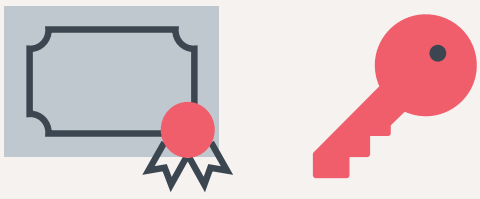
Gestion des certificats avec Jamf

Les certificats jouent un rôle essentiel dans la sécurisation, l'authentification et le maintien de la stabilité de votre parc Apple. Lorsqu'ils sont utilisés correctement, ils augmentent la visibilité tout en réduisant les risques de sécurité.

Les bases des communications basées sur des certificats

Les certificats peuvent sembler déroutants ou intimidants. C'est souvent parce qu'ils ont été mal utilisés ou mal compris, et que, sans aide, le déploiement d'un projet basé sur les certificats peut effectivement être compliqué.

Par ailleurs, les certificats sont souvent mal utilisés dans les environnements clients. Par exemple, votre service de sécurité vous indique qu'une douzaine de certificats doivent être installés sur votre parc de Mac. Vous utilisez donc Composer, sauvegardez les certificats et les intégrez à votre workflow de configuration.



Mais à quoi servent ces certificats ?

On l'ignore. Mais ils sont maintenant installés dans le trousseau. Sont-ils approuvés ? La chaîne est-elle complète ? Peut-être. Peut être pas.

Démystifions la création et le déploiement des certificats !

Que sont les certificats ?

Un certificat n'est qu'un fichier texte. Rien de plus. En coulisses, il se passe bien d'autres choses, et vous pouvez vous pencher sur la signature, le chiffrement et l'infrastructure à clé privée (PKI) si le cœur vous en dit. Mais le certificat lui-même est le fichier de base.

Comment créer un certificat ?

Pour créer un certificat, nous avons besoin d'une demande de certificat, ou CSR. Ensuite, nous contactons un serveur de certificats qui communique avec l'autorité de certification (CA) et ajoute sa partie à la conversation. Parfois, nous ajoutons également le certificat racine. Nous avons ainsi un certificat signé numériquement.

Si vous ouvrez un certificat dans un éditeur de texte, vous ne verrez que du code hexadécimal illisible, car le certificat est chiffré. Sur un Mac, vous pouvez toujours inspecter le contenu d'un certificat à l'aide de Spotlight en appuyant sur la barre d'espace ou en l'ouvrant dans Keychain Access.

Quelles données contient un certificat ?

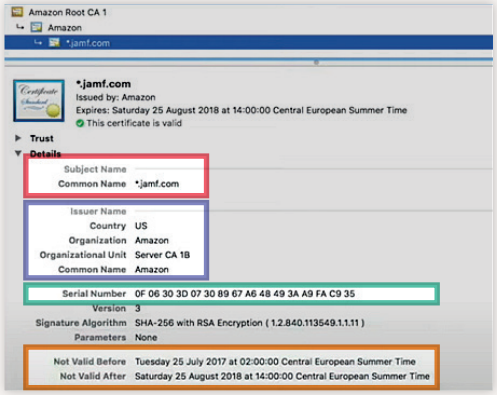
Des données d'identification. Un certificat est un peu comme une carte d'identité. C'est une source d'identification signée et fiable, comme un passeport. Tout comme pour un passeport, la validité du document est basée sur l'autorité émettrice.

Si j'ai un permis de chariot élévateur délivré au Canada, cela ne me permet pas d'en conduire un en Allemagne. De même, une carte Auchan ne me permet pas de faire des achats chez Carrefour.

Un passeport peut servir de pièce d'identité valide partout, mais c'est uniquement parce que les organismes émetteurs ont tous accepté de se faire mutuellement confiance. Si le Pérou dit que vous êtes péruvieux sur votre passeport, le Canada l'accepte parce que c'est un document fiable.

Si, par exemple, quelqu'un produisait un passeport galactique et affirmait qu'il est maître Jedi, personne ne croirait le contenu de ce document, parce qu'il ne provient pas d'une source fiable.

Étudions côte à côte un certificat et un passeport pour voir exactement ce que les deux ont en commun.



