht. In diesem Fall hilft Spatial Reuse durch Veränderung des entsprechenden Grenzwertes, so dass parallele Kommunikation auf demselben Kanal unter gewissen Voraussetzungen möglich ist.

Der oben genannte Grenzwert teilt sich bei Kommunikation gemäß IEEE 802.11

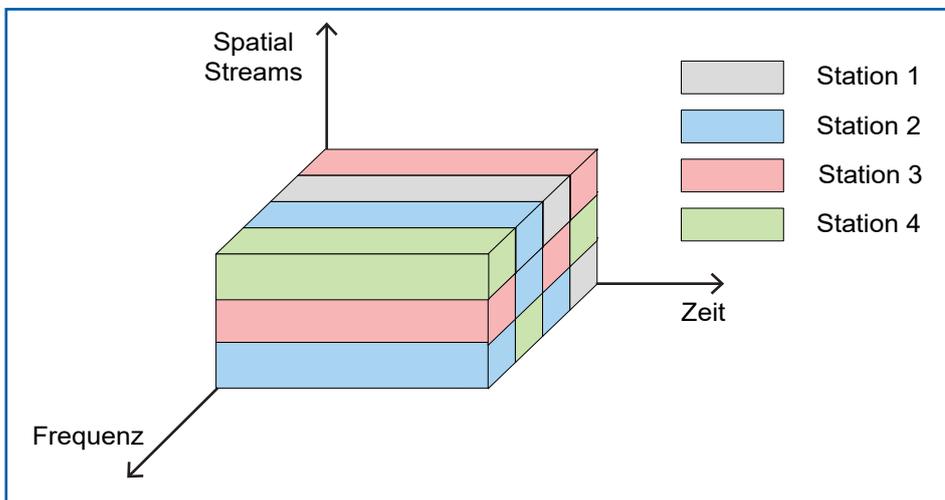


Abbildung 3: OFDMA und MU-MIMO

Blick in die Zukunft: Ein neuer Registrierungsmodus in iOS13 für BYOD wirft seinen Schatten voraus!

Blick in die Zukunft: Ein neuer Registrierungsmodus in iOS13 für BYOD wirft seinen Schatten voraus!

Fortsetzung von Seite 1



Mark Zimmermann weist mehrere Jahre Erfahrung in den Bereichen Mobile Sicherheit, Mobile Lösungserstellung, Digitalisierung und Wearables auf. 2009 hat er ein Team zur mobilen Lösungsentwicklung für einen der großen Energieversorger Deutschlands aufgebaut. Dieses Team hat über die Zeit sowohl Endkunden-Apps als auch Apps für den internen Einsatz agil gemeinsam mit dem Fachbereich entwickelt. Für eine dieser Lösungen wurde im Jahr 2013 der Best-Practice-Award 2013 des Bensberger Kreises vergeben. Er versteht es, mobile Themen aus den unterschiedlichen Herausforderungen darzustellen. Hierzu ist er auf nationaler Ebene mit Vorträgen und als freier Autor für Fachpublikationen tätig.

Die bisher gebotenen Modi für die MDM Geräteregistrierung

- Profil-basierte Registrierung (durch MDM Client aus dem AppStore oder per Apple Configurator)
- und DEP-Geräteregistrierung

bieten leistungsstarke Funktionalitäten auf unternehmenseigenen Endgeräten. Dabei adressieren diese Modi hauptsächlich COPE (Corporate Owned, Personally Enabled) und COBO (Corporate Owned, Business Only) Endgeräte.

Derart registrierte Geräte erlauben es einem MDM-Administrator, dieses zu löschen, sperren und sehr stark einzuschränken. Mithilfe des Betreuungsmodus (Supervised) können diese Konfigurationen noch tiefer gehend erfolgen. Zusätzlich können MDM-Administratoren einen so genannten Unlock-Token einsetzen, um ein Gerät von seinem PIN-Code zu befreien. Auch das Aufheben der Apple ID Bindung ist möglich.

