



Tablets im Schuleinsatz managen

Version 1.5 – Stand 09/17

**Dieser Artikel beschreibt den Einsatz von Tablets im Schulbetrieb
und zeigt Möglichkeiten der effizienten Verwaltung auf.**

© 2017 M-Way Solutions GmbH, Stresemannstr. 79, 70191 Stuttgart
Tel: 0711/25254-60

<http://www.relution.io>

Alle Rechte vorbehalten

Inhalt

Inhalt.....	2
Zugehörige Links.....	2
Tablets in der Schule.....	3
Ausbaustufe 1 – Klassensätze	3
Ausbaustufe 2 – ein Tablet pro Schüler	4
Relution for Education	4
Vorgehensweise	5
1) Einschreiben der Tablets	5
2) Vergeben von Richtlinien	6
3) Anlegen von Regelwerken (optional)	6
4) Ausführen von Aktionen	7
Der Betrieb von Relution	7
Relution-Systembeschreibung	8
Zusätzliche Anforderungen für Mobiles Gerätemanagement.....	9
HTTPS-Zertifikat	9
Relution Client	10
Mobile Endgeräte	10
iOS-Client.....	10
Android-Gerätemananger	11
App Launcher	11
Organisations-Struktur	11
Häufig gestellte Fragen	12

Zugehörige Links

Relution Software (Server/Clients):

<http://repo.relution.io/package/latest/relution-package.zip>

http://repo.relution.io/apps/ios/latest/Relution_Enterprise.ipa

<http://repo.relution.io/apps/android/latest/Relution-normal-release.apk>

Relution Änderungshistorie:

<http://repo.relution.io/package/latest/changelog.pdf>

Relution-Handbuch und Installationsanleitung:

<http://repo.relution.io/package/latest/manual.pdf>

<http://repo.relution.io/package/latest/installguide.pdf>

Tablets in der Schule

Im Zuge der Digitalisierung des Bildungswesens beschäftigen sich immer mehr Schulen mit der Einführung von Tablets. Die Einsatzmöglichkeiten sind vielfältig: Tablets ermöglichen einen interaktiven, lebendigen Unterricht mit digitalen Ausflügen ins Internet und die Verwendung interaktiver Lerninhalte, die mittlerweile in zahlreichen Apps angeboten werden. Man braucht nicht viel Vorstellungskraft, um einzusehen, dass der gute alte Computerraum mit seinen stationären PC's wohl keine große Zukunft mehr vor sich hat. Beim Tablet-Einsatz an Schulen kommen grundsätzlich zwei Varianten zur Anwendung:

Ausbaustufe 1 – Klassensätze

Die erste "Ausbaustufe" besteht in der Regel aus einem oder mehreren Tablet-Klassensätzen, die in passenden Rollkoffern von den Lehrern in die Klassen mitgebracht werden können. Die Tablets werden an die Schüler verteilt und nach Unterrichtsende wieder eingesammelt.

Aus IT-Sicht ergibt sich hier die Herausforderung, die Tablets mit einem einheitlichen Software-Stand auszurüsten, einige Sicherheitsrichtlinien einzustellen und bei Bedarf die erstellten Daten einfach löschen zu können.

Ein schultaugliches Tablet-Management-System (auch Mobile Device Management oder MDM genannt) muss dazu die entsprechenden Funktionen bereitstellen:

- Automatisches Enrollment (Inventarisierung) der Geräte (Apple DEP, Samsung KME)
- Verteilen von Apps auf die Geräte durch Push-Verfahren sowie Updates
- Zentrales Konfigurieren der Geräte (z.B. WLAN, Kiosk-Modus, Einschränkungen der Funktionalität)
- Sperren (und Entsperren) der Geräte, etwa bei Verlust
- Löschen und Wiederherstellen der Geräte
- Betriebssystem-Updates steuern

- evtl. Benutzermanagement (Login, Datenverzeichnis, etc.)