NOM OU SUJET

ORGANISME ÉMETTEUR (PÉROU OU AMAZON)

SÉRIALISATION UNIQUE

DATE DE VALIDITÉ

Finalement, les certificats ne sont pas totalement incompréhensibles !

Pourquoi utiliser des certificats en informatique ?

Au nom de la sécurité. L'utilisation de certificats approuvés permet une communication chiffrée, ce qui peut empêcher l'interception des informations pendant le transit.

Lorsque vous visitez un site Web à l'aide de https et que vous voyez une coche verte ou une icône de verrou dans la barre d'adresse, vous communiquez avec ce serveur à l'aide d'un certificat. La connexion partagée avec ce site est sécurisée.

Les certificats comme informations d'identification

Les certificats peuvent être utilisés comme une alternative aux informations d'identification de l'utilisateur. Lorsqu'un client présente un certificat, le serveur l'inspecte et décide s'il va faire confiance à ce client en fonction du contenu et de l'autorité de certification qui a créé ce certificat.

Où pouvons-nous utiliser cette forme d'identification sécurisée ?

Avec le Wi-Fi 802.1x, souvent appelé Wi-Fi basé sur les certificats. C'est bien meilleur qu'un mot de passe WPA traditionnel, car les certificats utilisés ne peuvent pas être partagés.

En règle générale, votre authentificateur réseau utilisera le protocole d'authentification extensible (EAP) ou Radius (un autre protocole d'authentification), selon les choix de chiffrement.

Jamf a l'avantage de valider le client qui se connecte au réseau. L'appareil client peut présenter des informations utilisateur à l'intérieur du certificat qui prouvent exactement qui utilise un appareil donné sur votre réseau.

C'est très utile pour les personnes responsables de la sécurité de l'information.

Utilisation de certificats pour se connecter aux VPN

Une autre utilisation courante des certificats est la connexion à un réseau privé virtuel (VPN). Comme avec le Wi-Fi, le nom d'utilisateur et le mot de passe peuvent ne pas être suffisants pour établir la confiance. Nous voulons être en mesure de valider que l'appareil lui-même est également approuvé. L'accès est refusé si les informations d'identification de l'utilisateur sont désactivées ou si le certificat a été révoqué.

Authentification des réseaux filaires avec des certificats

Vous pouvez vous assurer que les données de votre entreprise sont sécurisées avec des certificats.

L'authentification 802.1x n'est pas limitée au Wi-Fi : vous pouvez également l'utiliser sur un réseau filaire. C'est une autre façon d'empêcher n'importe qui d'accéder à une connexion réseau et à des données privées.

Utilisation de certificats avec des e-mails chiffrés

Lorsque les certificats sont signés et approuvés, un e-mail ne peut pas être lu sans les certificats appropriés installés. Cette technologie garantit également que le message n'a pas été modifié en transit après sa signature et son envoi.

Gestion des certificats avec Jamf Pro

Déploiement de certificats

Le déploiement de certificats avec une solution MDM Apple est simple : le fournisseur MDM, par exemple Jamf, maintient le cycle de vie du certificat. Pour des raisons de sécurité, les fournisseurs ont divers moyens de révoquer l'accès des utilisateurs s'ils :

- Enfreignent des règles de conformité
- Quittent l'entreprise

Le rôle des certificats avec Apple et la MDM

- **Notifications push (APNS)**
  L'ensemble du système de notifications push d'Apple repose sur une chaîne de certificats de confiance pour la communication. Rien de tout cela ne fonctionnerait sans certificats.
- **Identités de supervision**
  Dans le cas d'Apple Configurator, Jamf crée une identité de supervision basée sur un certificat et qui peut être partagée entre plusieurs Mac pour superviser et inscrire des appareils iOS. Cette même identité de supervision peut être ajoutée à Jamf Pro pour les appareils supervisés.
- **Signature du développeur**
  En tant que développeur, vous maniez des dizaines de types de certificats issus de la signature de vos applications, et même des certificats Apple Pay. Vous utilisez probablement déjà certains de ces certificats dans Jamf.

