

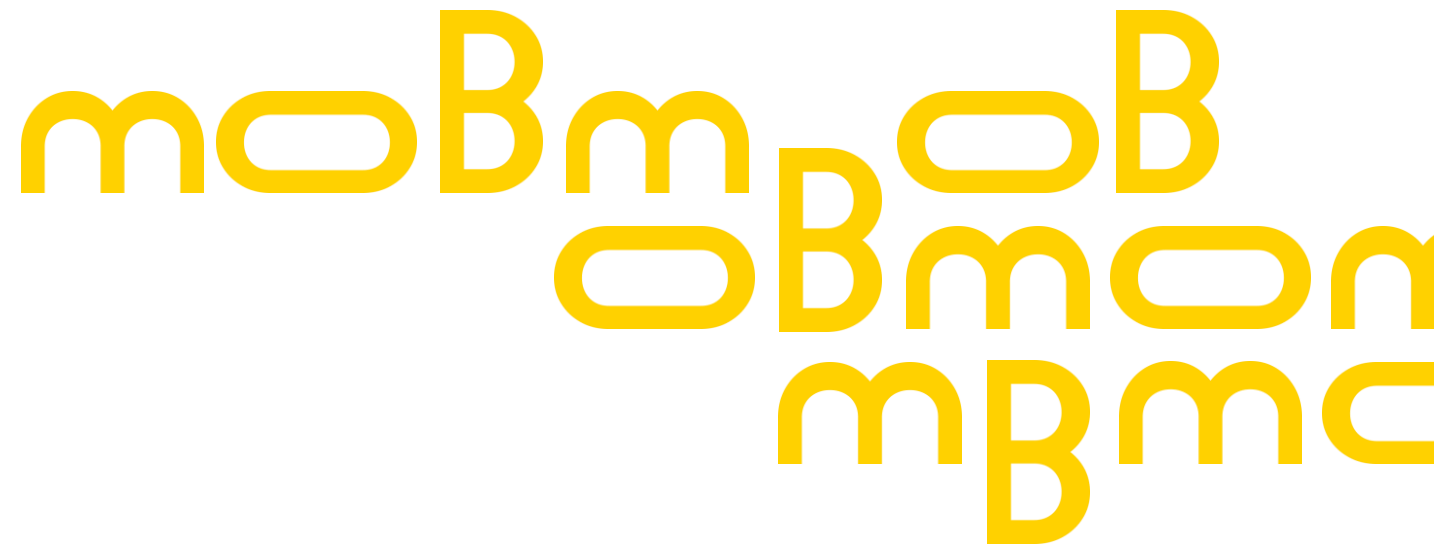
Vault

Guide de configuration en preview et
preprod



Sommaire

1. Prérequis
2. Installation des certificats
3. Configuration Keycloak
4. Configuration Postman
5. Configuration API



Prérequis



Vault démarré et initialisé



<https://vault-master.preview.moncomptemobilite.fr>

Certificats

Récupérer et installer les certificats du
Vault sur sa machine



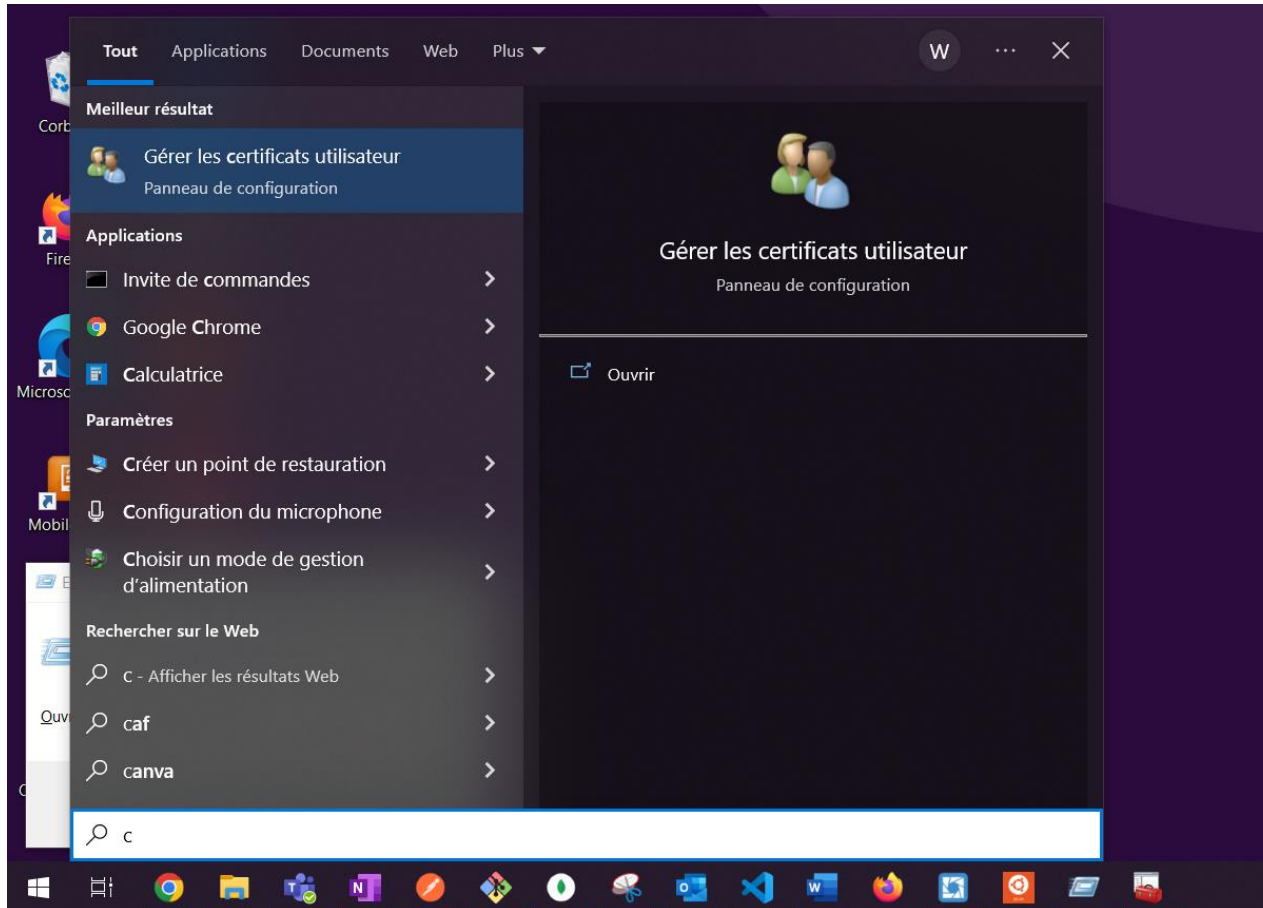
Installation des certificats dans le navigateur pour tester le déchiffrement

