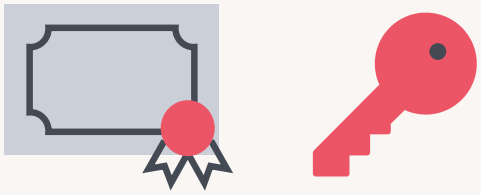
Administración de certificados con Jamf

Los certificados desempeñan un papel fundamental a la hora de asegurar, autenticar y mantener la estabilidad de su flota Apple. Si se utilizan correctamente, aumentarán la visibilidad y reducirán los riesgos de seguridad.

Fundamentos de las comunicaciones basadas en certificados

Los certificados pueden parecer confusos o abrumadores. A menudo, esto se debe a que se han utilizado mal o se han malinterpretado, y la puesta en marcha de un proyecto exitoso basado en certificados
puede ser confusa y abrumadora sin ayuda.

Además, los certificados suelen utilizarse mal en el entorno de los clientes. Por ejemplo, el área de seguridad le dice que hay una docena de certificados que deben instalarse en su flota de equipos Mac. Así que usa Composer, hace una copia de seguridad y los pone en su flujo de trabajo de aprovisionamiento.



Pero, ¿para qué sirven esos certificados?

No lo sabemos. Pero ahora están instalados en el llavero. ¿Son de confianza? ¿Está la cadena completa? Tal vez sí. Tal vez no.

Desmitifiquemos la creación e implementación de certificados.

¿Qué son los certificados?

Un certificado es solo un archivo de texto. Eso es todo. Hay mucho más entre bastidores en cuanto a la firma, el cifrado y la infraestructura de clave privada (PKI) en la que usted puede profundizar, pero ese es el archivo básico.

¿Cómo se hace un certificado?

Para crear un certificado, necesitamos una solicitud de certificado, o CSR. A continuación, nos dirigimos a un servidor de certificados que habla con la Autoridad de Certificados (CA) y esta añadirá su parte a la conversación. A veces añadimos también el certificado raíz. Entonces, tenemos un certificado firmado digitalmente.

Si abre un certificado en un editor de texto, sólo verá un código hexadecimal ilegible, porque el certificado está cifrado. En un equipo Mac, todavía se puede inspeccionar el contenido de un certificado utilizando Spotlight, al pulsar la barra espaciadora, o abriéndolo en el acceso al llavero para ver lo que hay dentro.

¿Qué datos contiene un certificado?

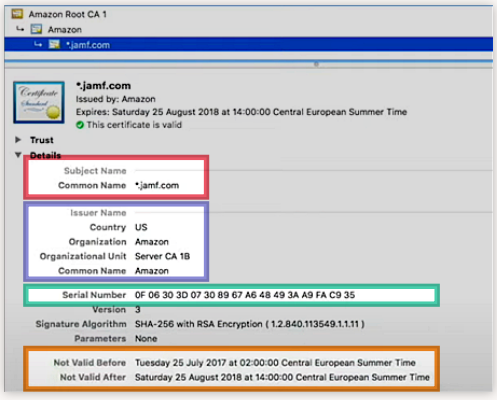
Datos de identificación. Un certificado es esencialmente un documento de identidad. Un certificado es una fuente de identificación firmada y confiable, algo así como una licencia de conducir o un pasaporte. Al igual que el pasaporte, la validez de confianza del documento se basa en la autoridad emisora.

Si tengo una licencia para manejar montacargas expedida en Canadá, eso no significa que esté autorizado a manejar un montacargas en Alemania. Del mismo modo, una tarjeta de Sam's Club no me permite comprar en Costco.

Algo como el pasaporte sólo funciona como identificación válida en todas partes porque los organismos emisores han acordado confiar entre sí. Si Perú dice que eres ciudadano, Canadá lo acepta porque es un documento confiable.

Si, por ejemplo, alguien presentara un pasaporte galáctico cubierto de arena y afirmara que esta persona tiene el rango de Maestro Jedi, nadie creería en el contenido de ese documento porque no proviene de una fuente confiable.

Comparemos un certificado con un pasaporte y veamos exactamente cuánto tienen en común.