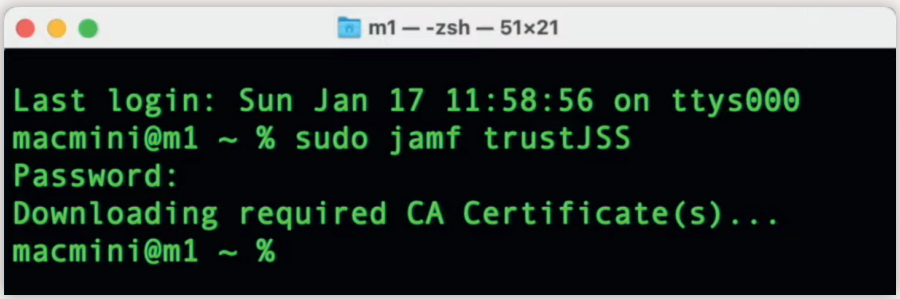
Autorité de certification intégrée

Jamf Pro possède sa propre autorité de certification (CA) intégrée. Cette autorité de certification autosignée produit un certificat racine qui doit être approuvé sur l'appareil avant de pouvoir approuver le profil MDM.

Comment et où Jamf Pro utilise les certificats ?

La réponse courte : presque partout. Les certificats jouent un rôle dans :

- Les profils d'inscription
- La gestion des périphériques avec les binaires Jamf
- SSL Apache Tomcat : Pour un serveur externe, vous devrez installer un certificat approuvé public.



La commande trustJSS

- L'autorité de certification intégrée est l'endroit où vous configurez Jamf pour communiquer avec un serveur CA externe. Les paramètres du proxy SKAT et du connecteur ADCS sont également configurables ici.
- Auditeur de santé : Utilise des certificats pour sécuriser la communication à l'intérieur du réseau de l'hôpital.
- Authentification unique
- LDAP-S sur SSL
- Le processus d'inscription

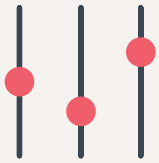
CONSEIL DE PRO !

Jamf Cloud s'occupe automatiquement de tout le travail de cette application Web. Vous n'aurez plus jamais à vous soucier des paramètres de votre TomCat.

- Signature du package QuickAdd : nécessite un certificat de distribution d'application d'Apple. Ce même certificat est utilisé par Composer pour signer vos autres packages.
- Profils de configuration : Les profils de configuration créés dans Jamf Pro sont signés automatiquement. Cela les maintient en sécurité lorsqu'ils sont déployés. Si vous téléchargez une configuration directement depuis la console, elle est déjà signée. C'est pourquoi vous ne pouvez pas afficher les données XML brutes avec un éditeur de texte. Si vous devez modifier un profil de configuration créé avec Jamf, vous devez d'abord annuler sa signature.
- Profil de configuration d'applications : Un profil de configuration est un autre type de profil qui utilise également un certificat. Lorsque vous travaillez avec des applications iOS personnalisées, votre développeur peut avoir besoin que vous déployiez l'application avec un profil de configuration. C'est moins courant aujourd'hui, mais Jamf prend ce cas en charge.
- Certificat de développeur : vous obtenez ce certificat sur developer.apple.com, entre autres certificats dont vous pourriez avoir besoin. La méthode la plus courante de nos jours consiste à laisser Xcode créer et intégrer automatiquement les certificats de distribution et les profils de configuration. Une fois que cela est fait, vous aurez vous-même une application interne : une application iOS personnalisée qui peut être déployée à l'aide de Jamf pour enregistrer les appareils de test. Si vous devez déployer votre application personnalisée sur des centaines d'appareils iOS ou plus, vous aurez besoin d'un certificat de signature de développeur d'entreprise.
- Portails de déploiement Apple : à proprement parler, ce sont en fait des jetons, une clé privée. L'inscription d'appareils et l'achat en volume reçoivent tous deux leurs certificats d'Apple à l'aide du jeton fourni. (Voir Apple School Manager ou Apple Business Manager pour des exemples modernes.)
- GSX (Global Service Exchange)
- Point de distribution cloud (JCDS)
- Proxy push Jamf : si vous envoyez des notifications à vos appareils via le libre-service, vous aurez besoin de certificats de proxy push. Ils sont générés automatiquement, donc la configuration est facile ici.
- Gestion des correctifs et mesures de l'expérience client : bien qu'invisibles pour l'administrateur Jamf, ces systèmes communiquent à l'aide de certificats et envoient leurs données de façon sécurisée à nos serveurs.