Récupération des certificats

- Certificat du gestionnaire : [manager-client-cert.pfx](#)
- Certificat de l'autorité de certification : [client-ca.pem](#)

Installation des certificats dans le navigateur pour tester le déchiffrement

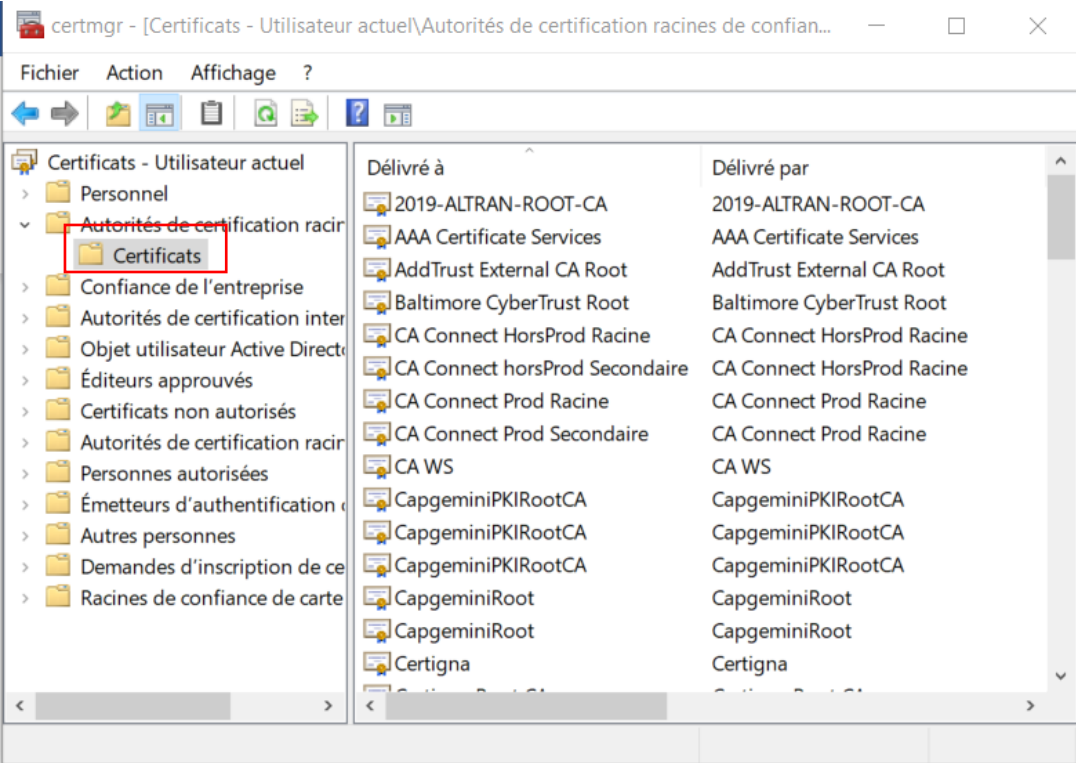
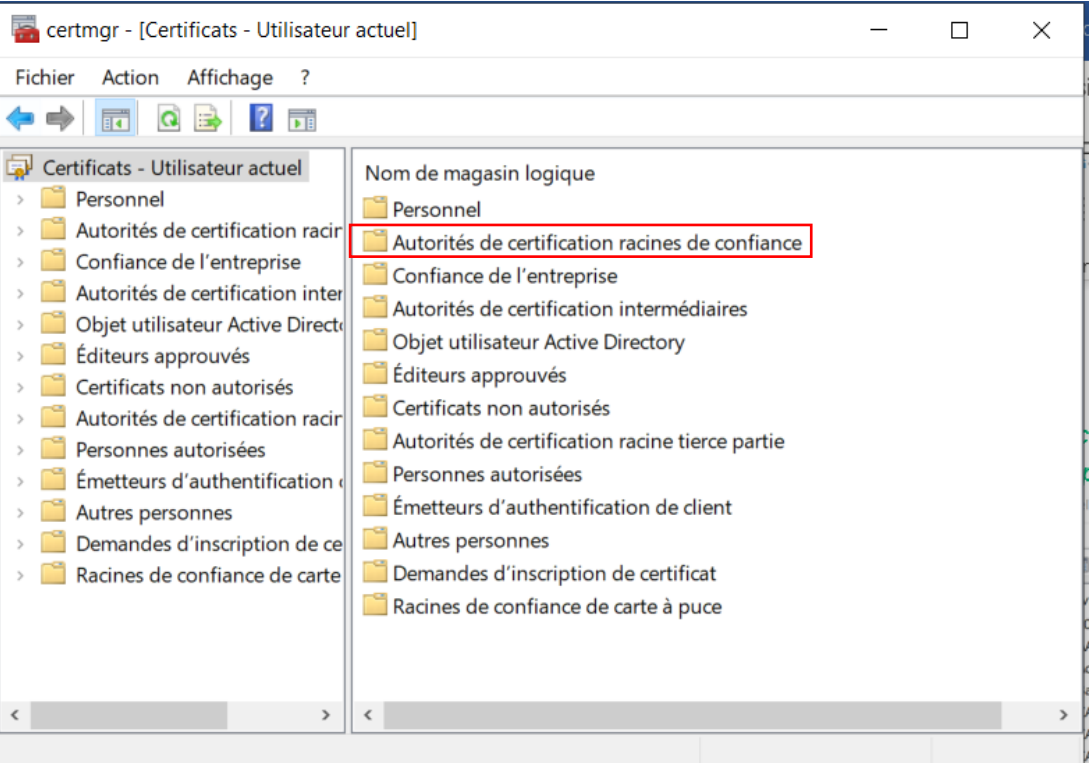
Ouvrir le gestionnaire de certificats



