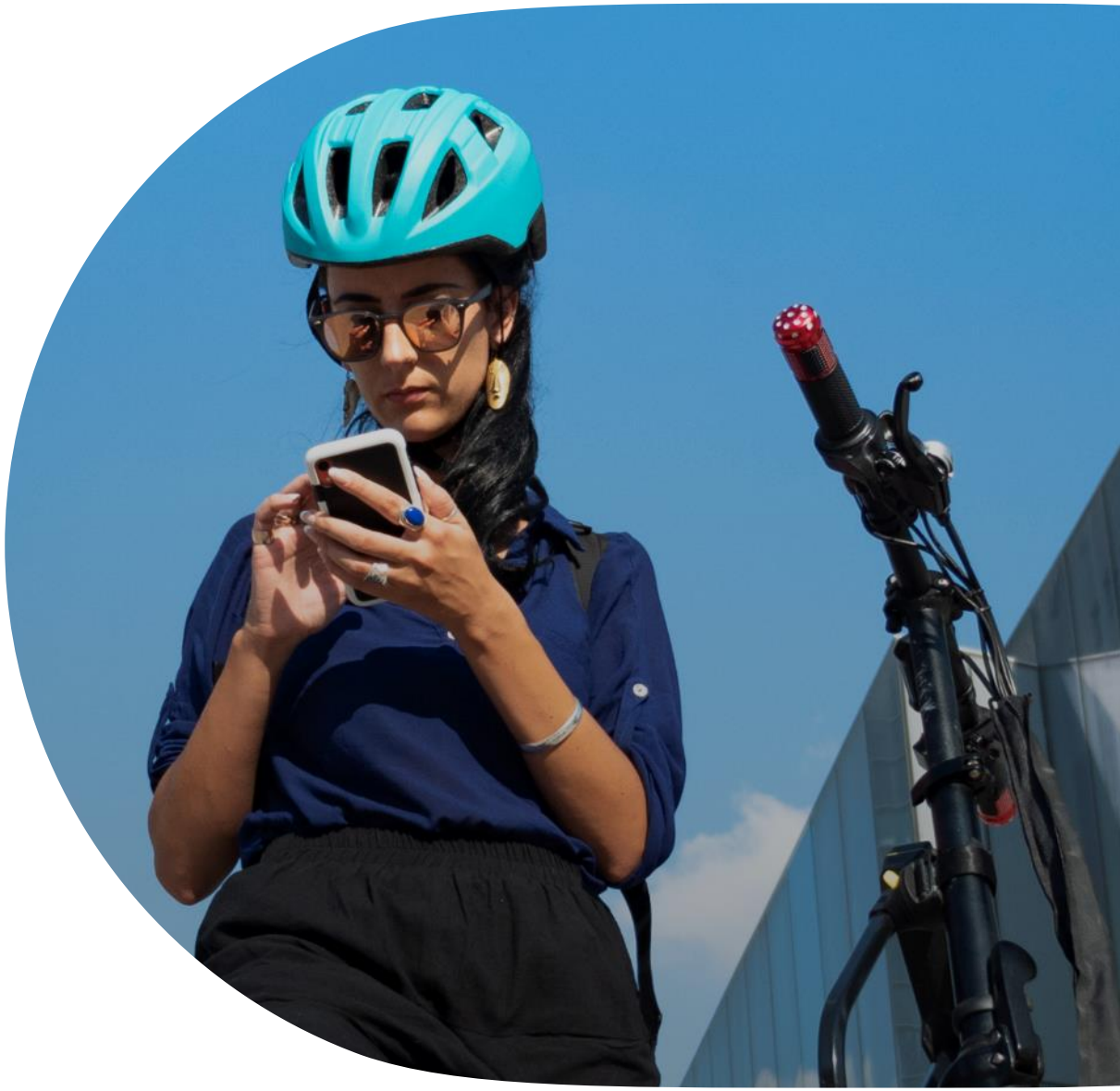
Mon Compte Mobilité

Chiffrement des dossiers de souscription à une aide | Solution proposée



Février 2022

Agenda

Contexte, principes et besoins identifiés

Détail des cinématiques associées

Spécifications techniques chiffrement

Enabler « Key Manager »

Capgemini Invent 2022 All rights reserved

CONTEXTE ET ENJEUX DE SÉCURITÉ

Motivations

- Le citoyen peut être amené à **déposer des pièces justificatives sensibles** (carte d'identité, passeport, …) que le financeur est susceptible de demander.
- La plateforme MCM sera opérée par Capgemini (CloudBox) : des opérateurs auront accès aux éléments déployés, voire aux données.
- En cas de compromission de la plateforme MCM, il **ne doit pas y avoir de moyens de lire de données sensibles**.
- Afin de **garantir la confidentialité** des données transmises par l'usager, **seul le financeur doit** être en mesure de **consulter les pièces justificatives**
- Les **métadonnées** de souscription (de la demande) **ne font pas partie du périmètre** de **chiffrement** car elles ne sont pas jugées sensibles.