Je nach Betriebssystem des Tablets (Apple iOS, Google Android) stehen zur Unterrichtsdurchführung unterschiedliche Funktionen zur Verfügung; bei Apple-Geräten gibt es die Classroom-App, mit der der Lehrer gezielt Inhalte auf den anderen Tablets aufrufen und bei Bedarf die Tablets der Schüler entsprechend einschränken und überwachen kann. Bei Android-Tablets bietet Samsung eine ähnliche Funktion an.

Ausbaustufe 2 – ein Tablet pro Schüler

Die zweite "Ausbaustufe" ist ein 1:1-Szenario: hier hat jeder Schüler ein "eigenes" Tablet, das entweder von der Schule gestellt oder in einem Leasing-Modell von den Eltern (mit)finanziert wird. Hier ergeben sich natürlich weitere Anwendungsmöglichkeiten, etwa das dauerhafte, fächerübergreifende Arbeiten mit dem Tablet oder auch das Nutzen des Tablets außerhalb der Schule.

IT-seitig muss beim 1:1-Szenario zwischen den verschiedenen Betriebsarten "Unterricht" und "Freizeit" unterschieden werden. Im Unterricht ist natürlich die Schule für das Absichern und Betreiben des Tablets verantwortlich, außerhalb des Schulgebäudes soll der Schüler andererseits das Tablet möglichst vielseitig nutzen können, etwa auch zum Spielen und Kommunizieren mit Freunden, was während des Unterrichts natürlich nicht möglich sein sollte. Das MDM-System muss daher in der Lage sein, zwischen diesen Betriebsarten hin- und herzuschalten, und zwar entweder zeit- oder ortsgesteuert. Außerhalb der Schulzeiten sind in vielen Fällen sicher auch die Eltern daran interessiert, eine gewisse Kontrolle über das Tablet ihres Kindes auszuüben, etwa die Nutzung zeitlich oder inhaltlich einzuschränken. Dazu gibt es zum MDM-System passende Eltern-Apps, die diese Kontrolle ermöglichen.

Relution for Education

Relution for Education ist eine Tablet-Management-Software speziell für Schulen und Lehrbetriebe. Relution ermöglicht die Einhaltung höchster

Datensicherheits-Standards wie der Europäischen Datenschutz-Richtlinie (GDPR) bei einfachster Bedienung und einem beeindruckenden Leistungsumfang. Es deckt beide oben beschriebenen Szenarien sowohl für Android-Tablets (bevorzugt Samsung) als auch für iPads ab. Durch seine Mandantenfähigkeit können z.B. alle Schulen eines Schulträgers bequem von einem einzigen Server aus bedient werden; dank seiner intuitiven Oberfläche kann das Tablet-Inventar ohne große Einarbeitung verwaltet, abgesichert und konfiguriert werden.

Wichtig dabei: Relution for Education wird in Deutschland entwickelt und betrieben – wahlweise als Cloud-Lösung, zur Installation in der Schule oder beim Schulträger.

Vorgehensweise

Beim erstmaligen Einrichten von Relution wird wie folgt vorgegangen:

1) Einschreiben der Tablets

Der Einschreibevorgang inventarisiert das Tablet und stellt es unter die Kontrolle des MDM-Systems. Bei Relution funktioniert das entweder vollautomatisch oder manuell.

Vollautomatisch: Für Apple-Geräte mittels Device Enrollment Program, kurz DEP

Für Samsung-Geräte mittels Knox Mobile Enrollment, kurz KME

Die Geräte werden vom Hersteller in einem eigenen Web-Portal erfasst und können über eine Schnittstelle in Relution importiert werden. Dieses Portal wird mit dem Relution-Server verknüpft. Dabei werden alle für die Einschreibung erforderlichen Daten bereits hinterlegt, sodass das Gerät sich beim ersten Einschalten automatisch beim Relution-Server einschreibt.

Diese Einschreibung kann so geschützt werden, dass sie vom Benutzer nicht mehr zu entfernen ist. Damit ist ein reibungsloses Hinzufügen neuer Tablets ohne Zutun des Administrators möglich.