Installation des certificats dans le navigateur pour tester le déchiffrement

Ajouter le certificat de l'autorité de certification

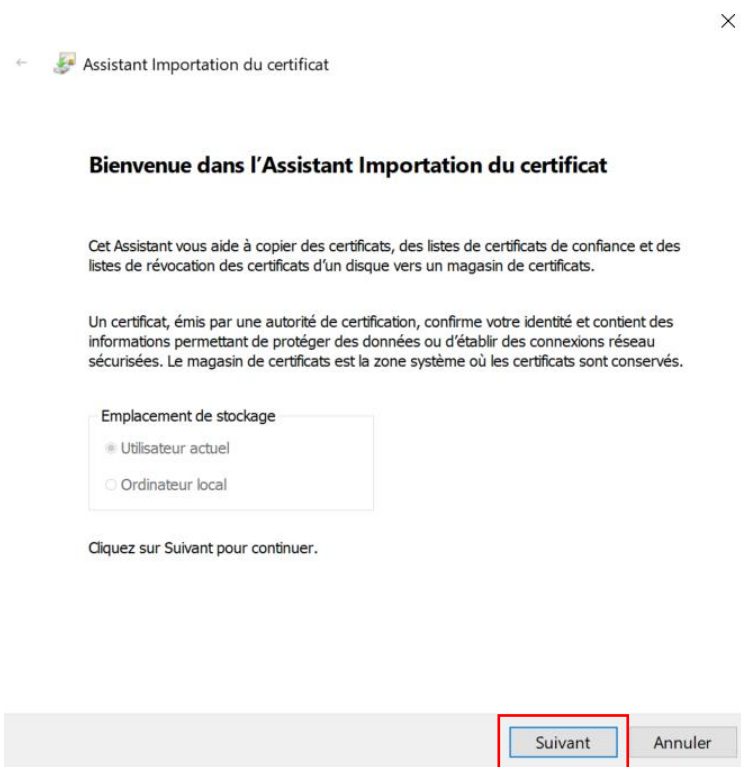
Clic droit sur Certificats puis cliquer sur Toutes les tâches puis cliquer sur Importer



Installation des certificats dans le navigateur pour tester le déchiffrement

Ajouter le certificat de l'autorité de certification

Cliquer sur Parcourir et sélectionner le fichier client-ca.pem cliquer sur Suivant



← Assistant Importation du certificat

Bienvenue dans l'Assistant Importation du certificat

Cet Assistant vous aide à copier des certificats, des listes de certificats de confiance et des listes de révocation des certificats d'un disque vers un magasin de certificats.

Un certificat, émis par une autorité de certification, confirme votre identité et contient des informations permettant de protéger des données ou d'établir des connexions réseau sécurisées. Le magasin de certificats est la zone système où les certificats sont conservés.

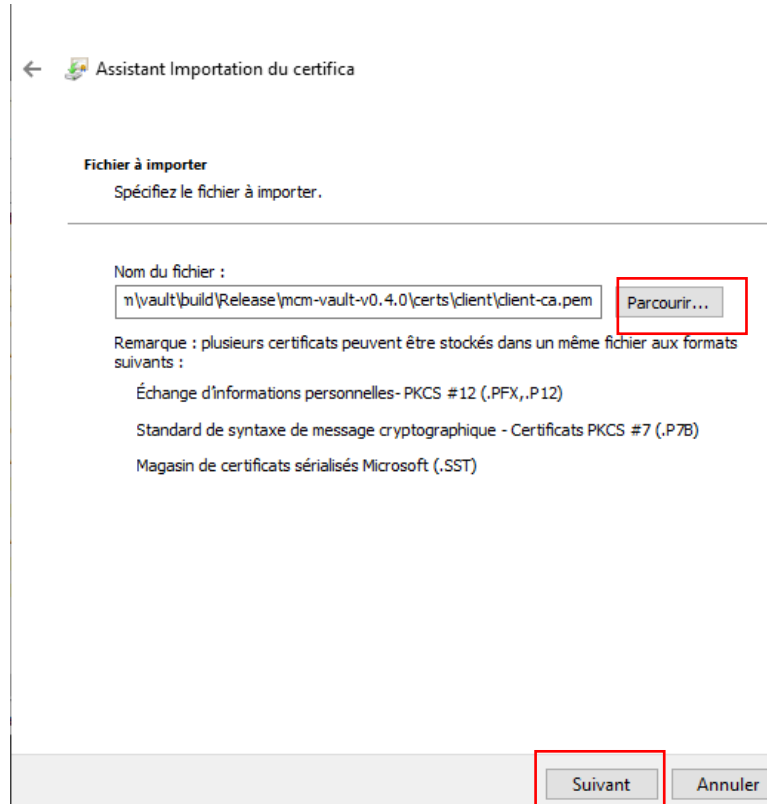
Emplacement de stockage

☒ Utilisateur actuel

☐ Ordinateur local

Cliquez sur Suivant pour continuer.

Suivant Annuler



← Assistant Importation du certifica

Fichier à importer

Spécifiez le fichier à importer.

Nom du fichier :

n:\vault\build\Release\mcm-vault-v0.4.0\certs\client\client-ca.pem **Parcourir...**

Remarque : plusieurs certificats peuvent être stockés dans un même fichier aux formats suivants :