La recommandation du RSSI *est d'effectuer un chiffrage de bout en bout sur le stockage et téléchargement des données personnelles*

Company Confidential © Capgemini 2021. All rights reserved |

CHAINE DE GESTION D'UN DOSSIER DE SOUSCRIPTION À UNE AIDE

1 **Le Financeur s'inscrit dans MOB** et met en place les **prérequis** pour le traitement des dossiers

2 **Le Citoyen est authentifié** à MOB et procède à une **Recherche d'aide**

3 Le Citoyen **trouve une aide et souscrit** à celle-ci dans **MOB** ou via un **MAAS** en soumettant les **PJs requises**

Chiffrement

4 **Le dossier** de souscription à l'aide **est transmis** au **Financeur**

Les dossiers contenant des données personnelles et des justificatifs, ces derniers **doivent être transmis chiffrés**

5 **Le Financeur qualifie le dossier** après avoir **déchiffrer les PJs** dont lui **seul** est **habilité** à le faire

Déchiffrement

Les justificatifs transmis par les Citoyens étant confidentiels, le **Financeur doit être le seul à pouvoir déchiffrer ces justificatifs**

Company Confidential © Capgemini 2021. All rights reserved |

PRINCIPES DE LA SOLUTION

Afin de garantir la confidentialité des données transmises par l'usager jusqu'au Financeur, nous nous appuyons sur un chiffrement hybride, symétrique puis asymétrique :

- Un couple clé privée/clé publique asymétrique serait **généré par le Financeur**. **Sans** la **clé privée**, il est **impossible de déchiffrer** l'objet chiffré avec la clé publique.
- La clé privée doit rester **strictement côté financeur**, la clé publique étant transmise à MOB, il est nécessaire de **garder la clé privée secrète et accessible à tous les gestionnaires/superviseurs qui ont besoin de déchiffrer les pièces justificatives**
- Lors du dépôt d'une demande par un citoyen, il s'agit de **chiffrer les justificatifs avec une clé symétrique aléatoire puis, chiffrer cette clé à l'aide de la clé publique** du financeur.

Ainsi :

- Seul le destinataire Financeur sera en mesure de déchiffrer.
- Impossible d'accéder aux justificatifs en clair depuis MOB.
- Les justificatifs seraient à l'abri de tentatives de social ingénierie, de malveillances internes, et d'éventuels intrus seraient également

Company Confidential © Capgemini 2021. All rights reserved |

LA SOLUTION DOIT RÉPONDRE À DES BESOINS IDENTIFIÉS

- Le Financeur doit pouvoir, quelque soit son accostage à MOB :
  - **Générer un couple** de clé privée / clé publique asymétrique
  - **Envoyer la clé publique à MOB, son identifiant ainsi que sa date d'expiration lors de son inscription, ceci périodiquement, à chaque renouvellement**
  - **Garder la clé privée secrète** mais **accessible** à tous ses utilisateurs gestionnaires/superviseurs
  - **Récupérer la clé privée** à l'aide de l'identifiant de la clé transmis par MOB pour déchiffrer la clé symétrique puis le dossier, qu'il soit connecté à l'interface MOB ou à son SI RH

- MOB doit pouvoir :
  - **Recevoir la clé publique du Financeur**
  - **Générer une clé symétrique aléatoirement** pour chaque dossier soumis
  - **Chiffrer les pièces jointes des dossiers** avec la clé symétrique
  - **Chiffrer la clé symétrique** à l'aide de la dernière clé publique transmise par le Financeur et la stocker chiffrée
  - **Transmettre le dossier et la clé symétrique chiffrée** de manière sécurisée au Financeur en spécifiant l'identifiant de la clé de chiffrement

Company Confidential © Capgemini 2021. All rights reserved |

DIFFICULTÉS

Principalement **l'accès et la gestion de la clé privée**

- Comment s'assurer que la clé reste côté Financeur, aussi bien dans le cas MOB standalone (sans SI Financeur accosté), que dans le cas d'une délégation à un outil RH du Financeur (SI accosté) ?

- Les financeurs sont susceptibles de mettre en place une organisation pour répartir la charge de gestion des demandes entre plusieurs collaborateurs. Par conséquent, plusieurs utilisateurs disposant de privilèges distincts pourront être déclarés pour un financeur. Comment s'assurer que chaque responsable ait accès à la clé privée de l'entreprise ?

Company Confidential © Capgemini 2021. All rights reserved |

LA SOLUTION DOIT ÊTRE VALIDE QUELQUE SOIT LE MODE D'ACCOSTAGE AVEC MOB CHOISI PAR LE FINANCEUR

- Financeur **sans SIRH accosté** à Mob
  - Les dossiers de souscriptions sont **traités** par les collaborateurs du Financeur **directement dans l'interface Front Office MOB**
- Financeur **avec SIRH accosté directement** à MOB
  - Les dossiers de souscriptions sont **traités** par les collaborateurs du Financeur **via l'interface Front Office de son SIRH**
  - Prérequis supplémentaire :
    - la ½ interface de connexion à MOB doit être implémentée par le Financeur (connecteur)
- Financeur **avec SIRH accosté indirectement** via un prestataire à MOB – *Cas Neocase*
  - Les dossiers de souscriptions sont **traités** par les collaborateurs du Financeur **via l'interface Front Office prestataire du SIRH**
  - Prérequis supplémentaire :
    - la ½ interface de connexion à MOB doit être implémentée par le prestataire du SIRH (connecteur)

Prérequis global *: quelque soit le mode d'accostage, le financeur (collectivité ou entreprise) doit avoir une* ***solution interne dans son SI qui permet l'accès à la clé privée et la transmission de la clé publique à MOB***

Le recours à un agent web déployé au sein du SI Entreprise comme point d'accès est un cas courant que l'on peut retrouver notamment dans le cas d'intégration avec de grands éditeurs tels que SAP et Oracle par exemple.

