Communication eHealth: IAM Connect

26/02/2025

Le service IAM Connect va avoir une évolution technologique lors de la release R20251, ce qui va engendrer plusieurs impacts listés ci-dessous, il vous sera demandé de vous assurer de prendre les dispositions nécessaires en validant cela dans votre environement d'acceptance.

Veuillez aussi prendre en compte de la nouvelle version du cookbook : IAM Mobile Integration - Tech Specs, celle-ci sera disponible sur le portail ehealth et sera disponible pour la date 27/02/2025

A/uthorization Code Flow

La RFC 9207 (Identification de l'émetteur du serveur d'autorisation OAuth 2.0.
Voir https://www.rfc-editor.org/rfc/rfc9207.html) a été mise en œuvre comme une contre-mesure efficace contre les "mix-up attacks". Cela introduit un nouveau paramètre appelé **iss**. Ce paramètre est utilisé pour inclure explicitement l'identifiant de l'émetteur du serveur d'autorisation dans la réponse d'autorisation d'un flux d'autorisation OAuth.

Veuillez vérifier que votre librairie clientete peut gérer ce nouveau paramètre.

Refresh

À partir de cette nouvelle version, le paramètre **scope** dans OAuth2/OIDC Endpoint pour le token refresh est désormais pris en charge. En utilisant ce paramètre il est possible de faire une requête d'Access tokens avec un ensemble de scopes plus restreint que celui initialement accordé, mais vous ne pouvez pas augmenter le scope du token initial. Cette limitation de scope n'affecte pas le scope du refresh token renouvelé. Cette fonction fonctionne comme décrit dans la spécification OAuth2.

Logout

Modifications ayant un impact sur le logout:

- Le paramètre **id_token_hint** est recommandé, mais optionnel dans la spécification (https://openid.net/specs/openid-connect-rpinitiated-1_0.html#Security). L'implémentation a été modifiée, de sorte qu'aucune erreur n'est désormais déclenchée si **id_token_hint** est manquant, sauf si **post_logout_redirect_uri** est définie et que **client_id** est également manquant. A la place, une page de confirmation sera affichée.
- Le paramètre **redirect_uri** est obsolète**,** il n'est plus pris en charge. Les utilisateurs verront une page de confirmation s'ils n'utilisent pas les paramètres fournis dans la norme du logout.
- Lorsque le paramètre **post_logout_redirect_uri** est ajouté, le client doit également ajouter le paramètre **id_token_hint** ou **client_id.**

Token Exchange

Changements ayant un impact sur les flux d'échange de jetons :

- Lorsqu'un jeton est envoyé au endpoint userinfo, nous ne prenons plus en compte la dernière session client authentifiée active pour définir les scopes à mapper. Nous regardons désormais les scopes référencés dans le jeton qui est envoyé. Cela permet de

gérer ce qui est retourné par token exchange. Si vous utilisez l'endpoint userinfo, veuillez vérifier s'il fonctionne toujours comme prévu.
- Pour prendre en charge le changement de profil, le scope 'iam:exchange:profile:switch' doit être présent dans le scope du jeton original lors de l'authentification, si le client qui souhaite échanger le jeton veut changer de profil. Le scope lors de l'échange ne peut pas être plus large que le scope du jeton source (voir OIDC Refresh)

Javascript Client

Auparavant, nous hébergions un fichier source Javascript pour charger un adaptateur Javascript Keycloak dans un script Javascript. Étant donné qu'il est considéré comme une mauvaise pratique de charger des scripts externes, ce fichier a été supprimé. Les anciens adaptateurs Javascript Keycloak et autres scripts Javascript qui dépendaient de ce fichier pour les flux OIDC devront être mis à jour vers une version plus récente ou une autre implémentation.

SHA1

Le format de signature SHA1 n'est plus accepté. Veuillez-vous assurer que les signatures des messages n'utilisent pas SHA1. Dans le cas contraire, nous vous prions d'apporter les modifications nécessaires.

Account Service/Console

L'interface utilisateur du service Account a été modifiée, toutefois, les fonctionnalités restent identiques et continuent de fonctionner de la même manière.

Consent

Nouveau Look & Feel pour la page de consentement.

En cas de questions, n'hésitez pas à contacter le **CENTRE DE CONTACT** via le courriel ***support@ehealth.fgov.be*** ou au numéro **02/788 51 55** (chaque jour ouvrable de 7h à 20h)

Er is een technische evolutie van de dienst IAM Connect gepland bij de release R20251, wat een aantal gevolgen zal hebben, zoals hieronder toegelicht. Er wordt gevraagd ervoor te zorgen dat u de nodige maatregelen neemt door dit te valideren in uw acceptatieomgeving.