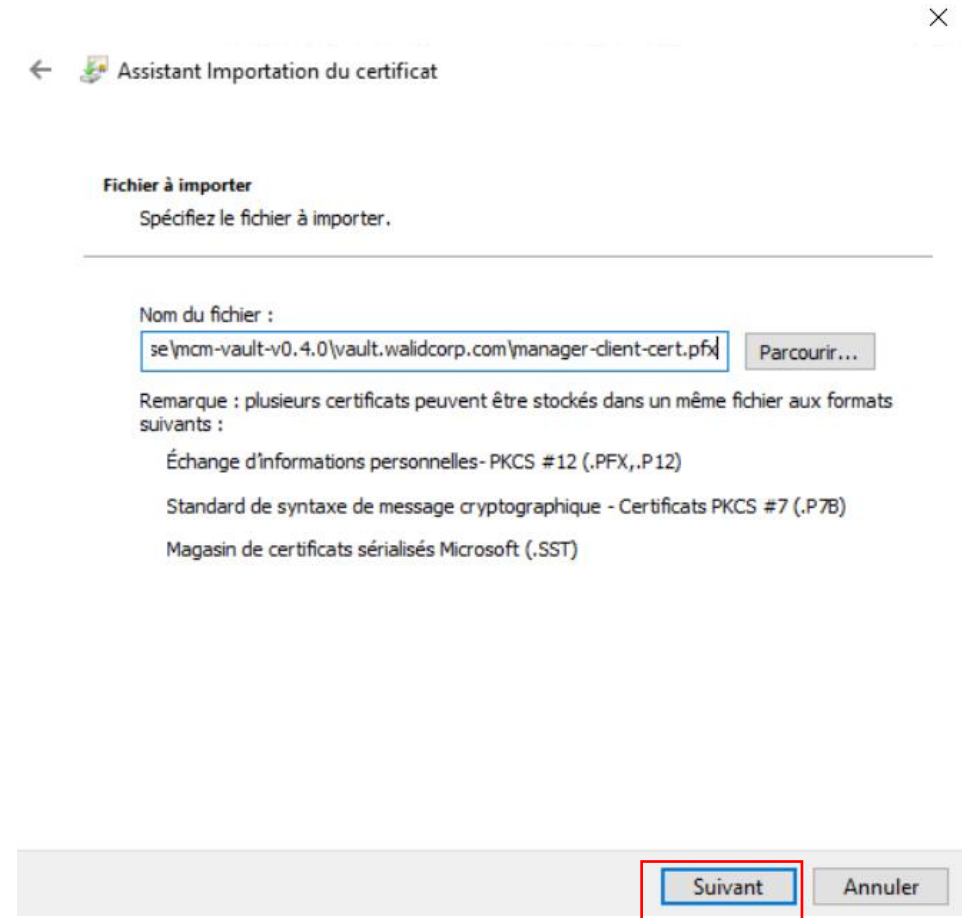
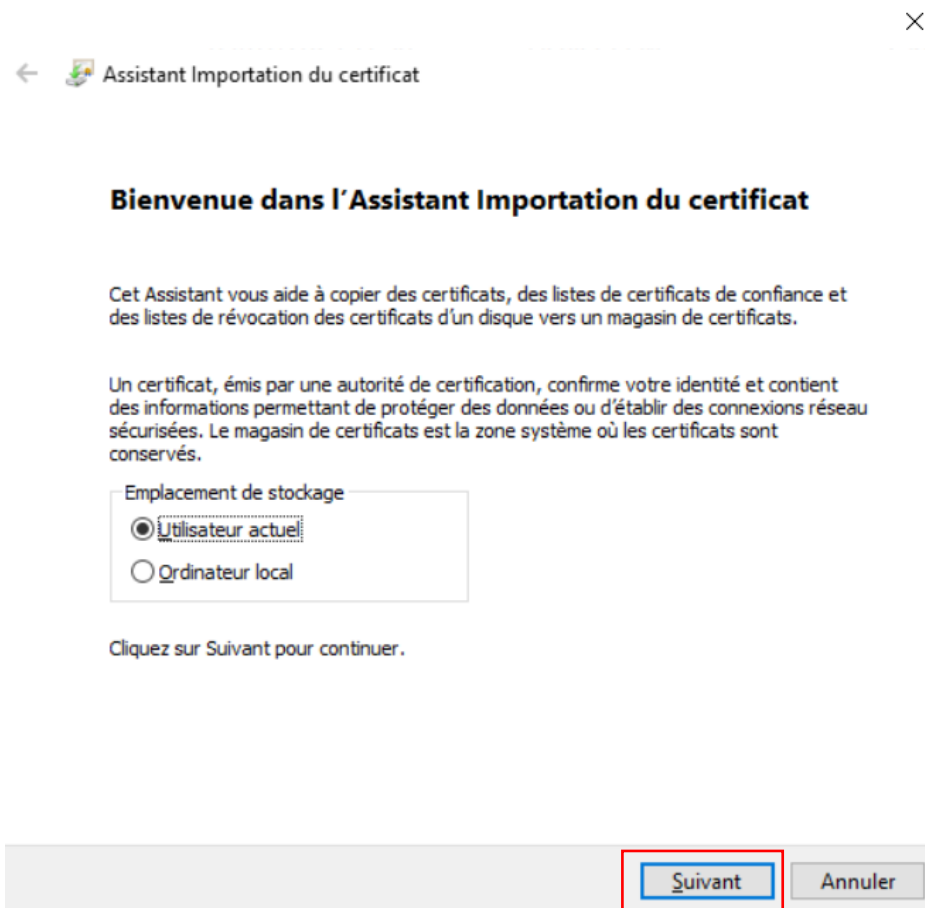
- Échange d'informations personnelles- PKCS #12 (.PFX,.P12)
- Standard de syntaxe de message cryptographique - Certificats PKCS #7 (.P7B)
- Magasin de certificats sérialisés Microsoft (.SST)

Suivant Annuler

Installation des certificats dans le navigateur pour tester le déchiffrement

Ajouter le certificat Manager dans les certificats personnels de l'utilisateur

Double clic sur manager-client-cert.pfx et cliquer 2 fois sur Suivant



Installation des certificats dans le navigateur pour tester le déchiffrement

Ajouter le certificat Manager dans les certificats personnels de l'utilisateur

Entrer le mot de passe « pass » et cliquer sur Suivant, sélectionner le magasin de certificats personnel et cliquer sur Suivant puis terminer

Assistant Importation du certificat

Protection de clé privée

Pour maintenir la sécurité, la clé privée a été protégée avec un mot de passe.

Tapez le mot de passe pour la clé privée.

Mot de passe :

pass

☒ Afficher le mot de passe

Options d'importation :

☐ Activer la protection renforcée de clé privée. Une confirmation vous est demandée à chaque utilisation de la clé privée par une application, si vous activez cette option.

☐ Marquer cette clé comme exportable. Cela vous permettra de sauvegarder et de transporter vos clés ultérieurement.

☐ Protéger la clé privée à l'aide de la sécurité par virtualisation (non exportable)

☒ Indure toutes les propriétés étendues.

Suivant

Annuler

Assistant Importation du certificat

Magasin de certificats

Les magasins de certificats sont des zones système où les certificats sont conservés.

Windows peut sélectionner automatiquement un magasin de certificats, ou vous pouvez spécifier un emplacement pour le certificat.

☐ Sélectionner automatiquement le magasin de certificats en fonction du type de certificat

☒ Placer tous les certificats dans le magasin suivant

Magasin de certificats :

Personnel

Parcourir...

Suivant

Annuler

Assistant Importation du certificat

Fin de l'Assistant Importation du certificat

Le certificat sera importé après avoir cliqué sur Terminer.

Vous avez spécifié les paramètres suivants :

