MASTER SERVICE AGREEMENT

Mission: eHealth core services

Reference: **MSA-eHealth**

Version: 7.0

Date: September 12th, 2025

This MSA including its attachments is made between:

eHealth

(Hereafter referred to as “Constituent”)

and:

Smals

(Hereafter referred to as “Service Provider”)

Table of content

1. Management of this document

1.1. Version Management

Table below gives an overview of the different versions which were discussed and/or approved with the Constituent. Approved versions always have a version reference X.0. Intermediate versions have a version reference X.Y

Version	Date	Author	Description of the changes
2.0	Feb 13th, 2012	C. Pouliakis	Update after meeting Feb 10th
3.0	Dec 16th, 2013	P. Hollande	3rd approved version after meeting on 13/12/13 between eHealth Service Management and Smals Service Management
4.0	Dec 12th, 2014	P. Hollande	Approved version after confirmation at meeting on 9/12/14 with eHealth Service Management.
5.0	Jun 23rd, 2016	P. Hollande	5th approved version
6.0	May 23rd, 2022	P. Hollande	6th approved version
6.1	June 16th, 2025	P. Hollande	Synchronisation with last template and adaptation of the working hours of the Contact Center
6.2	September 1st, 2025	P. Hollande / P. Heller	Update after first review of eH.
7.0	September 12th, 2025	P. Hollande	7th approved version

1.2. Document distribution

Every approved version of this document will be distributed to the following people by e-mail.

Name	Function	Organisation
Mr. F. Robben	Administrateur Generaal	eHealth
Mr. M. Stuckens	Service manager	eHealth
Mrs. A.-S. Gewelt	Communication manager	eHealth
Kurt Maekelberghe	Security manager	eHealth
Mr. P. Heller	Service Delivery expert	eHealth
Mrs. K. Guenter	Service Delivery	eHealth
Mr. J.-L. Vanneste	Director ICT & Operations	Smals
Mr. S. Akkermans	Service Manager eHealth (&VAS)	Smals
Mrs. D. Puttaert	Gestionnaire Clients	Smals

1.3. Related documents[1]

Title	Date	Author
SLA Certificates		P. Hollande
SLA CoBRHA / CoBRHA+		P. Hollande
SLA Timestamping		P. Hollande
SLA Consult RN		P. Hollande
SLA User Access Management		P. Hollande
SLA IAM STS		P. Hollande
SLA IAM SSO		P. Hollande
SLA Coding		P. Hollande
SLA E2E encryption		P. Hollande
SLA Portal eHealth		P. Hollande
SLA eHealth Box		P. Hollande
SLA Consent		P. Hollande
SLA Metahub		P. Hollande
SLA Therapeutic Links		P. Hollande
SLA Therapeutic Exclusion		P. Hollande
SLA Link		P. Hollande
SLA ID Support		P. Hollande
SLA AddressBook		P. Hollande
SLA Unique Portal (IANUA/UPPAD)		P. Hollande
SLA eH2eBox		P. Hollande
SLA DaaS		P. Hollande
SLA Directory		P. Hollande
SLA Link		P. Hollande
SLA API Gateway		P. Hollande
SLA Pseudonymisation		P. Hollande
SLA Matrix		P. Hollande
SLA ESB		P. Hollande
SLA Software Registry		P; Hollande
IAM Connect - Exchange		P; Hollande
IAM Connect – Token		P; Hollande
IAM Metadata		
(SLA SecLog)		P. Hollande

[1] Status of the annexes at the time of finalization of this SLA. This list will not be systematically updated during subsequent developments or if additional documents are created.

