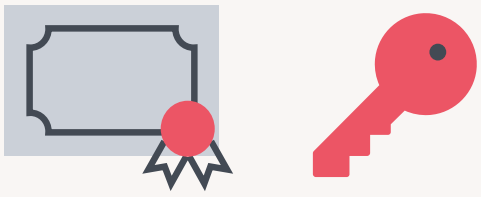
Zertifikate mit Jamf verwalten

Zertifikate spielen eine entscheidende Rolle bei der Sicherung, Authentifizierung und Erhaltung der Stabilität Ihrer Apple Geräte. Wenn sie richtig verwendet werden, erhöhen sie die Transparenz und reduzieren die Sicherheitsrisiken.

Grundlagen der zertifikatsbasierten Kommunikation

Zertifikate können verwirrend oder zu komplex wirken. Das liegt oft daran, dass sie falsch verwendet oder missverstanden wurden, und ohne externe Hilfe kann der Start eines erfolgreichen zertifikatbasierten Projekts durchaus verwirrend oder kompliziert sein.

Außerdem werden Zertifikate in einer Kundenumgebung oft falsch verwendet. Beispielsweise sagt Ihnen die Sicheheitsabteilung, dass Sie etwa ein Dutzend Zertifikate auf Ihren Macs installieren müssen. Also verwenden Sie Composer, stellen Backups her und platzieren sie in Ihrem Bereitstellungsworkflow.



Aber wozu dienen diese Zertifikate?

Wir wissen es nicht. Aber sie sind jetzt im Schlüsselbund (Keychain) installiert. Sind sie vertrauenswürdig? Ist der Schlüsselbund komplett? Vielleicht. Vielleicht nicht.

Sehen wir uns die Einrichtung und Bereitstellung von Zertifikaten einmal ganz logisch an!

Was sind Zertifikate?

Ein Zertifikat ist lediglich eine Textdatei. Das ist alles. Natürlich gibt es viele Aspekte hinter den Kulissen, mit denen Sie sich genauer beschäftigen können – Signierung, Kryptografie und Private Key Infrastructure (PKI). Aber das ist die eigentliche Datei.

Wie erzeugen Sie ein Zertifikat?

Um ein Zertifikat zu erstellen, benötigen wir eine Zertifikatsanfrage oder CSR. Dann kontaktieren wie einen Zertifikatsserver, der wiederum mit der Zertifizierungsstelle (CA) spricht und seinen Teil zu dieser Unterhaltung beiträgt. Manchmal fügen wir auch das Root-Zertifikat hinzu. Dann haben wir ein digital signiertes Zertifikat.

Wenn Sie ein Zertifikat in einem Texteditor öffnen, sehen Sie nur einen nicht lesbaren Hex-Code, da das Zertifikat verschlüsselt ist. Auf einem Mac können Sie trotzdem den Inhalt eines Zertifikats mit Spotlight überprüfen, indem Sie die Leertaste drücken, oder indem Sie es mit Schlüsselbundzugriff öffnen, um den Inhalt anzusehen.

Welche Daten enthält ein Zertifikat?

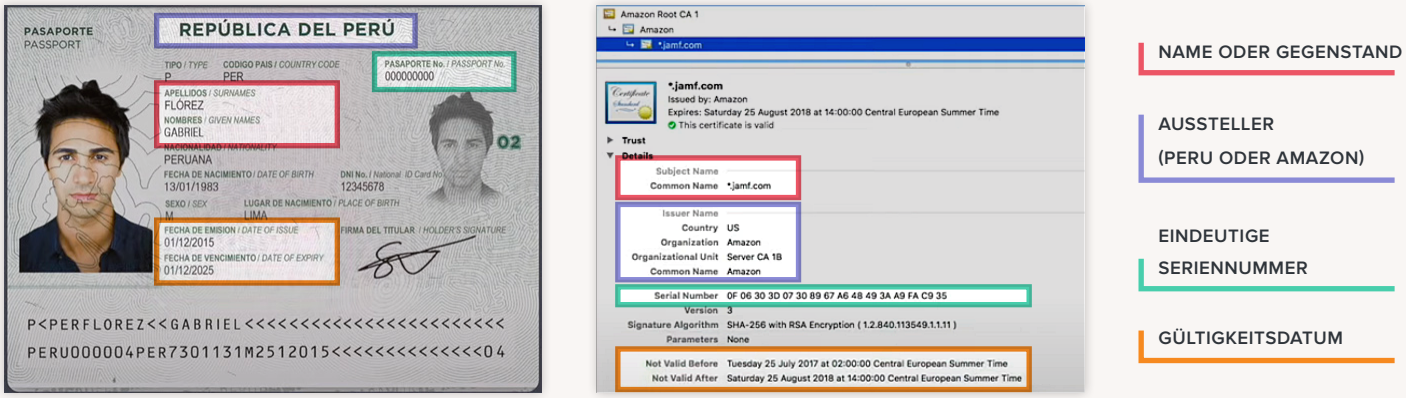
Identifikationsdaten. Ein Zertifikat ist im Grunde ein Ausweis. Ein Zertifikat ist eine signierte und vertrauenswürdige Identifizierungsquelle, wie ein Führerschein oder ein Reisepass. Wie bei einem Pass basiert die Vertrauenswürdigkeit des Dokuments auf der ausstellenden Behörde.

