



**eHealth Pseudonymisation v1 REST
Directives et recommandations
v1.2**

Dit document wordt u kosteloos aangeboden door het

eHealth-platform

Willebroekkaai 38

1000 BRUSSEL

Table of content

Table of content	2
1. Gestion de la documentation	3
1.1 Historique.....	3
2. Introduction	4
3. Implementation des méthodes	5
4. Directives et recommandations pour les propriétaires des domaines	6
4.1 Rotation de la clé secrète partagée.....	6
4.2 Traitement de plusieurs données d'entrée	6
4.3 Mise en cache des pseudonymes en transit.....	6
4.4 Optimisation des access tokens et des pseudonymes en REST.....	6
5. Directives et recommandations pour les client-intégrateurs	7
5.1 Récupération des propriétés d'un domaine.....	7
5.2 Traitement de plusieurs données d'entrée	7
5.3 Caching des pseudonymes en transit.....	7

Ter attentie van de IT-experts die verantwoordelijk zijn voor het integreren van deze web service.



1. Gestion de la documentation

1.1 Historique

Version	Date	Author	Description
1.0	24/04/2024	Plate-forme eHealth	Initial version
1.1	17/06/2024	Plate-forme eHealth	Mise à jour de la section : <i>Mise en cache des pseudonymes en transit</i>
1.2	12/06/2024	Plate-forme eHealth	Mise à des recommandations pour l'utilisation de l'opération /domains/{domainKey}



2. Introduction

Le service de pseudonymisation REST doit être utilisée conformément aux directives et recommandations des propriétaires de domaine et des intégrateurs, afin d'assurer l'efficacité de nos services et d'aligner la demande des utilisateurs avec la capacité de notre infrastructure.

Nous vous demandons donc de respecter ces directives, telles qu'indiquées dans la section suivante, tant pour les environnements de test que de production.

En cas de violation de ces directives (qu'elle soit intentionnelle ou due à une erreur logicielle), le client IAM CONNECT permettant l'obtention d'un jeton d'accès pour consulter le service de pseudonymisation sera désactivé.

Dans ce document, les termes "DOIT", "NE DOIT PAS", "EXIGE", "DEVRAIT", "NE DEVRAIT PAS", "VA", "RECOMMANDÉ", "PEUT" et "OPTIONNEL" sont indiqués en majuscules et doivent être interprétés comme définis dans [RFC2119].



3. Implementation des méthodes

Toutes les implémentations des méthodes dans le service web doivent être réalisées conformément aux descriptions fournies dans les guides techniques disponibles sur le portail de la Plateforme eHealth.

Pour plus d'informations, veuillez consulter les liens suivants

- FR: <https://ehealth.fgov.be/ehealthplatform/fr/service-pseudonymisation-anonymisation>
- NL: <https://ehealth.fgov.be/ehealthplatform/fr/service-pseudonymisation-anonymisation>



4. Directives et recommandations pour les propriétaires des domaines

4.1 Rotation de la clé secrète partagée

Nous **RECOMMANDONS** aux propriétaires de domaine de consulter périodiquement – **toutes les 6 heures** – le the domain endpoint en utilisant la méthode **GET /domains/{domainKey}** pour les raisons suivantes :

- A midi:
Une nouvelle clé secrète partagée est générée et publiée sur les endpoints.
- A minuit:
La clé secrète actuellement active est supprimée.
La clé générée est activée.

Important : cette méthode ne doit pas être appelée plus de **4 fois par jour**.

4.2 Traitement de plusieurs données d'entrée

Lorsque vous devez effectuer des méthodes de pseudonymisation, d'identification ou de conversion impliquant plus de deux données d'entrée simultanément, nous **EXIGEONS** que vous utilisiez les méthodes multiples au lieu de répéter la même méthode pour chaque entrée.

A titre de rappel, voici les méthodes simples et multiples ::

Méthodes simples: **GET /pseudonimiseren, /identifieren, /converteren**

Méthodes multiples: **GET /pseudonimiserenMultiple, /identifierenMultiple, /converterenMultiple**

4.3 Mise en cache des pseudonymes en transit

Un pseudonyme en transit **DOIT** être mis en cache. La durée du caching est déterminée en fonction de la valeur du champ de date d'expiration (exp) dans l'entête sécurisé de l'information de transit (transitInfo). Le pseudonyme en transit mis en cache **DOIT** être utilisé avant l'expiration du délai. Pour des détails supplémentaires sur le transitInfo, veuillez consulter l'annexe TransitInfo dans le manuel technique.

4.4 Optimisation des access tokens et des pseudonymes en REST

Lorsqu'un appel est effectué pour récupérer le pseudonyme en transit via le endpoint userinfo, le pseudonyme calculé en REST et le access token utilisé doivent être mis en cache dans le backend.

Ces données mises en cache doivent être réutilisées tant que le access token est utilisé.



5. Directives et recommandations pour les client-intégrateurs

5.1 Récupération des propriétés d'un domaine

L'appel à **GET /domains/{domainKey}** peut être effectué une seule fois en phase de développement pour récupérer les propriétés statiques d'un domaine, comme la courbe elliptique et la taille du buffer, et les stocker statiquement, car elles ne changeront jamais durant la durée de vie du domaine.

5.2 Traitement de plusieurs données d'entrée

Lorsque vous devez effectuer des opérations de pseudonymisation, d'identification ou de conversion impliquant simultanément plus de deux données d'entrée, nous EXIGEONS que vous utilisiez les méthodes multiples plutôt que de répéter la même opération pour chaque entrée

A titre de rappel, voici les méthodes simples et multiples :

- Méthodes simples: **GET /pseudonimiseren, /identifieren, /converteren**
- Méthodes multiples: **GET /pseudonimiserenMultiple, /identifierenMultiple, /converterenMultiple**

5.3 Caching des pseudonymes en transit

Un pseudonyme en transit DOIT être mis en cache. La durée de cette mise en cache est déterminée par la valeur du champ de date d'expiration (exp) dans la transitInfo payload. Le pseudonyme en transit mis en cache DOIT être utilisé avant l'expiration de ce délai. Pour plus de détails sur transitInfo, veuillez consulter l'annexe TransitInfo dans la documentation technique :

- FR: <https://ehealth.fgov.be/ehealthplatform/fr/service-pseudonymisation-anonymisation>
- NL: <https://ehealth.fgov.be/ehealthplatform/fr/service-pseudonymisation-anonymisation>

