

**Service Level Agreement
Base Service: User Access Management (UAM)
Version 2.1**

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

Base Service UAM

Between

Service provider

eHealth Platform
Quai de Willebroeck, 38
1000 BRUXELLES

Service customer

User Community

To the attention of: the user community

Author: eHealth Service Management
Date: May 30th, 2018
Version: 2.1
Status: Final
Type: Public
Confidentiality:
Language: English
Exhibit of: MSA



1. Table of Content

1.	Table of Content	3
2.	Document management.....	4
2.1.	Document history	4
2.2.	Validation	4
2.3.	Document references.....	4
2.4.	Purpose of the document.....	5
2.5.	Validity of the Agreement.....	6
2.6.	Service and Maintenance Windows.....	6
2.6.1.	Service window	6
2.6.2.	Support Window.....	7
2.6.3.	Maintenance window & planned interventions.....	7
2.6.4.	Unplanned interventions	7
3.	Service scope	8
3.1.	Architecture overview.....	8
3.2.	Functionalities	9
3.3.	Business criticality.....	11
3.4.	Interdependencies	11
4.	List of Service Levels	12
5.	Detailed Service Level per service	13
5.1.	Checking of qualities and relationships: Availability	13
5.1.1.	Availability: Checking of qualities and relationships Service	13
5.2.	Checking of qualities and relationships: Response time	13
5.2.1.	Response time: checking of qualities and relationships service.....	13
5.3.	Authorisation service: Availability	14
5.3.1.	Availability: Authorisation Service	14
5.4.	Authorisation service: Response time	15
5.4.1.	Response time: Authorisation service	15

2. Document management

2.1. Document history

Version	Date	Author	Description of changes / remarks
2.0	August 2011	eHealth platform	Update
2.1	30/05/2018	eHealth platform	Update

2.2. Validation

Date	Version	Name	Role	Remarks
		Frank Robben	eHealth CEO	
May 2017		Heller Philippe	eHealth Service Manager	
30/05/2018		Heller Philippe	eHealth Service Manager	

2.3. Document references

ID	Title	Version	Date	Author
	Master Service Agreement	1.0		



2.4. Purpose of the document

The objective of this document is to define the Service Level Agreement for the set of services included in the *Base Service for the UAM (User Access Management)* 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.

This document contains a short description of the set of services offered by UAM. The User access management is composed of two major set of services. The first set of services ensures the authentication, the identification, the determination with regards of certain qualities and the authorisation of a user. The second set of service ensure the management of user accounts (as for the creation of mandate, the use of the access management tool for entities and organisation, the responsibility management tool, the FAS tool)

The **first** set of service covers the three initial authorisation and authentication steps:

- Step of identification and authentication of the identity of a person: this step starts with Login screen proposed on the eHealth Portal. It covers the identification and the authentication of the identity of an individual by the electronic identity card or the citizen token. It requires several interactions with the user. It includes the identification and the authentication of the user by external sources from the eHealth platform;
- Step of checking of qualities and relations of a user: as soon as the user is identified and authenticated, by means of its electronic identity card or citizen token, the eHealth platform draws up its list of qualities and mandates. If necessary, the UAM gathers the list of organisations and/or mandates which have been checked and linked to the identified user who is then proposed to the user in order to allow him to select the organisation or the possible mandate with which he wishes to be presented;
- Step of authorisation of the user: the step of authorisation questions according to selected qualities the relevant authentic sources and the data base of management of the access related to the applications and services which the user wishes to reach.

The step of identification and authentication is ensured by an external supplier of service (BOSA) which manages these processes.

The **second** set of service covers service managing authorisations:

- The access management service for companies and organisations (User Management) ¹ which allow the identification of people working in the same organisation.
- The Responsibility Management for Public Health (ReMaPH) service in order to let someone of a specific organisation provide access to some collaborators to different added value services.
- The Kephass tool which allow the management of access rules by eHealth with regard to different access scenario's and applications.

In addition, this document contains a short description of, or a link to a location where such a description can be found:

- Some technical and/or functional components the web services depend on.
- Measurements and KPIs intended to account for a certain number of performance indicators.