NOMBRE, O ASUNTO

ORGANISMO EMISOR (PERÚ O AMAZON)

SERIALIZACIÓN ÚNICA

FECHA DE VALIDEZ

¡Los certificados no son totalmente incomprensibles!

¿Por qué utilizar certificados en informática?

Por seguridad. El uso de certificados de confianza permite la comunicación cifrada, lo que puede evitar que la información sea interceptada mientras está en tránsito.

Cuando visita un sitio web que utiliza https y aparece una marca de verificación verde o un icono de candado en la barra de direcciones, se está comunicando con ese servidor mediante un certificado. La conexión compartida con ese sitio es segura.

Función de los certificados como credenciales

Los certificados pueden utilizarse como alternativa a las credenciales de usuario. Cuando un cliente presenta un certificado, el servidor lo inspecciona y decide si va a confiar en ese cliente basándose en su contenido y en la autoridad de certificación que lo ha elaborado.

¿Dónde podemos utilizar esta forma de identificación segura?

Con el WiFi 802.1x, normalmente denominado WiFi basado en certificados. Esto es mucho mejor que una contraseña WPA tradicional, porque los certificados utilizados no se pueden compartir.

Normalmente, el autentificador de su red utilizará el Protocolo de Autenticación Extensible (EAP) o Radius (otro protocolo de autenticación), dependiendo de las opciones de cifrado.

Jamf tiene la ventaja de validar el cliente que se conecta a la red. El dispositivo cliente puede presentar la información del usuario dentro del certificado que demuestra exactamente quién está utilizando un determinado dispositivo en su red.

Esto es muy útil para sus amigos de InfoSec.

Uso de certificados para conectarse a las VPN

Otro uso común de los certificados es la conexión a una red privada virtual (VPN). Al igual que ocurre con el WiFi, el nombre de usuario y la contraseña pueden no ser suficientes para establecer la confianza. Queremos poder validar que el dispositivo también es de confianza. El acceso se deniega si las credenciales del usuario están deshabilitadas o si el certificado ha sido revocado.

Autenticación de redes cableadas con certificados

Usted puede garantizar la seguridad de los datos de su empresa con certificados.

La autenticación 802.1x no se limita a Wi-Fi. Aunque es menos habitual, también puede utilizarse en una red cableada. Es otra forma de evitar que cualquiera pueda acceder a una conexión de red y acceder a datos privados.

Uso de certificados con correo electrónico cifrado

Cuando los certificados están firmados y son de confianza, no se puede leer un mensaje de correo electrónico sin los certificados correctos instalados. Esta tecnología también garantiza que el mensaje no haya sido modificado en tránsito después de ser firmado y enviado.

Administración de certificados con Jamf Pro

Implementación de certificados

Implementar certificados con una MDM de Apple es sencillo: el proveedor de MDM, como Jamf, mantiene el ciclo de vida de los certificados. En cuanto a la seguridad, tienen varias posibilidades de revocar el acceso de los usuarios si ellos:

- Incumplen la normativa
- Dejan la empresa

El papel de los certificados en Apple y MDM

- **Notificaciones push (APNS)**
  Todo el sistema de notificaciones push de Apple se basa en una cadena de certificados de confianza para la comunicación. Nada de esto funcionaría sin los certificados.
- **Identidades de supervisión**
  En el caso de Apple Configurator, Jamf crea una identidad de supervisión basada en un certificado que puede compartirse entre varias Mac de aprovisionamiento utilizadas para supervisar e inscribir dispositivos iOS. Esta misma identidad de supervisión se puede añadir a Jamf Pro para los dispositivos que supervisa.
- **Firma de desarrolladores**
  Como desarrollador, se ve envuelto en decenas de tipos de certificados, desde la distribución de la firma de apps hasta los certificados de Apple Pay. Probablemente ya esté utilizando algunos de estos certificados en Jamf.

