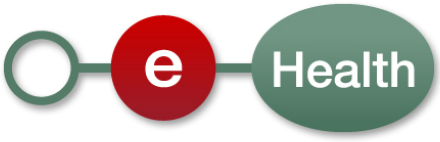



# Technical specifications
# Identity & Authorization Management (I.AM)
# Overview
# Version 1.0

This document is provided to you free of charge by

**The eHealth platform**

**Willebroekkaai 38 – Quai de Willebroeck 38**

**1000 BRUSSELS**

# Table of contents

# 1 Document management

## 1.1 Document history

| Version | Date | Author | Description of changes / remarks |
|---|---|---|---|
| 1.0 | 11/07/2013 | eHealth | Initial version |

# 2 Introduction

## 2.1 Introduction

The goal of this document is to give a high level overview of eHealth's Identity & Authorization Management (I.AM), the project of eHealth platform for cross-enterprise identification, authentication and authorization in healthcare environments.

eHealth I.AM consists of several components working together to perform single-sign-on, authentication, authorization and identity propagation of healthcare users requesting access to services, hosted by healthcare organisations and the ehealth platform.

These components follow international standards for cross-enterprise communications in order to guarantee security and stability and ease integration.

## 2.2 Attributes

One of the key concepts in eHealth I.AM is the use of Attributes to transfer information about an entity from one component to another.

In order to understand how eHealth I.AM works, you must be aware of this as the architecture is based on internationally defined protocols to transfer data about entities in the form of attributes.

Attributes can be simple identification values such as social security number, firstname, lastname.

They can claim a quality of a person, like isDoctor, isNurse.

They can also be more complex and structured, like HomeAddress.

## 2.3 Trust

Another key concept is the use of Trust relations. As ehealth I.AM is designed for cross-enterprise exchange of identity and authorization data, a trust relation between requester and receiver is mandatory.

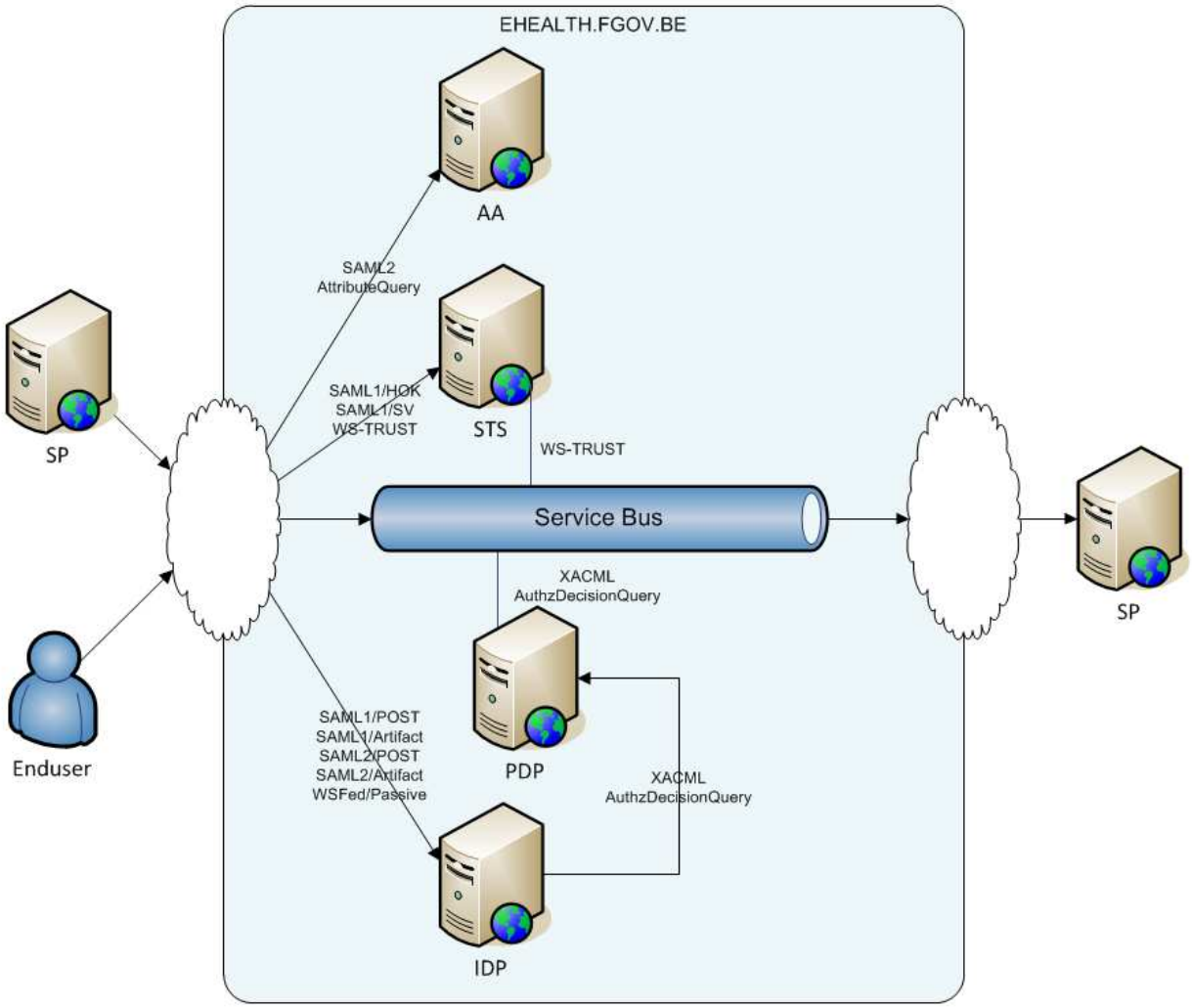
Various means for authentication are available.