Wenn ich einen Gabelstapler-Führerschein habe, der in Kanada ausgestellt wurde, heißt das nicht, dass ich damit in Deutschland einen Gabelstapler fahren darf. Ebenso erlaubt es mir eine Kundenkarte von Media Markt nicht, bei Tchibo billiger einzukaufen.

Etwas wie ein Pass funktioniert nur überall als gültiger Ausweis, weil die Aussteller sich darauf geeinigt haben, einander zu vertrauen. Wenn Peru Sie als Staatsbürger ausweist, akzeptiert Kanada das, weil der Pass ein vertrauenswürdiges Dokument ist.

Aber falls jemand beispielsweise einen mit Sand-bedeckten galaktischen Reisepass vorzeigt und behauptet, ein Jedi-Meister zu sein, würde niemand dem Inhalt dieses Dokuments glauben, da es nicht aus einer vertrauenswürdigen Quelle stammt.

Sehen wir uns ein Zertifikat neben einem Pass an, um zu vergleichen, was sie gemeinsam haben.



Zertifikate sind also nicht völlig unverständlich!

Warum werden Zertifikate auf Computern verwendet?

Um Sicherheit zu bieten. Die Verwendung von vertrauenswürdigen Zertifikaten ermöglicht eine verschlüsselte Kommunikation, die während der Übertragung nicht abgefangen werden kann.

Wenn Sie eine Website über https besuchen und ein grünes Häkchen oder ein Schloss-Symbol in der Adressleiste erscheint, kommunizieren Sie mittels eines Zertifikats mit diesem Server. Die geteilte Verbindung zu dieser Website ist sicher.

Zertifikate als Anmeldedaten

Zertifikate können als Alternative zu Anmeldedaten von Benutzern verwendet werden. Wenn ein Client ein Zertifikat präsentiert, untersucht der Server dieses und entscheidet, ober er dem Client auf der Basis des Inhalts und der Zertifizierungsstelle vertraut.

Wo können wir diese Form einer sicheren Identifizierung verwenden?

Mit 802.1x WLAN, das normalerweise als ein zertifikatsbasiertes WLAN bezeichnet wird. Das ist viel besser als ein traditionelles WPA-Passwort, da die verwendeten Zertifikate nicht geteilt werden können.

Üblicherweise verwendet Ihre Netzwerk-Authentifizierungsstelle Extensible Authentication Protocol (EAP) oder Radius (ein weiteres Authentifizierungsprotokoll), je nach gewählter Verschlüsselung.

Jamf hat den Vorteil, dass es den Client validiert, der sich mit dem Netzwerk verbindet. Das Client-Gerät kann Benutzerinformationen innerhalb des Zertifikats präsentieren, die genau zeigen, wer ein bestimmtes Gerät in Ihrem Netzwerk verwendet.

Das ist für Ihre Kollegen im InfoSec-Team äußerst nützlich.

Verwendung von Zertifikaten zur Verbindung mit VPNs

Ein weiterer häufiger Verwendungszweck für Zertifikate ist die Verbindung zu einem Virtual Private Network (VPN). Wie bei einem WLAN sind Benutzername und Passwort vielleicht nicht ausreichend, um Vertrauen zu schaffen. Wir wollen sicherstellen können, dass das Gerät auch vertrauenswürdig ist. Der Zugriff wird verweigert, wenn die Anmeldedaten der Benutzer deaktiviert sind oder das Zertifikat widerrufen wurde.

Authentifizierung von drahtgebunden Netzwerken mit Zertifikaten

Sie können mit Zertifikaten sicherstellen, dass Ihre Unternehmensdaten sicher sind.

Die 802.1x Authentifizierung ist nicht auf WLAN beschränkt. Obwohl das weniger oft vorkommt, kann es auch bei einem drahtgebundenen Netzwerk verwendet werden. Das bietet eine weitere Methode um zu verhindern, dass praktisch jeder Zugriff auf eine Netzwerkverbindung erhält und vertrauliche Daten einsehen kann.

