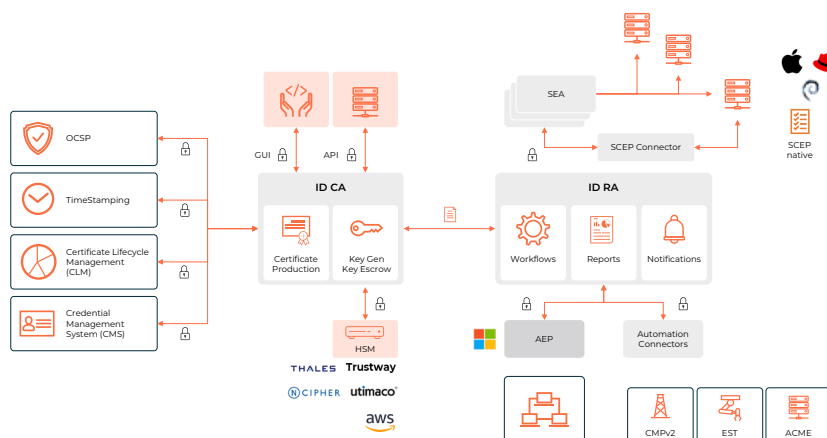


## IDnomic PKI

# Identités numériques de confiance

Mettre en place un processus hautement sécurisé pour contrôler l'accès, authentifier l'identité des utilisateurs et des objets, vérifier l'intégrité des documents et des communications, représente un défi majeur pour toute organisation. IDnomic PKI permet à toutes les organisations publiques et privées d'établir et de maintenir un système d'information digne de confiance en émettant des identités numériques pour l'authentification forte, le chiffrement des données et la signature électronique.

Une solution pour la sécurité de tous les cas d'utilisation de la transformation numérique



## En phase avec la croissance de votre activité

IDnomic PKI est une solution de pointe qui fournit une infrastructure à clé publique (PKI) puissante et avancée pour sécuriser tous les processus numériques en délivrant des certificats électroniques pour les utilisateurs et les objets.

Basée sur les normes X.509v3, elle permet le déploiement d'infrastructures de confiance et gère le cycle de vie des certificats électroniques et des autorités de certification qui les émettent, simplifiant ainsi grandement le processus de gestion des identités.

Son architecture est basée sur une approche modulaire qui combine un haut niveau de flexibilité pour les

besoins évolutifs avec une approche de conception ergonomique et moderne, offrant des interfaces conviviales et adaptées aux besoins de votre entreprise.

Couvrant un large éventail de cas d'utilisation de l'identité numérique, la suite IDnomic PKI est disponible "On Premise", installée sur les sites des clients, ou en mode « Software as a Service » (software en tant que service), depuis notre datacenter hautement sécurisé.

IDnomic PKI peut être combiné avec d'autres modules IDnomic; en particulier avec IDnomic CLM (Gestion du cycle de vie des certificats), IDnomic CMS (Système de gestion

des dispositifs cryptographiques), IDnomic TimeStamping (application d'horodatage) ou encore IDnomic Sign (signature électronique).

Suivant notre politique d'un niveau de sécurité maximal, IDnomic PKI a été certifiée critères communs EAL4+. Nos équipes de consultants et d'experts vous offrent un support complet pour vous aider à mener à bien chaque étape de votre projet de transformation numérique. Bénéficiez de notre expérience pour définir, mettre à niveau ou assurer la conformité de vos solutions de sécurité pour les utilisateurs, les machines, les objets, les documents et les transactions.

## IDnomic PKI – une solution modulaire

### ID CA

#### **Autorité de Certification**

Entité centrale, chargée de la génération des identités numériques de confiance. Elle est responsable de la création, de l'organisation et de la gestion des identités numériques de confiance et des autorités de certification à travers la production de certificats électroniques.

### ID RA

#### **Autorité d'Enregistrement**

Ce module gère le cycle de vie des certificats et définit les différents workflows associés aux profils et leurs modes d'émission. ID RA répond à tous les cas d'utilisation des machines et supporte plusieurs protocoles d'enrôlement (ACME, EST, SCEP, CMP, AEP).

### ID OCSP

#### **Online Certificate Status Protocol**

Fournit une preuve en temps réel de la validité d'un certificat numérique (révoqué, suspendu, actif). Ce composant s'ajoute aux listes de révocation de certificats (CRL), produites par ID CA nativement.

## Les avantages client

**IDnomic PKI offre plusieurs avantages fonctionnels pour la gestion des identités numériques de confiance**

- » Une conception moderne et ergonomique - facile à déployer, à configurer, à maintenir et à utiliser
- » Orienté hautes performances et extrêmement évolutif - gestion de 1000 à 100 millions de certificats
- » Niveau de Sécurité le plus élevée - certification critères communs EAL 4+.
- » Mutualisée par conception - déployer, configurer et gérer plusieurs PKI indépendamment avec une seule instance logicielle
- » On Premise ou en Cloud - déploiements adaptés à vos besoins et capacités opérationnelles
- » Exportation de la configuration - transition facile d'un environnement de pré-production à un environnement de production.
- » Capacité d'utiliser des linters certifiés selon les recommandations du CAB FORUM
- » Prise en charge d'une grande variété de protocoles d'enrôlement (EST, SCEP, ACME, CMP)

## Standards et spécifications techniques

### Normes and standards

- » Format de certificat X.509v3, RFC 5280 et RFC 3739
- » Requêtes de certificat : PKCS#10, CSR, SPKAC
- » Algorithmes de signature RSA (1024 - 4096) , (RSA PKCS#1 v1.5, RSA PSS PKCS#1 v2.1), ECDSA (192- 521) Algorithmes de Hash SHA-224, SHA-256, SHA-384, SHA-512, SHA-256 MGF1, SHA-384 MGF1, SHA512 MGF1
- » Contenu de certificat : UTF8, T61, printable, email, SAN (RFC822, UPN), etc.

### Conformité

- » Certifié RGS pour toutes ses classifications (1, 2 et 3).
- » Conformité eIDAS : obtention du certificat LSTI N° 8029-1318-V3.0 / EN319411-1 V1.1.1

### Configuration requise

- » Système d'exploitation Redhat, SUSE ou Rocky Linux
- » Java Development Kit (JDK) installé
- » Le produit est entièrement intégré avec des composants Open-Source : Apache, PostgreSQL, PHP, Tomcat, Keycloak, Ansible

En savoir plus sur nous: [www.idnomic.com](http://www.idnomic.com)

Connectez-vous avec



[eviden.com](http://eviden.com)