Encryption to guarantee confidentiality is at the least provided on the transport level.

Some protocols also support encryption at message level.

The services presented below are designed to accept, request and return attributes about an entity with verifications of who may request and receive what information.

# 3 Overview




**Figuur 1 : eHealth I.AM – Overview**

eHealth I.AM provides Single Sign-on support to services outside of a user's organization while still protecting their privacy.

Different services are involved here, amongst which are:

- An Identity Provider (IDP) for Web SSO
- A Secure Token Service (STS) for Ws SSO
- An Attribute Authority (AA) to enrich identity
- A Policy Decision Point (PDP) for Access Control

## 3.1 Web SSO

The eHealth I.AM Project provides Single Sign-on between all webapplications that are protected by Service Providers that rely on the eHealth IDP to perform authentication of the user. Single Sign-On is maintained during the active browser session of the user and ends irreversible when the user closes his browser.

The main actors in a web-based SSO system are:

- ***Web Browser***: represents the user within the SSO process.
- ***Resource***: contains access-restricted content that the user wants, hosted by the SP.
- ***Identity Provider (IDP)***: authenticates the user.
- ***Service Provider (SP)***: performs the SSO process for the resource. There is a trustrelation between the SP and the IDP.

An SP protecting webapplication resources will interact with the eHealth IDP to receive a token with information on the enduser. To build this token, the IDP will authenticate the enduser and gather required identity and authorization data.

Different internationally approved protocols are supported for communication between different types of SPs and the eHealth IDP.

After receiving the token, it is up to the SP to permit or deny access to the protected application for this enduser.

SSO for webapplications is achieved by the fact that endusers do not need to re-authenticate when they want access to a second application (behind the same SP or another). The SP will receive a different token with identity and authorization data for this second application without forcing the user to re-enter his credentials (eID, username-token, …).

## 3.2 Ws SSO

The eHealth I.AM Project provides Single Sign-on between all webservices that are protected by Service Providers that rely on tokens delivered by the eHealth STS containing the identity of of the user. Single Sign-On is maintained during the validity of the token and ends irreversible when the time condition in the token has expired or when the token is deleted from the client's system.

The main actors in a webservice-based SSO system are:

- ***Resource***: Webservice that the user wants to access, hosted by a Target SP.
- ***Secure Token Service (STS)***: authenticates the user and provides a secure token containing attributes with identity data.
- ***Enduser clientsoftware***: builds signed requests on behalf of the user within the SSO process. There is NO trustrelation between the enduser and the STS.
- ***Service Provider (SP)***: a distinction is made between 'Source' SPs that request tokens so they can be used to target other services and 'Target' SPs that host those other services.

- *Source*: builds signed requests on behalf of the user within the SSO process and vouches for him. There is a trustrelation between the SP and the STS.
- *Target*: accepts tokens from the STS as authentication of the user. There is a trustrelation between the SP and the STS.

Both end-users and SPs can request tokens from the eHealth STS.

Amongst the supported tokens are SAML Holder-Of-Key for end-users and SAML Sender-Vouches for SPs.

To build the token, the STS supports the X.509 Certificate Token Profile to let users authenticate with an X.509 Certificate, retrieve identity information from it and search for extra identity data on demand, as specified in the request.

Different protocols are supported for communication between different types of requesters and the eHealth STS.

After receiving the token, the requester can use it in subsequent requests to services for which such a token is acceptable as input for authentication.

Those services can be hosted by the eHealth Platform or target SPs that support the SAML Token Profile and trust eHealth STS as issuer of those SAML tokens.

SSO for webservices is achieved by the fact that such tokens have a validity period in which they can be reused for subsequent requests and this for multiple services without forcing the user to re-authenticate using his X.509 authentication credential.

The information included in the token can differ on demand and it is the requestor that decides which identity information is included and certified by eHealth.

## 3.3 Attribute Authority

The eHealth Attribute Authority[1] (AA) is a service that binds Attributes to Identities, much like the IDP (for Web SSO) and the STS (for Ws SSO).