Verwendung von Zertifikaten mit verschlüsselter E-Mail

Wenn Zertifikate signiert und vertrauenswürdig sind, kann eine E-Mail nicht ohne die Installation der korrekten Zertifikate gelesen werden. Diese Technologie gewährleistet auch, dass die Nachricht nach der Signierung und Absendung nicht während der Übermittlung modifiziert wurde.

Verwaltung von Zertifikaten mit Jamf Pro

Bereitstellung von Zertifikaten

Die Bereitstellung von Zertifikaten mit einem Apple MDM ist unkompliziert: Der MDM-Anbieter wie Jamf kümmert sich um den Lebenszyklus des Zertifikats. Zu Sicherheitszwecken haben Anbieter verschiedene Möglichkeiten, den Zugriff der Benutzer zu widerrufen, wenn diese:

- Gegen die Compliance verstoßen
- Das Unternehmen verlassen

Die Rolle der Zertifikate bei Apple und MDM

- **Push-Benachrichtigungen (APNS)**
  Das gesamte Push-Benachrichtigungssystem von Apple verwendet bei der Kommunikation eine Kette von vertrauenswürdigen Zertifikaten. Ohne Zertifikate würde das nicht funktionieren.
- **Betreuungs-Identitäten (Supervision Identities)**
  Im Fall von Apple Configurator erstellt Jamf eine zertifikatsbasierte Betreuungs-Identität, die zwischen mehreren bereitstellenden Macs geteilt werden kann, um iOS Geräte zu überwachen und zu registrieren. Diese Betreuungs-Identität kann Jamf Pro für die Geräte hinzugefügt werden, die es betreut.
- **Codesignierung durch Entwickler**
  Als Entwickler haben Sie es mit Dutzenden verschiedener Zertifikate zu tun, von der App-Signierung bei der Distribution bis zu Apple Pay Zertifikaten. Sie verwenden wahrscheinlich bereits einige dieser Zertifikate in Jamf.

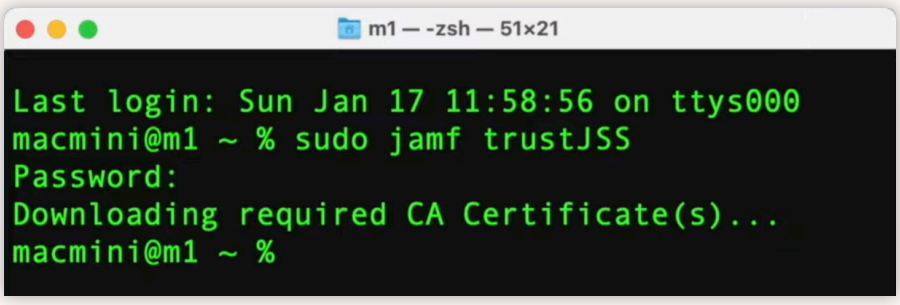
Integrierte Zertifizierungsstelle

Jamf Pro hat eine eigene integrierte Zertifizierungsstelle (CA). Diese selbstsignierte CA erzeugt ein Root-Zertifikat, dem man auf dem Gerät vertrauen muss, bevor es dem MDM-Profil vertrauen kann.

Wie und wo verwendet Jamf Pro Zertifikate?

Die kurze Antwort: fast überall. Zertifikate spielen eine Rolle in folgenden Fällen:

- Registrierungsprofile
- Geräteverwaltung mit dem Jamf Binary



Der Befehl trustJSS

- Apache Tomcat SSL: Für einen nach außen gerichteten Server müssen Sie ein öffentlich vertrauenswürdiges Zertifikat installieren.
- Die integrierte Zertifizierungsstelle ermöglicht es Ihnen, Jamf so zu konfigurieren, dass es mit einem externen CA-Server kommunizieren kann. Hier werden auch die Einstellungen für SKAT Proxy und ADCS Connector konfiguriert.
- Health Care Listener: Verwendet Zertifikate, um eine sichere Kommunikation in einem Krankenhausnetzwerk zu gewährleisten.

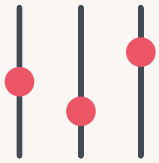
Profi-Tipp:

Jamf Cloud kümmert sich automatisch um all diese Web-App-Arbeit. Sie müssen sich nie wieder um Ihre TomCat-Einstellungen kümmern.