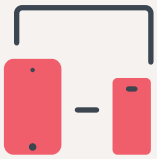
Donc oui. Jamf utilise des certificats presque partout dans son portefeuille. Mais ce ne sont pas des certificats générés pour une installation sur vos appareils.

Création de certificats avec Jamf



Livraison via le profil de configuration

Pour créer des certificats avec Jamf, vous pouvez passer par le profil de configuration de charge utile. Jamf peut également combiner des certificats et des charges utiles Wi-Fi pour plus de simplicité.



Fonctionne avec Mac ou iOS

Cette méthode de création de certificats fonctionne pour macOS, iOS et même tvOS. Vous pouvez également inclure plusieurs certificats dans une seule charge utile si nécessaire.

Tout est une question de contexte

Lorsque vous parlez de certificats d'utilisateur et de certificats d'appareil, ou certificats de machine, il est important de connaître le contexte. Pour la plupart, un certificat utilisateur contient les informations utilisateur dans le sujet, et un certificat machine contient des informations dans le sujet sur l'appareil spécifiquement.

Ce qu'il est important de savoir, c'est que si vous choisissez de déployer le certificat au niveau de l'appareil, vous installez ce certificat dans le trousseau du système. Il est alors disponible pour tous les utilisateurs actuels et futurs de cet appareil.

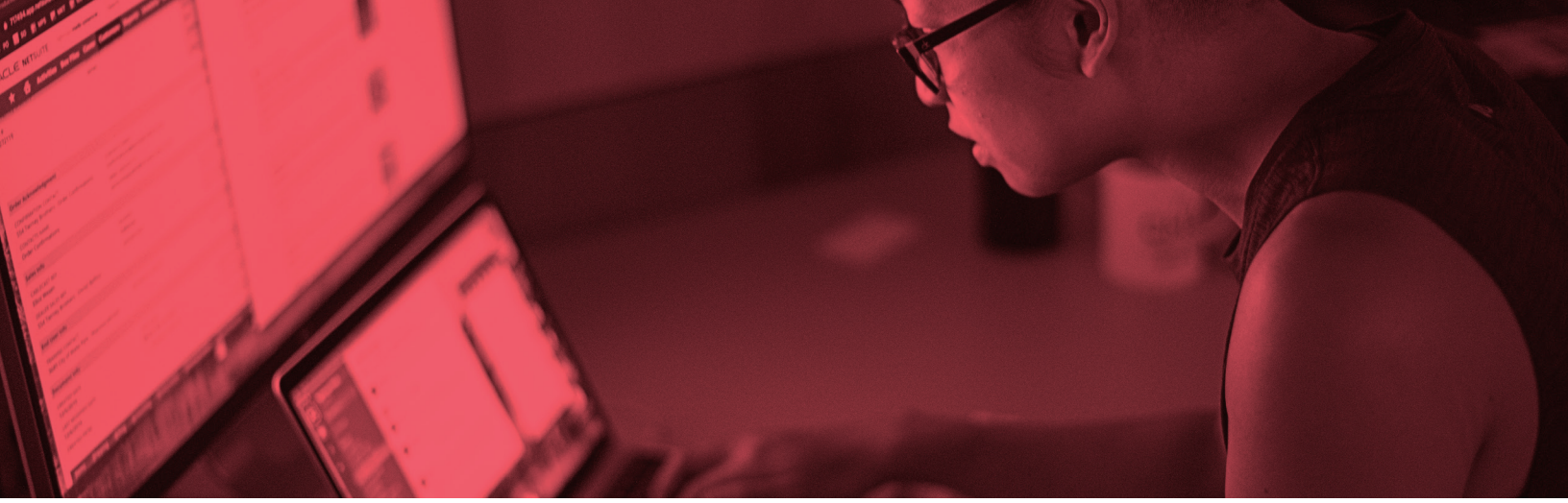
Si vous le déployez au niveau utilisateur, il est installé directement dans le trousseau de cet utilisateur et ne sera disponible pour aucun autre utilisateur du système.