Manuell: Mit ein paar Klicks wird eine Einschreibung im Relution-Admin-Portal angelegt; der dabei erzeugte Link kann dabei per E-Mail oder SMS auf das Gerät gesendet oder per QR-Code direkt aufgerufen werden. Damit wird die Einschreibung auf dem Gerät vollzogen.

Bei der Einschreibung wird automatisch die Relution-App auf dem Gerät installiert und mit den erforderlichen Rechten versehen. Anschließend steht das Gerät unter der Kontrolle des Administrators, der im Web-Admin-Portal umfassende Möglichkeiten zum Managen der Geräte hat.

2) Vergeben von Richtlinien

Richtlinien bestehen aus Konfigurations-Profilen für die unterschiedlichen Funktionen des Tablets, wie z.B. WLAN-Zugänge, Email-Konten, erlaubte und verbotene Apps, Sicherheitsmaßnahmen (etwa Passwortsrichtlinien) und vieles mehr. Sie können beliebig viele Richtlinien anlegen und sie anschließend einem oder mehreren Geräten zuweisen. Unterscheiden muss man dabei zwischen Android- und iOS-Geräten, da die Richtlinien aufgrund der verschiedenen Funktionen der Betriebssysteme plattformabhängig sind.

3) Anlegen von Regelwerken (optional)

Regelwerke bestehen aus einer Liste von frei definierbaren Wenn-Dann-Regeln, die das Verhalten des Systems bei bestimmten Ereignissen festlegen. So kann bei einer Konformitätsverletzung des Geräts (z.B. indem eine App gelöscht wurde) automatisch nach einer bestimmten Zeit der Benutzer oder der Administrator benachrichtigt werden. Sogar Aktionen auf dem Gerät können per Regel ausgeführt werden, etwa das Sperren des Geräts oder das komplette Zurücksetzen.

4) Ausführen von Aktionen

Jedes unter MDM-Kontrolle stehende Gerät kann Aktionen vom Relution-Server empfangen und ausführen. Je nach Betriebssystem reichen die Möglichkeiten vom Installieren und Löschen von Apps über das Orten des Geräts bis hin zur kompletten Sperrung bei Verlust oder dem Zurücksetzen auf Werkszustand. So kann der Administrator jederzeit per Mausklick die von ihm verwalteten Geräte steuern.

Der Betrieb von Relution

Sind alle Tablets eingeschrieben und per Richtlinien konfiguriert, überwacht Relution die Geräte selbsttätig und meldet - falls gewünscht - erkannte Probleme an den Administrator. Dessen Aufgabe besteht nur noch darin, im Fehlerfall oder bei Änderungen der Anforderungen einzugreifen. Damit ist der Administrations-Aufwand im täglichen Betrieb gering, und der Schulbetrieb wird nicht beeinträchtigt.

Über die Inventar-Ansicht im Relution-Portal kann sich der Administrator einen schnellen Überblick über die von ihm verwalteten Geräte schaffen, dabei wird der Status jedes Geräts mit einer einfachen Ampel-Logik visualisiert: Grün bedeutet "alles ok", rot deutet auf ein Problem hin. Für jedes Gerät steht darüberhinaus eine Detail-Ansicht zur Verfügung, die weitergehende Informationen bis hin zur Betriebssystemversion, dem Akku-Ladezustand und dem Speicherverbrauch bereithält.

Teil des Relution-Systems ist außerdem ein eigener App-Store, der im Prinzip genauso funktioniert wie die bekannten öffentlichen Stores von Google und Apple. Eigene Apps können hier hochgeladen und den Benutzern zur Verfügung gestellt werden. Dabei dient die Relution-App als App-Store-Client. Über ein benutzerbasiertes Berechtigungssystem kann dabei gezielt gesteuert werden, wer welche Apps zur Verfügung gestellt bekommt.