Der Schutz der Privatsphäre eines Anwenders eines solchen Gerätes ist allerdings gefährdet. Administratoren sind zumindest grundsätzlich in der Lage, die Geräte zu inventarisieren. Hierzu besteht die Chance, die installierten Apps genau so einzusetzen. Auch das Umleiten von vermeintlich privater Kommunikation durch VPN oder WiFi Proxy Regeln ist möglich.

Viele MDM Hersteller haben hier zwar Vorkehrungen getroffen, dass derartige Einblicke und Veränderungen in einem BYOD Modus unterbunden werden - das Vertrauen der Anwender blieb jedoch trotzdem in Teilen aus.

Mit der neuen Benutzerregistrierung (**User Enrollment**) zielt Apple daher nun dar-

auf ab, die Möglichkeiten eines MDM-Systems stark einzuschränken und trotzdem die Unternehmensdaten, sowie die Privatsphäre des Anwenders gleichermaßen zu schützen.

Worin unterscheidet sich die Benutzerregistrierung von der bisherigen Geräteregistrierung?

Die Benutzerregistrierung schränkt die Berechtigungen, die ein MDM-Administrator beim Verwalten eines Geräts hat, im Vergleich zu früheren Registrierungsmodi erheblich ein. Nachfolgend finden Sie eine Zusammenfassung der wichtigsten Änderungen:

- **Geräteinformation:** Das MDM kann keine Informationen zur Geräteidentifizierung wie beispielsweise eine Seriennummer, eine UDID (Universal Device Identifier), eine IMEI oder eine MAC-Adresse mehr abrufen. Stattdessen stellt das Gerät eine anonymisierte Kennung (EnrollmentID) bereit, die für die Dau-

er der MDM-Registrierung gültig ist. Im ActiveSync Umfeld existiert der EAS-DevicelIdentifier. Dieser unterliegt denselben Regularien. Wenn sich ein Gerät abmeldet und zu einem späteren Zeitpunkt erneut anmeldet, wird eine neue EnrollmentID erstellt. Dies trägt zur Wahrung der Anonymität des Endbenutzers und seiner Hardware bei.

- **Profile und Konfigurationen:** Mit der Benutzerregistrierung stehen dem MDM-Administratoren nur noch eine Handvoll an Konfigurationsoperationen im Umgang mit dem verwalteten Bereich auf dem Gerät zur Verfügung, hierzu gehören:
 - dienstliche Apps und dienstliche Konten installieren und konfigurieren,
 - für das Gerät einen „komplexen“ Passcode (6-stellig, Zahlen) erzwingen,
 - Per-App-VPNs konfigurieren.
- Administratoren können für die Firmen-E-Mail- (**MailDomains**), -Kontakte- (**ContactsDomains**) und -Kalender

BETREUUNGSMODUS (SUPERVISION)

- ▶ Der Betreuungsmodus (Supervision) ist ein spezieller Modus in iOS, der eine **tieferer Verwaltung** und Konfiguration durch einen MDM-Server ermöglicht.
- ▶ Eine **wachsende Anzahl von Konfigurationen** ist nur verfügbar, wenn das betreffende Gerät betreut wird. Es empfiehlt sich, firmeneigene Geräte im Betreuungsmodus zu betreiben.
- ▶ Beispiele für Konfigurationen, die **nur** im Betreuungsmodus möglich sind:
 - ▶ Kamera deaktivieren
 - ▶ App Store deaktivieren
 - ▶ Safari deaktivieren
 - ▶ Hinzufügen von E-Mail-Accounts deaktivieren
 - ▶ und vieles mehr

Abbildung 1: Der Betreuungsmodus erlaubt noch tiefer gehende Konfigurationen.

Blick in die Zukunft: Ein neuer Registrierungsmodus in iOS13 für BYOD wirft seinen Schatten voraus!

derserver (**CalendarDomains**) eine Domain-VPN-Regel festlegen, sofern der Second-Level-Domain des VPN Servers mit den Sync-Werten der genannten Keys übereinstimmen. Hier spielen Firmenkonfigurationen und persönlicher Datenschutz eine entscheidende Rolle. Auf einem derart registrierten Gerät kann der MDM-Administrator so keine VPN-Regel vorgeben, die sich auf die Anbindung privater E-Mail-Konten auswirken kann.

