

EVIDEN

IDnomic PKI Intune Connector

Déploiement transparent d'identités numériques pour l'écosystème Microsoft®

Les environnements de travail actuels reposent sur des équipements tels que les smartphones, les tablettes et les ordinateurs. Leur intégration dans l'infrastructure informatique des entreprises est indispensable, d'autant plus que des tendances telles que le BYOD (Bring Your Own Device) complexifient les schémas de déploiement et renforcent les besoins en matière de sécurité. De plus, les applications mobiles nécessitent des méthodes spécifiques pour la gestion des données critiques.

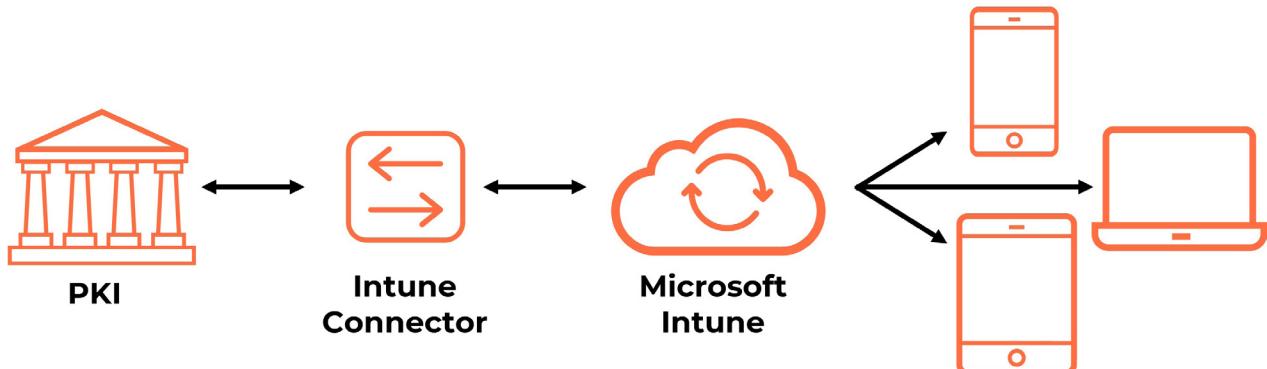
Microsoft Intune est un service cloud qui gère les appareils et les applications, garantissant sécurité et conformité. Il prend en charge le BYOD en gérant à distance la protection des applications et une intégration transparente avec Microsoft 365 et Azure. Le connecteur Intune, associé à l'une de nos solutions IDnomic PKI (ID PKI ou OT PKI), permet d'intégrer des certificats numériques dans les appareils mobiles et les ordinateurs gérés par Microsoft Intune. Ces certificats peuvent être utilisés pour l'authentification, la signature et le chiffrement des courriels.

L'intégration d'un connecteur Intune avec IDnomic PKI permet aux organisations de gérer en toute sécurité les certificats sur les appareils mobiles et les ordinateurs de bureau, renforçant ainsi la sécurité de l'accès aux ressources et aux communications. Cela facilite la gestion des appareils d'entreprise tout en maintenant des normes de sécurité élevées.

Le connecteur IDnomic PKI Intune permet de mettre en œuvre un large éventail de cas d'utilisation, et en particulier les plus courants tels que :

- **Authentification Wi-Fi** : Déploiement de certificats pour une authentification sécurisée via le protocole 802.1X.
- **VPN** : Distribution de certificats pour une authentification sécurisée auprès des serveurs VPN.
- **S/MIME** : Fourniture de certificats pour signer et chiffrer les courriels via S/MIME.
- **Accès aux applications d'entreprise** : Intégrez des certificats pour accéder aux ressources internes, telles que les intranets ou les applications sécurisées.