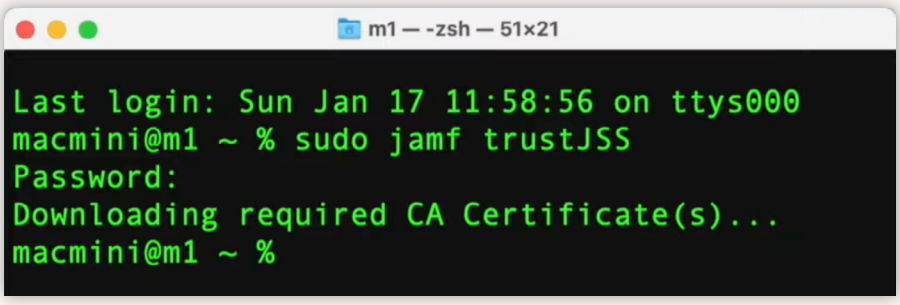
Autoridad de certificación incorporada

Jamf Pro posee su propia Autoridad de Certificación (CA) integrada. Esta CA autofirmada produce un certificado raíz que debe ser de confianza en el dispositivo antes de que pueda confiar en el perfil MDM.

¿Cómo y dónde utiliza Jamf Pro los certificados?

Respuesta corta: casi en todas partes. Los certificados desempeñan un papel en:

- Perfiles de inscripción
- Administración de dispositivos con el binario Jamf



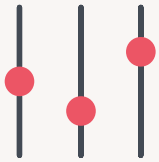
El comando trustJSS

- Apache Tomcat SSL: Para un servidor de cara al exterior necesitará instalar un certificado de confianza público.
- La autoridad de certificación incorporada es donde usted configuraría Jamf para hablar con un servidor CA externo. Aquí también se configuran los ajustes del proxy SKAT y del conector ADCS.
- Listener de atención sanitaria: Utiliza certificados para asegurar la comunicación dentro de la red del hospital.
- Inicio de sesión único
- LDAP-S sobre SSL
- El proceso de inscripción
- Firma del paquete QuickAdd: requiere un certificado de distribución de apps de Apple. Este mismo certificado es utilizado por Composer para firmar sus otros paquetes.
- Perfiles de configuración: Los perfiles de configuración creados en Jamf Pro se firman automáticamente. Así se mantienen seguros cuando están implementados. Si descarga una configuración directamente desde la consola, ya está firmada. Por eso no se pueden ver los datos xml en bruto con un editor de texto. Si necesita editar un perfil de configuración creado con Jamf, tendrá que desactivar su firma primero.
- Perfil de aprovisionamiento de apps: Un perfil de aprovisionamiento es un tipo diferente de perfil que también utiliza un certificado. Cuando trabaje con apps personalizadas para iOS, es posible que su desarrollador necesite que implemente la app con un perfil de aprovisionamiento. Hoy en día es menos común, pero Jamf lo admite.
- Certificado de desarrollador: lo obtendrá en developer.apple.com, entre otros certificados que pueda necesitar. El método más común hoy en día es dejar que Xcode cree e incorpore los certificados de distribución y los perfiles de aprovisionamiento por usted de forma automática. Una vez hecho esto, tendrá su propia app interna: una app iOS personalizada que puede ser implementada usando Jamf para registrar dispositivos de prueba. Si necesita implementar su app personalizada en cientos de dispositivos iOS o más, necesitará un certificado de firma para desarrolladores de empresa.
- Portales de implementación de Apple: estrictamente hablando, estos pocos que siguen son en realidad tokens, una clave privada. Tanto la inscripción de dispositivos como la compra por volumen obtienen sus certificados de Apple utilizando el token proporcionado. (El lugar más moderno para encontrar esa información es Apple School Manager o Apple Business Manager).
- GSX (Global Service Exchange)
- Punto de distribución en la nube (JCDS)
- Proxy Jamf Push: si usted envía notificaciones a sus dispositivos a través del autoservicio, necesitará un certificado de proxy push. Se generan automáticamente, por lo que es fácil de configurar.
- Métricas de administración de parches y experiencia del cliente: aunque son invisibles para el administrador de Jamf, se comunican mediante certificados y se envían de forma segura a nuestros servidores.

> **¡CONSEJO PROFESIONAL!**
>
> Jamf Cloud se encarga de que toda esta app web trabaje de forma automática. No tiene que volver a preocuparse por los ajustes de Tomcat.