Proxy Jamf Simple Certificate Enrollment Protocol (SCEP) et connecteur ADCS

Si vous comptez déployer des certificats VPN ou le Wi-Fi 802.1x, vous devrez en utiliser un pour le faire. Ce sont des produits liés mais différents. Ils existent tous deux comme alternatives à la liaison de votre Mac à Active Directory pour obtenir le certificat, l'avantage étant que les deux solutions peuvent fonctionner pour produire des certificats pour les appareils Mac, iOS et tvOS.

Proxy ADCSC ou SCEP : que choisir ?

Le bon choix dépend de tant de facteurs qu'il n'y a pas de réponse universelle. Ne voyez pas cela comme une bataille entre SCEP et ADCS. Vous pouvez même utiliser une combinaison des deux. Chez Jamf, nous sommes ravis d'avoir ces conversations avec vous pour décider de la meilleure solution pour le succès de vos projets reposant sur des certificats. **N'hésitez pas à nous contacter.**



Déploiement de certificats

Il existe plusieurs façons de déployer des certificats :

- Manuellement, en accédant à un portail Web et en saisissant les informations. C'est la méthode la plus fastidieuse.
- Via des applications tierces telles que Nomad ou Jamf Connect. Ces outils peuvent utiliser des informations déjà fournies par l'utilisateur, puis effectuer la demande de certificat en son nom. Quelques difficultés : l'utilisateur doit toujours saisir certaines données, et le fait que la demande doit être émise à partir du réseau ou via un VPN peut causer des problèmes. De plus, ces applications ne sont disponibles que sur macOS.
- Demande directe de certificat : Jamf Pro peut créer la demande, et l'appareil peut communiquer directement avec le serveur. Cela signifie que tout peut être automatisé. La communication se fait entre l'appareil et le serveur de certificats, ce qui signifie que l'appareil doit être sur le même réseau que le serveur de certificats.

Demande directe de certificat

Si vous avez des appareils en dehors du réseau qui essaient de contacter le serveur de certificats pour ce certificat, il est très peu probable que l'équipe de sécurité autorise cette opération.