Company Confidential © Capgemini 2021. All rights reserved |

Agenda

Contexte, principes et besoins identifiés

Détail des cinématiques associées

Spécifications techniques chiffrement

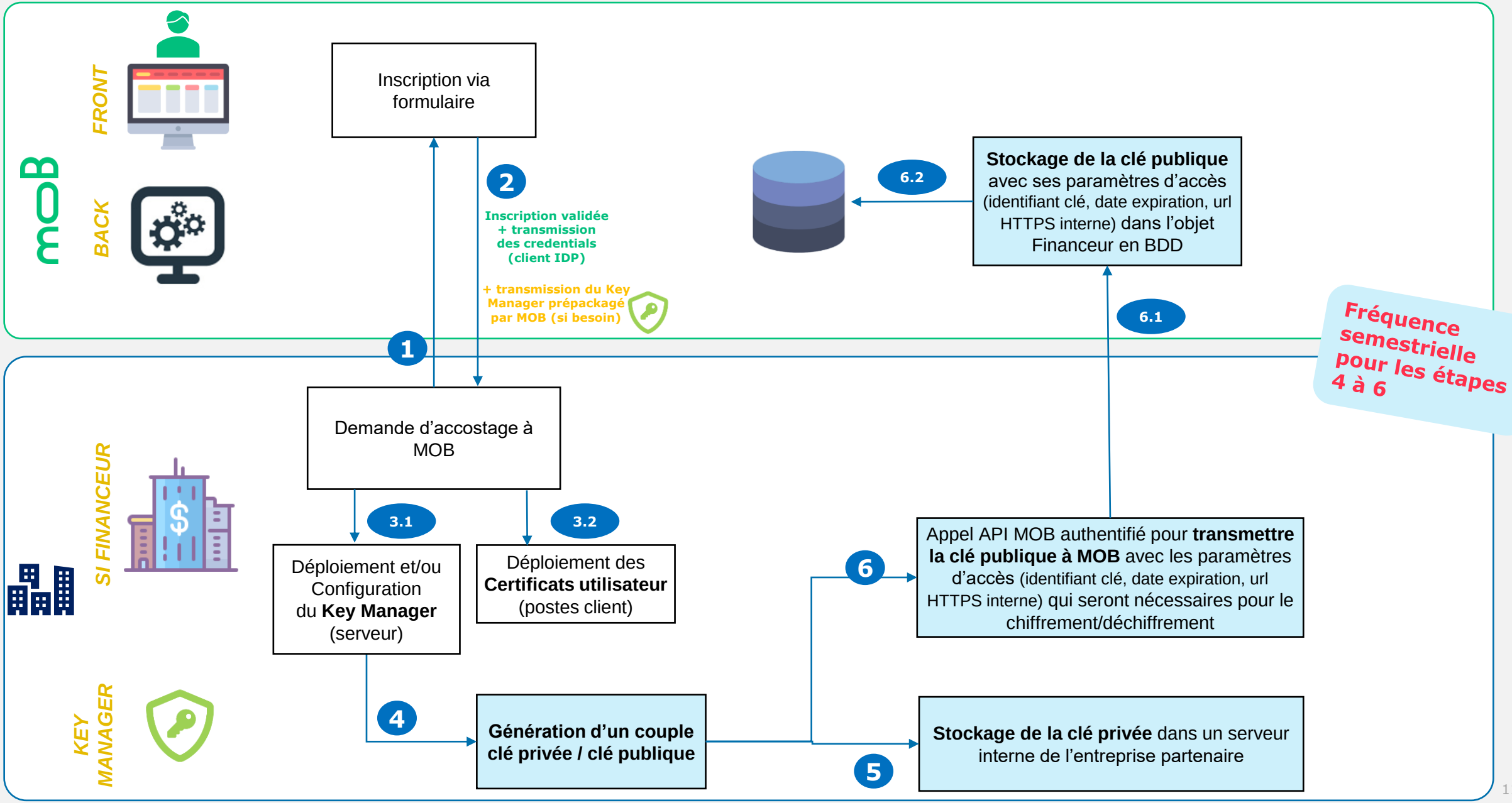
Enabler « Key Manager »

Capgemini Invent 2022 All rights reserved

LE CHIFFREMENT DE BOUT-EN-BOUT EN 3 PHASES

Company Confidential © Capgemini 2021. All rights reserved |

Phase 1 : Accostage et Inscription du Financeur (Setup)



Phase 1 : Accostage et Inscription du Financeur (Setup)

1. Le financeur fait une demande d'accostage à MOB. L'équipe MOB voit avec lui pour définir le mode d'accostage et l'accompagner sur les prérequis nécessaires au traitement des dossiers.
2. **L'administrateur MOB complète le formulaire d'inscription du financeur**
   - L'inscription est validée et confirme son inscription au financeur. Un client IDP confidentiel est créé pour ce financeur.
   - **Le projet MOB propose l'enabler** Key Manager **au financeur** qui va lui permettre de gérer les clés nécessaires au déchiffrement des dossiers.
3. Le Financeur déploie un Key Manager dans son SI et le configure (soit avec l'enabler MOB, soit avec une solution propre)
4. OU il configure un Key Manager existant répondant aux prérequis. Ce composant :
   - Génère le couple clé publique / clé privée
   - Stocke la clé privée (ou sur un autre serveur interne à l'entreprise)
   - Expose une API HTTPS (avec certificat) permettant d'accéder aux clés à partir d'un identifiant de clé. Cette API est accessible uniquement au sein du SI Financeur par les utilisateurs détenteurs d'un certificat client valide.
   - Appelle l'API MOB avec ses credentials IDP et transmet la clé publique, son identifiant, sa date d'expiration ainsi que l'adresse (URL HTTPS) interne permettant de récupérer la clé privée associée.