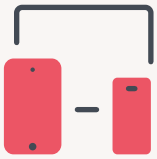
Entonces, sí. Jamf utiliza certificados en casi toda su cartera. Pero ninguno de ellos son los certificados que se están generando para instalar en sus dispositivos.

Creación de certificados con Jamf



Entregados a través de un perfil de configuración

Para crear certificados con Jamf, se hace en el perfil de configuración de la carga útil. Jamf también puede combinar certificados y cargas útiles de Wi-Fi para simplificar el proceso.



Funciona con equipos Mac o iOS

Este método para crear certificados funciona para Mac OS, iOS e incluso con tvOS. Usted también puede incluir varios certificados en una sola carga útil si es necesario.

Todo depende del contexto

Cuando se habla de certificados de usuario y certificados de dispositivo, es importante conocer el contexto que estamos utilizando. Oirá hablar de certificaciones de usuario y certificaciones de dispositivo o certificaciones de máquina. Por lo general, un certificado de usuario contiene la información del usuario en el asunto, y un certificado de máquina contiene información en el asunto sobre el dispositivo específicamente.

Lo que es importante saber es que si elige implementar el certificado en el nivel del dispositivo, está instalando ese certificado en el llavero del sistema y está disponible para todos los usuarios actuales y nuevos de ese dispositivo.

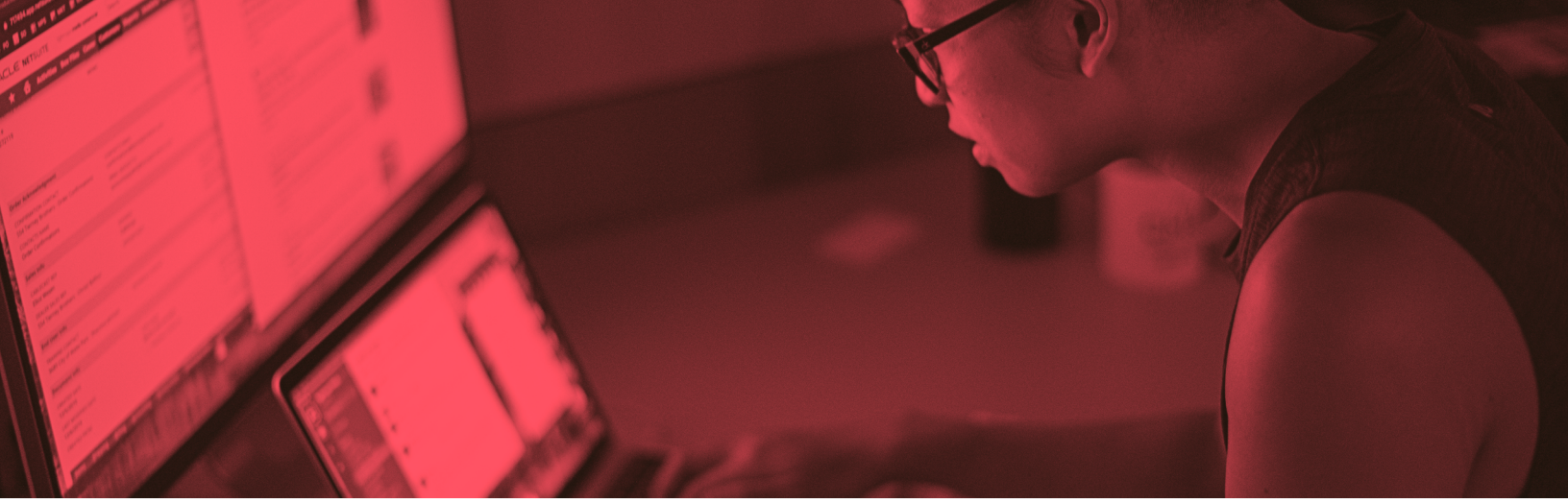
Si lo implementa en el nivel de usuario, se instala directamente en el llavero de ese usuario y no estará disponible para ningún otro usuario del sistema.

Proxy de protocolo simple de inscripción de certificados (SCEP) de Jamf y conector ADCS

Si va a implementar certificados VPN o a desplegar Wi-Fi 802.1x, tendrá que utilizar uno de estos para hacerlo. Son ofertas de productos relacionadas pero diferentes. Ambas existen como alternativas a la vinculación de su Mac a Active Directory para obtener el certificado; la ventaja es que ambas soluciones pueden funcionar para producir certificados para dispositivos Mac, iOS y tvOS.