Procesbeschrijving “Aanvraag en beheer van Certificaten”	A. Lips
General Change and Release Management Process description	Ph. Dellisse
Release Policy pour le service eHealth	Ph. Dellisse
eHealth Standard Changes list	
ASM	D. Puttaert
BSM’s	D. Puttaert

2. Objectives and Scope

2.1. Objective of the Master Service Agreement (MSA)

The objective of this document is to:

- Define a framework in which Service Level Agreements can be developed for all the Basic Services available on the different environment of the eHealth platform, taking into account their changing role.
- Formalize the general directives in order to obtain quality Service descriptions, reporting and Service enhancement. Directives are:
    - Service levels will provide a mutual understanding of Service level definition, expectations and their measurement methods.
    - Every KPI will have 2 SLO's defined:
        - The minimum (committed) Service level guaranteed by Service Provider
        - The target Service level = The expected Service level
    - List of reports to be provided
        - Monthly report containing:
            - SLA reporting
            - Incident and Problem reporting
            - Incident and Change performance reporting
            - Contact Center / supervision performance reporting
            - General evaluation of the Service
- Centralize all information that is common to all Services such as Service descriptions, generic process descriptions, standard definitions, etc.
- This document, as well as the SLA's for the different Basic Services, describes in an unambiguous way the commitments, responsibilities and objectives of the parties involved.
- The process of setting objectives, evaluating the delivered quality against these objectives and developing Service Improvement Plans, will enhance the delivered quality, so that it will meet the (changing) expectations of the Constituent.
- This MSA defines the directives to be respected by both Smals and eHealth platform regarding the delivery of eHealth services. Approval of both parties is needed before publication of this document or parts of it.
- ”

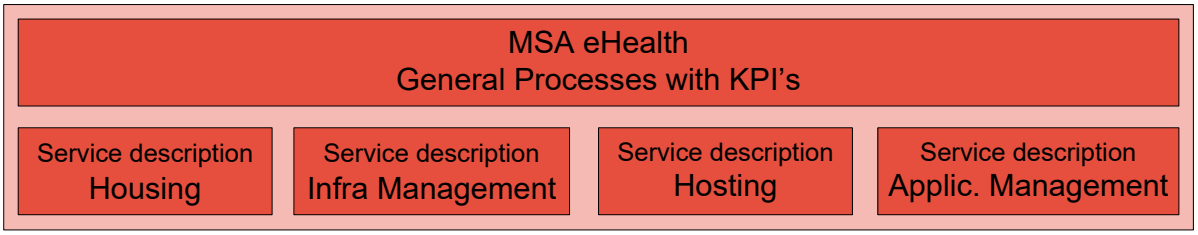
2.2. Positioning of the Master Service Agreement and the relation with its attachments

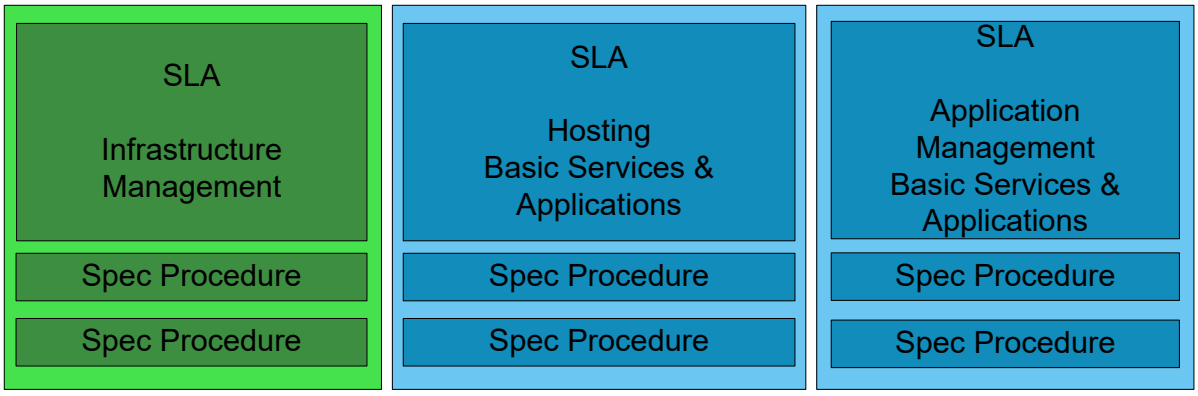
The MSA contains commitments, procedures, Service descriptions and other specifications that are generic for all the activities performed in the scope of eHealth.