   Dans le cas où le financeur ne souhaite pas utiliser l'enabler fourni par Mob, il implémentera lui-même une solution ou utilisera une solution open source
5. MOB stocke la clé publique et ses paramètres d'accès dans l'objet financeur en BDD
6. Le service IT du financeur déploie des certificats clients à ses utilisateurs gestionnaires ayant le droit de déchiffrer les dossiers MOB des citoyens (*ainsi dans le Key Manager acceptera seulement les utilisateurs détenteurs d'un certificat émis par l'autorité de certification du certificat serveur*)

Company Confidential © Capgemini 2021. All rights reserved |

Phase 1 : Accostage et Inscription du Financeur (Setup)

Financeur avec SIRH accosté indirectement via un prestataire à MOB – Cas Neocase

Validé avec Neocase le 6/04

FRONT

BACK

Inscription via formulaire

2

Inscription validée + transmission des credentials API (client_id/client_secret)

6.2

Stockage de la clé publique avec son identifiant et sa date d'expiration dans l'objet Financeur en BDD

6.1

Fréquence semestrielle pour les étapes 4 à 6

1

Demande d'accostage à MOB

SI RH

3

Configuration du **Key Manager**

KEY MANAGER

Azure Key Vault

4

Génération d'un couple clé privée / clé publique asymétrique

6

Appel API MOB authentifié pour **transmettre à MOB la clé publique, son identifiant et sa date d'expiration** qui seront nécessaires pour le chiffrement/déchiffrement

5

Stockage de la clé privée

Phase 2 : Dépôt d'un dossier de souscription avec chiffrement des pièces justificatives (Chiffrement Hybride)

mob

Optionnel
(Financeur avec SIRH accosté à Mob)

Soumission d'un **dossier de souscription avec PJs**

1 — Chiffrement HTTPS (flux)

Réception du dossier

2 — Chiffrement HTTPS

Analyse Antivirus des PJs

3 — Chiffrement HTTPS

Chiffrement des PJs avec une **clé symétrique générée aléatoirement** pour chaque dossier soumis

4

Chiffrement de la clé symétrique avec la clé publique du financeur

4.1 — Chiffrement HTTPS

Chercher la **clé publique** à l'aide de l'identifiant **du financeur**

4.2 — Chiffrement HHTPS

Stockage des PJ chiffrés dans MinIO
Enregistrement du dossier en BDD avec la clé symétrique chiffrée et l'identifiant de la clé publique
(cryptage natif SGBD pour les données formulaire de souscriptions)

5

Changement d'état du dossier **A_TRAITER**

6

Notification de **nouveau dossier A_TRAITER**
(données formulaire + liens PJs chiffrés + id clé chiffrement + clé symétrique chiffrée)

Capgemini Invent 2020. All rights reserved |

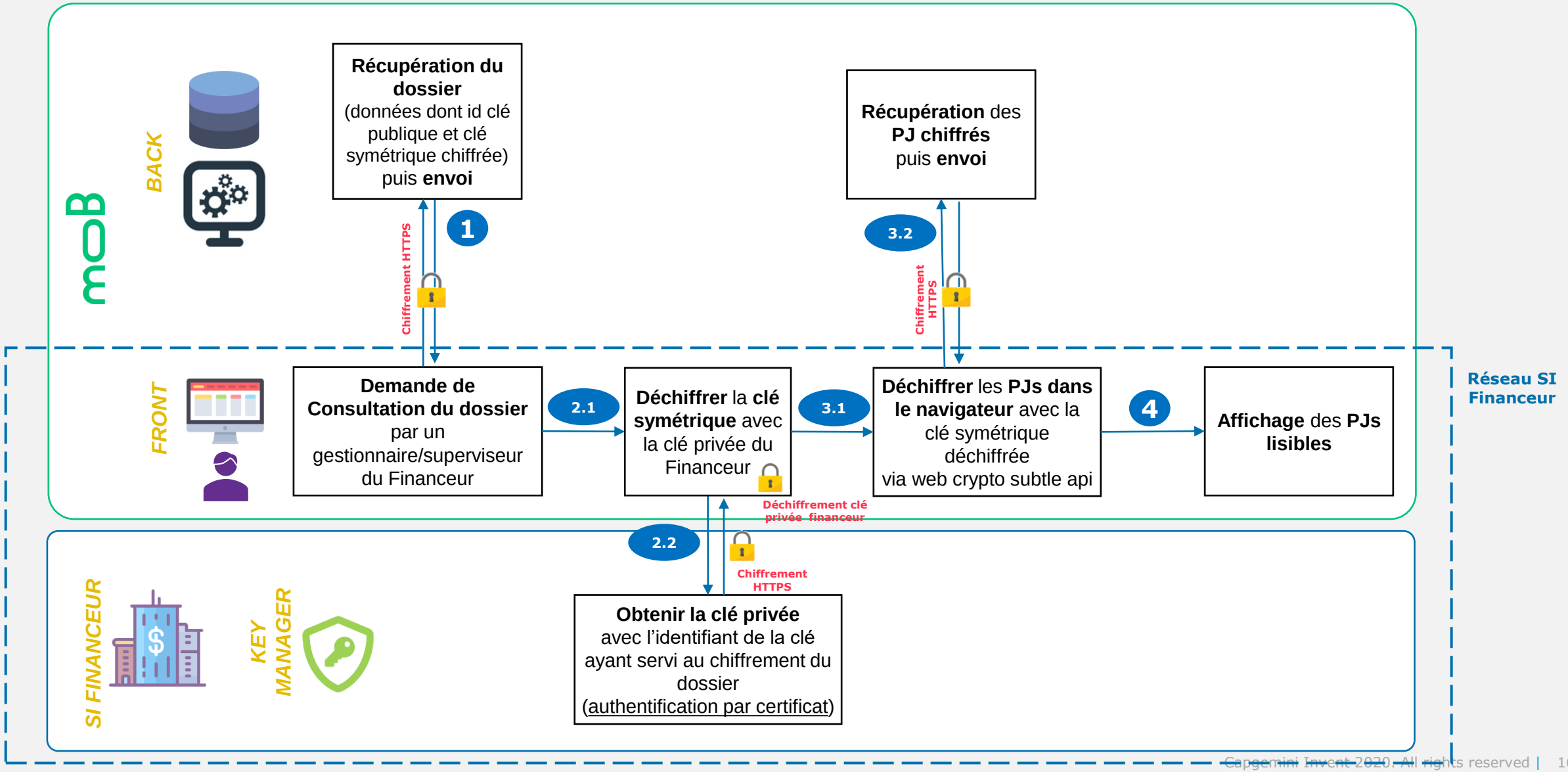
Phase 2 : Dépôt d'un dossier de souscription avec chiffrement des pièces justificatives (Chiffrement Hybride)