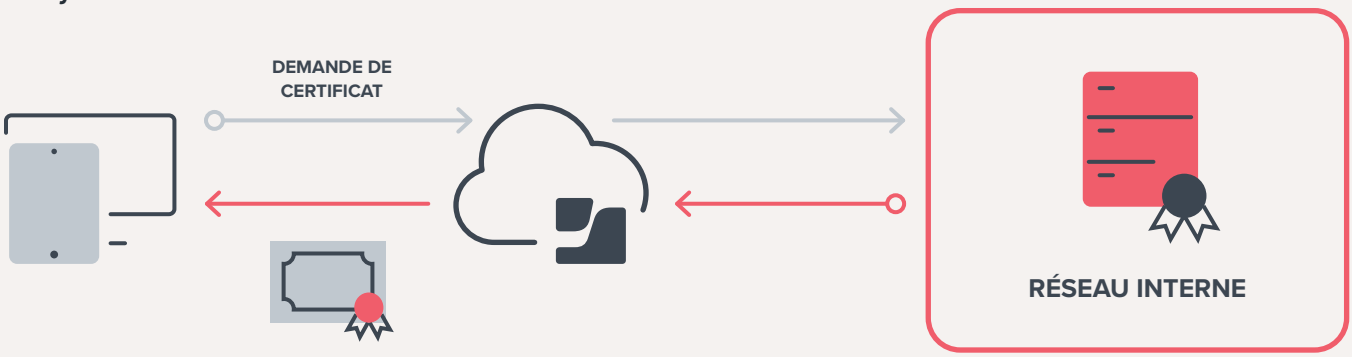
Proxy de certificat Jamf

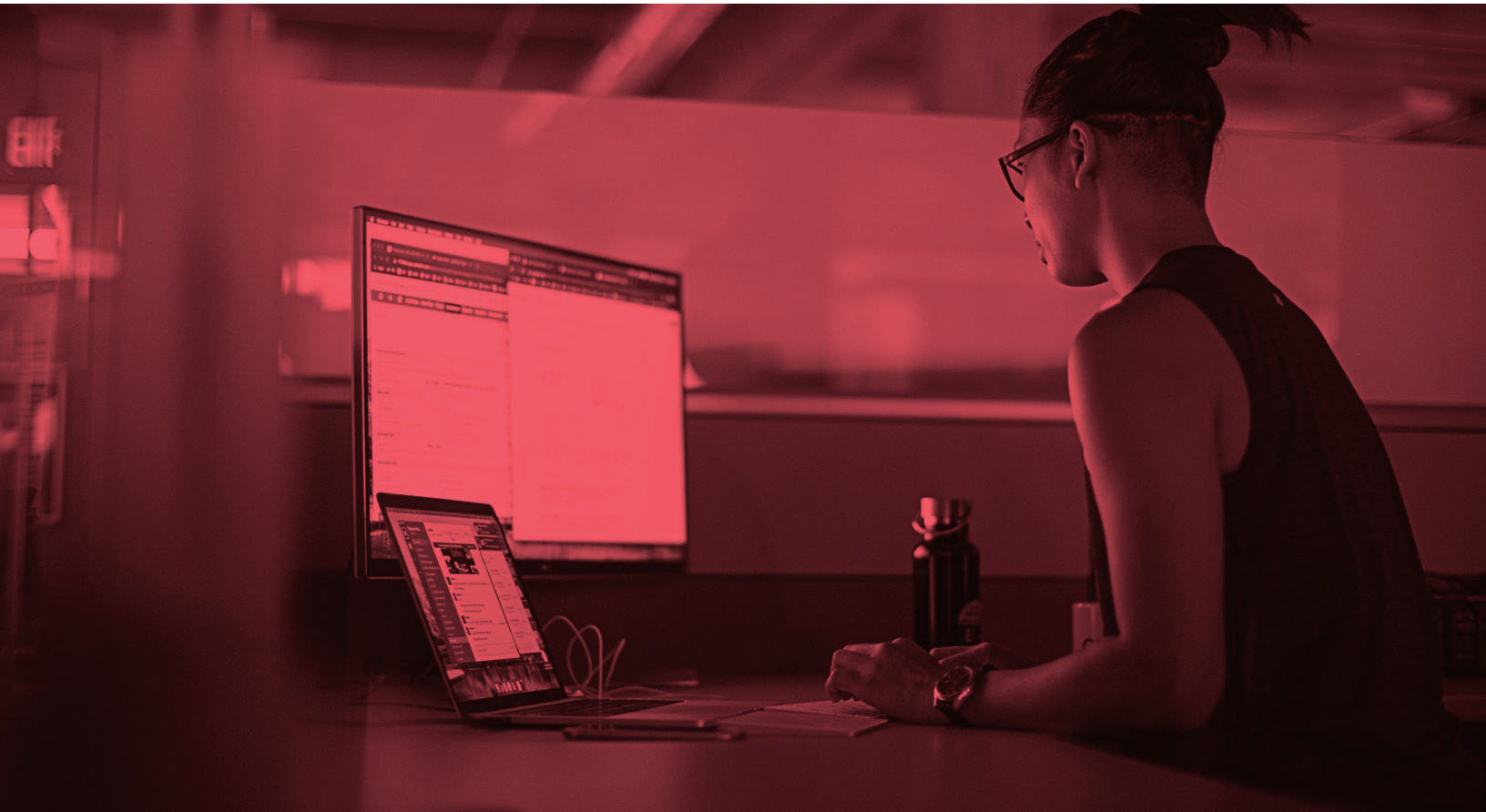
C'est là que Jamf Pro peut vous aider sans compromettre la sécurité, et c'est la méthode la plus courante pour demander des certificats.

Jamf Pro agit comme un proxy entre l'appareil et le serveur de certificats à l'aide de SCEP ou d'ACS Connector. Cela offre les avantages des méthodes précédentes, avec en plus un flux de communication simplifié. L'appareil a seulement besoin de pouvoir contacter le serveur Jamf Pro : il peut être sur n'importe quel réseau et toujours obtenir les certificats requis.