Relution-Systembeschreibung

Das Mobile App Management-Modul dient der zentralen App-Verwaltung und –Verteilung. Es funktioniert auch unabhängig vom MDM-Modul, wenn z.B. ein App Store für nicht gemanagte Geräte benötigt wird.

Die MAM-Funktionen im Einzelnen:

- 1 Relution Enterprise App Store zur Verteilung von Apps auf die mobilen Endgeräte der Benutzer, hierarchisch strukturierbar
- 2 Unterstützung von nativen Apps (Binaries), Apps aus den öffentlichen Stores (Apple, Google, Microsoft) und Weblinks
- 3 App-Versionsverwaltung (mehrere Versionen einer App in verschiedenen Status wie Entwicklung, Test, Produktion)
- 4 App-Metadatenverwaltung inkl. Auslesen der Eigenschaften aus den Binaries, mehrsprachiger Texte, Screenshots und Icons
- 5 Frei definierbare App-Kategorien
- 6 Automatischer App-Update-Prozess (keine veralteten App-Versionen im Umlauf, inkl. Push-Benachrichtigung)
- 7 Granulare Abbildung von Rechten je App in jedem Freigabestatus
- 8 Konfigurierbarer App-Freigabeprozesse (Q-Gates)
- 9 Anbindung von Source-Code-Repositories und Build-Systemen
- 10 Volume Purchase Program (Lizenzmanagement von iOS-Apps)
- 11 Automatische (Re-)Signierung von Apps
- 12 Upload von Apps in andere MDM-Systeme
- 13 Sammeln von Crash Reports

Das Mobile Device Management Modul übernimmt das Management der mobilen Geräte und stellt auf diese Weise sicher, dass nur Apps auf Geräten installiert werden, die diese auch fehlerfrei ausführen können. Weiter können über das MDM Informationen wie Status, Lokation usw. aus den Geräten direkt abgefragt werden. Durch Richtlinien und das dazugehörige Regelwerk kann die Sicherung und Einhaltung von Sicherheits-Vorgaben konfiguriert und gesteuert werden.

Die folgenden Funktionen liefert das MDM-Modul:

- 1 Automatisches Einschreiben via DEP und KME
- 2 Konfiguration von E-Mail Konten und Kalendern
- 3 Durchsetzen von Passwort-Richtlinien
- 4 Einstellen von Geräte-Restriktionen:
 - Kiosk Mode
 - App Black-/Whitelisting
 - Erlauben/Verbieten der Kamera
 - Aktivieren/Deaktivieren von Bluetooth
- 5 Konfiguration von VPN-Zugängen
- 6 Verteilen von Zertifikaten
- 7 Automatische Einrichtung von WLAN-Netzwerken
- 8 Automatische (De-)Installationen von Apps und Weblinks
- 9 Dateien und Zertifikate auf Geräte pushen
- 10 Nachrichtenversand
- 11 Sperren und Löschen von Geräten, Lost Mode
- 12 Passwörter zurücksetzen
- 13 Alarm auslösen
- 14 Geräte orten

Der Relution Server ist eine OSGI/Java-basierte Anwendung, die self-contained läuft, d.h. alle zum Betrieb notwendigen Module mitbringt. Die Datenhaltung erfolgt in einer relationalen Datenbank (MySQL), die im Rechenzentrum zur Verfügung gestellt wird.

Als Java-Anwendung wird Relution auf einem Linux- oder Windows-Server mit installierter Java Virtual Machine (JVM 1.8 oder höher) eingesetzt.

Zusätzliche Anforderungen für Mobiles Gerätemanagement

HTTPS-Zertifikat

Die Sicherheit der Benutzerdaten wird durch eine verschlüsselte Kommunikation zwischen Relution-Server und Relution-App gewährleistet. Um den Server per TLS abzusichern, wird ein Server-Zertifikat im .pem-Format benötigt.

TLS 1.0, 1.1 und 1.2 werden unterstützt; die empfohlene Schlüssellänge beträgt 2048 Bit.

Zusätzlich wird der RSA Private Key (kein pkcs8) benötigt.