1. Le **citoyen soumet son dossier** depuis l'IHM du site web MOB (website → API).
2. Le backend **MOB réceptionne le dossier.** Une **analyse antivirus des pièces justificatives** est lancée avant stockage.
3. Si l'analyse est OK et le dossier recevable, une **clé symétrique est générée aléatoirement** pour le dossier soumis par le citoyen
4. Le backend **MOB chiffre les pièces justificatives** du dossier, **à l'aide de la clé symétrique générée**
5. le backend **MOB récupère la clé publique** du financeur dans la BDD, à l'aide de l'identifiant du financeur de l'aide souscrite.
6. Le backend **MOB chiffre la clé symétrique**, **à l'aide la clé publique** récupérée, puis, upload ces PJs chiffrés dans un bucket MinIO
7. Une fois les PJs chiffrés uploadés, **MOB enregistre le dossier** du citoyen **avec l'identifiant de la clé publique et la clé symétrique chiffrée** avec laquelle le chiffrement a été effectué.
8. MOB **envoie une confirmation** du dépôt de dossier au citoyen
9. Dans le cas des entreprises accostés à MOB, le backend MOB dépose un **message dans le bus de messages** pour notifier les entreprises de l'existence d'un nouveau dossier à traiter. Ce message comprend certaines métadonnées du dossier **dont la clé symétrique chiffrée nécessaire au déchiffrement** ainsi que les liens permettant d'accéder aux PJs chiffrés.

Company Confidential © Capgemini 2021. All rights reserved |

Phase 3 : Consultation d'un dossier de souscription avec déchiffrement des pièces justificatives

Financeur sans SIRH accosté à Mob



Capgemini Invent 2020. All rights reserved |

Phase 3 : Consultation d'un dossier de souscription avec déchiffrement des pièces justificatives

1. **Dans l'interface Financeur MOB**, le gestionnaire/superviseur du financeur à partir du navigateur de son poste de travail **demande à consulter un dossier** de souscription à une aide.

2. A partir du numéro de souscription, **MOB récupère** les données du **dossier**, **l'identifiant de la clé** de chiffrement, la **clé symétrique chiffrée** et la **liste des pièces justificatives chiffrés** (liens HTTPS).

3. La dossier est affiché. Le gestionnaire/superviseur souhaite alors **consulter une pièce justificative du dossier**.

4. Le navigateur demande la clé privée en invoquant l'API exposée par le Key Manager, avec en paramètre l'identifiant de la clé de chiffrement associé au dossier et sa version. L'authentification est validée grâce au certificat utilisateur présent sur le poste du gestionnaire/superviseur.
5. Le navigateur déchiffre la clé symétrique utilisée pour chiffrer le dossier.

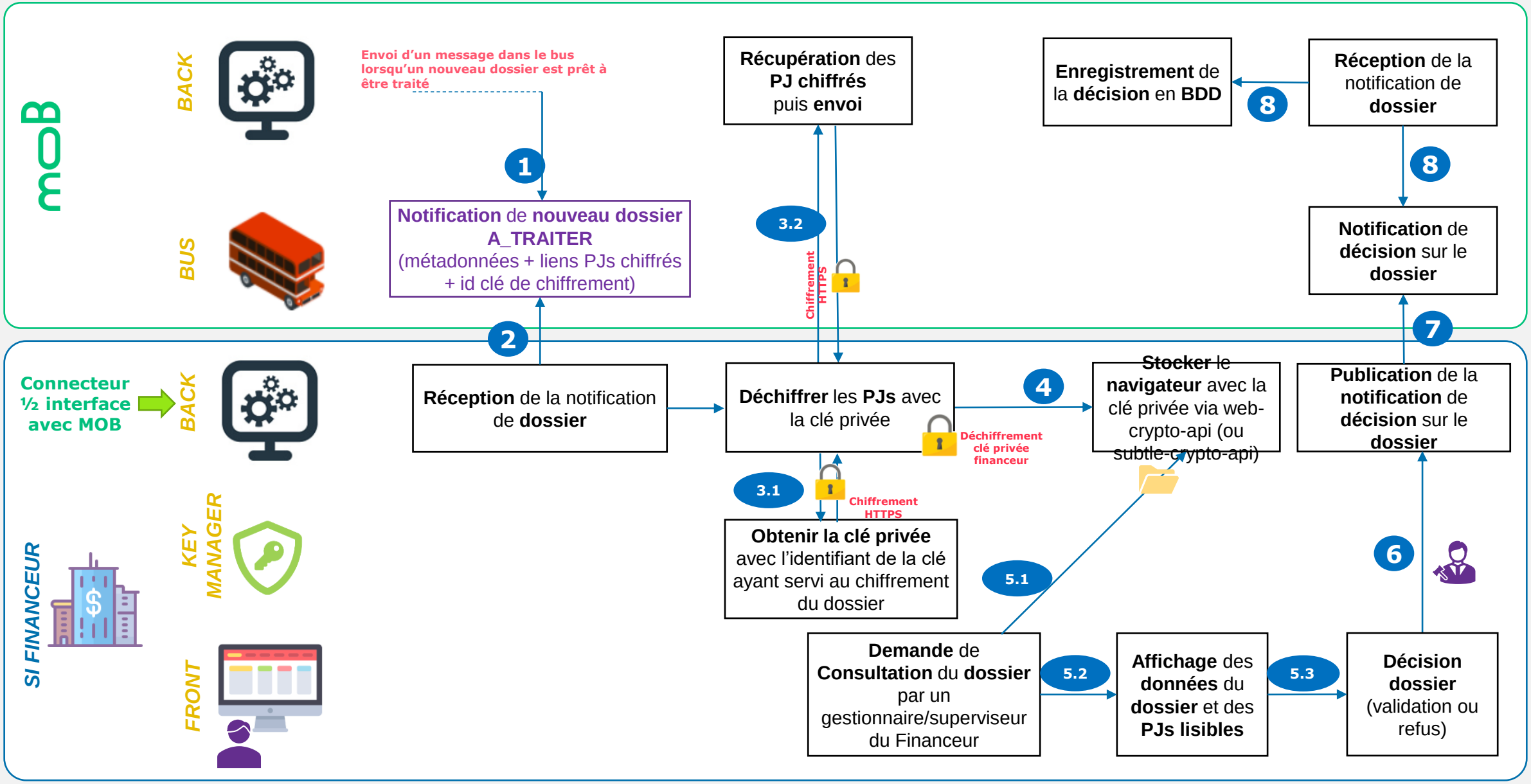
6. Le navigateur télécharge la pièce justificative chiffrée via API. L'authentification auprès de l'API MOB est réalisé via le jeton du gestionnaire/superviseur.