- Single-Sign-On
- LDAP-S über SSL
- Der Registrierungsprozess
- Signierung des QuickAdd-Pakets: Erfordert ein App-Distributionszertifikat von Apple. Dieses Zertifikat wird dann von Composer zur Signierung Ihrer anderen Pakete verwendet.
- Konfigurationsprofile: Die in Jamf Pro erstellten Konfigurationsprofile werden automatisch signiert. Das sichert sie bei der Bereitstellung. Wenn Sie eine Konfiguration direkt von der Konsole aus herunterladen, ist diese bereits signiert. Deshalb können Sie die XML-Rohdaten nicht mit einem Texteditor anzeigen. Wenn Sie ein mit Jamf erstelltes Konfigurationsprofil bearbeiten wollen, müssen Sie zuerst die Signierung aufheben.
- App-Bereitstellungsprofil: Ein Bereitstellungsprofil ist eine andere Art von Profil, das auch ein Zertifikat verwendet. Wenn Sie mit benutzerdefinierten iOS Apps arbeiten, verlangt Ihr Entwickler möglicherweise, dass Sie die App mit einem Bereitstellungsprofil bereitstellen. Das kommt heutzutage seltener vor, aber Jamf unterstützt das.
- Entwicklerzertifikat: Sie erhalten dieses Zertifikat unter developer.apple.com, neben anderen Zertifikaten, die Sie eventuell benötigen. Heute besteht die häufiger verwendete Methode darin, die Distributions-Zertifikate und Bereitstellungsprofile von Xcode erstellen und einbetten zu lassen. Sobald das fertig ist, haben Sie eine hauseigene App: Eine benutzerdefinierte iOS App, die mit Jamf zur Registrierung von Testgeräten verwendet werden kann. Wenn Sie Ihre benutzerdefinierte App auf Hunderten von iOS Geräten oder mehr bereitstellen müssen, erfordert das ein Enterprise Entwickler-Signierungszertifikat.
- Apple Bereitstellungsportale: Genau gesagt handelt es sich bei diesen nächsten Optionen um Token, einen privaten Schlüssel. Die Geräteregistrierung und das Volume Purchasing erhalten beide ihre Zertifikate von Apple mithilfe des zur Verfügung gestellten Tokens. (Die aktuellste Quelle für diese Informationen ist Apple School Manager oder Apple Business Manager.)
- GSX (Global Service Exchange)
- Cloud-Verteilungspunkt (JCDS)
- Jamf Push Proxy: Wenn Sie Mitteilungen über den Self-Service an Ihre Geräte senden, benötigen Sie ein Push-Proxy-Zertifikat. Sie werden automatisch generiert, daher ist die Einrichtung ein Kinderspiel.
- Patch Management und Customer Experience Metrics: Während diese für den Jamf Administrator unsichtbar sind, kommunizieren sie mithilfe von Zertifikaten und werden sicher an unsere Server gesendet.

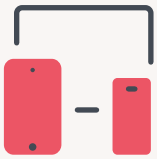
Also ja. Jamf verwendet fast überall in seinem Portfolio Zertifikate. Aber keine davon sind die Zertifikate, die zur Installation auf Ihren Geräten generiert werden.

Erstellung von Zertifikaten mit Jamf



Bereitstellung über Konfigurationsprofil

Um Zertifikate mit Jamf zu erstellen, verwenden Sie das Payload-Konfigurationsprofil. Jamf kann auch der Einfachheit halber Zertifikate und WLAN-Payloads kombinieren.



Funktioniert mit macOS oder iOS

Diese Methode zur Erstellung von Zertifikaten funktioniert bei macOS, iOS und sogar tvOS. Sie können bei Bedarf auch mehrere Zertifikate in einer einzigen Payload einbinden.

Es geht ganz um den Kontext

Wenn man über Benutzerzertifikate und Gerätezertifikate spricht, ist es wichtig, den dabei verwendeten Kontext zu kennen. Sie werden immer wieder von Benutzerzertifikaten und Gerätezertifikaten oder Maschinenzertifikaten hören. Generell enthält ein Benutzerzertifikat die Benutzerinformationen im Namen und ein Maschinenzertifikat enthält Informationen über das spezifische Gerät.

Wichtig ist, dass Sie bei der Bereitstellung des Zertifikats auf Geräteebene dieses im Systemschlüsselbund installieren und es für alle aktuellen und neuen Benutzer dieses Geräts zur Verfügung steht.