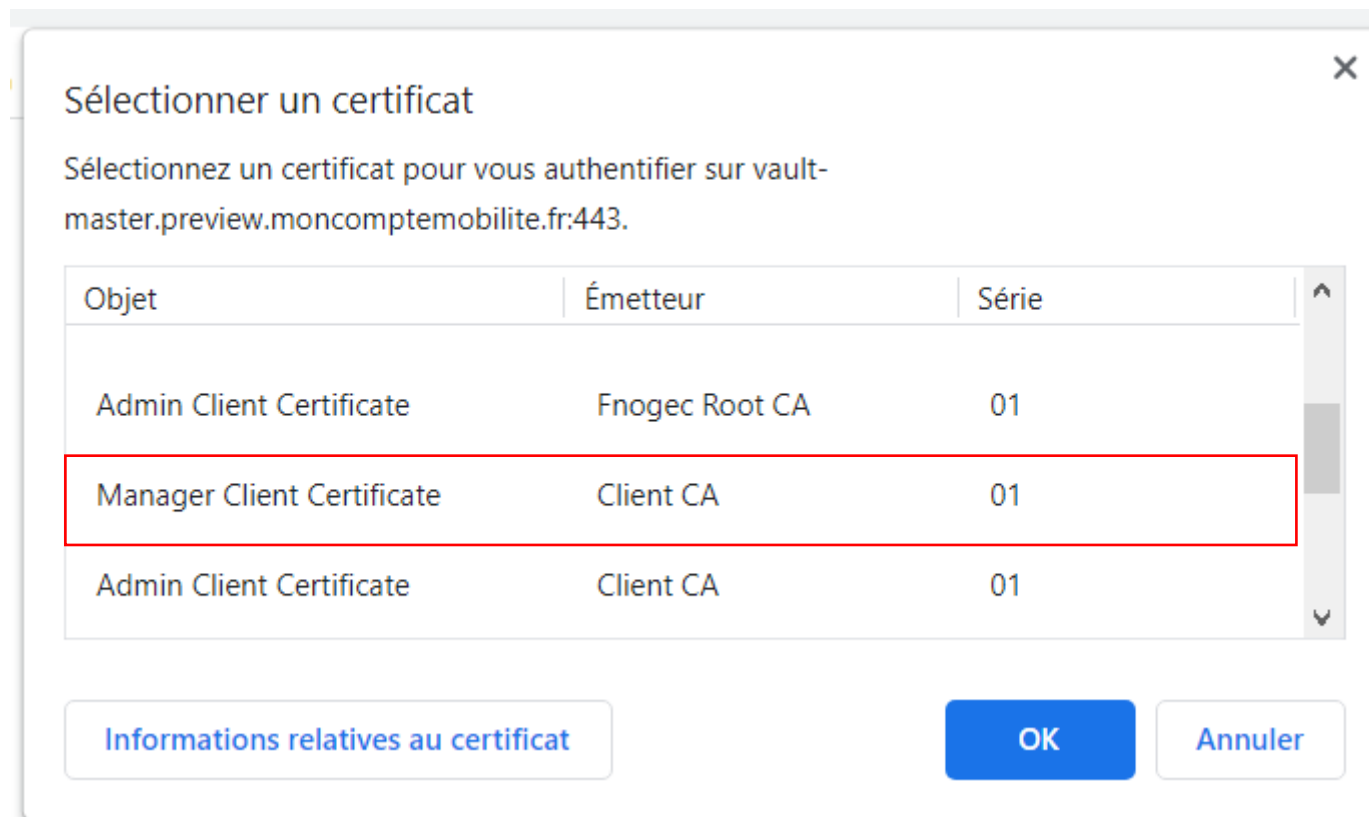
Magasin de certificats sélectionné par l'utilisateur	Personnel
Contenu	PFX
Nom du fichier	\\wsl.localhost\Ubuntu-20.04\home\w

Terminer

Annuler

Installation des certificats dans le navigateur pour tester le déchiffrement

Lorsque vous allez télécharger un justificatif, sélectionner Manager Client Certificate quand vous êtes prompté pour sélectionner un certificat



Configuration Keycloak

Sélectionner les clients et financeurs
autorisés à utiliser le vault



Configuration KC

Mcm ▾

Master

Add realm

Clients

Client Scopes

Roles

Identity Providers

User Federation

Authentication

Manage

Groups

Users

Sessions

Events

Import

Export

Clients

[Lookup ?](#)

<input type="text" value="Search..."/> <input type="button" value="Q"/>		
Client ID	Enabled	Base URL
account	True	http://localhost:9000/auth/realms/mcm/account/
account-console	True	http://localhost:9000/auth/realms/mcm/account/
admin-cli	True	Not defined
administration	True	Not defined
api	True	Not defined
broker	True	Not defined
platform	True	Not defined
realm-management	True	Not defined
security-admin-console	True	http://localhost:9000/auth/admin/mcm/console/
simulation-maas-backend	True	Not defined
simulation-maas-client	True	Not defined
simulation-maas-client-cme	True	Not defined
simulation-test-maas	True	Not defined
Total-backend	True	Not defined

Configuration KC

Création des roles vault et service_vault

Mcm

Configure

Realm Settings

Clients

Client Scopes

Roles

Identity Providers

User Federation

Authentication

Clients > simulation-maas-backend

Simulation-maas-backend

Settings Credentials Keys Roles Client Scopes Mappers Scope Revocation Sessions Offline Access Clustering Installation Service Account Roles

Search...

View all roles

Add Role

Role Name	Composite	Description	Actions
-----------	-----------	-------------	---------

Configuration KC

Création des rôles vault et service_vault

Add Role

Role Name *

service_vault

Description

Save

Cancel

Configuration KC

Création des roles vault et service_vault

Mcm

Configure

Realm Settings

Clients

Client Scopes

Roles

Identity Providers

User Federation

Authentication

Clients > simulation-maas-backend

Simulation-maas-backend

Settings Credentials Keys Roles Client Scopes Mappers Scope Revocation Sessions Offline Access Clustering Installation Service Account Roles

Search...

View all roles

Add Role

Role Name	Composite	Description	Actions
-----------	-----------	-------------	---------

Configuration KC

Création des rôles vault et service_vault

Add Role

Role Name *


Description








Save

Cancel

Configuration KC

Création des mappers

Simulation-maas-backend 

- Settings
- Credentials
- Keys
- Roles
- Client Scopes 
- Mappers 
- Scope 
- Revocation
- Sessions 
- Offline Access 
- Clustering
- Installation 
- Service Account Roles 

Search...

Q

Create

Add Builtin

Name	Category	Type	Priority Order	Actions	
maas_name	Token mapper	Hardcoded claim	0	Edit	Delete
Client IP Address	Token mapper	User Session Note	0	Edit	Delete
Client ID	Token mapper	User Session Note	0	Edit	Delete
Client Host	Token mapper	User Session Note	0	Edit	Delete
groups	Token mapper	Group Membership	0	Edit	Delete
maas_role	Token mapper	Hardcoded Role	20	Edit	Delete

Configuration KC

Création des mappers

[Clients](#) > [Total-backend](#) > [Mappers](#) > Create Protocol Mappers

Create Protocol Mapper

Protocol ?	<input type="text" value="openid-connect"/>
Name ?	<input type="text" value="groups"/>
Mapper Type ?	<input type="text" value="Group Membership"/> ▼
Token Claim Name ?	<input type="text" value="membership"/>
Full group path ?	<input checked="" type="checkbox"/> ON <input type="checkbox"/>
Add to ID token ?	<input type="checkbox"/> OFF
Add to access token ?	<input checked="" type="checkbox"/> ON <input type="checkbox"/>
Add to userinfo ?	<input type="checkbox"/> OFF
	<input type="button" value="Save"/> <input type="button" value="Cancel"/>

Configuration KC

Création des mappers

[Clients](#) > [simulation-maas-backend](#) > [Mappers](#) > Create Protocol Mappers

Create Protocol Mapper

Protocol ?	<input type="text" value="openid-connect"/>
Name ?	<input type="text" value="vault_name"/>
Mapper Type ?	<input type="text" value="Hardcoded claim"/>
Token Claim Name ?	<input type="text" value="vault_name"/>
Claim value ?	<input type="text" value="simulation-maas-backend"/>
Claim JSON Type ?	<input type="text" value="Select One..."/>
Add to ID token ?	<input type="checkbox"/> OFF
Add to access token ?	<input checked="" type="checkbox"/> ON
Add to userinfo ?	<input type="checkbox"/> OFF
includeInAccessTokenResponse.label ?	<input type="checkbox"/> OFF
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

Configuration KC

Création des mappers

Clients > simulation-maas-backend > Mappers > Create Protocol Mappers

Create Protocol Mapper

Protocol ?

openid-connect

Name ?

vault_role

Mapper Type ?