- **Geräteaktionen obliegen dem Anwender:** Die Privatsphäre und die Kontrolle über das eigene Gerät obliegt dem Endbenutzer. Durch die Benutzerregistrierung wird MDM-Administratoren die Möglichkeit genommen, einen Geräte-PIN festzulegen oder diesen zu entfernen. Geräte lassen sich nicht mehr in Gänze löschen. Auch andere Vorgänge auf Geräteebene lassen sich nicht mehr durchführen.
- **App-Verwaltung:** Ein MDM-Administrator kann Apps wie zuvor installieren und entfernen. Er kann jedoch nur die von ihm verwalteten Apps im Rahmen einer Inventarisierung sehen. Installiert ein Anwender selbst Apps, sind diese für das MDM nicht sichtbar. Das Pflegen von White-/Blacklisten ist für den MDM-Administrator nicht möglich.
- **App-Konfiguration:** Eine im Rahmen der Benutzerregistrierung installierte und verwaltete App kann - wie bisher auch - per MDM eigene Steuerkommandos (App-Config) erhalten.

Alles dreht sich um die verwaltete Apple ID

Die Apple VPP- und Apple DEP-Portale (deploy.apple.com) wurde durch den Apple Business Manager (ABM) in einem Single-Sign-In-Portal mit einer einheitlichen Benutzeroberfläche vereint.

Wie zuvor mit DEP können Administratoren mehrere MDM-Serverobjekte erstellen und diesen Endgeräte zuweisen. Der VPP-Aspekt von ABM ist ebenfalls eine Verbesserung. Navigieren durch gekaufte Apps und Bücher ist einfacher und optisch ansprechender geworden. Die alten Web-Portale werden zum Jahresende abgeschaltet, damit dürfte der ABM eine 100% Marktabdeckung im Firmenumfeld - bei Einsatz von Apple Endgeräten - erfahren.

Damit eine Benutzerregistrierung für ein Endgerät eingesetzt werden kann, bedarf es einer personenbezogenen verwalteten Apple ID. Eine derartige Apple ID kann von Personenverantwortlichen bzw. Administratoren im Apple Business Manager angelegt werden.

Für größere Organisationen dürfte dabei interessant sein, dass Apple eine Anbindung an Microsoft Azure Active Directory für den Apple Business Manager im Laufe des Jahres angekündigt hat. Verwaltete Apple-IDs lassen sich so automatisch im Apple Business Manager erstellen, sofern ein entsprechendes User-Objekt als Azure Identität vorhanden ist.

Verwaltete Apple-IDs wurden initial mit dem Apple School Manager, der speziell für den Bildungsbereich entwickelt wurde, eingeführt. Eine verwaltete Apple-ID, im Umfeld von ABM, ist eine Apple-ID, die einer Organisation gehört. Eine verwaltete Apple ID bietet derzeit verschiedene Funktionen:

- **Lizenzierung von Apps:** Werden Apps per MDM verteilt, verwaltet der Apple Business Manager die Volume Lizenzen einer Firma. Apps können zwar an ein Gerät, aber auch an eine verwaltete Apple ID verteilt werden. Die Eigentumsverhältnisse verweilen in beiden Fällen weiterhin bei der Firma.
- **iCloud-Zugriff:** Apple wird dieses Jahr iCloud-Dienste auf Unternehmensebene einführen. Hierzu gehören Enterprise iCloud (Shared Storage für ein Unternehmen) und Enterprise Notizen. Die verwaltete Apple-ID dient als Berechtigungsnachweis für den Zugriff auf diese Ressourcen.
- **Zugriff auf Beta-Software:** Mit einer verwalteten Apple ID können sich Anwender am „AppleSeed for IT Programm“ anmelden. Hier stehen Testpläne, Beta-Feedback Gruppen und Kanäle genauso zur Verfügung wie die aktuellen Beta-Softwarebestände aus Cupertino.