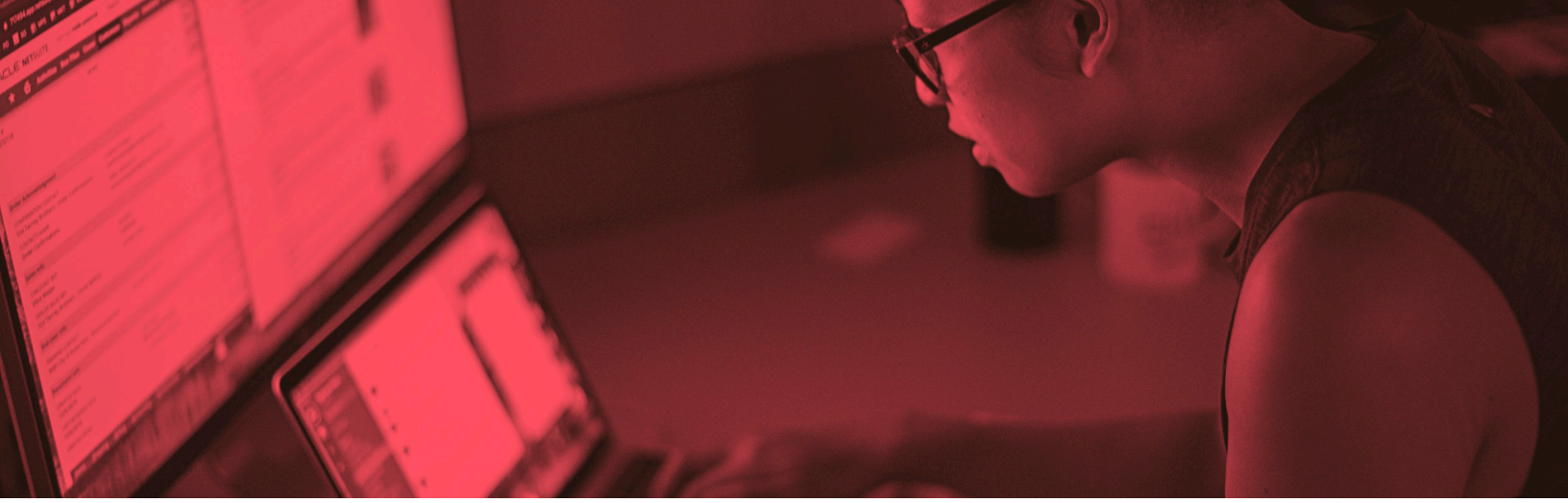
Wenn Sie dieses auf Benutzerebene bereitstellen, wird es direkt in den Schlüsselanhänger des Benutzers installiert und steht keinem anderen Benutzer im System zur Verfügung.

Jamf Simple Certificate Enrollment Protocol (SCEP) Proxy und ADCS Connector

Wenn Sie VPN-Zertifikate bereitstellen oder 802.1x WLAN anbieten, müssen Sie eine dieser Optionen verwenden. Dabei handelt es sich um ähnliche, aber nicht identische Produktangebote. Beide existieren als Alternativen zur Bindung Ihres Mac an Active Directory, um das Zertifikat zu erhalten. Der Vorteil bei beiden Lösungen ist, dass sie Zertifikate für Mac, iOS und tvOS Geräte produzieren können.

ADCSC oder SCEP Proxy? Wofür entscheiden Sie sich?

Die korrekte Wahl zwischen den beiden Optionen hängt von so vielen Details ab, dass es keine einzige richtige Antwort gibt. Betrachten Sie das nicht als SCEP gegen ADCS. Vielleicht werde Sie sogar eine Kombination davon verwenden. Bei Jamf möchten wir den richtigen Weg für Ihre zertifikatbasierten Projekte finden. Wenden Sie sich gerne an uns.

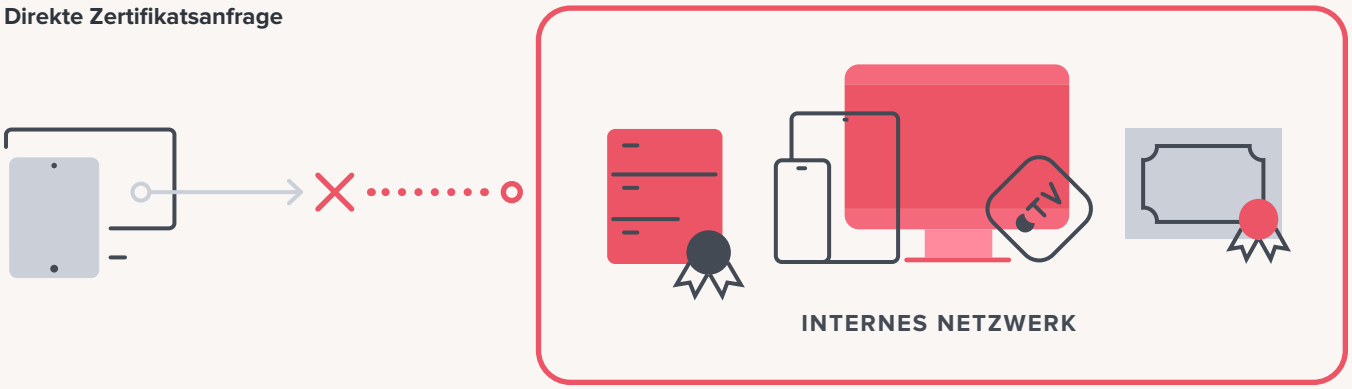


Bereitstellung von Zertifikaten

Es gibt mehrere Möglichkeiten, Zertifikate zu bereitstellen:

- Manuell durch ein Webportal und die Eingabe der Informationen. Das ist die umständlichere Art.
- Durch Drittanbieter-Anwendungen wie Nomad oder Jamf Connect. Diese Tools können bereits bereitgestellte Informationen von Benutzern übernehmen und dann in deren Namen das Zertifikat anfordern. Potenzielle Herausforderungen: Hierfür müssen die Benutzer immer noch einige Daten eingeben, und die Tatsache, dass die Anfrage aus dem gleichen Netzwerk oder über ein VPN erfolgen muss, kann Probleme verursachen. Darüber hinaus sind diese Apps nur auf macOS verfügbar.
- Direkte Zertifikatsanfrage: Jamf Pro kann die Anfrage erstellen und das Gerät kann direkt mit dem Server kommunizieren. Das bedeutet, dass das ganz automatisiert werden kann. Die Kommunikation erfolgt zwischen dem Gerät und dem Zertifikatserver, was bedeutet, dass das Gerät im gleichen Netzwerk wie der Zertifikatsserver sein muss.

Direkte Zertifikatsanfrage



Wenn Sie Geräte außerhalb des Netzwerks haben und versuchen, den Zertifikatsserver für dieses Zertifikat zu kontaktieren, ist es sehr unwahrscheinlich, dass das Sicherheitsteam dies erlaubt.

