Configuration en tant que ServiceProvider

Génération de la paire de clés:

Dans le répertoire du tenant

```
openssl req -x509 -sha256 -newkey rsa:2048 -nodes -keyout publik-sp.key -out publik-sp.crt -batch
-subj '/CN=connexion.demarches.ville.fr' -days 3652
```

Pour Authentic multitenant, copier les fichiers générés dans le répertoire du tenant:

```
cp sp-saml.key /var/lib/authentic2-multitenant/tenants/<connexion.demarches.ville.fr>/
cp sp-saml.crt /var/lib/authentic2-multitenant/tenants/<connexion.demarches.ville.fr>/
```

Métadonnées du fournisseur d'identités:

Télécharger le fichier des métadonnées, ou si pas accessible directement via HTTP, le demander au client.

Pour Authentic multitenant copier le fichier dans le répertoire du tenant:

```
cp idp-metadata.xml /var/lib/authentic2-multitenant/tenants/<connexion.demarches.ville.fr>/
```

Settings

Pour Authentic multitenant créer le fichier settings.json dans le répertoire /var/lib/authentic2-multitenant/tenants/<connexion.demarches.ville.fr>/ avec le contenu suivant:

```
{
  "A2_AUTH_SAML_ENABLE": true,
  "MELLON_PUBLIC_KEYS": ["/var/lib/authentic2-multitenant/tenants/<connexion.demarches.ville.fr>/p
ublik-sp.crt"],
  "MELLON_PRIVATE_KEY": "/var/lib/authentic2-multitenant/tenants/<connexion.demarches.ville.fr>/pu
blik-sp.key",
  "MELLON_PROVISION": true,
  "MELLON_IDENTITY_PROVIDERS": [
    {
      "A2_ATTRIBUTE_MAPPING": [
        {
          "attribute": "email",
          "mandatory": true,
          "saml_attribute": "email"
        },
        {
          "attribute": "last_name",
          "mandatory": false,
          "saml_attribute": "last_name"
        },
        {
          "attribute": "first_name",
          "mandatory": false,
          "saml_attribute": "first_name"
        },
        {
          "action": "toggle-role", <= si besoin d'affecter un rôle aux comptes en provenance du fo
urnisseur
          "role": {
            "name": "Agent"
          }
        }
```

```
      ],
      "SLUG": "my-idp",
      "LOOKUP_BY_ATTRIBUTES": [
        {
          "user_field": "email",
          "saml_attribute": "email"
        }
      ],
      "METADATA": "/var/lib/authentic2-multitenant/tenants/<connexion.demarches.ville.fr>/idp-meta
data.xml"
       ou bien
      "METADATA_URL": "https://annuaire.ville.fr/.../metadata.xml",
    }
]
}
```

Dans le cas ou le fournisseur d'identité est un serveur ADFS, les noms des attributs usagers peuvent être des URIs: exemple

Communiquez les métadonnées aux clients pour qu'il puisse faire la configuration de son coté

https://connexion.demarches.ville.fr/accounts/saml/metadata/