7. Le navigateur (via un code javascript) va alors réaliser le déchiffrement de la pièce justificative avec la clé symétrique déchiffrée. Il affiche alors le document dans le navigateur (PDF) ou le télécharge (autres formats).

Company Confidential © Capgemini 2021. All rights reserved |

Phase 3 SIRH : Consultation d'un dossier de souscription avec déchiffrement des pièces justificatives

Financeur avec SIRH accosté directement à MOB



Phase 3 SIRH : Consultation d'un dossier de souscription avec déchiffrement des pièces justificatives (Cas chiffrement Hybride)

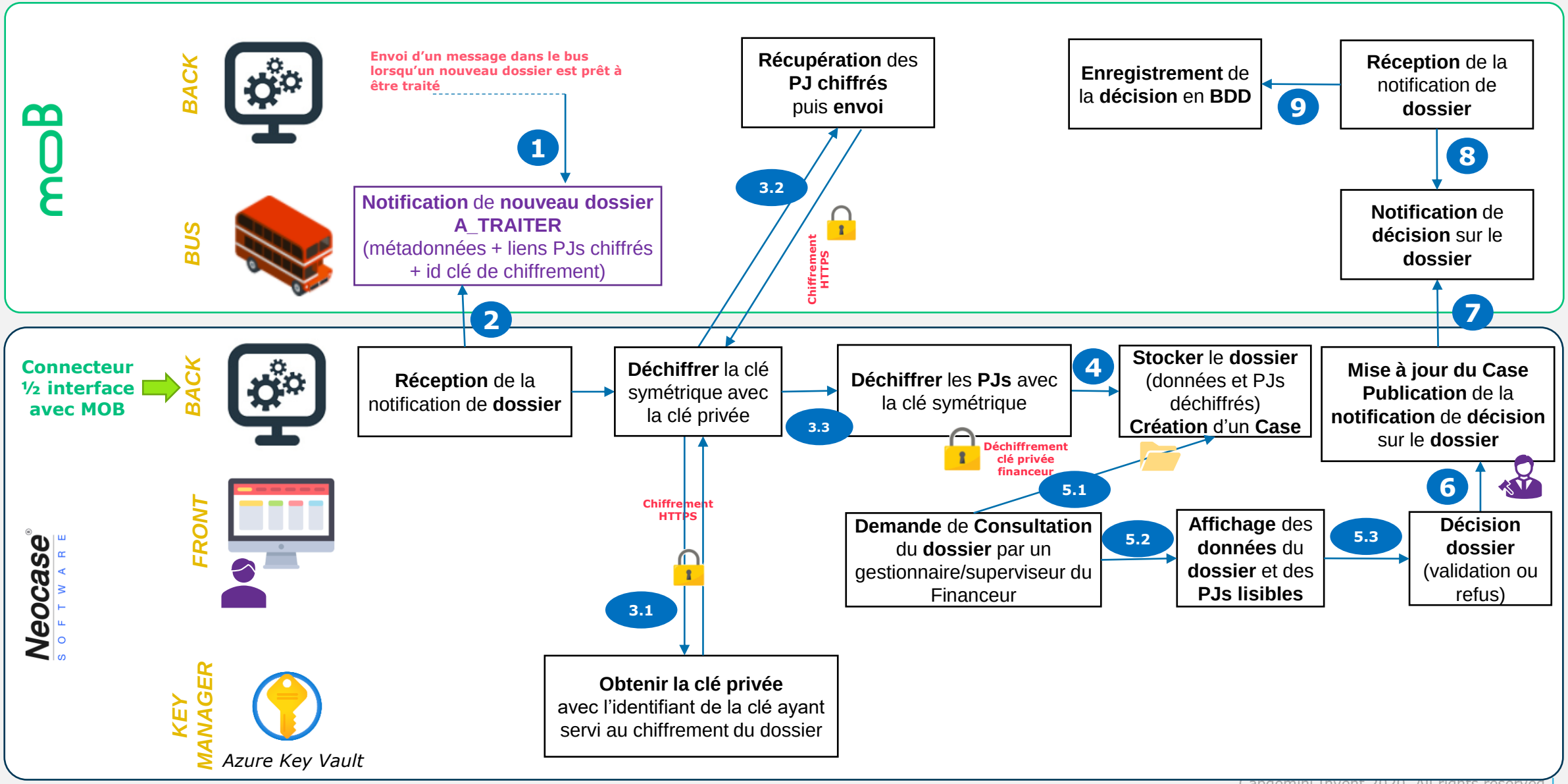
1. Le backend **MOB publie** dans le bus une **notification de dossier**.
2. Le **connecteur** MOB du SIRH Financeur (1/2 interface) **réceptionne** cette **notification** comprenant les métadonnées du **dossier**.
3. Afin de déchiffrer les justificatifs attachés au dossier, le connecteur :
    1. **Récupère** la **clé privée** en invoquant l'API exposée par le **Key Manager**, avec en paramètre l'identifiant de la clé de chiffrement associé au dossier. L'authentification est validée avec des credentials.
    2. **Télécharge** les **pièces justificatives chiffrées** via API. L'authentification auprès de l'API MOB est réalisé via les credentials client du SI RH.
    3. **Déchiffre la clé symétrique chiffrée par Mob**, avec la clé privée obtenue en amont
    4. **Déchiffre** les **pièces justificatives** avec la clé symétrique déchiffrée.
4. Le **connecteur stocke** les détails du **dossier** et les **pièces justificatives dans** le **SIRH**.
5. **Dans l'interface du SIRH**, le gestionnaire/superviseur du financeur à partir du navigateur de son poste de travail **demande à consulter un dossier** de souscription à une aide.
6. Le **dossier** est **affiché**. Les **pièces justificatives** sont **disponibles déchiffrés**.
7. Le gestionnaire/superviseur rend sa décision. Elle est enregistrée dans le SIRH.
8. Le **connecteur** MOB **publie** une **notification de décision dans le bus de messages MOB**.
9. **MOB réceptionne** la **notification** et **enregistre** la **décision** dans le système. Le souscripteur est notifié par mail.

