IDnomic Vericert

Renforcer et centraliser la validation des certificats

Les certificats électroniques permettent aux applications d'intégrer des services de sécurité tels que l'authentification des utilisateurs, la non répudiation des transactions et la confidentialité des échanges de données. La validité des certificats doit être vérifiée avant leur utilisation et après, pour la non répudiation et la confidentialité des données. Atos, acteur européen de la sécurité des systèmes d'information propose **vericert,** une solution complète de validation des certificats s'appuyant sur des politiques de validation personnalisées

SÉCURITÉ CERTIFICATION

SÉCURITÉ CERTIFICATION

Produits certifiés CSPN
ANSSI-CSPN-2014/10

vericert version 2.1.2

Les politiques de validation

Une politique de validation est un ensemble de règles définissant les conditions de validation des certificats. Elle peut couvrir des cas plus ou moins complexes. Une ou plusieurs politiques de validation peuvent être définies puis personnalisées afin de répondre au mieux aux besoins des différentes applications.

La validation d'un certificat donné requiert au minimum :

- un chemin de certification jusqu'à une autorité de certification (AC) reconnue
- une politique de validation

Le statut de validation de chaque certificat appartenant au chemin de certification doit être vérifié à l'aide de CRLs (Certificate revocation list) ou de réponses OCSP (On-line Certificate Status Protocol).

Des contraintes supplémentaires peuvent être définies dans la politique de validation, telles que des politiques de certification reconnues, la longueur du chemin de certification ou les conditions d'utilisation des clés.

Vericert, un service centralisé de validation des certificats

La centralisation proposée par vericert simplifie l'accès aux informations nécessaires pour la validation des certificats. Les certificats des AC, les CRLs correspondantes sont collectés par vericert qui les fournit en retour au demandeur. Les informations collectées pour répondre à une requête peuvent être partiellement ou totalement réutilisées pour une autre demande, permettant ainsi d'améliorer le délai de réponse et de réduire la charge du réseau. Quand la validation d'un certificat se réfère à une date antérieure à la requête, les certificats, les CRLs et les réponses OCSP, déjà fournis par vericert, doivent être retournés par le demandeur.

Atos, acteur européen de la sécurité

Leader européen de la sécurité intégrée, Atos a développé une expertise unique de la sécurité des systèmes d'information, conjuguant ses savoir-faire de conseil, d'intégrateur et d'expert des technologies de confiance.

La maîtrise des identités électroniques pour tous les composants du système d'information

Vericert est distribué en Appliance Virtuelle ou sous forme de modules installables par le client dans son environnement. Il est géré par le biais d'une interface web. Quand un certificat est validé conformément à une politique de validation, **vericert** est accessible via une interface web (RPC-SOAP) utilisant HTTP ou HTTPS (SSL). Les réponses peuvent être signées.

Vericert est aussi accessible via le protocole OCSP (RFC 6960).

Vericert est disponible avec les composants fonctionnels suivants

- Le stockage des certificats pour mettre les certificats d'AC en lieu sûr
- L'optimisation des performances via le préchargement des CRLs obtenues à partir de points de distribution prédéfinis
- Un serveur OCSP pour fournir les statuts de révocation des certificats
- Le chargement des TSL (« Trusted Service List ») pour le support des AC reconnues
- En option, un client OCSP pour Apache
- En option, un HSM (Hardware Security Module) qui protège les clés utilisées pour signer les réponses de validation ou les réponses OCSP. Vericert peut supporter différents HSM fournis par Atos ou par d'autres sociétés

Personnalisation des politiques de validation

En utilisant une interface web, il est possible d'administrer :

- des certificats d'autorités de certification
- les chemins de certification
- les politiques de certification reconnues
- des valeurs d'usage de clés
- des valeurs d'usage étendues des clés

Exigence techniques

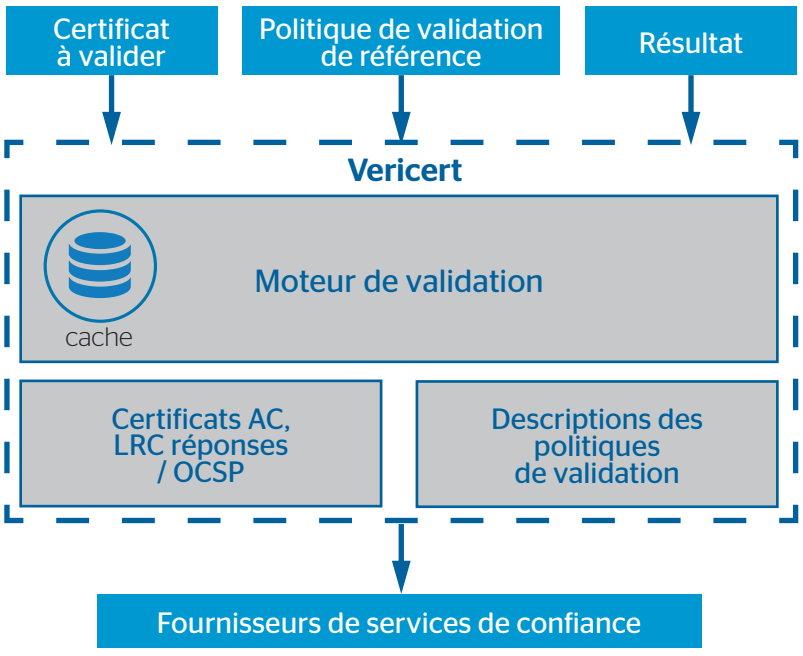
Serveur VMware pour la distribution en Appliance Virtuelle. Version installable par modules:

- Plateforme Linux (e.g. RedHat ou CentOS)
- Java JRE SE 8
- Une interface PKCS#11 adaptée pour connecter un HSM afin de signer des réponses
- Composants Open source utilisés par vericert : Apache Tomcat 8.x, OpenLDAP, PostgreSQL

Normes et standards

Format de certificat compatible avec ITU-T X.509v3 et RFC 5280.

- Information de révocation compatible avec ITU-T X.509v2 CRL et le protocole OCSP (RFC 6960)
- SOAP 1.1 et WSDL 1.1
- REST
- RFC 6960 pour les statuts de révocation des certificats
- Connexion : HTTP, LDAP et HTTPS
- Norme ETSI pour les TSL v5 (ETSI TS 119 612 V2.2.1)



Find out more about us

https://atos.net/fr/solutions/cybersecurite-produits/digital-identities/vericert

CT-201105-AS-IDnomic_Vericert_french