¿Qué proxy: ADCSC o SCEP? ¿Cuál eligir?

La elección correcta entre los dos depende de tantos detalles que no hay una única respuesta correcta. No lo piense en la forma "SCEP contra ADCS". Incluso puede utilizar una combinación de ambos. En Jamf estamos ansiosos y dispuestos a mantener esas conversaciones con usted para decidir la mejor vía de éxito para sus proyectos basados en certificaciones. [Por favor, póngase en contacto con nosotros.]

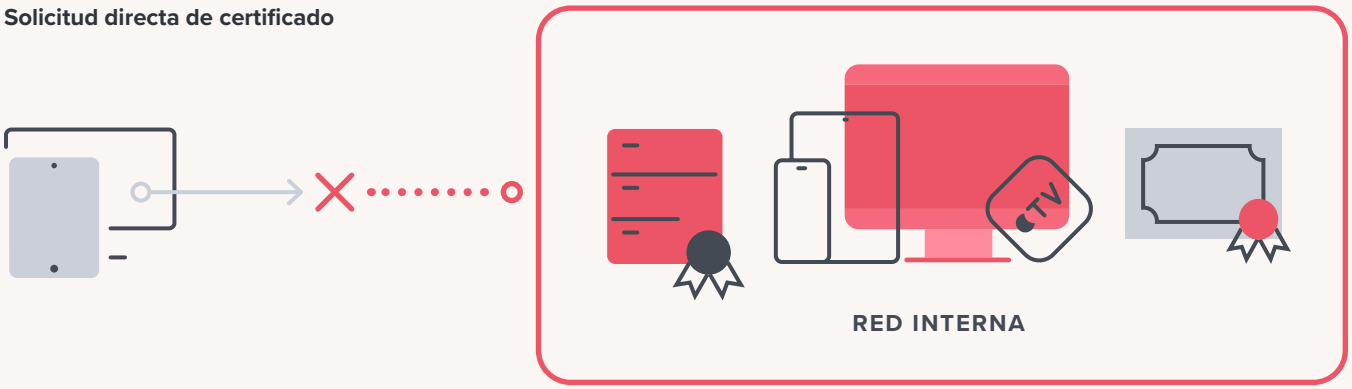


Implementación de certificados

Hay varias formas de implementar los certificados:

- Manualmente, entrando en un portal web e introduciendo la información. Esta es la forma más engorrosa.
- A través de aplicaciones de terceros como Nomad o Jamf Connect. Estas herramientas pueden tomar la información ya proporcionada por el usuario y luego hacer la solicitud de certificado en su nombre. Algunos desafíos: esto sigue requiriendo que el usuario introduzca algunos datos, y el requisito de que la solicitud se haga desde la red o a través de una VPN puede causar problemas. Además, estas apps sólo están disponibles en macOS.
- Solicitud directa de certificado: Jamf Pro puede crear la solicitud y el dispositivo puede comunicarse directamente con el servidor. Esto significa que todo puede ser automatizado. La comunicación se realiza entre el dispositivo y el servidor de certificados, lo que significa que el dispositivo debe estar en la misma red que el servidor de certificados.

Solicitud directa de certificado



Si tiene dispositivos fuera de la red y tratan de contactar con el servidor de certificados para obtenerlos, es muy poco probable que el equipo de seguridad lo permita.

