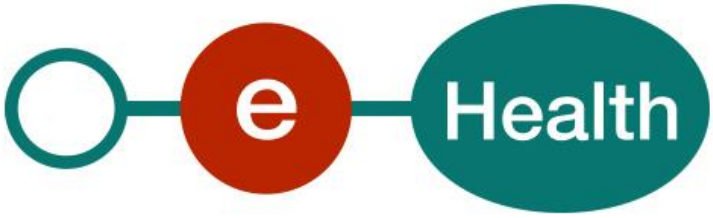


Service Level Agreement
Basic Service: Secure Token Service
Version 1.2

eHealth platform

Willebroekkaai 38 – 1000 Brussel

38, Quai de Willebroeck – 1000 Bruxelles

Service Level Agreement

Secure Token Service

Between

Service provider

eHealth Platform

Quai de Willebroek, 38

1000 BRUSSELS

Service customer

User Community

To the attention of: the user community

Author: Service Management
Date: 18/06/2025
Version: *1.2*
Status: Final
Type: Public
Confidentiality: /
Language: English
Exhibit of: MSA

1. Table of content

2. Document management

2.1. Document history

Version	Date	Author	Description of changes / remarks
1.1	04/03/2025	Service Management	Initiate the document
1.2	18/06/2025	Service Management	Add KPi

2.2. Document references

ID	Title	Version	Date	Author
	Master Service Agreement	2022.1	12/04/2022	

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 Secure Token Service (STS) 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. The health care party, a web service consumer (WSC), contacts this service to obtain a session ticket (SAML token), which can be used to invoke the services offered by a web service provider (WSP).

2.5. Validity of the agreement

This document is valid as long as the Secure Token *Service* 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
Day period	00:00 – 07:00							
	07:00 – 08:00							
	08:00 – 16:30							
	16:30 – 19:00							
	19:00 – 20:00							
	20:00 – 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.
	Timeslots where the service will be available provided there are no blocking Incidents. If these incidents do appear, no corrective action will be taken.
	Timeslots where unavailability can occur.

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	
	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)
	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

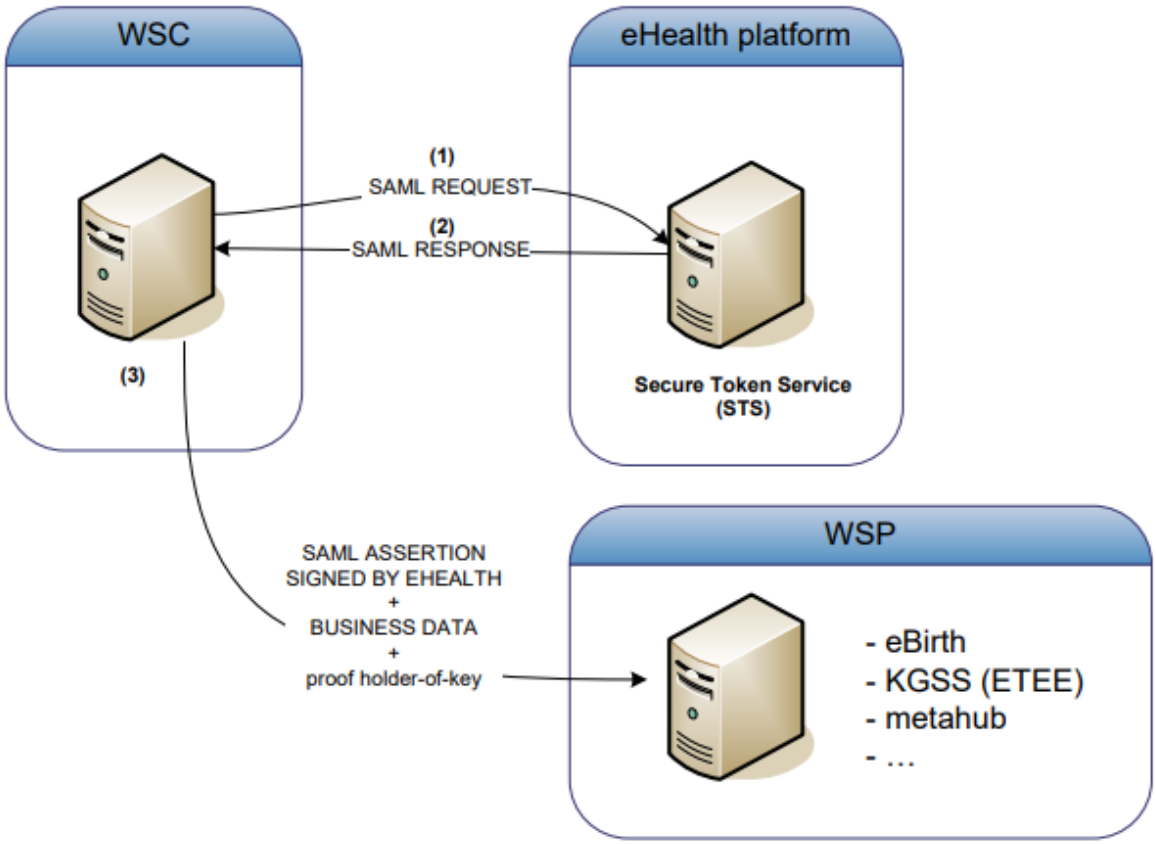
Under exceptional circumstances, unplanned interventions may be needed in order to restore the service.