The different SLA's contain commitments, procedures and Service Level Objectives specific to the concerned Basic Service.

Service structure is documented in "Attachment 01 – Service Structure"

- Infrastructure Services (green)
  - Housing: Use of Datacenter facilities
  - Infrastructure Management: Management of hardware, Operating System, Middleware and Database
- Application Services (blue)
  - Hosting: Release management, monitoring and Incident detection
  - Management: Hosting and Support (Incident and Problem management)





2.3. Scope

This document contains or refers to:

- General Terms & Conditions
- Collaboration procedures
- Governance

This Master Service Agreement is applicable to the Basic Services available on the eHealth platform. The Services to be delivered are not the same for all Basic Services. Following chapters give a detailed scope for the different Basic Services.

2.3.1. Infrastructure management

Infrastructure management Services are delivered on all the Infrastructure components of eHealth environments.

The Production environment is installed in two separate datacenters or Availability Zones (AZ). Each AZ is capable of running the whole production workload. Both AZ are always-on and constantly syncing data. In case of incident in one AZ, the other AZ will take over the whole production workload.

Each AZ is subdivided into three Fault Domains (FD). The Fault Domains are an independent hardware layer, aiding into the high availability of each AZ. The business applications can run on two FD, so an incident or intervention on one FD will not have business impact.

There are four environments:

- The Production environment
- The Acceptance environment
- The Integration environment (INT-RC & INT)
- The Test environment

The production equipment covered by this Service can be found in the CMDB-Cartography which keeps up-to-date information about installed equipment. The Constituent has access to this information.

All new CI's installed in the eHealth environment during the validity period of this SLA will automatically be added to the scope of the MSA/SLA.

2.3.2. Application Management of Services

Application management Services are delivered for following Basic Services of the eHealth environment.

- Portal eHealth
- User Access Management eHealth (only User Management, WALI)
- Certificates
- AddressBook

The SLO's for each of the Basic Services are defined in separate SLA's.

2.3.3. [2]Application Hosting of Services

Hosting Services are delivered for following Basic Services of the eHealth environment.

- UAM (Remaph, IAM, , STS, SSO, Metadata, IAM Connect)
- Timestamping
- Coding
- EHealth Box
- eH2eBox
- RN consult
- Loggings
- End to end encryption
- Metahub (Reference Directory and Hub Implementation)
- Consent
- Therapeutic Links
- Therapeutic exclusion
- Link
- Matrix
- Directory
- Orchestration (API Gateway, ESB/SOA)
- Validated Authentic Source (CoBRHA & CoBRHA+) of healthcare providers
- ID Support
- Unique Portal (IANUA /UPPAD)
- DAta Attribute Service (DaaS)
- Pseudonymisation
- Software Registry

The SLO's for each of the Basic Services are defined in distinct SLA's.