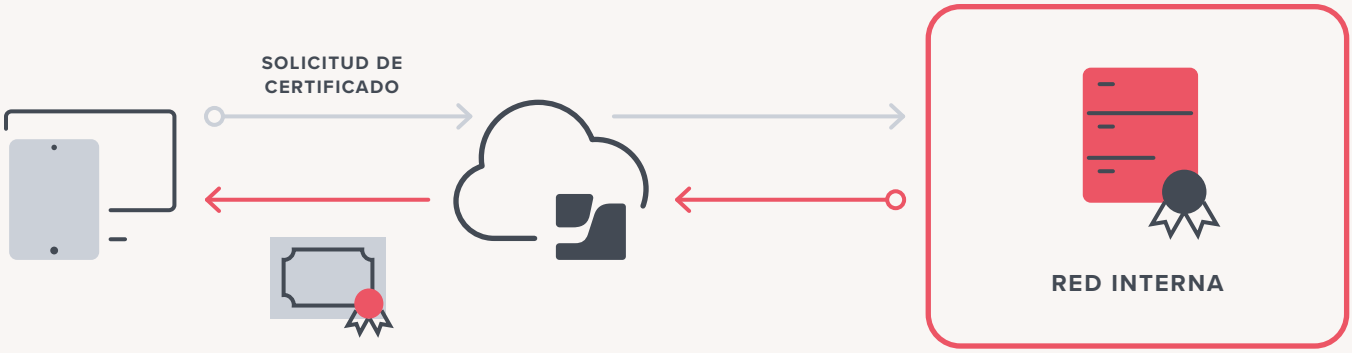
Proxy de Jamf Certificate

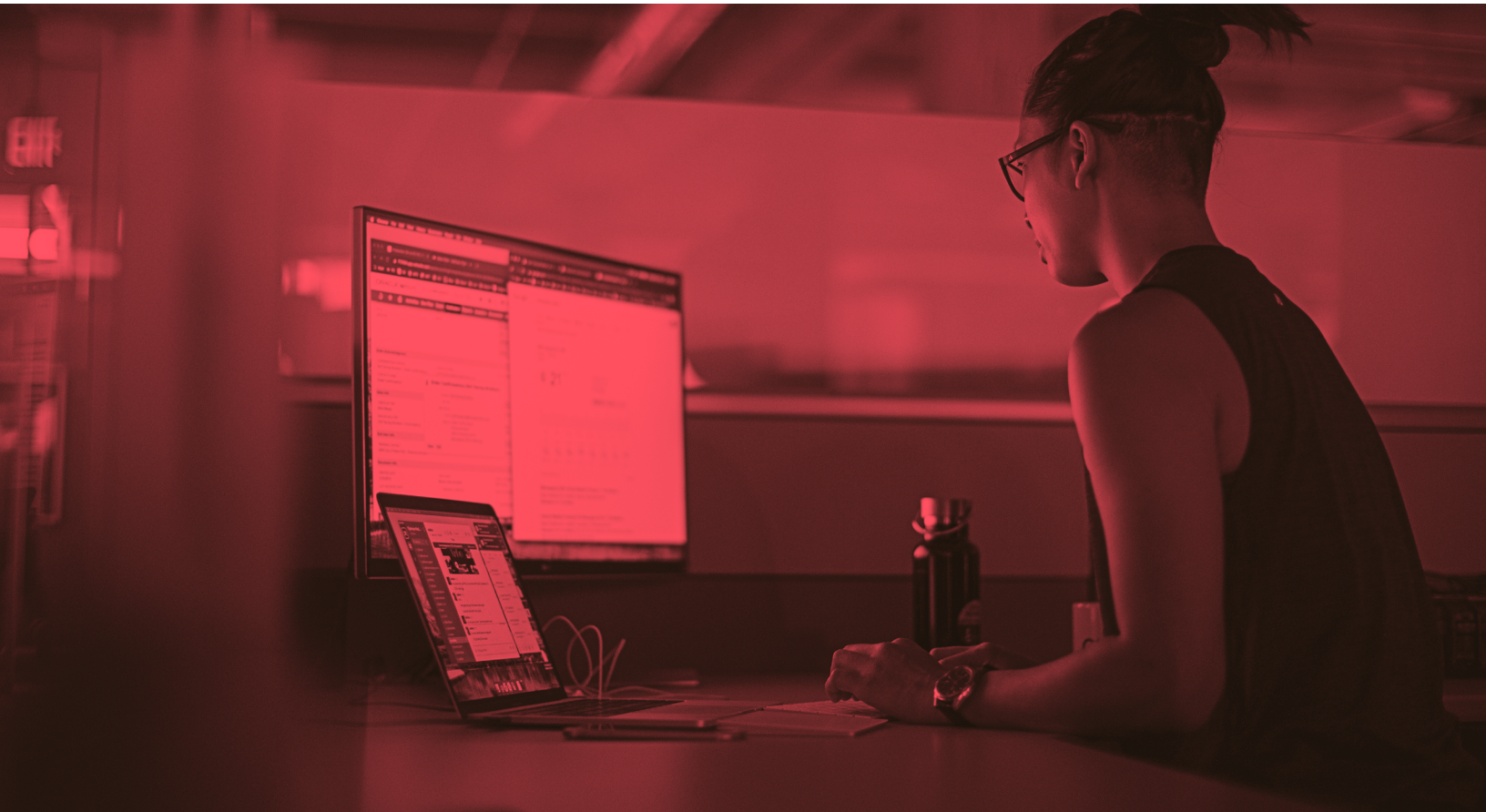
Aquí es donde Jamf Pro puede ayudar sin comprometer la seguridad, y es el método más común para solicitar certificados.