This document is a complement to the *Master Service Agreement (MSA)*. The information given in this document version takes precedence over the data regarding the same subjects given in former versions and in the MSA. Items described in the MSA include, for instance:

¹ The User management service is ensured by an external supplier of service

- A broad description of the business services offered by the eHealth platform to the applications which may want to make use of them
- Description of cross-sectional services offered on the eHealth platform
- Description of support services, including registering, managing and solving possible incidents with the UAM set of services, managing changes
- Performance indicators related to those services.

2.5. Validity of the Agreement

This document is valid as long as the *Base Service UAM* is part of the eHealth offering.

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




2.6. Service and Maintenance Windows

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 quarterly maintenance periods and Bank Holidays.

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 – 07:00							
	07:00 – 08:00							
	08:00 – 16:30							
	16:30 – 19:00							
	19:00 – 20:00							
	20:00 – 24:00							

Legend	
	Timeslots for which the eHealth Call Center is available for the End-Users
	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 window & 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.

- Portal, Network interventions and application release: 2 times a year.

2.6.4. Unplanned interventions

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

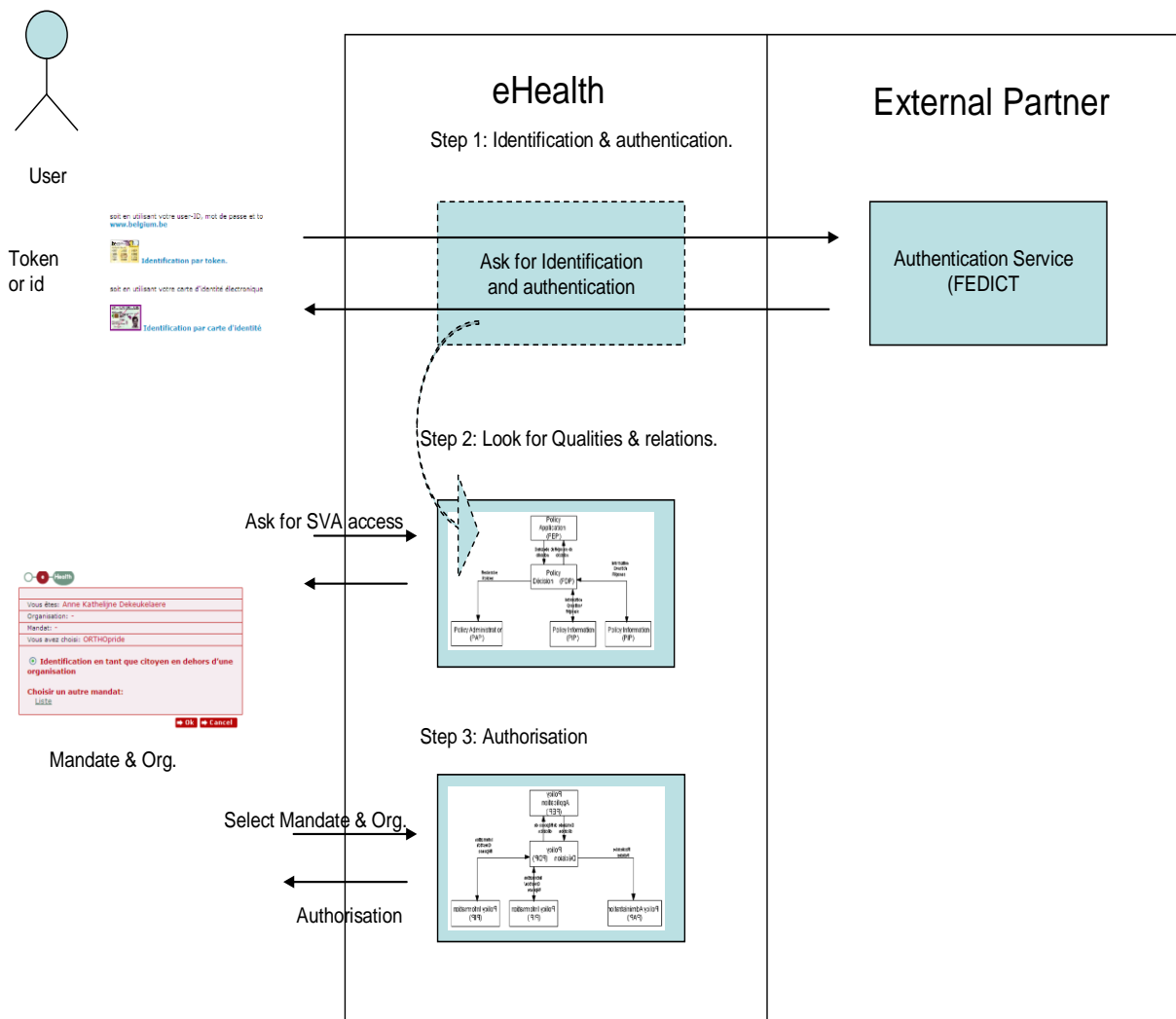


3. Service scope

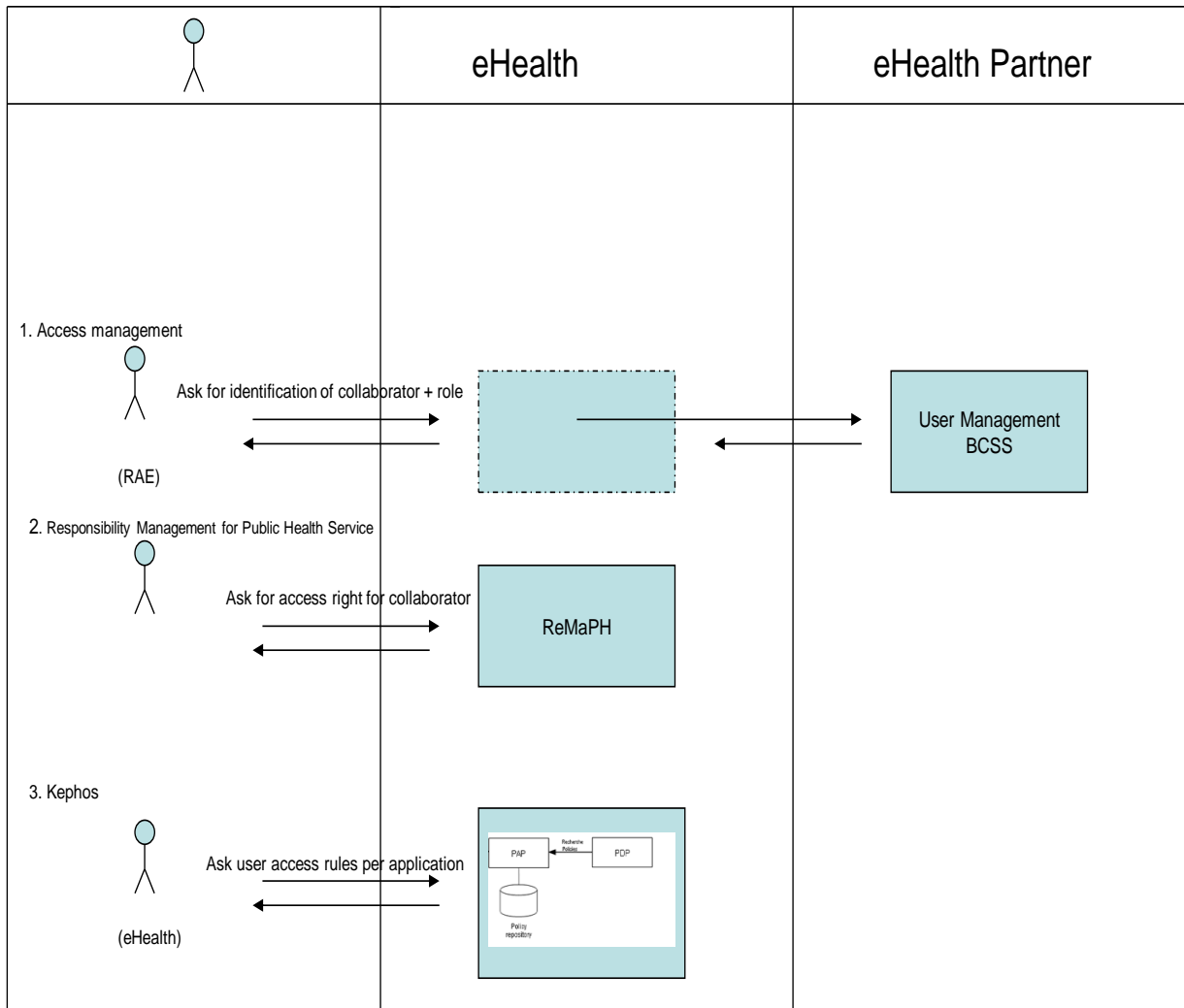
3.1. Architecture overview

The eHealth UAM service is based on two main processes:

1. The identification, authentication, checking of qualities & relations and authorisation process