3. Service scope

3.1. eHealth service

3.1.1. General

Every health care party can contact this service to obtain a session ticket (SAML token) and use this token to communicate with services that are accessible 'through' the eHealth-platform. Only web service based solutions are supported by this service.



Step 1: A web service consumer (WSC) requests a SAML token from the STS. The message contains two parts: identification information relative on the WSC and information to be confirmed by eHealth.

Step 2: eHealth sends a signed SAML assertion to the WSC with the message containing the confirmed information.

Step 3 (out of scope): From now on, the WSC can use the obtained SAML token for further communication with the different WSP's. When the SAML assertion is invalid, the WSC must request a new SAML token (Step1)

For example, a general practitioner (GP) wants to use two different applications that every GP can access. The end user requests a SAML token to obtain proof of being a GP. The eHealth platform validates this claim against its validated Authentic sources (VAS). In case of a positive response, the STS sends a session ticket to the requestor . This session ticket contains the proof that he is a GP. Every session ticket has a lifetime: when a session has expired, the end user must request a new one. When the GP contacts a target application, he must send the session ticket along with the business data. Due to the session ticket, the applications have certified proof that the requestor is a GP and can conduct his business.

3.1.2. Abbreviations

GP	General Practitioner
UAM	User and Access Management
STS	Secure Token Service
SSO	Single Sign On
VAS	validated Authentic sources
WSC	Web service consumer
WSP	Web Service provider

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 Basic Service Secure Token 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
Secure Token Service	Availability Secure Token Service WS		Transaction passes	Fictitious request		Mo – Su 0:00 – 24:00	99.5%	99,9%
	Performance Secure Token Service WS		Response time < 1 sec	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

<table>
<tr><th colspan="5">Objectives</th></tr>
<tr><td>Definition</td><td colspan="4">The eHealth WS Secure Token Service is considered to be available when it is reachable via the Gateway
Planned interventions executed within the Maintenance Window are not recorded as unavailable time.</td></tr>
<tr><td>Measuring method</td><td colspan="4">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 another result, the test “failed”
Measuring is always done on test scenarios.</td></tr>
<tr><td>Calculation</td><td colspan="4">$$Availability = \frac{\sum Passed\ Tests\ x\ 100}{\sum Total\ Tests}\%$$
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:
by a Validated Authentic Source or partner application out of scope of this SLA
by a failing monitoring tool</td></tr>
<tr><td>Reporting and evaluation period</td><td colspan="4">The availability is calculated and reported monthly. Corrective interventions are initiated when appropriate.
The formal evaluation however is done on a yearly basis.</td></tr>
<tr><td rowspan="2">Service Level Objectives</td><td rowspan="2">Functionality</td><td rowspan="2">Service Window</td><td colspan="2">Service Level Objective</td></tr>
<tr><td>Committed</td><td>Target</td></tr>
<tr><td>Availability Secure Token Service WS</td><td>Mo – Su
0:00 – 24:00</td><td>99.5%</td><td>99,9%</td></tr>
</table>

5.2. Performance

<table>
<tr><th colspan="5">Objectives</th></tr>
<tr><td>Definition</td><td colspan="4">The performance of the eHealth Secure Token Service WS refers to its response time meaning the time needed to execute a request. This request can be:
Challenge (RequestSecurityTokenResponse)
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.</td></tr>
<tr><td>Measuring method</td><td colspan="4">• 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.</td></tr>
<tr><td>Calculation</td><td colspan="4">• All response times are calculated: Stop time – Start time for every request.
• The percentage that meets the target is calculated based on following formula:
$$Performanœ = \frac{\sum Tests\ meeting\ the\ target\ x\ 100}{\sum Total\ Tests}\%$$</td></tr>
<tr><td>Reporting and evaluation period</td><td colspan="4">• The performance is calculated and reported monthly. Corrective interventions are initiated when appropriate.
• The formal evaluation however is done on a yearly basis.</td></tr>
<tr><td rowspan="3">Service Level Objectives</td><td rowspan="2">Functionality</td><td rowspan="2">Target</td><td colspan="2">Service Level Objective</td></tr>
<tr><td>Committed</td><td>Target</td></tr>
<tr><td>Performance Secure Token Service WS</td><td>< 1 sec</td><td>98%</td><td>99%</td></tr>
</table>