Hardcoded Role

▼

Role ?

simulation-maas-backend.service_vault

Select Role

Save

Cancel

Configuration KC

Ajout des financeurs dans le service account user du client

Mcm

Master

Add realm

Clients

Client Scopes

Roles

Identity Providers

User Federation

Authentication

Manage

Groups

Users

Sessions

Events

Import

Export

Clients > Total-backend

Total-backend

Settings

Credentials

Keys

Roles

Client Scopes

Mappers

Scope

Revocation

Sessions

Offline Access

Clustering

Installation

Service Account Roles

Service Account

Service Account User

service-account-total-backend

Service Account Roles

Realm Roles

Available Roles

citoyens

citoyens_fc

content_editor

financeurs

gestionnaires

Add selected

Assigned Roles

default-roles-mcm

Remove selected

Effective Roles

default-roles-mcm

offline_access

uma_authorization

Client Roles

Select a client...

Configuration KC

Ajout des financeurs dans le service account user du client

Mcm

Configure

Realm Settings

Clients

Client Scopes

Roles

Identity Providers

User Federation

Authentication

Manage

Groups

Users

Sessions

Events

Import

Export

Users > service-account-total-backend

Service-account-total-backend

Details

Attributes

Credentials

Role Mappings

Groups

Consents

Sessions

Identity Provider Links

Group Membership

Search...

Q

View all groups

Leave

/collectivités/Mulhouse

Available Groups

Search...

Q

View all groups

Join

admins

citoyens

collectivités

- Muldeouse
- Mulhouse**
- simulation-maas

entreprises

- Capgemini
- SIRH
- Test 1
- Test 2

financeurs

- gestionnaires
- superviseurs
- simulation-maas

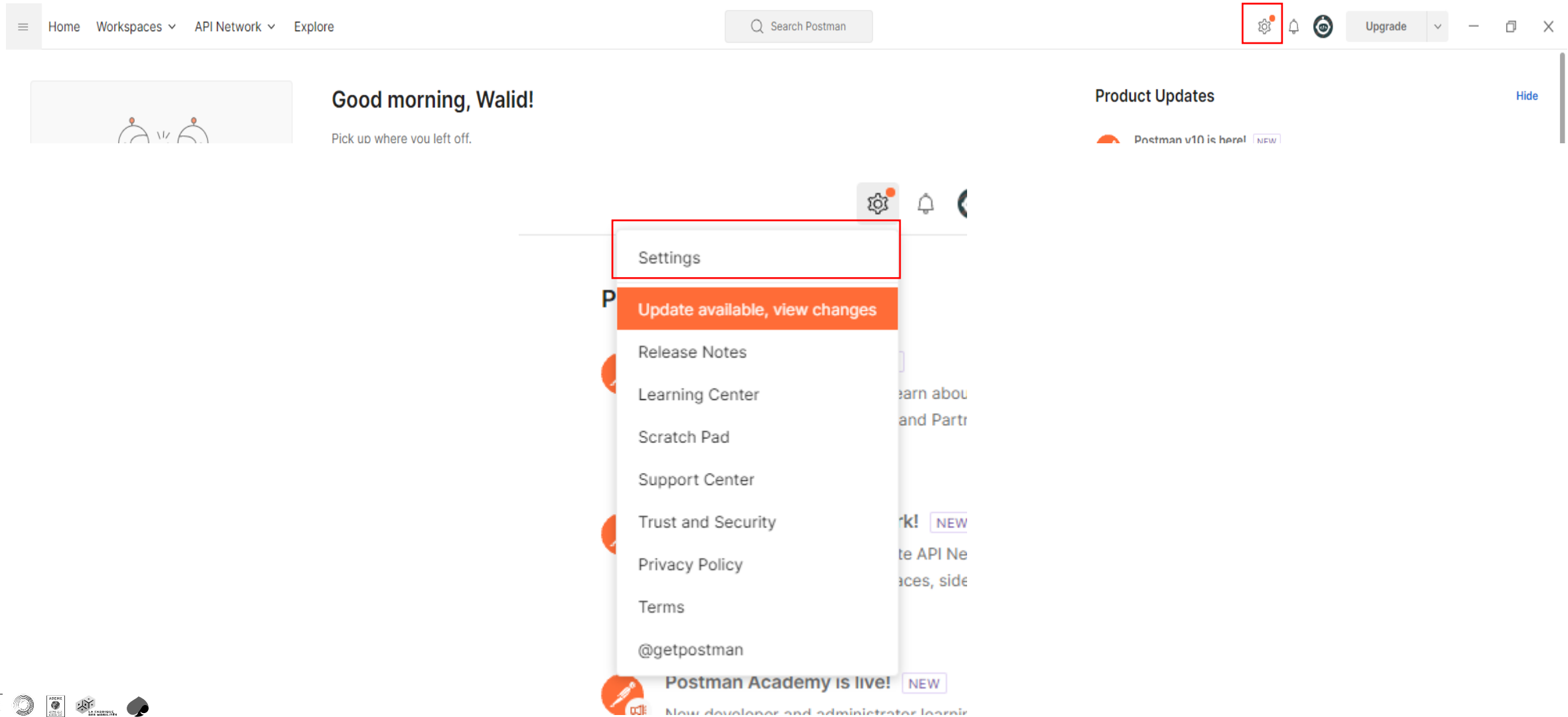
Configuration Postman

Ajouter les certificats du vault dans la
config Postman pour pouvoir appeler
l'API du Vault