- The process of managing the authorisations, consisting of maintenance of accesses and authorisations for individuals as well as maintenance of rules for applications.



3.2. Functionalities

The operations performed by eHealth UAM and/or by the user decompose into the following sequences of actions; all three will be measured, but currently, only the 2nd and the 3rd step will come into play for SLA's:

- Identification and authentication of a person**
Login screen, proposed by eHealth, including validation of the user credentials outside eHealth, in a sequence of steps with a high degree of user interaction, resulting in his authentication.
- Checking of qualities and relations of a user**
Following this part of the identification and authentication step, further checking of qualities and relations of a



user are done by eHealth UAM, which results in a list of organisations and mandates (both if applicable) being returned for selection by the user.

- **Authorisation of the user**

Following the choice made by the user, authorisation is being performed by eHealth UAM, by consulting the database of authorisation rules and the pertinent Validated Authentic Sources, in conjunction with the application.

Furthermore, the Base Service UAM includes tools, utilities and services to perform supporting functions. Nevertheless, the following services are not part of our current service level proposition:

- managing the authorisation of users on the eHealth platform (administration of users belonging to an organisation). Responsible for accessing entities (“VTE” – “RAE”) and the Local Manager (“LB” – “GL”) of an organisation are involved in some parts of the process of managing the authorisations (resp., appointing an LB – GL and maintaining the set of authorisation roles and privileges for the users belonging to their organisation).
- managing the mandates
- managing the integration of applications on the eHealth platform (access rules, integration of applications).