Company Confidential © Capgemini 2021. All rights reserved |

Phase 3 SIRH : Consultation d'un dossier de souscription avec déchiffrement des pièces justificatives

Financeur avec SIRH accosté indirectement via un prestataire à MOB – Cas Neocase

Validé avec Neocase le 6/04



Capgemini Invent 2020. All rights reserved

Agenda

Contexte, principes et besoins identifiés

Détail des cinématiques associées

Spécifications techniques chiffrement

Enabler « Key Manager »

Capgemini Invent 2022 All rights reserved

Exigences techniques

- Principes
  - La **clé symétrique est créée aléatoirement par MOB** pour **chaque demande** soumise par le citoyen
  - La **clé publique** est envoyée à MOB **2 semaines avant l'expiration de la clé en vigueur**

- Fréquence d'expiration de la paire de clés : la paire de clé publique/clé privée est renouvelée de manière semestrielle.

- Paramètres de chiffrement :
  - Utilisation de la librairie **node crypto** intégrée à Node.js
  - Utilisation d'une **clé de chiffrement symétrique** de type **AES-256-CBC**
  - Utilisation d'une **clé RSA** de **2048 bits** au format **pkcs8** et d'un hash **SHA-256**
  - Utilisation d'un **padding RSA_PKCS1_OAEP_PADDING** de **42 bytes**

Capgemini Invent 2020. All rights reserved |

Mise en œuvre technique retenue

- Le **chiffrement asymétrique ne permet pas le chiffrement des fichiers volumineux** (plus d'infos ici).

Ainsi :

- Pour pouvoir chiffrer un fichier, il est possible d'utiliser un **chiffrement hybride**, en cryptant d'abord le fichier avec une **clé symétrique** (générée aléatoirement), puis, **chiffrer cette clé symétrique avec la clé publique**.
- La clé symétrique chiffrée peut être stockée, et également renvoyée au partenaire en même temps que les PJs
- Pour pouvoir déchiffrer le fichier, **la clé symétrique est d'abord déchiffrée à l'aide de la clé privée**, puis, on **déchiffre le fichier** à l'aide de cette clé.

Exemple:	**Time Taken to execute**
Chiffrement hybride côté api avec 3 PJs: 1 image de 473Ko, 1 image de 1,70Mo et 1 pdf de 5Mb :	0.196 seconds
Déchiffrement côté Website	Image de 470ko = 0.121 seconds Image de 1,70Mo = 0.329 seconds Pdf de 5Mb = 0.447 seconds
Chiffrement hybride côté api d'une PJ (PDF) de 12 Mb :	0.262 seconds
Déchiffrement du PDF de 12Mb côté Website :	0.827 seconds

Le endpoint **GET /v1/subscriptions/{subscriptionId}/attachments/{filename}** renvoie un buffer UTF8 en Unicode, ce qui rajoute un 0 à chaque caractère.
Cela n'est pas optimal : c'est inutile, cela ajoute de la complexité et surtout cela double le trafic réseau inutilement .