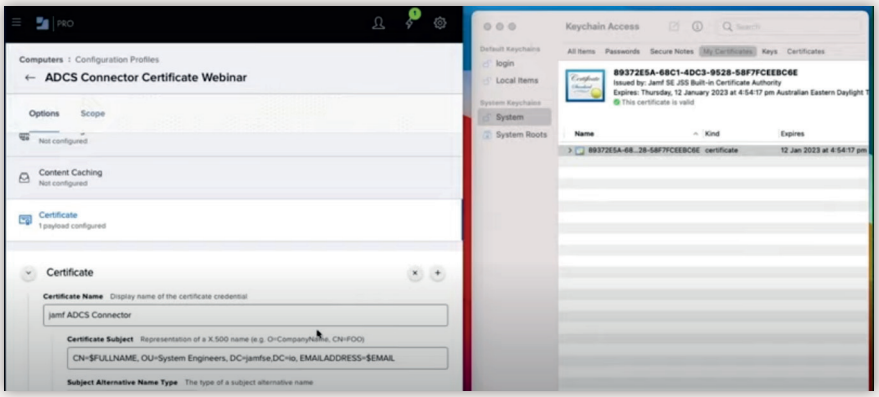
Voici à quoi ressemble la communication :

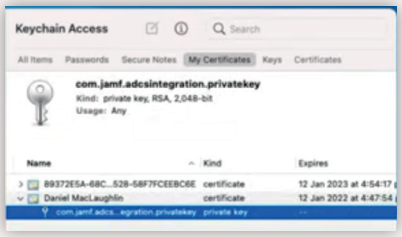
Proxy utilisant Jamf Pro





Et voici à quoi cela ressemble pour l'administrateur Apple avec le connecteur ADCS (similaire à l'utilisation de SKEP), qui a déjà été configuré. Dans cet exemple, l'appareil a déjà été inscrit et le processus se déroule sur un réseau invité, sans connexion au serveur ni de liaison Active Directory :





Sur la droite, nous pouvons voir l'application d'accès au trousseau qui affiche déjà un certificat : le certificat d'inscription de l'appareil.

Vous pouvez voir le contenu de la demande : nom complet et adresse e-mail pour les variables de contenu. L'administrateur accède ensuite à l'onglet Étendue, ajoute l'appareil et enregistre.

À partir de ce moment, Jamf Pro communique avec le serveur Jamf. Il demande le certificat au serveur de certificats et le délivre, puis Jamf le déploie sur l'appareil.

Le certificat peut désormais être utilisé comme méthode d'authentification pour la connexion Wi-Fi ou VPN.

Pour en faire un certificat *approuvé*, vous devrez déployer le certificat racine du serveur pour fournir une chaîne d'approbation.

Vous avez le certificat : comment l'utiliser ?

Un utilisateur final peut sélectionner manuellement le certificat et l'utiliser pour authentification auprès du réseau sans fil de l'entreprise.

Lorsque l'utilisateur tente de se connecter à un réseau d'entreprise 802.1x, il change le mode en EAP/TLS, puis sélectionne un certificat dans le trousseau.

De même, avec VPN, l'utilisateur final verra des options similaires, en fournissant ce type de certificats de support VPN comme méthode d'authentification. Vous devrez travailler auprès des équipes respectives de votre organisation pour cela.

Tout cela peut être automatisé en incluant la charge utile des paramètres réseau et VPN dans le profil de configuration qui contient la charge utile du certificat.

Comment démarrer le processus de création de certificat dans votre organisation

Vous aurez besoin de :

- Une version prise en charge du système d'exploitation sur l'appareil
- Une autorité de certification prise en charge, comme l'autorité de certification Microsoft, Digicert, Entrust Certificate Solutions ou Venafi
- L'assistance des autres équipes de votre organisation
  - Mise en réseau
  - Sécurité
  - Équipe de certification

Contactez un représentant Jamf pour savoir comment nous pouvons vous aider à réussir le déploiement de certificats au sein de votre organisation. Nous pouvons communiquer avec vos équipes pour expliquer ce qui est requis pour chaque service afin d'assurer un déploiement réussi.

Vous avez des questions ? Contactez-nous à info@jamf.com : nous serons ravis d'y répondre !

Ressources :

Jamf :

Présentation des certificats - JNUC : jamf.it/jnuc-cert

Jamf en tant que proxy SCEP : **jamf.it/scep**

Connecteur Jamf ADCS : jamf.it/adcsc

Webinaire sur les bases du déploiement de certificats : jamf.it/cert-101

Apple:

Guide de certification MDM : jamf.it/mdm-cert

Conditions requises pour les certificats approuvés : jamf.it/apple-cert-trust

Limites des certificats approuvés : jamf.it/apple-cert-limits