2.3.4. Business Operation Services

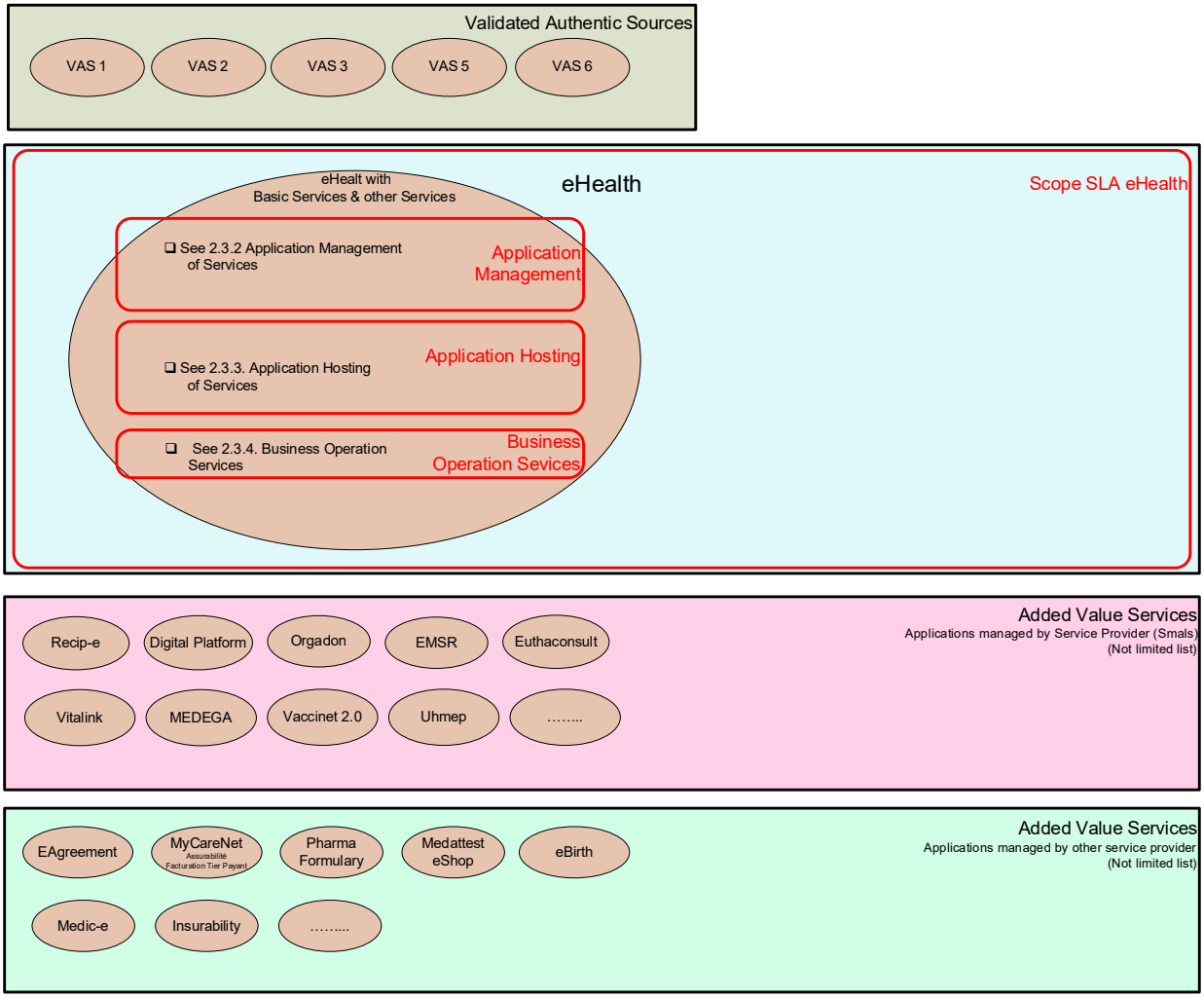
Business Operation Services are delivered for following Basic Services of the eHealth environment.

- Standard (First line support on kmehr/standards related question)
- Any Software, tool, library, … published by eHealth (First line support and afterwards 2nd line support) (e.g. the Sumher Validation tool, connectors, …)
- Business and Integration Support

[2] List of the applications at the time of finalization of this SLA. This list will not be systematically updated during subsequent developments or if additional documents are created

2.3.5. Graphical overview of the eHealth scope

Following picture gives an example of the different Services within (and outside) the Scope of this MSA in the production environment



Some components as for the simulation hub are only covered in the acceptance environment.

2.3.6. Service management

This Master Service Agreement describes the ITIL processes used to deliver services within the scope of the eHealth platform. For the different processes, Key Performance Indicators (KPI) will be defined, measured, reported to the Constituent and where needed, Service Improvement Plans will be put in place by Service Managers.

