Backlog RM - Anomalie #25236

[Authentication] OpenSSL 3.0 et génération de token

06/06/2023 15:12 - Jérôme BOUCHER

Statut:	R&D - En test	**Début:**	06/06/2023
Priorité:	2-Sérieux	**Echéance:**	
Assigné à:	Cyril VAZQUEZ		
Catégorie:			
Version cible:	3.0		
Tags RM:			

Description

Depuis la mise à jour d'openssl, la connexion à maarchRM est impossible (307 redirection vers la home.

Un bug apparaît lors de l'exécution de la fonction openssl_encrypt() dans encrypt() dans laabs.php. Une erreur est retournée (faire openssl_error_string() afin d'afficher l'erreur).
Une piste de fix éfinitive serait de revoir la taille des padding pour le calcul de $data

Quickfix:
Éditer la conf du fichier openssl.cnf (sous /etc/ssl/openssl.cnf)avec ces valeurs

[default_sect]
activate = 1
[legacy_sect]
activate=1

List of providers to load

[provider_sect]
default = default_sect
legacy = legacy_sect

Historique

#1 - 31/01/2024 11:56 - Cyril VAZQUEZ

- Statut changé de A qualifier à A traiter

- Version cible changé de 364 à 3.0

#2 - 11/03/2024 15:18 - Cyril VAZQUEZ

- Assigné à changé de Cyril VAZQUEZ à Jérôme BOUCHER

Modifier l'algorithme par défaut dans core
Vérifier celui proposé dans VHOST.default

Rédiger une procédure dans MIGRATION.md pour la regénération des jetons de comptes de service et autres valeurs liées aux utilisateurs.

#3 - 08/04/2024 16:06 - Jérôme BOUCHER

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

- Assigné à changé de Jérôme BOUCHER à Cyril VAZQUEZ

À tester sur feat/25236/openssl_3_compatibility