IDnomic PKI Intune Connector – Schéma

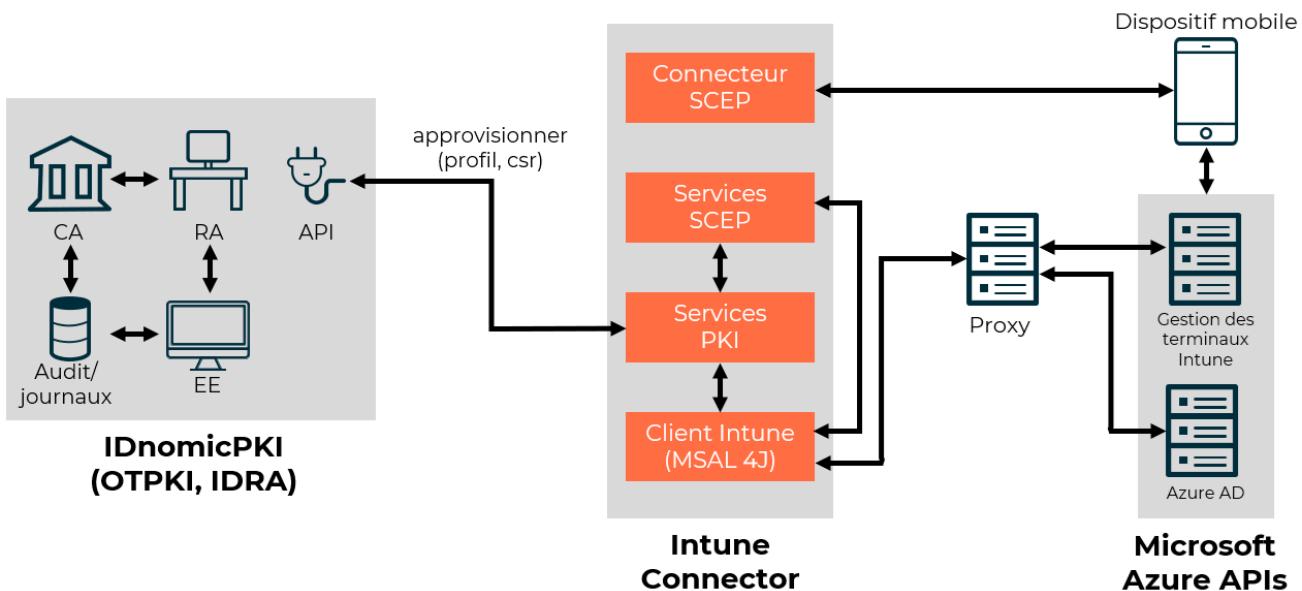


Le connecteur Intune permet la délivrance de certificats numériques en connectant IDnomic PKI à l'écosystème des appareils Microsoft.

PKI Intune Connector – La Solution

Le connecteur IDnomic Intune récupère les certificats numériques générés par une infrastructure PKI et les transmet aux appareils concernés. Les éléments clés sont les suivants :

- **Serveur PKI** : La PKI émet des certificats pour utilisateurs et objets.
- **Connecteur Intune** : Il s'agit d'un composant logiciel qui relie Intune à l'infrastructure PKI afin d'obtenir, de renouveler, de révoquer ou de distribuer des certificats sur les appareils inscrits. Ce connecteur doit être installé sur un serveur du réseau d'entreprise
- **Microsoft Intune** : Intune gère l'inscription des appareils, l'application des politiques de sécurité et la distribution des certificats via des profils de configuration.
- **SCEP**: Le connecteur Intune utilise le protocole SCEP pour émettre des certificats.



Options Supportées

Enrôlement de dispositifs



Lorsqu'un appareil est inscrit dans Intune, il peut être configuré pour recevoir des certificats numériques d'un serveur PKI afin de garantir la sécurité des communications et des processus d'authentification.

Distribution de certificats



Le dispositif interagit avec le connecteur Intune pour déployer des certificats via des profils de configuration. Dans le cadre du processus de distribution des certificats, le connecteur sert d'intermédiaire entre les dispositifs et Intune. Il transmet et redirige les informations.

Authentification & autorisation



Les certificats peuvent être utilisés pour l'authentification afin de sécuriser les réseaux (Wi-Fi, VPN), les applications ou les services internes.

Les avantages clients

- **Compatibilité native** avec IDnomic PKI, permettant une rationalisation des coûts d'infrastructure. Le connecteur Intune permet à une organisation de bénéficier de la flexibilité et des performances d'IDnomic PKI sans aucune limitation au niveau de son infrastructure matérielle.
- **Renouvellement transparent** des certificats, sans impact sur les utilisateurs finaux. Gérez le cycle de vie des identifiants de manière transparente, en masquant toute la complexité liée à la délivrance et au renouvellement des certificats grâce à des workflows automatisés et flexibles.
- **Augmentez la productivité** en réduisant les processus d'assistance coûteux liés à la délivrance manuelle de certificats pour des appareils spécifiques.
- **Garantissez la sécurité** et le contrôle d'accès pour tous les appareils connectés à l'infrastructure informatique d'une entreprise en utilisant des certificats pour l'authentification et le chiffrement, déployés via IDnomic Intune Connector.

Standards and Spécifications Techniques

Protocoles

- » SCEP

Serveurs

- » Redhat Enterprise Linux 6/7/8 (x86_64)
- » Rocky Linux 8 (x86_64)
- » SLES 11/12/15 (x86_64)

Dispositifs mobiles

- » Microsoft Windows 10
- » Android 11
- » iOS 15

PKI

- » IDnomic PKI
- » OpenTrust PKI

En savoir plus sur nous: www.crypto-vision.com

Connectez-vous avec nous



eviden.com