Technical specifications
Identity & Authorization Management (I.AM)
SSO from eHealth I.AM IDP to fat client
Version 1.0

This document is provided to you free of charge by the

eHealth platform

Willebroekkaai 38

38, Quai de Willebroek

1000 BRUSSELS

All are free to circulate this document with reference to the URL source.

Table of contents

To the attention of: "IT expert" willing to integrate this web service.

1. Document management

1.1 Document history

Version	Date	Author	Description of changes / remarks
1.0	15/09/2015	eHealth	Initial version

2. Introduction

2.1 Context

A user, authenticated in his browser at the eHealth IDP, wants to obtain a sessionToken to continue his work in a local software package for which he needs such a token to call remote services. As the user is already authenticated at the eHealth IDP, he does not need to reauthenticate to obtain such a token.

2.2 Goal of the document

This document describes in technical detail how to **request** a secure token, delivered by the IDP, as identity proof to start a Single Sign On Session for fat clients.

It does not contain details on how to **use** such a secure token in a fat client. You can use the eHealth Connectors[1] for this or provide your own implementation.

---

[1] *https://www.ehealth.fgov.be/nl/support/tools/connectors*

3. Support

3.1 Support in general

For issues in production only

eHealth ContactCenter:

- Phone: 02/788 51 55

- Mail: ***support@ehealth.fgov.be***

- *Contact Form :*

    - *https://www.ehealth.fgov.be/nl/neem-contact-op-met-de-openbare-instelling-eHealth-platform (Dutch)*

    - *https://www.ehealth.fgov.be/fr/contactez-institution-publique-plate-forme-eHealth (French)*

FOR PARTNERS AND SOFTWARE DEVELOPERS ONLY

- For business issues please contact: ***info@ehealth.fgov.be***

- For technical issues in production please contact: ***support@ehealth.fgov.be*** *or call 02/788 51 55*

- For technical issues in acceptance please contact: ***Integration-support@ehealth.fgov.be***
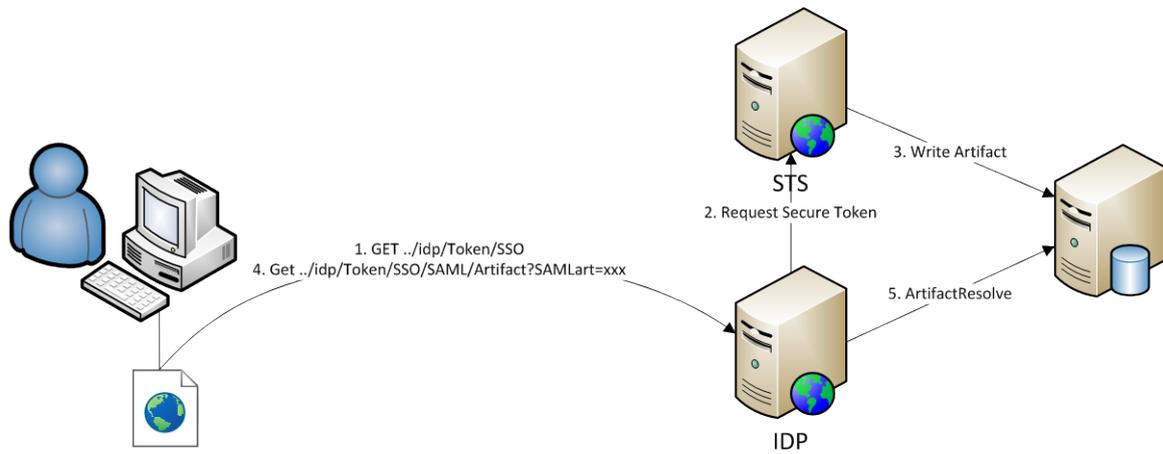
4. Global overview

Figure 1 SSO Process Flow

5. Step-by-step

5.1 Steps 1-3: Run SSO Wizard

The user starts the SSO wizard by requesting a page in eHealth IDP.