The Service Provider is responsible for collecting the raw data necessary to calculate the Key Performance Indicators (KPI) defined in this document or in attached SLA. Service Provider will check the completeness and the validity of these data calculate the results for the concerned period and produce and publish a Service Level Report.

Processes that are covered in this Master Service Agreement are:

- Incident Management
- Change and Release Management
- Service Level Management
- Capacity Management

Additionally, Problem Management process exists within Service provider (internal process) to reduce amount of incidents and improve the KPI's when needed.

2.3.7. Supported Products

- Specific applications are developed on demand of the Constituent. The support and maintenance strategy will be defined based upon a mutual agreement between Service Provider and Constituent.
- The Service Provider will implement and maintain, as defined in the support and maintenance strategy, the necessary teams to support these specific applications.
- The support feasibility is partly dependent of the support strategy of the hardware and software manufacturers and of the Service Provider. These manufacturers may, for example, decide to stop supporting certain versions/types of their products. This will cause the support strategy to be reviewed and or adapted.
- The needed actions will be taken to avoid lack of support, compatibility problems …etc. This will also be done by mutual agreement.

2.4. Out of Scope

2.4.1. Validated Authentic Sources

For the Validated Authentic Sources outside the responsibility of de Service Provider, no formal commitment will be recorded unless the owner of the Validated Authentic Sources accepts to provide an SLA on the Service he delivers or a copy of the Validated Authentic Sources exists in the managed infrastructure. However, where ever possible, an End-to-end KPI will be defined, measured and reported. A not binding target will then also be defined. A Validated Authentic Sources will not have a specific SLO. The SLO for a Validated Authentic Sources will be included in the SLO of the Basic Service using these Validated Authentic Sources.

In addition, the Service Provider hosts several authentic sources or copy of them for the Constituent. The consultation interfaces to those validated authentic source are in the scope of this MSA.

2.4.2. Value Added Services

The Value Added Services or “VAS” using the Basic Services of eHealth, can have a specific SLA for the VAS itself. This SLA is out of scope of this MSA and may be provided by the company providing the Service.

The Constituent, as owner of the Basic Services, has published SLA’s (Public SLA) for the different Basic Services on the eHealth Portal. This MSA and related SLA’s support the Public SLA’s.

The Service Provider will not offer an SLA for the use of eHealth Basic Services towards the owner of an VAS.

Nevertheless, it is the Service Providers responsibility to identify any specific business incident related to the VAS, addressed to the eHealth first line support and to redirect them towards their respective first line support. Collaboration agreements with major partners describing the service interactions will be developed.

2.5. Risks, conditions and dependencies

2.5.1. Hosting of Basic Services and VAS

Basic Services not developed by the Service Provider, will be submitted for testing prior to Acceptance and deployment on the eHealth production environment.

2.5.2. Case of Force Majeure

The Service Provider can’t be held responsible of non-compliance with its commitments in case of termination, interruption or delay of services due to earthquake, flood, fire, storm, natural disaster, war, hostilities (including Computer Crimes) or any other event which can be considered as a case of force majeure (event characterised according to the classic legal criteria of externality, unpredictability and irresistibility).

If necessary, the Service Provider will inform the Constituent and will make every effort to minimise any damage due to force majeure and to come back to his commitments within a reasonable period.

2.5.3. Conditions

In case of Disaster, the SLA's only stay active if the Constituent have a DRP foreseen for the same kind of scenario, known by the Service Provider and tested (like foreseen in the DRP) on regular basis.

In all other cases, the SLA's are temporary put on hold and will be reactivated after restore of the normal conditions.