Relution Client

Der Relution Client ist eine App für die jeweilige Zielplattform (hier: Android), die u.a. folgende Funktionen bietet:

- Sichere Kommunikation mit dem Relution Server über HTTPS mit SSL/TLS
- Abbildung der MDM-Client-Funktionen
- Launcher-Funktion mit Kiosk-Mode
- Enterprise App Store mit Rechteverwaltung (MAM-Client)
- Endpoint zum Empfang von Push-Services

Mobile Endgeräte

Relution unterstützt mobile Endgeräte (Smartphones und Tablets) mit folgenden Betriebssystemen:

- Android 4.6 und höher
- Samsung KNOX Version 3 und höher
- Apple iOS 7.1.2 und höher
- Windows Phone 8

Abweichend von Standard-Geräten können auch kundenspezifische Geräte unterstützt werden – etwa solche, die über keine eigene Push-Infrastruktur verfügen.

Die clientseitige Architektur sieht folgenden Aufbau vor:

iOS-Client

Der iOS-Relution-Client implementiert lediglich die MAM-Funktionalitäten auf den Devices. Die MDM-Funktionen werden clientseitig durch iOS

selbst zur Verfügung gestellt. Der Relution-Client kann dabei an die Anforderungen des Kunden angepasst werden.

Android-Gerätanager

Der Android-Relution-Client implementiert die MDM- und MAM-Funktionalitäten auf den Devices. Dazu benötigt er unter Android die Rolle des Gerätemanagers. Der Gerätemanager stellt das technische Gegenstück zum Relution-Backend dar und übernimmt die Kontrolle über das Gerät. Der Relution-Client kann dabei an die Anforderungen des Kunden angepasst werden.

App Launcher

Der Relution-Android-Client ist gleichzeitig Android-Launcher und stellt somit die Bedieneroberfläche dar. Technisch läuft der Relution-Client im Kiosk-Modus und ermöglicht lediglich das Aufrufen freigegebener Apps. Ein "Ausbrechen" aus dieser App ist nicht möglich; die App muss daher zwingend Startpunkt nach dem Start des Gerätes sein.

Organisations-Struktur

Relution baut auf einem sog. Organisationsmodell auf, das die Mandantenfähigkeit des Systems sicherstellt.

Es gibt eine übergeordnete Ebene (Store-Orga), die einen übergeordneten App-Store zur Verfügung stellt. Sie hat damit die globale Kontrolle über alle Apps.

Benutzer sehen ausschließlich die Apps, die für Ihre Orga (= ihre Schule) freigegeben sind. Pro Schule gibt es einen oder mehrere „Orga Admins“. Sie sind für den App-Freigabeprozess auf Schulebene verantwortlich. Zur Freigabe stehen dabei alle neuen App-Versionen zur Verfügung, die in der Store-Orga für diese Schule freigegeben wurden.

Häufig gestellte Fragen

- F: Wie kann ich verhindern, dass Schüler das Tablet aus dem MDM entfernen?
- A: Unter iOS: DEP verwenden und damit das MDM-Profil schützen
Unter Samsung: Relution-App per Richtlinie als erforderliche App hinzufügen
- F: Wie kann ich öffentliche Apps verteilen, ohne auf jedem Gerät einen Store-Account zu benötigen?
- A: iOS: Volume Purchase Program (VPP) verwenden
Android: APK herunterladen und in den Relution-Store als native App hochladen
- F: Wie kann ich verhindern, dass bei der Einschreibung ein Store-Account benötigt wird, um die Relution-App herunterzuladen?
- A: Die APK- und IPA-Dateien herunterladen und in den Relution-Store hochladen, dann unter Einstellungen-Organisation-Relution Client Apps diese hochgeladenen Apps als MDM-Clients auswählen
- F: Wie stelle ich sicher, dass im Unterricht eine bestimmte App ausgeführt wird und nichts anderes?
- A: iOS: Die Apple Classroom-App (aus dem AppStore) verwenden
Android: Den Kiosk-Modus (Richtlinie) verwenden