It differs from those identity services as it does not provide information on users by forcing them to perform a strong authentication directly. Instead it relies on the requestor to specify the allready authenticated user as Subject of the request using a list of attributes which together form the identity of the user.

Its purpose is to deliver extra attributes on behalf of the authenticated user that cannot be delivered by the IDP or STS for any reason.

It supports the SAML AttributeQuery Profile as defined in the SAML 2.0 Specifications.

To protect the privacy, requestors must have a trust relation with the Attribute Authority in which a policy is defined which Attributes they may request for a certain entity (Subject).

[1] Not to be confused with the AttributeAuthority, embedded in the eHealth IDP, which purpose is merely to conform to the SAML 1.1 Browser/POST Profile with a Pull mechanism, as designed by Shibboleth, as a way to transfer data from IDP to SP without using the standard form, POSTed using the client's browser. More information on this in 'eHealth I.AM – IDP'.

## 3.4 Access Control

The eHealth I.AM Project provides Access Control to services, based on Access Rules Policies executed by a Policy Engine.

The main actors in an Access Control system are:

- ***Subject***: the user that requires access to a protected resource.
- ***Resource***: contains access-restricted content that the user wants.
- ***Policy Enforcement Point (PEP)***: The system entity that performs access control, by making decision requests and enforcing authorization decisions.
- ***Policy Decision Point (PDP)***: The system entity that evaluates applicable policy and renders an authorization decision.
- ***Policy Administration Point (PAP)***: The system entity that creates a policy or policy set.
- ***Policy Information Point (PIP)***: The system entity that acts as a source of attribute values.

Before Access Control to the Resource is verified, the Subject is identified by the IDP (Web SSO) or the STS (Ws SSO)[2].

The PDP is not available outside the eHealth Platform. The PEP, which is responsible to enforce the authorization decision, is located on the eHealth Platform itself and will be executed for any resource for which Access Control is enabled.

- For webservices, accessible through the eHealth Service Bus, unauthorized requests will be blocked immediately on the Service Bus.
- For webapplications, unauthorized requests can be blocked immediately in the IDP (a standard 'no access' page is shown to the user) or the authorization decision can be sent in the token to the SP of the partner which must take apropriate action depending on the decision ('no access' page of the SP, additional access rules, …).

## 3.5 Service Bus

eHealth has a Service Bus which is used to target different services on the eHealth Platform itself or hosted by other partners.

### 3.5.1 Authentication

The Service Bus supports mainly 2 Web Service Security Token Profiles to authenticate the consumer.

- **X509**

Tokens need to be issued by a trusted CA.
Consumers can obtain such a token using the ETEE Requestor application[3].

[2] Some services at eHealth also support the X.509 Certificate Token Profile which allows users (persons, systems) to authenticate directly with an X.509 Certificate.

[3] https://www.ehealth.fgov.be/nl/support/basisdiensten/ehealth-certificaten

- **SAML**

Tokens need to be issued by eHealth.
Consumers can obtain such a token by sending a request tot the eHealth Secure Token Service (STS).

### 3.5.2 Access Control

Access Control is achieved using the data-flow model of XACML.

A PEP will call the eHealth PDP for an authorization decision based on an Access Policy set for the requested resource.

See section Access Control.

### 3.5.3 Identity Propagation

The Service Bus can simply propagate the identity of the consumer in a new SAML Token for the TargetService.

Based on the present usercredentials and the targetService, it can also request a new SAML Token from the eHealth STS with a specific set needed for the targetService. Attributes containing sensitive identity information can be filtered out, extra attributes can be added if required by the targetService.

# 4 Documentation

The eHealth I.AM documentation is split up into different documents.

- **Overview**
  - *eHealth I.AM – Overview*: this document
- **Identity Services**
  - *eHealth I.AM – IDP*: eHealth's Identity Provider for Web SSO.
  - *eHealth I.AM – STS*: eHealth's Secure Token Service for Ws SSO.
  - *eHealth I.AM – AA*: eHealth's Attribute Authority.
- **Service Providers**
  - *eHealth I.AM – SP Shibboleth*: How To integrate a Webapplication protected by a Shibboleth SP.
  - *eHealth I.AM – SP Wali*: How To integrate a Webapplication protected by a Wali SP.
  - *eHealth I.AM – Logout*: Local and Global Logout in the eHealth I.AM Federation for applications participating in Web SSO.
- **Access Control**
  - *eHealth I.AM – AccessControl*: Data-flow model used for eHealth Authorizations.
- **Registration**
  - *eHealth I.AM – Registration*: form that a partner must send to eHealth to register in the eHealth I.AM Federation to setup a trust relation between the partner and eHealth.
- **Federation**
  - *eHealth I.AM – Federation Attributes*: lists all the basic authentication attributes supported by the Identity Services with a description for each.
  - *eHealth I.AM – Federation Metadata*: explains the use of SAML 2.0 Metadata in the eHealth I.AM Federation.