From a business point of view, the UAM services are further comprised of several components².

Consumers of these services may be citizens as well as Health Care Providers; Health Care Providers have access to these services either through the eHealth Portal, or through their eHealth partner applications, on the premise that they have been granted proper access and / or comply with legal requirements. The services are intended to relieve the eHealth partner applications from the task of implementing themselves those three functions.

From a user point of view, identification, authentication, checking of qualities & relations and authorisation take place along one of the following 3 scenarios:

1. *User connects and log himself to the eHealth Portal before his selection of any application,*

- logs in by using her/his Citizen Token or eID, (Step 1)
- Selection and request to access an application :
 - After eHealth services has checked qualities and relations of a user (Step 2), the user select an organisation (if applicable), and a mandate from the list of mandates available (if applicable),
 - Based on qualities and organisations selected, the authorisation (step 3) occurs by consulting all Validated Authentic Sources coming into play for the specific combination of his credentials and application choice

2. *User requests to access to a specific application or added value service from the portal,*

- Selection and request to access an application on the portal :
 - logs in by using her/his Citizen Token or eID, (Step 1)
 - After eHealth services has checked qualities and relations of a user (Step 2), the user select an organisation (if applicable), and a mandate from the list of mandates available (if applicable),

² These service components are available from the main services only: identification and authentication, checking qualities & relations, authorisation, managing the authorisations, but are not offered as a separate service to the user community.



