Service Level Agreement
Basic Service: <IAM Single Sign On>
Version 1.0

This document is provided to you free of charge by the

eHealth platform

Willebroekkaai 38 – 1000 Brussel

38, Quai de Willebroeck – 1000 Bruxelles

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

Service Level Agreement

< IAM Single Sign On >

Between

Service provider

eHealth Platform

Quai de Willebroek, 38

1000 BRUSSELS

To the attention of: the user community

Author:	Service Management
Date:	05/03/2026
Version:	*1.0*
Status:	Final
Type:	Public
Confidentiality:	/
Language:	English
Exhibit of:	MSA

Service customer

User Community

1. Table of content

2. Document management

2.1. Document history

Version	Date	Author	Description of changes / remarks
1.0	05/03/2026	eHealth Service Management	First Version

2.2. Document references

ID	Title	Version	Date	Author
	Master Service Agreement	7.0	16/09/2025	

2.3. Purpose of the document

The objective of this document is to define the Service Level Agreement for the set of services included in the <*IAM Single Sign On*> proposed by the eHealth-platform. It defines the minimum level of service offered on the eHealth-platform, and provides eHealth's own understanding of service level offering, its measurement methods and its objectives in the long run.

The purpose of the portal eHealth is to offer a central entry point for dedicated information and access to healthcare related applications.

2.4. Features

The goal of this service is to offer a web service based single-sign-on solution (SSO) for the health care sector.A user (physical person), in possession of a sessionToken received from the eHealth SecureTokenService (STS), needs to continue his work in a remote web application / client that requires authentication with the eHealth platform. Therefore, he needs to identify himself at the eHealth IdentityProvider (IDP) or eHealth IAM Connect. As the user already has a sessionToken from the STS, he can reuse it to authenticate at the IDP or IAM Connect.

2.5. Validity of the agreement

This document is valid as long as the *IAM Single Sign On* is part of the eHealth-platform offering services.

Once a year, the levels of service proposed will be reviewed and confirmed for the next year.

2.6. Service and maintenance window

2.6.1. Service window

The time frame during which the eHealth services are offered to the client applications, is defined in terms of days and hours. Standard working days are all days of the year, except during the biannual maintenance periods.

The following table summarises the eHealth service window.

Service Window								
		Day of the week (closing days of Service Provider = Sunday)						
		Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
	00:00 – 24:00							

Legend	
🟩	Timeslots where the service must be available according to the SLA and where corrective actions will be taken to resolve detected Incidents.

2.6.2. Support Window

Support Window							
		Day of the week (Closing days of Service Provider = Sunday)					
		Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
Day period	00:00 – 8:00							
	08:00 – 16:30							
	16:30 – 18:00							
	18:00 – 24:00							

Legend	
🟩 (light green)	Timeslots for which the eHealth Call Center is available for the End-Users with a second line support for Infrastructure (HW, OS, Middleware and DB)
🟩 (dark green)	Timeslots for which the eHealth Call Center is available for the End-Users with a second line support, including Application Support
🟨	Timeslots for which the eHealth Call Center is unavailable for the End-Users. The End-User will have the possibility to record a voice message that will be treated on the next Workday.

2.6.3. Maintenance Windows & Planned Interventions

The eHealth platform will strive for limiting as much as possible the impact and duration of the planned interventions. Today, eHealth is committed to make efforts so planned unavailability's do not exceed one to a few hours per year. In case of maintenance requiring support from users, or impacting them, eHealth will notify them at least one week ahead.
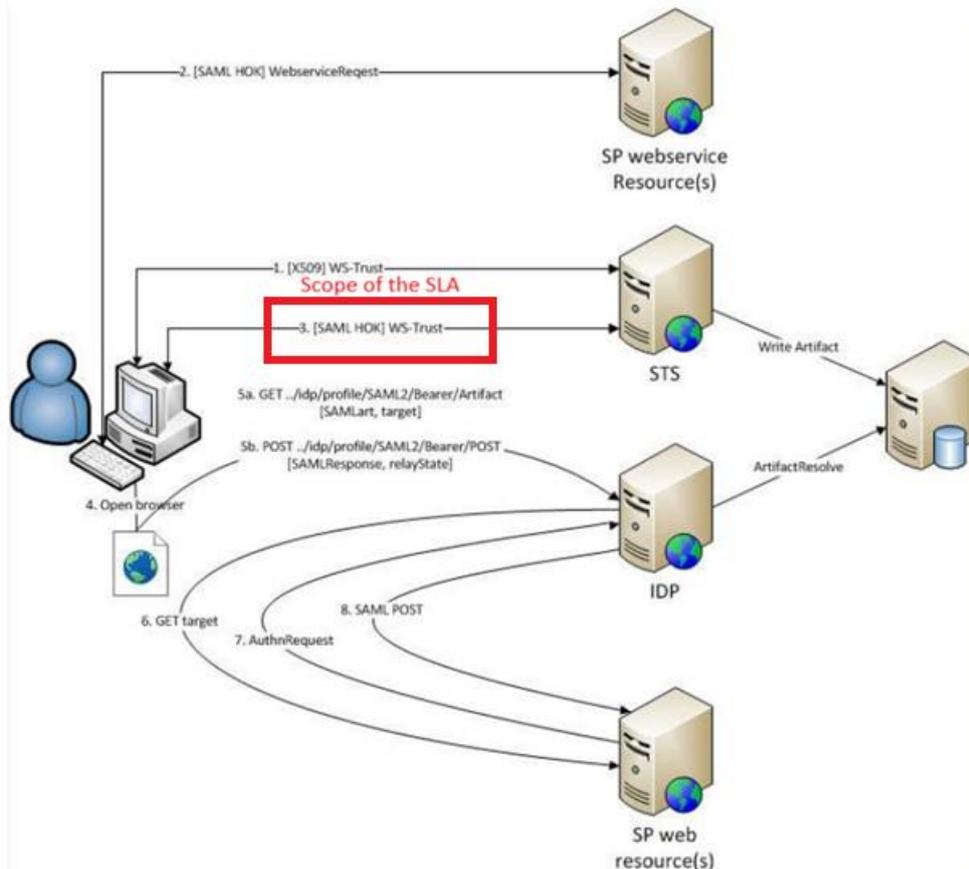
2.6.4. Unplanned Interventions