Capgemini Invent 2020. All rights reserved |

Agenda

Contexte, principes et besoins identifiés

Détail des cinématiques associées

Spécifications techniques chiffrement

Enabler « Key Manager »

Capgemini Invent 2022 All rights reserved

ENABLER « Key Manager » – Spécifications générales

Fonctions

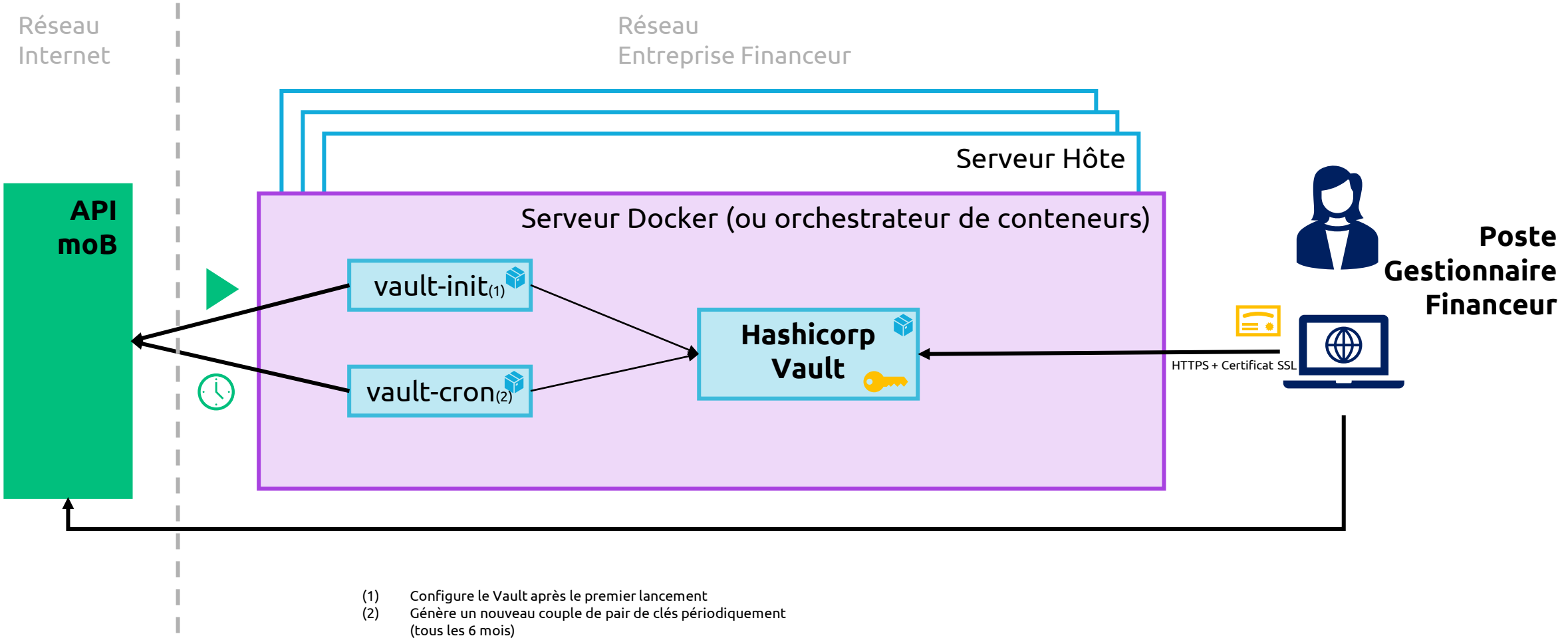
- Agent de gestion de clés interne à l'entreprise (Key Manager), à déployer dans le SI Financeur, qui a pour but de :
  - **Générer le couple** clé privée / clé publique asymétrique
  - **Transmettre la clé publique, son identifiant** (ex. : *keyA*) **et sa date d'expiration en invoquant l'API MOB avec des credentials (client OIDC confidentiel)**
  - **Mettre la clé privée à disposition** du navigateur du gestionnaire/superviseur connecté à MOB (sous réserve de réussite de l'authentification du certificat utilisateur client).
  - **Gérer le cycle de vie de la paire de clés**
    - Déclencher un nouvelle génération de clés périodiquement (tous les 6 mois)
    - A chaque fois que le couple de clés change, **transmettre la nouvelle clé publique à MOB** en spécifiant son identifiant (*keyB*, *keyC*, …), sa date d'expiration

Spécification technique

- **Service** qui s'exécute **sur le réseau interne du financeur** uniquement (non exposé à l'extérieur) et se compose de :
  - **Conteneur Hashicorp Vault OpenSource** (standard)
    - Stocke les clés et expose l'API Vault permettant de récupérer la clé privée + déchiffrer la clé symétrique
    - Certificat serveur émis par l'autorité de certification du Financeur
  - **Script CRON** déclenché selon une périodicité configurable (Chaque 6 mois)
    - Génère un couplé clé publique/privée asymétrique
    - Inscrit le couple dans le Vault
    - Envoie la nouvelle clé publique à MOB via appel API authentifié (client_id / client_secret)

Company Confidential © Capgemini 2021. All rights reserved |

ENABLER « Key Manager » – Schéma d'Architecture



(1) Configure le Vault après le premier lancement
(2) Génère un nouveau couple de pair de clés périodiquement (tous les 6 mois)

Company Confidential © Capgemini 2021. All rights reserved |

About Capgemini

Capgemini is a global leader in partnering with companies to transform and manage their business by harnessing the power of technology. The Group is guided everyday by its purpose of unleashing human energy through technology for an inclusive and sustainable future. It is a responsible and diverse organization of 270,000 team members in nearly 50 countries. With its strong 50 year heritage and deep industry expertise, Capgemini is trusted by its clients to address the entire breadth of their business needs, from strategy and design to operations, fuelled by the fast evolving and innovative world of cloud, data, AI, connectivity, software, digital engineering and platforms. The Group reported in 2020 global revenues of €16 billion.

Get the Future You Want | www.capgemini.com

This presentation contains information that may be privileged or confidential and is the property of the Capgemini Group.

Copyright © 2021 Capgemini. All rights reserved.