- Based on qualities and organisations selected, the authorisation (step 3) occurs by consulting all Validated Authentic Sources coming into play for the specific combination of his credentials and application choice

3. User requests to access directly to a specific application or added value service directly,

- Same as for scenario 2 behalf the fact that user tries to connect to a specific application from outside the eHealth portal.

3.3. Business criticality

The business criticality of the User access management functionalities are **Gold** as it supports mandatory business processes that should be processed synchronously and within some legal periods.

3.4. Interdependencies

The services covered by this Service Level Agreement are functionally dependent upon services offered by the National Register (RR/RN), the National Institute for Health Insurance and Invalidity (RIZIV/INAMI), the Federal Public Health Service (FOD-VVVL/SPF-SP) and the CBSS (KSZ/BCSS) (for access to data related to the organisations to which Health Care Providers may belong).



4. List of Service Levels

1. UAM		
Identification/Authentication		
Login ehealth < 1 sec	Performance	98,00%
Module for quality checks and relationships		
CLC	Availability	99,50%
CLC < 4 sec	Performance	95,00%
Authorization Module		
I. AM AA (Attribute Authority - major authentic source)	Availability	99,50%
I. AM AA (Attribute Authority - minor authentic source)	Availability	99,50%
I. AM AA (Attribute Authority - external authentic source)	Availability	99,50%
UAM PDP ("PEP")	Availability	99,50%
I.AM (scénario simple) < 1,5 sec	Performance	98,00%
I.AM (scénario global) < 4 sec	Performance	90,00%
STS	Availability	99,50%
STS < 4 sec	Performance	98,00%
S2S SYSTEM_WS	Availability	99,50%
S2S SYSTEM_WS < 1,5 sec	Performance	98,00%

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



5. Detailed Service Level per service

5.1. Checking of qualities and relationships: Availability

5.1.1. Availability: Checking of qualities and relationships Service

5.1.1.1. Definition(s)

Percentage of time the checking of qualities and relationships has been available based on regular monitoring.

The service is considered as available when a successful response is provided at each access by the monitoring script. Successful responses are all front web application and / or web service responses which are not blocked by the unavailability of a specific component needed to route a request from its reception at a front web application and / or web service till the answer is delivered.

5.1.1.2. KPI Objectives

Ensure that the specific components involved in the Checking of qualities and relationships steps are available on the eHealth platform.

5.1.1.3. Measurement method

Every two minutes, a monitoring script runs in order to measure the availability of the module of checking qualities and relations of a user.

A hit is an access to the front web application and / or web service of eHealth.

A successful hit is an access to the front web application and / or web service of eHealth with a response excluding any component unavailability.

Therefore, this KPI measures the availability of the checking of qualities and relationships functionalities at the front web application and / or web service by a monitoring script.

5.1.1.4. KPI Formula

$$UIA1 = (\sum NSH / \sum NH) \times 100$$

where

NSH = Number of Successful Hits

NH = Number of well-formed Hits received

UIA1 is the KPI for availability of the checking of qualities and relationships service.

5.1.1.5. Calculation window

Monthly (with a minimum of 100 hits per month).

5.2. Checking of qualities and relationships: Response time

5.2.1. Response time: checking of qualities and relationships service

5.2.1.1. Definition(s)

Time spent between receiving a request for checking of qualities and relationships on the eHealth infrastructure and returning the user an answer (list of organisations and/or mandates) which allows him to proceed (authorisation).



Starting point of the checking of qualities and relationships step is when the application receives a request from the user to proceed with forwarding her / his credentials (password, token); end point is when the application returns a screen to the user with a list of organisations and/or mandates to select from.

5.2.1.2. KPI Objectives

Ensure that each request for checking of qualities and relationships steps is being processed within the response time limit (see Table 1). It ensures the follow-up of the checking of qualities and relationships service performance.

5.2.1.3. Measurement method

The response time is the answering time registered for all successful requests, as obtained from logs of incoming and outgoing requests on the components involved, i.e. as measured between starting and end point on the eHealth Portal.

The key performance indicator measures the percentile corresponding to values below the response time limit.

