mon compte mobilité

KEY MANAGER & KEY ROTATION

Partage et rotation de la clé de chiffrement pour un Financeur utilisant son propre gestionnaire de clés

Capgemini

LA FABRIQUE DES MOBILITÉS

Version du document

Auteur(s)		Vérificateur(s)		Approbateur(s)	
Nom	Date/Visa	Nom	Date/Visa	Nom	Date/Visa
SADAOUI W. LEBREQUIER	27/07/2022 28/07/2022			GIFFARD A.	06/02/2023

Diffusion

Pour validation	Pour information

Historique

Version	Date	Auteur	Description
1.0	25/07/2022	Walid SADAOUI	Initialisation du document
1.1	27/07/2022	Walid SADAOUI	
1.2	06/02/2023	Arnaud Giffard	Relecture et validation de fin d'expérimentation

Sommaire

1. Introduction

La plateforme moB permet aux citoyens de faire des souscriptions à des aides proposées par des financeurs. Afin que les financeurs puissent traiter ces souscriptions, les citoyens peuvent joindre des justificatifs pour prouver leur éligibilité aux différentes aides proposées.

Pour respecter la règlementation RGPD, seuls les utilisateurs financeurs autorisés doivent être capables de consulter ces justificatifs, toute personne ou tout système extérieur ne doit pas avoir la possibilité d'accéder au contenu de ces documents pouvant être sensibles.

Pour répondre à cette problématique, la solution choisie a été de chiffrer tous les justificatifs fournis par les citoyens et de ne donner la possibilité de déchiffrer ces documents qu'aux personnes autorisées.

2. Fonctionnement de la rotation de clé

2 possibilités s'offrent au Financeur souhaiter intégrer moB et devant donc supporter le déchiffrement et chiffrement des justificatifs :

- ✓ Utiliser le Key Manager qui est fourni aux financeurs par moB. C'est une solution générique fournie par MOB. Elle contient des scripts et une tâche périodique qui permettent d'automatiser l'envoi de la première clé à moB et la rotation de cette clé tous les 6 mois. Le financeur est responsable de la mise en place des différents processus de sécurisation des accès au Key Manager, conformément à leurs politiques de sécurité internes.

- ✓ Utiliser leur propre solution pour stocker les clés de chiffrement, qui seront utilisées pour déchiffrer les justificatifs transmis par un citoyen lors de la souscription à une aide d'un financeur.

La mise en place du Key Manager et en particulier la transmission d'une première clé publique à moB est un prérequis pour autoriser un citoyen à souscrire à une aide proposée par un financeur.

2.1. Prérequis

- Avoir un client IDP (IDentity Provider) déclaré dans moB et être en possession de son **client_id**, de son **client_secret**
- Avoir un compte Entreprise financeur et son **funderId**. Le compte financeur doit déjà avoir été créé dans moB pour pouvoir interagir avec l'API moB.

3. Envoyer une clé publique à moB

3.1. Obtention du token d'authentification

URI et méthode
POST ${IDP_URL}/auth/realms/mcm/protocol/openid-connect/token

Client credentials
Il s'agit de s'authentifier en tant que client via un compte de service en fournissant dans le corps de la requête IDP :

+ **grant_type** : client_credentials
+ **client_id** : <identifiant de l'application client>

+ **client_secret** : <secret de l'application client>

Réponse

Récupérer le champ ***access_token*** pour l'utiliser en tant que jeton d'accès dans l'endpoint d'envoi de la clé publique à MOB ci-dessous.

3.2. Envoi de la clé publique à moB

URI et méthode

PUT ${API_URL}/v1/funders/${FUNDER_ID}/encryption_key

En-têtes

+ **Authorization Bearer** : <jeton d'accès>

Corps

Propriété	Type	Description
id	string	L'identifiant de la clé
version	number	Le consentement valide du citoyen au partage de données personnelles avec le financeur de l'aide
publicKey	string	Clé publique du financeur
expirationDate	Date	Date d'expiration de la clé
lastUpdateDate	Date	Date de dernière mise à jour de la clé
privateKeyAccess	Object(JSON)	Objet contenant les URLs permettant de récupérer la clé privée du financeur ✓ loginURL (string) : URL de connexion au Vault ✓ getKeyURL (string) : URL d'accès à la clé privée associée à la clé publique fournie dans le champ publicKey

Exemple


```
{
  "id": "1",
  "version": 1,
  "publicKey": "-----BEGIN PUBLIC KEY-----
\nMIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAytHQWS40nUZpO9emt6XW\nRiaoJfUpTN
8NftTLBrVnI876FMPM5YIptpBe6LyY/kvpmUPZLaRlJ3tOkdqj1eTR\n1VIyc03nWAh4Sbd/eWJU5g
qw89Jqaqyi72Xon3IdISTgjO/X5bIMAaohGH2WVDsW\nDDW7KAMMar9ExemlN9VgUoyYpwffxJSZVk
bf5egK5noHnPbyVPXvzPQPbG6xKKD2\nXR8y+YPNfpWSbUVSz7kXZq9DvGZdjRISze8U7734ddWHEi
USuSNg/i7TZdvN7P88\nUoVhY4/DYpjNEcupniRUXQOUyKKdUuCcyDa1M+8FbFWZazSk2MYvSNEXkU
Lj+rKV\n2xfUMnvH5yH4OAZAWG0Mp6JXfYXHsoEF7YfOhxJKo5wxMGv1rPvaRcPNeMfqacJX\n/7zy
1XX40Q18kwu/onKXS2BQxB5UuxYXUo5TA3YExUZIZPcoiwaiprBNcRoQFSss\n0SKI/G5bQX3IX0OU
N8vaUuJlnJf3g/vrY2VHm2hgAY9+JfdphdXw87Pn5SvQKqFg\nYffmMX3mxuf/nO5h9yADrgBrRfDd
xfjxjGifVNCymCStNVJNHhXJN/dCzz4IPkok\nU6UzMJkzJleQR6X8vyrw40P4EPEU2+fzJhYRMncU
4srw1fISclixd89tgda2PR0D\noOYOoDTWddvLzprlDyKqiIUCAwEAAQ==\n-----END PUBLIC
KEY-----",
  "expirationDate": "2022-12-17T14:22:01Z",
```

```
  "lastUpdateDate": "2022-06-17T14:22:01Z",
  "privateKeyAccess": {
    "loginURL": "https://keyvault/auth/cert/login",
    "getKeyURL": "https://keyvault/keyname"
  }
}
```

Règles de gestion

- ✓ Les champs **id**, **version**, **publicKey**, **expirationDate** et **lastUpdateDate** sont obligatoires.
- ✓ L'objet **privateKeyAccess** est obligatoire sauf pour les financeurs qui utilisent leur propre SIRH (et n'utilisent donc pas l'interface financeur MOB)

Réponse

La réponse succès (code HTTP 204) ne renvoie aucun contenu.