Proxy d'application : générer et utiliser un certificat pour les applications publiées avec Azure Key Vault

Présentation

- Certificat de signature SAML
- Géré dans Azure Key Vault
- Attaché à une App Registration
- Renouvellement automatique via GitHub Actions
- Zéro interruption (chevauchement des certificats)

Architecture globale dans Entra ID:

```
App Registration
 ├─ Certificats OAuth
 ├─ GitHub Actions (OIDC)
 ├─ Key Vault
 └─ Microsoft Graph
```

- Pas de secrets dans GitHub
- Authentification par OIDC Federated Credentials
- Conformité Microsoft / Zero Trust

Cas standard Microsoft OAuth :

- Protocole : OAuth 2.0 / OpenID Connect
- Méthode d'authentification : client*secret*post ou client*secret*basic
- Objet Entra ID utilisé : Inscription d'application
- SAML : NON ⇒ Application d'entreprise NON requise

Élément	Gérer SAML	Gérer certificats / secrets & automation
Inscription d'applications	NON	OUI
Applications d'entreprise	OUI	NON

Prérequis Entra ID

- Une App Registration existante
  - Type : Single tenant
  - Usage : SAML
- Un Key Vault
  - SKU Standard
  - Soft delete activé (par défaut)

Créer un Key Vaults (coffres de clé)

- créer un Key Vaults :
  - choisir l'abonnement
  - créer un groupe de ressources
  - définir le nom du coffre de clé
  - choisir la région et le niveau tarifaire standard

Lien d'information sur la tarification : https://azure.microsoft.com/fr-fr/pricing/details/key-vault/

- Accéder au coffre de clé :
  - dans le contrôle d'accès (IAM), donner le rôle **Agent des certificats Key Vault** plutôt que **Administrateur Key Vault** à l'utilisateur qui va créer et gérer les certificats
  - l'Onglet **Attributions de rôles** permet de vérifier les rôles affectés

Création de l'App Registration dans le Portail Azure

- Accéder au **portail Azure** puis **Microsoft Entra ID**.

- Choisir **Inscription d'applications**.
- Puis **Nouvelle inscription** :
    - Nom : signature-Valadon,
    - Type de compte : Locataire uniquement,
    - URI de redirection Web : https:*<your-domain>/api/auth/callback/microsoft * Cliquer sur **S'inscrire**. Noter : * ID client * ID du Tenant ===== Créer un certificat ===== * accéder au coffre de clé * dans la rubrique **Objets**, choisir **Certificats** * Cliquer sur **+ Générer / Importer***