Gelieve ook rekening te houden met de nieuwe versie van het cookbook : IAM Mobile Integration – Tech Specs, dat tegen 27/02/2025 beschikbaar zal zijn op het eHealth-portaal.

Authorization Code Flow

De RFC 9207 (identificatie van de verzender van de autorisatieserver OAuth 2.0. - zie https://www.rfc-editor.org/rfc/rfc9207.html) werd geïmplementeerd als een doeltreffende maatregel tegen “mix-up attacks’. Hierdoor wordt een nieuwe parameter **iss** ingevoerd. Deze

parameter wordt gebruikt om expliciet de verzender van de autorisatieserver te identificeren in het autorisatie-antwoord van een OAuth-autorisatiestroom.

Gelieve te controleren of uw client library deze nieuwe parameter kan beheren.

Refresh

Vanaf deze nieuwe versie wordt de parameter **scope** in OAuth2/OIDC Endpoint voor de token refresh ondersteund. Door deze parameter te gebruiken is het mogelijk om een request van Access tokens te verrichten met een beperkter geheel van scopes dan initieel toegekend, maar het is niet mogelijk om de scope van de initiële token te verhogen. Deze beperking van de scope heeft geen invloed op de scope van de hernieuwde refresh token. Deze functie werkt zoals beschreven in de specificatie OAuth2.

Logout

Wijzigingen met een impact op de logout:

- De parameter **id_token_hint** is aanbevolen, maar optioneel in de specificatie (https://openid.net/specs/openid-connect-rpinitiated-1_0.html#Security). De implementatie werd gewijzigd, zodat er geen fout meer ontstaat wanneer **id_token_hint** ontbreekt, behalve als **post_logout_redirect_uri** gedefinieerd is en de **client_id** ook ontbreekt. In plaats daarvan zal een bevestigingspagina getoond worden.
- De parameter **redirect_uri** is achterhaald en wordt niet meer ondersteund. De gebruikers zullen een bevestigingspagina zien wanneer ze geen gebruik maken van de parameters die opgegeven zijn in de logout-norm.
- Wanneer de parameter **post_logout_redirect_uri** toegevoegd wordt, moet de klant ook de parameter **id_token_hint** ou **client_id** toevoegen.

Token Exchange

Wijzigingen met een impact op token exchange flows:

- Wanneer een token verstuurd wordt naar de endpoint userinfo, houden we geen rekening meer met de laatst actieve geauthentiseerde client sessie om de te mappen scopes te definiëren. Wij kijken voortaan enkel naar de scopes opgegeven in de verzonden token. Op die manier kan worden beheerd wat via token exchange wordt teruggestuurd. Indien u de endpoint userinfo gebruikt, gelieve te controleren of die nog steeds werkt zoals voorzien.
- Om de profielwijziging in aanmerking te nemen moet de scope 'iam:exchange:profile:switch' aanwezig zijn in de scope van de originele token bij de authenticatie, indien de klant die de token wenst om te wisselen van profiel wil veranderen. De scope bij de omwisseling mag niet ruimer zijn dan de scope van de originele token (zie OIDC Refresh).

Javascript Client

Voorheen hostten we een Javascript-bronbestand om een Javascript Keycloak adapter te laden in een Javascript-script. Aangezien het als een slechte praktijk beschouwd wordt om externe scripts te laden, werd dit bestand verwijderd. De oude Javascript Keycloak adapters en andere Javascript-scripts die van dit bestand afhingen voor de OIDC-stromen zullen moeten worden geüpdatet naar een recentere versie of een andere implementatie.

SHA1

Het handtekeningformaat SHA1 wordt niet meer aanvaard. Gelieve na te gaan dat er bij de ondertekening van berichten geen gebruik wordt gemaakt van SHA1. Als dit wel zo is, gelieve de nodige wijzigingen aan te brengen.

Account Service/Console

De gebruikersinterface van de dienst Account werd gewijzigd, maar de functionaliteiten blijven dezelfde en blijven ook op dezelfde manier werken.

Consent

Nieuwe look & feel voor de pagina met betrekking tot de consent.

Als u vragen hebt, kunt u steeds terecht bij het **CONTACTCENTER** via mail aan ***support@ehealth.fgov.be*** of op het nummer **02-788 51 55** (elke werkdag van 7u tot 20u).