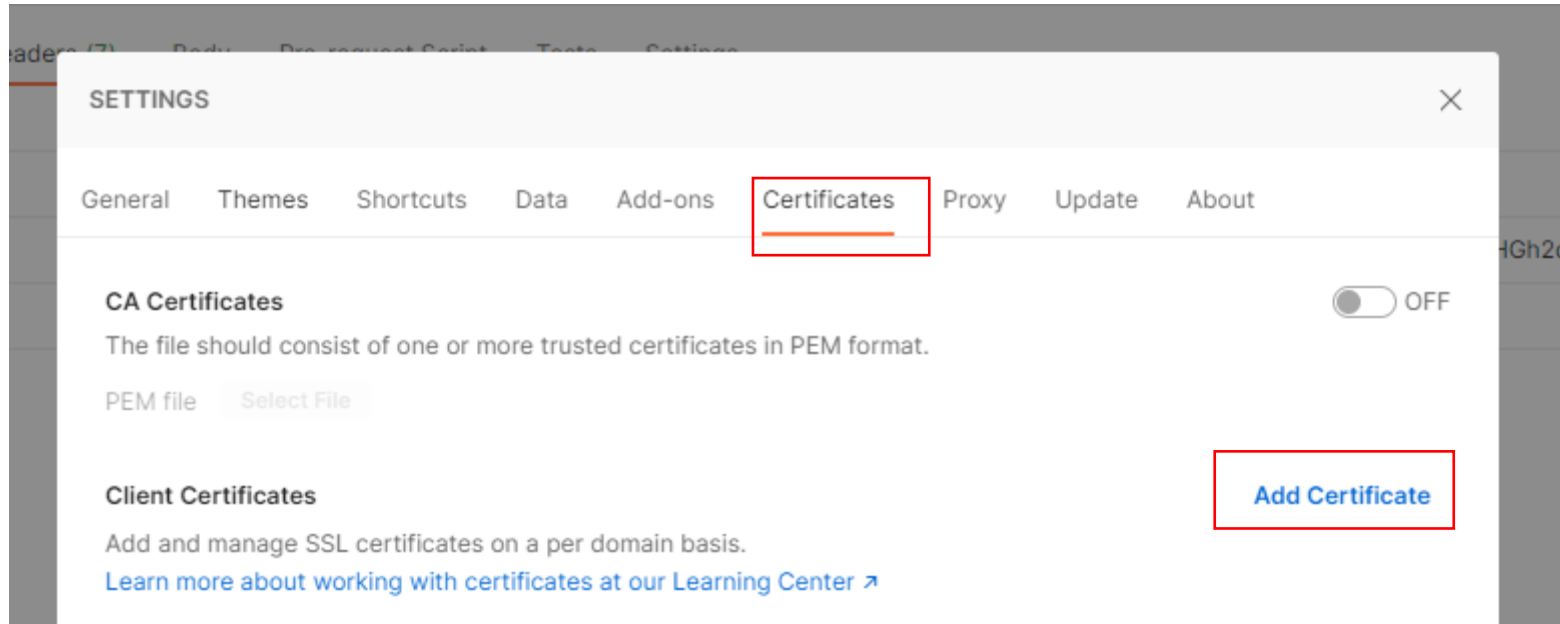
Configuration Postman

Ajouter les certificats dans la config Postman



Configuration Postman

Ajouter les certificats dans la config Postman



Configuration Postman

Ajouter les certificats dans la config Postman

SETTINGS

General

Themes

Shortcuts

Data

Add-ons

Certificates

Proxy

Update

About

Client Certificates › Add Certificate

Host

https:// vault-master.preview.moncomptemobilite.l : 443

CRT file

Select File

KEY file

Select File

PFX file

Select File

Passphrase

pass

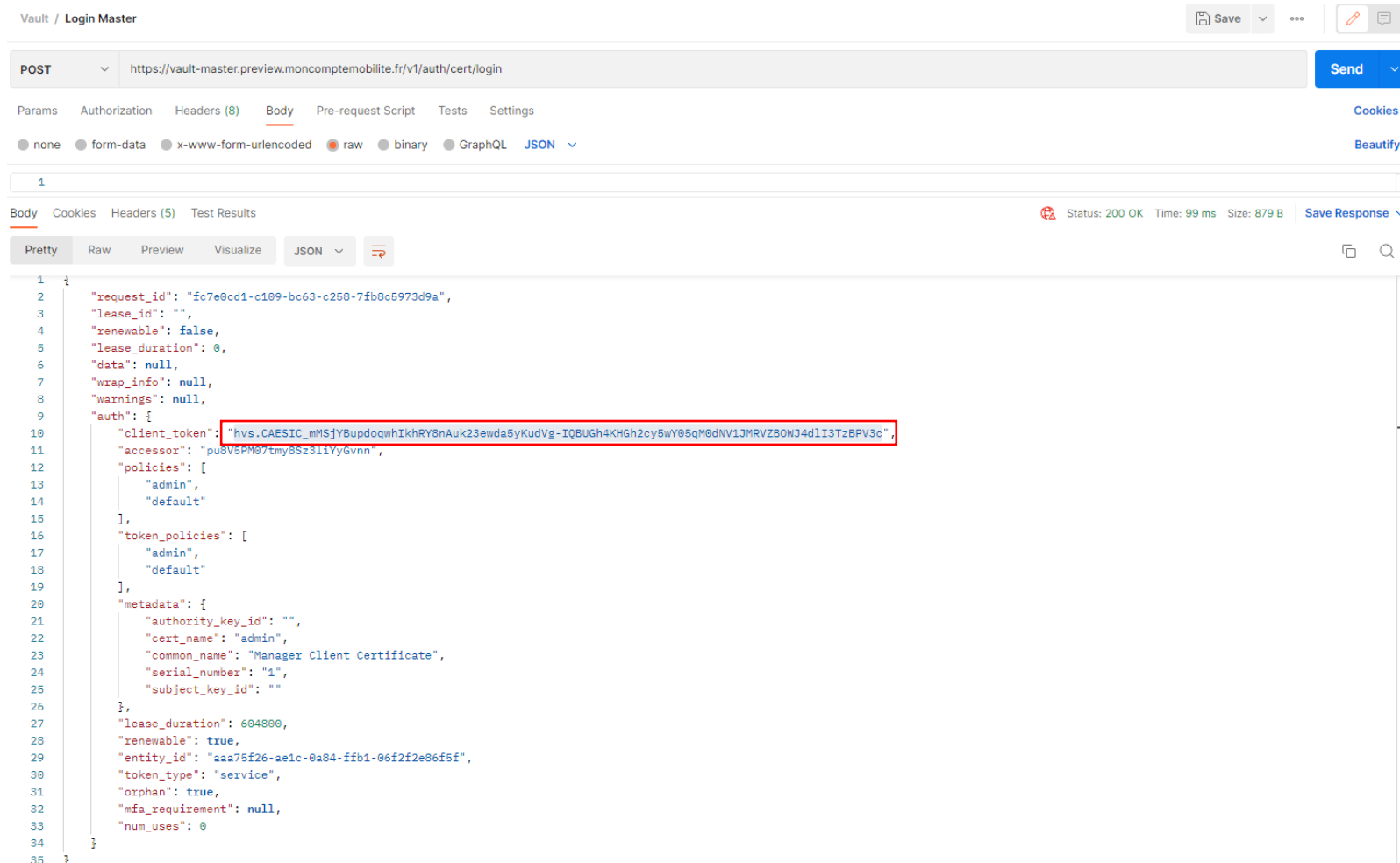
Add

Cancel

[Learn more about working with certificates at our Learning Center.](#)