2.5.4. Dependencies

Many Services are complex and involve components managed by different Partners, Service Providers, or Constituents. In the various SLAs, the scope of the Services to be delivered is defined as precisely as possible. However, it is not always possible to monitor only the defined scope. Instead, the end-to-end flow is monitored. During the reporting process, certain periods of unavailability can be corrected (reported as available) when the cause of the unavailability is due to an element outside the scope of the SLA.

2.6. Responsibilities of the Constituent

- The Constituent reports every deficiency as soon as possible to the Service Provider using the appropriate procedure. See Ch. 5.2.5
- The Constituent makes sure that the Hosted Basic Services it develops use the resources, offered by the infrastructure, conforming the specifications.
- The Constituent makes sure that the Users have been informed about the relevant procedures and that they respect them.
- For all Hosted Basic Services (see Ch. 2.3.3), the Constituent supports the 3rd level support.
- Constituent ensures an appropriate handover (training and documentation) of service developed by eHealth to the Service Provider so that monitoring can be implemented as well as the 1st and 2nd level support. In addition the Constituent defines requirements (SLO's) in order to let the Service Provider develop the appropriate monitoring.
- The Constituent communicates to the Service Provider the contact details of VAS first line support.
- Deliver 3rd line Support for Hosted Services in Production and Acceptance environments and 1st, 2nd and 3rd line Support for Services in Test and Integration environment.
- The Constituent communicates to the Service Provider when (a part) of the Service / SLA should be adapted due to legal or rule evolutions. The Constituent should evaluate any change of the needed capacity and inform the Service Provider as soon as possible.
- Where an SLA is agreed with a Service Window 'Mon – Sun 0:00 – 24:00' where part of the Service is delivered by the Sponsor or a third party on behalf of the Constituent, the Service Provider expects the Sponsor to also have on-call service (Mon – Sun 0:00 – 24:00) available from the Sponsor or the third party.

2.7. Implementation of the SLA's

The definition of the SLO for the new eHealth Basic Services (or implementation of a major release) as well as for the ITIL processes will be done on a pragmatic base. During a start-up phase (3 months as of the use in Production environment, can be extended in case of lack of traffic on the service), the results will be measured, reported and compared to the 3 SLO's mentioned in Ch. 2.1 "Objective of the Master Service Agreement (MSA)". Service Improvement Plans (SIP) will be put in place to achieve timely the "expected committed Service level for next years".

At the end of the start-up phase, the SLO will be fixed by mutual agreement (Constituent and Service Provider). This will be done by taking into account the achievements during the start-up phase, the statistical information about the installed equipment (MTBF, MTTR) and the degree of redundancy built into the infrastructure. The identified risks are also to be taken into consideration. An enhancement of the SLO requires that the identified risks are eliminated or at least monitored and mitigated.

All Service Improvement Plans will be evaluated by both the Service Provider and the Constituent to define the budgetary impact as well as the influence on the overall quality (availability, stability, performance, etc…)

2.8. Confidentiality

- By virtue of this agreement, the parties may have access to information that is confidential to one another ("Confidential Information")
- Confidential Information shall be limited to
    - All documentation and/or data obtained before, during or after the mission.
    - All documentation, information and/or data stored at the Service Providers premises and within the scope of this mission.
    - All minutes and reports related to this mission
- Each party shall

    (a) keep secret and confidential, and procure that its officers, employees and representatives keep secret and confidential, all Confidential Information of the other party.

    (b) use the same degree of care in relation to the Confidential Information of the other party as it normally uses to avoid unauthorized disclosure of its own confidential information;

    (c) use, and procure that its Representatives use the Confidential Information of the other party only in the performance of the party's obligations or the exercise of its rights under the Agreement;

    (d) only disclose to its Representatives Confidential Information of the other party that is reasonably required for the performance of the disclosing party's obligations or the exercise of its rights under this Agreement, inform them of the confidential nature of the Confidential Information, and obtain, if desirable, written confidentiality undertakings from them consistent with this clause;

    (e) promptly notify the other of any suspected or actual unauthorized disclosure of the Confidential Information of the other party and take all reasonable steps to prevent, limit or remedy the disclosure.
- All parties agree, unless required by law, not to make each other's Confidential Information available in any form to any third party for any purpose other than the implementation of the activities required for the eHealth platform Services.
- All personal data will be handled as determined in the Belgian law C-2018/40581 on 30 july 2018 (law on the protection of individuals with regard of the processing of personal data).