En este método, Jamf Pro actúa como proxy entre el dispositivo y el servidor de certificados mediante SCEP o ACS Connector. Esto proporciona las ventajas de los métodos anteriores con la ventaja añadida de que el flujo de comunicación cambia. El dispositivo sólo tiene que ser capaz de contactarse con el servidor Jamf Pro. Esto significa que el dispositivo puede estar en cualquier red y aún así obtener los certificados necesarios.

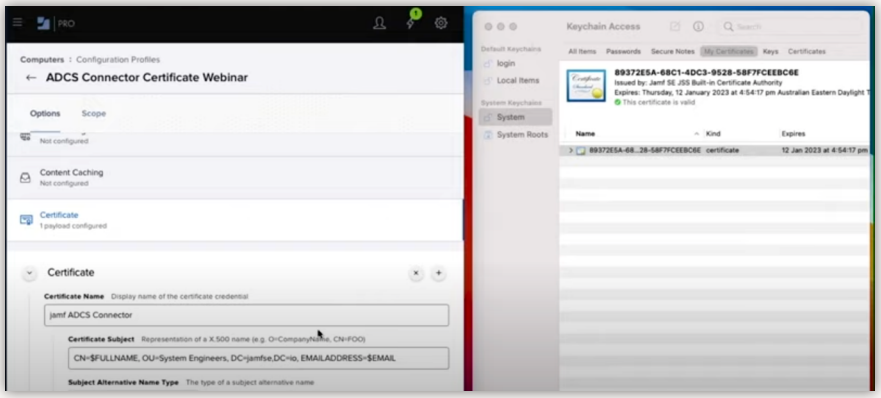
Así es la comunicación:

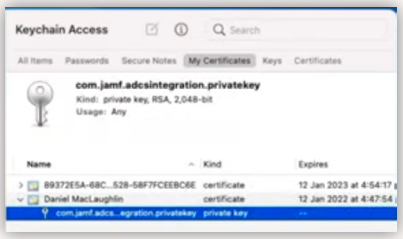
Proxy que usa Jamf Pro





Y así es como luce el administrador de Apple usando el conector ADCS (que es similar a la apariencia cuando usa SKEP), que ya ha sido configurado. Este dispositivo en particular ya ha sido inscrito. Y el proceso está ocurriendo en una red de invitados sin conectividad con el servidor y sin vinculación con Active Directory:





A la derecha podemos ver la aplicación de acceso al llavero que ya muestra un certificado: el de inscripción de dispositivos.

Puede ver el contenido de la solicitud: nombre completo y dirección de correo electrónico para las variables de contenido. El administrador irá entonces a la pestaña de alcance, añadirá el dispositivo y lo guardará.

A partir de este momento, Jamf Pro se comunicará con el servidor de Jamf. Solicitará el certificado al servidor de certificados, éste lo entregará y Jamf lo implementará en el dispositivo.

El certificado puede utilizarse ahora como método de autenticación para Wi-Fi o VPN.

Para convertirlo en un certificado de *confianza*, tendrá que implementar el certificado raíz del servidor para proporcionar una cadena de confianza.

Así que ahora tiene el certificado. ¿Cómo se utiliza?