Configuration Postman

Appeler l'endpoint /v1/auth/cert/login et récupérer le client_token



Vault / Login Master

POST https://vault-master.preview.moncomptemobilite.fr/v1/auth/cert/login

Params Authorization Headers (8) Body Pre-request Script Tests Settings

none form-data x-www-form-urlencoded raw binary GraphQL JSON

1

Body Cookies Headers (5) Test Results

Status: 200 OK Time: 99 ms Size: 879 B Save Response

Pretty Raw Preview Visualize JSON

```
1 {
2   "request_id": "fc7e0cd1-c109-bc63-c250-7fb8c5973d9a",
3   "lease_id": "",
4   "renewable": false,
5   "lease_duration": 0,
6   "data": null,
7   "wrap_info": null,
8   "warnings": null,
9   "auth": {
10    "client_token": "hvs.CAESIC_mMSjYBupdoqwhIkhRY8nAuk23ewda5yKudVg-IQBUGh4KHGh2cy5wY05qM0dNV1JMRVZBOWJ34d1I3Tz8PV3c",
11    "accessor": "pu8V5PM07tmy8Sz3liYyGvnn",
12    "policies": [
13      "admin",
14      "default"
15    ],
16    "token_policies": [
17      "admin",
18      "default"
19    ],
20    "metadata": {
21      "authority_key_id": "",
22      "cert_name": "admin",
23      "common_name": "Manager Client Certificate",
24      "serial_number": "1",
25      "subject_key_id": ""
26    },
27    "lease_duration": 604800,
28    "renewable": true,
29    "entity_id": "aaa75f26-ae1c-0a84-ffb1-06f2f2e06f5f",
30    "token_type": "service",
31    "orphan": true,
32    "mfa_requirement": null,
33    "num_uses": 0
34  }
35 }
```

Configuration Postman

Appeler l'endpoint `/v1/transit/keys/simulation-maas-backend` avec le `client_token` récupéré précédemment et récupérer la clé publique

Vault / Public RSA Key Master

GET `https://vault-master.preview.moncomptemobilite.fr/v1/transit/keys/simulation-maas-backend` Send

Params Authorization Headers (7) Body Pre-request Script Tests Settings Cookies

Headers 6 hidden

KEY	VALUE	DESCRIPTION
<input checked="" type="checkbox"/> X-Vault-Token	<code>hvs.CAESIC_mMSjYBupdoqwhkhRY8nAuk23ewda5yKudVg-IQBUGh4KHGh2cy...</code>	

Body Cookies Headers (5) Test Results Status: 200 OK Time: 20 ms Size: 1.28 KB Save Response

Pretty Raw Preview Visualize JSON Copy Search

```
0  data: {
1    "allow_plaintext_backup": false,
2    "auto_rotate_period": 0,
3    "deletion_allowed": false,
4    "derived": false,
5    "exportable": true,
6    "imported_key": false,
7    "keys": {
8      "1": {
9        "creation_time": "2022-11-10T17:07:37.883928085Z",
10       "name": "rsa-2048"
11       "public_key": "-----BEGIN PUBLIC KEY-----\nMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAd6Ha21RZP8S54vLfTDH\n/AvswrsZ9dct9lG1kTAHZj0vUXhN2zwz2GqYDX13hhdBPJNRDHVSUNERPD\nMxnm5+DErfQdQxdQqEIFh2tx05jrxuZeJtWlPV117Ab26dk8G6w3Gta8+mV\nUYGcx\nnuNh3KmwWebh0p+VpzK9ypCAQUwvt13MXipKKjw3oDgy2A\n+w1sU3oAXMHJHg20w0JI\nn50jh5jBlQ7T6Z1aP3wj+5oNh12WZeGfVXDqP38EhL8p6b\nf8dLwmKtqARB09CLVAA\nn9QIDAQAB\nn-----END PUBLIC KEY-----\n"
12     }
13   },
14   "latest_version": 1,
15   "min_available_version": 0,
16   "min_decryption_version": 1,
17   "min_encryption_version": 0,
18   "name": "simulation-maas-backend",
19   "supports_decryption": true,
20   "supports_derivation": false,
21   "supports_encryption": true,
22   "supports_signing": true,
23   "type": "rsa-2048"
24 },
25 "wrap_info": null,
26 "warnings": null,
27 "auth": null
28 }
```


Configuration API

Stocker la clé publique du vault dans
la collection du financeur



Configuration API

Appeler l'endpoint API PUT /v1/funders/{funderId}/encryption_key pour stocker la clé publique pour le financeur sélectionné

PUT

/v1/funders/{funderId}/encryption_key

Enregistre les paramètres de clé de chiffrement

Parameters

Cancel

Reset

Name	Description
funderId <small>* required</small>	L'identifiant du financeur
string (path)	
<input type="text" value="f2536237-d597-4315-b4d1-256dae783324"/>	

Request body

application/json

```
{
  "id": "1",
  "version": 1,
  "publicKey": "-----BEGIN PUBLIC KEY-----
\nMIIIBIIBANBgkqhkiG9w0BAQEFAAQ8AMIIBBgKCAQEAzd6Ha21RZPB554vLfTDH\nnz/k8LnGnu1bVExfGZz9Ex1Umx6jp4q4UpvxUArqbKNdFwID90Wxgsb/66aL7wArz\n\nN87/AvswrsZ9dct91G1kTAHZj0vUXhN2zwz2GqYDX13hhdBPJNRDHHVSUNERPD\nMx\nnm5+DE\nrfqDgQxdQqEIFh2tx05jrxuZeitW1PV117Ab25dk8G6w3Gta8+mV+UYYGcX\n\nnuNh3KmWebH0p+VpzK9ypCAQUwvt13MXipKKjW3oDgY2A+w1sU3oAXMHJHg\nz0w0JI\n\n50jh5jB1Q7T5Z1aP3wJ+5oNh12WZeGFVXDqP38EhL0p6bf0dLwmKtqAR\nB09CLVAA\n\n9QIDAQA8\n\n-----END PUBLIC KEY-----\n",
  "expirationDate": "2023-12-17T14:22:01Z",
  "lastUpdateDate": "2022-06-17T14:22:01Z",
  "privateKeyAccess": {
    "loginURL": "https://vault-master.preview.moncomptemobilite.fr/v1/auth/cert/login",
    "getKeyURL": "https://vault-master.preview.moncomptemobilite.fr/v1/transit/export/encryption-key/simulation-maas-backend/1"
  }
}
```

Execute

Clear