Backlog Parapheur - Fonctionnalité #23991

Utilisation d'une clé privée de type AES-256-CTR

24/02/2023 15:48 - Alex ORLUC

Statut:	R&D - Terminé	**Début:**	24/02/2023
Priorité:	0-Bloquant	**Echéance:**	
Assigné à:	Guillaume HEURTIER		
Catégorie:			
Version cible:	2301.0		
Tags Parapheur:			

Description

Utiliser une clé privé mp_secret.key au lieu d'une chaîne de caractère utilisé dans le vhost

Cette clé privée est utilisée pour chiffrer/déchiffrer :
- l'access token JWT
- le refresh token JWT
- le mot de passe du serveur de mail (configuration stockée en base)
- le mot de passe du certificat FAST (pour configuration FAST OTP, stockée en base)

le chemin de la clé sera a spécifier dans le config.json

2 cas possible :

Application issue d'une migration

mp_secret.key sera la chaîne de caractère qui était spécifié dans le vhost

Fresh install

mp_secret.key sera issue d'une génération :

openssl genrsa -aes256 -out mp_secret.key

Demandes liées:

Lié à Backlog Parapheur - Anomalie #23968: Clé privé => système cli / apache ...	**R&D - Terminé**	**23/02/2023**	
Lié à Backlog Courrier - Fonctionnalité #25796: Migration de la clé privée en...	**R&D - Terminé**	**04/07/2023**	**07/11/2023**

Historique

#1 - 24/02/2023 15:49 - Alex ORLUC

- Lié à Anomalie #23968: Clé privé => système cli / apache prb de mécanisme ajouté

#2 - 24/02/2023 15:50 - Emmanuel DILLARD

- Statut changé de A traiter à R&D - En cours

#3 - 24/02/2023 15:51 - Emmanuel DILLARD

- Assigné à Emmanuel DILLARD supprimé

#5 - 24/02/2023 17:19 - Guillaume HEURTIER

- Assigné à mis à Guillaume HEURTIER

#6 - 01/03/2023 14:04 - GIT LAB

[**CREATION**] MR sur **main** (**feat/23991/develop**) par Hamza HRAMCHI hamza.hramchi@xelians.fr

https://labs.maarch.org/maarch/MaarchParapheur/commit/67997ff268d3983d22cea011cdf83e7a80cee1ce

#7 - 03/03/2023 10:14 - Alex ORLUC

- Statut changé de R&D - En cours à R&D - En test

#8 - 03/03/2023 15:10 - Jean-Laurent DUZANT

- Statut changé de R&D - En test à R&D - Terminé

#9 - 09/03/2023 11:46 - Emmanuel DILLARD

- Version cible changé de Develop à 2301.0

#10 - 04/07/2023 12:17 - Emmanuel DILLARD

- Lié à Fonctionnalité #25796: Migration de la clé privée en fichier hors VHOST ajouté