2.9. Start and evaluation of the MSA

- This MSA takes effect on January 1st 2012, and remains active as long as it is confirmed by a BSM. The BSM is the official mission. The MSA describes the quality and operating procedures of the Services / deliverables mentioned in the BSM. The MSA and the BSM are therefore inseparable.
- The evaluation of the delivered Services is done on a regular basis (see Ch. 4.2 Steering meetings)
- Once a year, the year results will be evaluated as well as the content of the MSA and related SLA's. The MSA and related SLA's can be modified as described in Ch. "2.10 Modifications to the MSA and related documents". Related documents (e.g. SLA) can have start dates different from the MSA start date.

2.10.Modifications to the MSA and related documents

- Every request by the Constituent to change the contents (like activities, equipment, applications, Services or Service objectives) of this MSA and the related SLA will officially be sent to the Service Manager of the Service Provider.
- Similarly, the Service Manager of the Service Provider can submit requests for modification to this MSA to the Service Manager of the Constituent.
- The Changes will become active as soon as the MSA and SLA have been agreed upon and the necessary changes have been made to the BSM.
- Minor modifications to the scope of this MSA will be confirmed in the minutes of the Steering Meetings or by issuing a BSM. The MSA scope will be updated yearly.

2.11.Renewal of the mission

- Without a cancellation notice from the Constituent, the mission will be automatically renewed. This mission will also be confirmed by respective BSM

2.12.Notice periods and early termination

- The notice periods for early termination of an element or of the mission are described in the ASM and the BSM.
- As with the start-up of the Services by the Service Provider, a project will also be started upon termination in which all transition modalities are described and implemented. In this way, the data/applications, which have been stored or processed on the infrastructure of the Service Provider, are transferred to the Constituent or the owner(s) of the data.

3. Definitions

When referring to the Definitions in this Chapter, capital letters will always be used (in this and related documents)

Some definitions hereunder only appear in a limited amount of SLA. However, we keep these definitions because they are essential to avoid any confusion (for example in the documents, conversations or e–mails).

The definitions hereunder are generally used. If another definition is applicable, it will be mentioned the de specific definitions of the concerned SLA.

3.1. General definitions

Production environment

The environment that offers live eHealth Services to the end-users

Acceptance environment

The environment used by the development teams (Constituent and Service Provider) to test the Production readiness of a eHealth Service, and by partners to validate the integration of their VAS Services for R+1

Integration (INT-RC & INT)

The environment used by the development teams (Constituent and Service Provider) to test correct interaction with other eHealth components and Infrastructure

Test environment(s)

The environment(s) used by the development teams of the Constituent to test eHealth Services

Archiving

The process of moving data of a primary storage device (such as a hard drive) onto a secondary storage device (such as a backup tape), for permanent storage.

Back-up

Copying data to protect against loss of Integrity or Availability of the original

Restore

Replacing copied data (see Back-up) in order to recover lost or corrupted data.

Mission

The set of Services to be provided by the Service Provider following a demand from the Constituent

Process

A structured set of activities designed to accomplish a specific Objective.

Service

A Service is defined, within the context of Service management, as a logical grouping of functionality that is made available through the combination and specific configuration of hard- and software CI's.

A Service can also consist of one or more activities or Processes executed manually by an employee or a team of employees.

Constituent

Member Institution of the non-profit-making organization Smals (Service Provider), who has mandated a Mission to the Service Provider and who is signing this SLA

Service Provider

Institution providing the IT services to the Constituent and signing partner to this SLA. When performing this Mission, the Service Provider may call on external contractors or the collaboration of the Constituent or Partners.