Under exceptional circumstances, unplanned interventions may be needed in order to restore the service.

3. Service scope

3.1. eHealth service

3.1.1. General

Steps 1-2: SSO web services (STS)

> SSO is setup between WS hosted by the eHealth Platform or one of its trusted partners with eHealth IAM STS as Security Token Service.

Steps 3-5: SSO Web services – Web App (STS → IDP)

> SSO session for WS is transferred from fat to thin client.

- Request Bearer Token from STS

  The client sends a request to the STS to generate a new bearer token, based on the existing holder-of-key(HOK) token. The newly generated token will be valid for a short period (max 10 minutes).There are multiple options to request this token which will influence the result and remainder of the process flow.

- Open browser

  A new or existing browser window is opened to setup SSO between the client's browser as thin client and eHealth IDP.

- Authenticate at IDP

    Depending on the result of step 3, the client uses his browser to send his authentication details to the eHealth IDP.

Steps 6-8: SSO Web App (IDP)

    SSO is setup between web applications in the eHealth IAM Federation with eHealth IAM IDP as Identity Provider.

3.1.2. Abbreviations

IAM	Identity and Access Management
IDP	Identity Provider
MSA	Master Service Agreement
SAML	Security Assertion Markup Language
STS	Secure Token Service
SP	Service Provider
SSO	Single Sign-On

3.2. Business criticality

The business criticality of the service is **Platinum** as it supports mandatory business processes that should be processed synchronously and within some legal periods.

3.3. Interdependencies

The < *IAM Single Sign On* > Basic Service depends on the MSA and on the collaboration with the partner.

4. List of service levels

Service	KPI	SL ID	Condition	Measure based on	Limit	Service Window	Objective Committed	Objective Target
IAM/SingleSignOnService/v1	Availability Single Sign On (SSO) WS		Transaction passes	Fictitious request		Mo – Su 0:00 – 24:00	99.5%	99,9%
	Performance Single Sign On (SSO) WS		Response time < 1sec	Real transactions		Mo – Su 0:00 – 24:00	98%	99,0%

Table 1: List of key performance indicators (KPI) per service

5. Detailed service level per service

5.1. Availability

Objectives	
Definition	• The eHealth WS IAM Single Sign On is considered to be available when it is reachable via the Gateway (get request and evaluation of the response -keep Alive Test). • Planned interventions executed within the Maintenance Window are not recorded as unavailable time.
Measuring method	• The availability of the different functionalities is measured by executing the test scripts every 5 minutes. When the script is executed with as result a Status "OK", the test "passed". • When the script is executed with an other result, the test "failed" • Measuring is always done on test scenarios.

Calculation	$$Availability = \frac{\sum Passed\ Tests\ x\ 100}{\sum Total\ Tests}\%$$
	
	• Total Tests = Total number of tests launched within corrected timeframe
	
	• Passed Tests = Total number of tests that resulted in a status "OK" within the same timeframe
	
	• Corrections are applicable on tests that are not taken into account because they were caused:
	   o by a Validated Authentic Source or partner application out of scope of this SLA
	   o by a failing monitoring tool

Reporting and evaluation period	• The availability is calculated and reported monthly. Corrective interventions are initiated when appropriate. • The formal evaluation however is done on a yearly basis.

Service Level Objectives	Functionality	Service Window	Service Level Objective	
			Committed	**Target**
	Availability IAM Single Sign On	Mo – Su 0:00 – 24:00	99,5%	99,9%

5.2. Performance

Objectives	
Definition	• The performance of the eHealth <Service Name> WS refers to its response time meaning the time needed to execute a request. This request can be : RequestSecurityToken • Attention: The response time does not include: ○ The time needed to deliver the information over the Internet ○ The time needed to process the information at the End Users premises.
Measuring method	• This response time is measured on the Reverse Proxies. Both start time (request received) and stop time (answer sent to the End User) are measured and stored in a database. • Measuring is done on real transactions, and only on those having a "stop time" within the measuring period.
Calculation	• All response times are calculated: Stop time – Start time for every request. • The percentage that meets the target is calculated based on following formula: $$Performance = \frac{\sum Tests\ meeting\ the\ target\ x\ 100}{\sum Total\ Tests}\%$$
Reporting and evaluation period	• The performance is calculated and reported monthly. Corrective interventions are initiated when appropriate. • The formal evaluation however is done on a yearly basis.

Service Level Objectives	Functionality	Target	Service Level Objective	
			Committed	Target
	Performance IAM Single Sign On	< 1 sec	98%	99,0%