5.2.1.4. KPI Formula

Compute the percentile corresponding to values below the agreed KPI for the response time

$$UIA2 = \frac{\Sigma (\text{successful request with an answering time within the response time limit})}{\Sigma (\text{successful request})} \times 100 \%$$

where

UIA2 is the KPI for the response time of the checking of qualities and relationships service.

5.2.1.5. Calculation window

Monthly (with a minimum of 100 hits per month).

5.3. Authorisation service: Availability

5.3.1. Availability: Authorisation Service

5.3.1.1. Definition(s)

Percentage of time the authorisation service has been available based on regular monitoring.

Begin point of the authorisation service is from a faked user confirmation of a mandate (or none), and an organisation (or none). The begin point starts from the confirmation entering into the PEP component. The end point is when the PEP component returns an answer to the application, with either an authorisation or a denial to the request for gaining access to the application.

5.3.1.2. KPI Objectives

Ensure that the specific components involved in the authorisation service are available on the eHealth platform.

The service is considered as available when a successful response is provided at each monitoring request for authorisation. Successful responses are all web service and other components responses which are not blocked by the unavailability of a specific component needed to route a request from its reception at the PEP till an application screen is provided, with either authorisation or denial of access.



5.3.1.3. *Measurement method*

The availability of the module of authorisation is measured on basis of the availability of the module of consultation of the authentic sources. This availability is measured through the follow-up with intervals of minimum 2 minutes of the availability of the module.

A hit is an access to the PEP service component of the eHealth platform.

A successful hit is an access to the PEP resulting in a response excluding any component unavailability (i.e. a response of either authorisation or denial of access).

Therefore, this KPI measures the availability of the eHealth authorisation service.

5.3.1.4. *KPI Formula*

$$UIA3 = (\sum NSH / \sum NH) \times 100$$

where

NSH = Number of Successful Hits

NH = Number of well-formed Hits received

UAS1 is the KPI for the authorisation service.

5.3.1.5. *Calculation window*

Monthly (with a minimum of 100 hits per month).

5.4. Authorisation service: Response time

5.4.1. Response time: Authorisation service

5.4.1.1. *Definition(s)*

Time spent between receiving a request for authorisation on the eHealth infrastructure and returning the user an answer (application screen with authorisation or denial of access).

Starting point of the authorisation service is when the user clicks on a button to confirm her / his selection of a mandate (or none), and an organisation (or none), in other words when the user request is entering the PEP component; end point is when the PEP component returns an answer to the application, with either an authorisation or a denial to the request for gaining access to the application.

5.4.1.2. *KPI Objectives*

Ensure that each request for authorisation handled through the eHealth platform is being processed within the response time limit (see Table 1). It ensures the follow-up of the authorisation service performance.

The eHealth Platform identifies 2 distinct scenario's type with 2 distinct service level expectations:

- scenarios integrating the new UAM components,
- scenarios still needing to be adapted³ or complex scenarios of Orthopride, Medic-e, e-Birth, Safe, Quermid, ZNA Elimzo, Vesta.

5.4.1.3. *Measurement method*

The response time is the answering time registered for all successful requests, as obtained from logs of incoming and outgoing requests on the components involved, i.e. as measured between begin and end point.

The key performance indicator measures the percentile corresponding to values below the response time limit.

³ There is a minimum proof period of 6 month for new scenario's implemented

The measurement of the response time of the module of authorisation is applied only to the scenarios integrating the new components of the UAM. These components must be adapted for the complex scenarios of Quermid.

5.4.1.4. KPI Formula

Compute the percentile corresponding to values below the agreed KPI for the response time

$$\text{UIA4, UIA5} = \frac{\sum (\text{successful request with an answering time within the response time limit})}{\sum (\text{successful request})} \times 100 \%$$

where

UIA4 is the KPI for the response time of the authorisation service for scenarios integrating the new UAM components.

UIA5 is the KPI for the response time of the authorisation service for scenarios still needing to be adapted or complex scenarios.

5.4.1.5. Calculation window

Monthly (with a minimum of 100 hits per month).