Un usuario final puede seleccionar manualmente el certificado y utilizarlo como autenticación en la red inalámbrica de la empresa.

Cuando el usuario intenta conectarse a una red de empresa 802.1x, cambia el modo a EAP/TLS y luego selecciona un certificado del llavero.

Del mismo modo, el usuario final verá opciones similares con la VPN, siempre y cuando ese tipo de VPN admita certificados como método de autenticación. Para ello, deberá trabajar con los equipos respectivos de su organización.

Todo esto se puede automatizar incluyendo la carga útil de configuraciones de red y VPN dentro del perfil de configuración que contiene la carga útil del certificado.

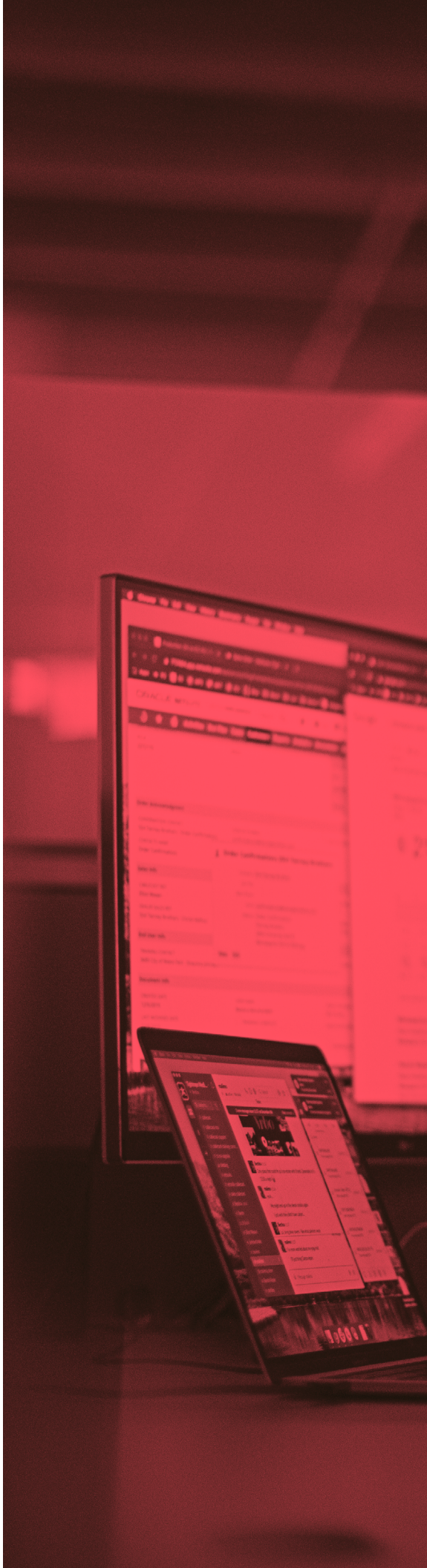
Cómo iniciar el proceso de creación de certificados en su organización

Necesitará:

- Una versión del sistema operativo compatible con el dispositivo
- Una CA compatible, como la autoridad de certificación de Microsoft, digicert, Entrust Certificate Solutions o Venafi
- Apoyo de otros equipos de su organización
  - Equipo de redes
  - de seguridad
  - de certificados

Póngase en contacto con un representante de Jamf para saber cómo ayudarle a implementar con éxito los certificados en su organización. Podemos comunicarnos con otros equipos de su organizaciónpara proporcionar el contexto de lo que se requiere de cada departamento con el fin de tener una implementación exitosa.

¿Tiene preguntas? Póngase en contacto con nosotros en info@jamf.com y estaremos encantados de concertar una cita con usted para hablar de ello.



Recursos:

De Jamf:

Charla sobre certificados en JNUC: jamf.it/jnuc-cert

Jamf como proxy SCEP: jamf.it/scep

Jamf ADCS Connector: jamf.it/adcsc

Webinar sobre implementación de certificados 101: jamf.it/cert-101

De Apple:

Guía del certificado MDM: jamf.it/mdm-cert

Requisitos para los certificados de confianza: jamf.it/apple-cert-trust

Límites de los certificados de confianza: jamf.it/apple-cert-limits