Im Vergleich zu klassischen Apple IDs sind die verwalteten Apple IDs aber auch in der Funktionsweise eingeschränkt. So erlauben diese keinen Einkauf (weder gebührenpflichtige noch kostenlose) im App/iTunes/iBooks Store durch den Anwender. Ebenso bieten sie keine Unterstützung für

- HomeKit
- iCloud Mail
- „Freunde suchen“,
- „Mein iPhone suchen“,
- „Find my“
- iMessage Nachrichten,
- FaceTime
- und die Cloud Familie Freigabe.

Verwaltete Apple-IDs stehen dabei nicht in Konflikt mit den klassischen Apple-IDs. Ein Anwender kann seine von der Firma zugewiesene verwaltete Apple ID parallel zu seiner persönlichen Apple ID verwenden.

Datentrennung dank APFS

Als Sicherheits- und Datenschutzmechanismus wird während der Benutzerregistrierung (**User Enrollment**) ein separates APFS-Volumen erstellt. Ein derartiges APFS-Volumen kann als eine weitere Partition - mit einer eigenen zufällig generier-

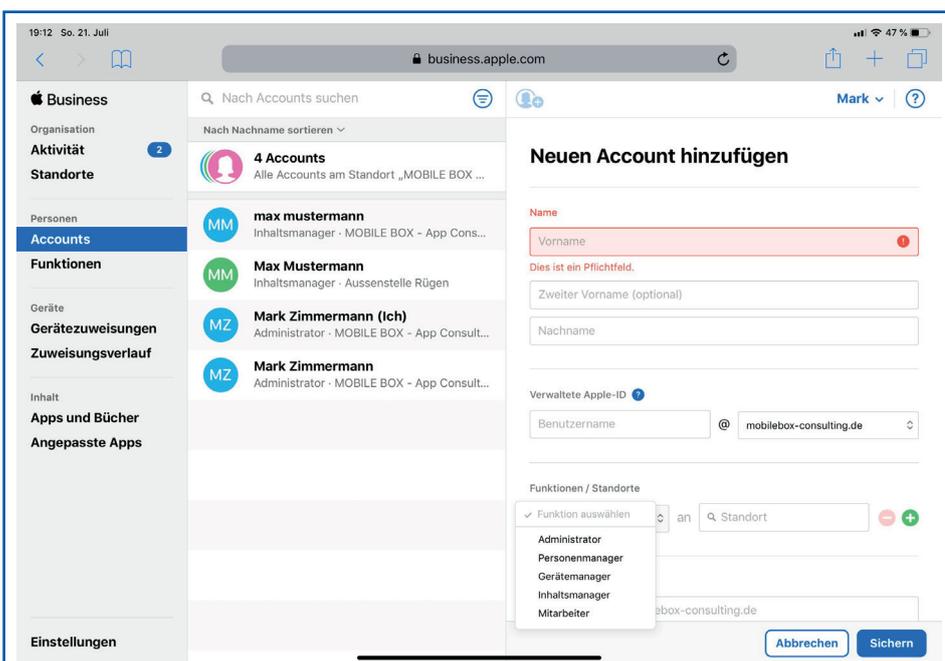


Abbildung 2: Verwaltete (managed) Apple IDs lassen sich im Apple Business Manager anlegen und verwalten.

Anmeldung

ComConsult Informationsservice

Verpassen Sie keine wichtigen Informationen mehr und tragen Sie sich in unserem ComConsult Informationsservice ein.

Unser Informationsservice informiert Sie regelmäßig per E-Mail und per Post über aktuelle Entwicklungen in der IT-Branche und über unsere Veranstaltungen und Neuerscheinungen. Der Service umfasst unser monatliches Magazin „Der Netzwerk Insider“, sowie regelmäßige E-Mails über unser aktuelles Produktangebot. Darüber hinaus senden wir Ihnen im Bedarfsfall unsere Technologie-Standpunkte und Technologie-Warnungen zu aktuellen Entwicklungen zu.

Anrede

Name

Firma

E-Mail-Adresse

oder online unter

<https://www.comconsult-research.de/insider-2/>