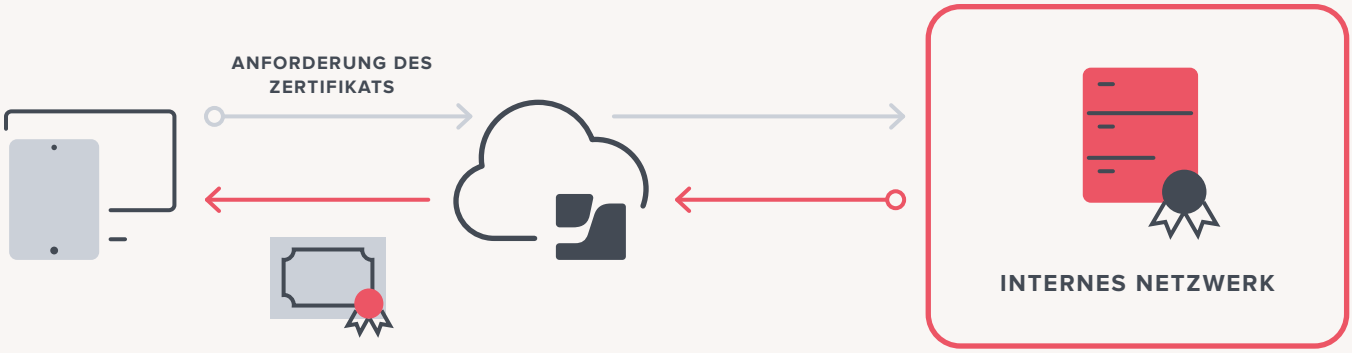
Jamf Certificate Proxy

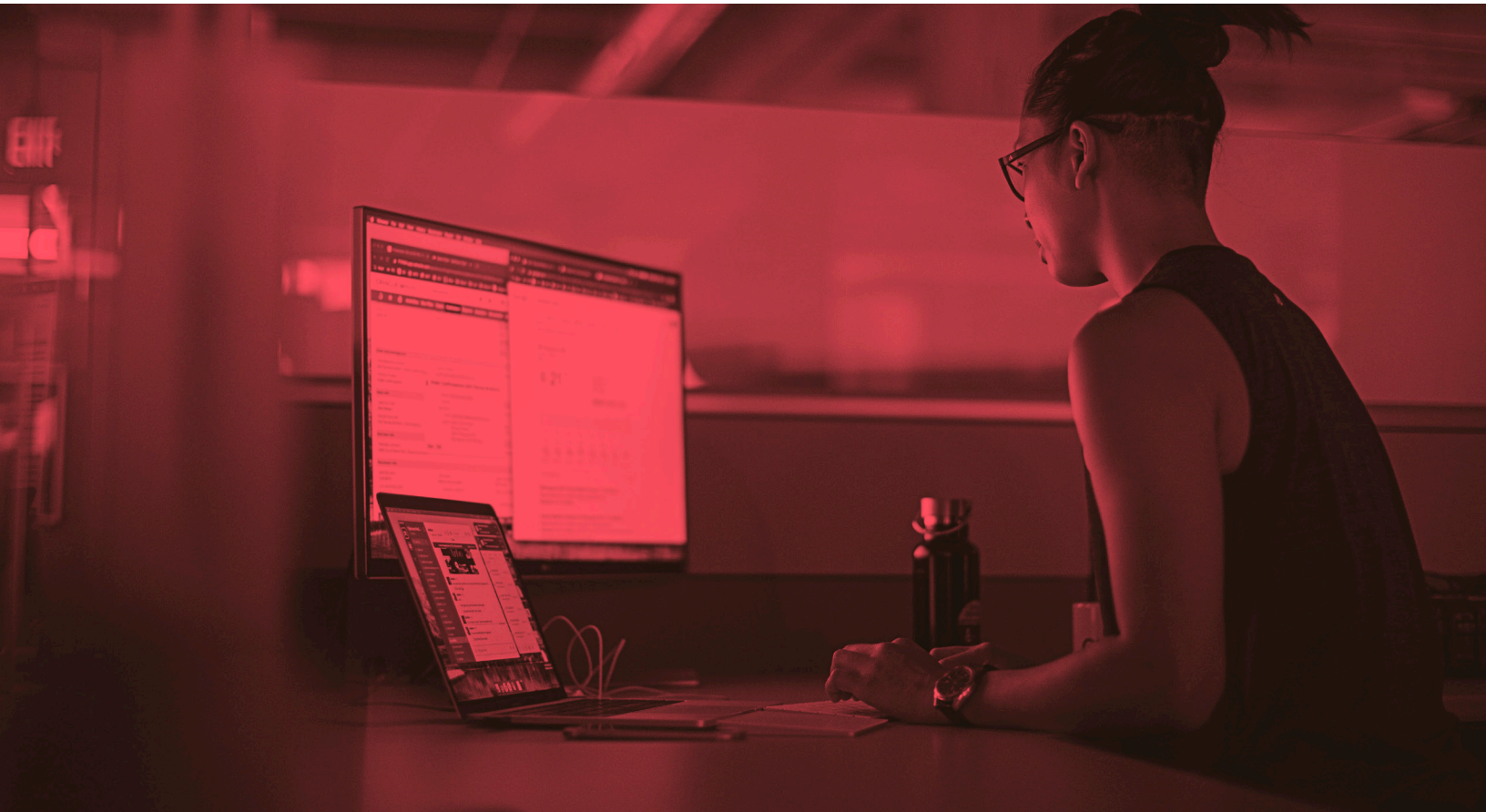
Hier kann Jamf Pro helfen, ohne die Sicherheit zu beeinträchtigen, und deshalb ist dies die am häufigsten verwendete Methode für die Anforderung von Zertifikaten.

Dabei fungiert Jamf Pro unter Verwendung von SCEP oder ACS Connector als Proxy zwischen dem Gerät und dem Zertifikatsserver. Das bietet die Vorteile der vorherigen Methoden und den zusätzlichen Nutzen eines veränderten Kommunikationsflusses. Das Gerät muss nur in der Lage sein, den Jamf Pro Server zu kontaktieren. Das bedeutet, dass das Gerät auf jedem beliebigen Netzwerk sein kann und trotzdem die erforderlichen Zertifikate erhält.

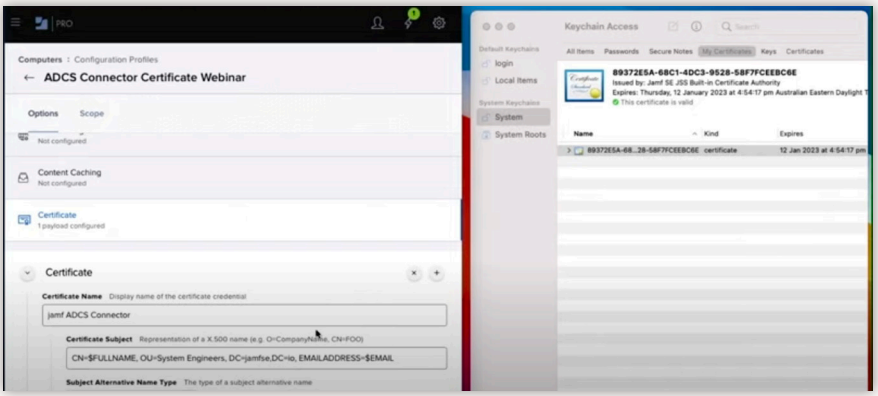
So sieht die Kommunikation aus:

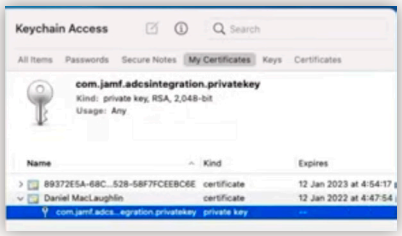
Proxy mit Jamf Pro





Und so sieht das für den Apple Administrator aus, der ADCS Connector verwendet (was ähnlich wie bei der Verwendung von SKEP aussieht), der bereits konfiguriert wurde. Dieses Gerät wurde bereits registriert. Und der Prozess ereignet sich auf einem Gastnetz ohne Verbindung mit dem Server und ohne Einbindung in Active Directory:





Rechts sehen wir die Anwendung, die Zugriff zum Schlüsselbund bietet und bereits ein Zertifikat aufweist – das Geräteregistrierungs-Zertifikat.

Sie sehen den Inhalt der Anfrage: Vollständiger Name und E-Mail-Adresse für die Inhaltsvariablen. Der Administrator wird dann auf die Registerkarte „Anwendungsbereich“ gehen, das Gerät hinzufügen und es speichern.

Ab nun kommuniziert Jamf Pro mit dem Jamf Server. Es fordert ein Zertifikat vom Zertifikatsserver an, liefert es und stellt es auf dem Gerät bereit.

Das Zertifikat kann jetzt als Authentifizierungsmethode für WLAN oder VPN verwendet werden.

Um das zu einem *vertrauenswürdigen* Zertifikat zu machen, müssen Sie das Root-Zertifikat des Servers bereitstellen, um eine Vertrauenskette zu bieten.

Jetzt haben Sie das Zertifikat. Wie benutzen Sie es?

Ein Endbenutzer kann das Zertifikat manuell auswählen und als Authentifizierung für das drahtlose Unternehmensnetzwerk verwenden.

Wenn Benutzer versuchen, eine Verbindung zu einem 802.1x Unternehmensnetzwerk herzustellen, ändern sie den Modus in EAP/TLS und wählen ein Zertifikat aus dem Schlüsselbund aus.

Ebenso sehen Endbenutzer bei einem VPN ähnliche Optionen, vorausgesetzt diese Art von VPN unterstützt Zertifikate als eine Methode der Authentifizierung. Sie müssen dafür innerhalb der jeweiligen Teams in Ihrer Organisation arbeiten.

Das kann alles automatisiert werden, indem die Payload des Netzwerkes und der VPN-Einstellungen in das Konfigurationsprofil integriert wird, das die Zertifikats-Payload enthält.

So beginnen Sie damit, in Ihrer Organisation Zertifikate zu erstellen

Sie benötigen:

- Eine unterstützte Version des Betriebssystems auf dem Gerät
- Eine unterstützte CA wie Microsoft Zertifizierungsstelle, Digicert, Entrust Certificate Solutions oder Venafi
- Unterstützung durch andere Teams in Ihrer Organisation
  - Netzwerk
  - Sicherheit
  - Zertifikats-Team

Wenden Sie sich an Ihren Ansprechpartner bei Jamf, um zu erfahren, wie wir Ihnen bei der Bereitstellung von Zertifikaten in Ihrer Organisation helfen. Wir können mit anderen Teams in Ihrer Organisation kommunizieren, um mehr Kontext darüber zu bieten, was von jeder Abteilung erwartet wird, um eine erfolgreiche Bereitstellung zu ermöglichen.

Haben Sie Fragen? Wenden Sie sich an germany@jamf.com und wir legen gerne einen Termin fest, um mit Ihnen darüber zu reden.

Englischsprachige Ressourcen:

Von Jamf:

JNUC Vortrag über Zertifikate: **jamf.it/jnuc-cert**

Jamf als SCEP Proxy: **jamf.it/scep**

Jamf ADCS Connector: **jamf.it/adcsc**

Webinar über die Zertifikat-Bereitstellung: **jamf.it/cert-101**

Von Apple:

MDM Zertifikat-Leitfaden: **jamf.it/mdm-cert**

Anforderungen an vertrauenswürdige Zertifikate: **jamf.it/apple-cert-trust**

Grenzen vertrauenswürdiger Zertifikate: **jamf.it/apple-cert-limits**