URL: [ehealth idp]/Token/SSO

- PROD: *https://www.ehealth.fgov.be/idp/Token/SSO*
- ACC: *https://wwwacc.ehealth.fgov.be/idp/Token/SSO*
- INT: *https://wwwint.ehealth.fgov.be/idp/Token/SSO*

If he is not yet authenticated or his active authentication level is not high enough (eID is required), he will be requested to authenticate using the standard authentication wizard in eHealth IDP (not added to the schema above for simplicity).

When he is authenticated, he will be requested for which profile he wants to receive a Secure Token: as citizen or as a qualified person (e.g. doctor, only available if he is known as a doctor).

Aanmelden voor eHealth SSO Service

| 1 | Kies uw taal
Nederlands | 2 | Identificatie
eID | 3 | Kies uw profiel |

Stap 3. **Kies uw profiel**   Hulp nodig?

U bent geïdentificeerd als: Frederik Eugeen Libert (Afmelden)

Ik wil me aanmelden als: Burger ▾

Aanmelden

Copyright ©2013 ○—e—Health Disclaimer ┊ Persoonlijke gegevens ┊ Gebruikersreglement ┊

After he has chosen his profile, eHealth will search for his active eHealth Certificate in the eHealth Certificate Store. If the user doesn't have an active eHealth Certificate, the wizard will fail.

In the backend, the IDP will request a SecureToken at the STS on behalf of the end user for the profile he has chosen and his personal certificate, found in the eHealth Certificate Store.

The requested token will be saved in eHealth Token Store and the user will be presented a reference to it on the summary page.

5.2   Steps 4-5: Download Secure Token

On the result page, the user can click on a link which will trigger a download of the secure token in his browser.

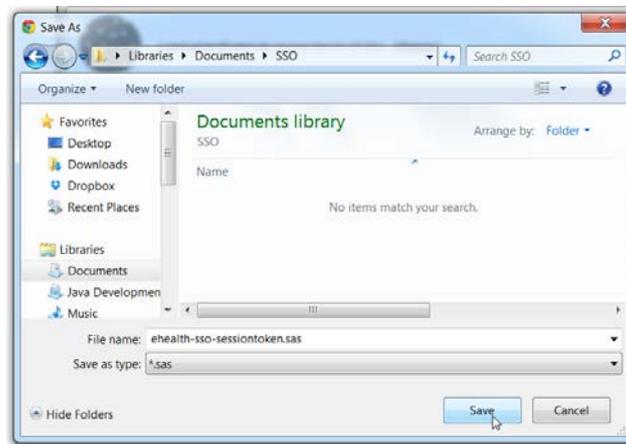He can also choose to scan a QR-Code to download the token on his mobile, equipped with a barcode scanner.

The downloaded token can now be used in a web service session from a fat client that uses the token as if it was retrieved from the eHealth STS itself.

The token will only be useable in combination with the user's personal eHealth certificate (more in particular he'll need to place a signature with the corresponding private key, in his possession only).

6. Test and release procedure

6.1 Procedure

This chapter explains the procedures for testing and releasing an application in acceptation or production.

6.1.1 Initiation

If you intend to use the eHealth service, please contact ***info@ehealth.fgov.be***. The Project department will provide you with the necessary information and mandatory documents.

6.1.2 Development and test procedure

You have to develop a client in order to connect to our web service. Most of the required integration info to integrate is published in the technical library on the eHealth portal.

6.1.3 Release procedure

When development tests are successful, you can request to access the eHealth acceptance environment.

From this moment, you start integration and acceptance tests. eHealth suggests testing during minimum one month.

After successful acceptance tests, the partner sends his test results and performance results with a sample of "eHealth request" and "eHealth answer" to the eHealth point of contact by email.

Then eHealth and the partner agree on a release date. eHealth prepares the connection to the production environment and provides the partner with the necessary information. During the release day, the partner provides eHealth with feedback on the test and performance tests.

For further information and instructions, please contact: ***integration-support@ehealth.fgov.be***.

6.1.4 Operational follow-up

Once in production, the partner using the eHealth service for one of its applications will always test first in the acceptance environment before releasing any adaptations of its application in production. In addition, he will inform eHealth on the progress and test period.