User

Organisation which uses the Services offered by the Service Provider. The User can be different from the Constituent.

End-user

A person, an institution, an external IT Service or an IT application who uses the IT Service.

Partner

Organisation, company which is neither the Constituent nor the Service Provider, but which can or must perform a number of activities in order to complete the Service.

Customer

A person, an institution, an external IT Service or an IT application who has integrated eHealth IT services in their specific IT Services or applications. Customers are distinct from End-user, as some customers do not use the IT Service directly.

Key-User

Employee from a Partner, a User, the Constituent or the Service Provider who deep knowlegde of a specific application or Service and who performs specific activities (e.g. Tester, first line support).

Closing days of Smals

All Saturdays and Sundays.

1 January, 2 January, Easter Monday, 1 may, Ascension day, White Monday, 21 July, 15 August, 1 November, 2 November,11 November, 15 November, 25 December, 26 December which are considered as Sundays.

Working hours (wh)

All Smals working days between 8:00 and 16:30. There is no relation between Working hours and Service Window and/or Support Window.

Working days (wd)

All weekdays except Closing days of Smals.

Service Window

Agreed time period during which a particular IT Service must be available and during which technical support must be available. For example, "Monday-Friday 08:00 to 17:00 except Closing Days of Smals". Service Window is defined in the Service Level Agreement in dark green.

Extended Service Window

Agreed time period during which a particular IT Service may be available but during which no technical support is be available (no corrective action taken to restore the Service in case of unavailability. Extended Service Window is defined in the Service Level Agreement in light green.

Service hours (serv.h)

All hours within the Service Window

Support Window

An agreed time period during which support can be reached by the Users. Typically this is the period when the Service Desk is available. The Support Window may differ according to the support team.

Opening hours of the Contact Center

All Working days between 8:00 and 18:00.

Support hours (sup.h)

All hours within the Support Window for the related support team

Maintenance Windows for Planned Interventions

An agreed time period during which Changes or Releases may be implemented with minimal impact on Services. Maintenance Windows are defined in the Service Level Agreement.

Downtime

Time during which an (IT) Service is not available

Detection time **(see also 5.2.4.)**

Time from the moment the incident occurs and the moment the incident is identified by the user or a monitoring service (still not communicated to the Service desk or the supervision). This period of time precedes the Response time.

Response time **(see also 5.2.4.)**

Time between a user or a monitoring service tries to communicate an identified incident or an event to the service desk and the moment the service desk respond to the event. (e.g. number of ring bell, time before a mail is being treated, time before an alert is being treated). This period of time precedes the Reaction time.

Reaction time **(see also 5.2.4.)**

The time between the moment that the Service Desk is informed of an event (or the moment which an incident is detected via the monitoring) and the moment that a ticket is created, including its assignment to a group for resolution. This period of time precedes the resolution time.

Resolution time **(see also 5.2.4.)**

The time from the initial assignment of ticket till the ticket is considered completed, in other words that an answer has been communicated for a request for information or a solution has been implemented.

Treatment time **(see also 5.2.4.)**

Time from the moment a user or a monitoring service tries to communicate an identified incident or an event to the service desk till the ticket is considered completed, in other words that an answer has been communicated for a request for information or a solution has been implemented. It's the Response time + Reaction time + Resolution time.

Implementation time

Time between registration of the request (RFC) and its realization (unless explicitly described otherwise in the description of the relevant RFC)

Configuration Item (CI)

A hard- or software component of the IT infrastructure. Software license certificates and documents can also be considered as Configuration Items.

System Software

Basic software as MS Windows, Linux, Oracle, etc.

Application Software

Software developed in order to meet specific Constituent requirements

---

Master Service Agreement (MSA)

An Agreement between an (IT) Service Provider and a Constituent. The MSA contains general descriptions and agreements applicable for all the Service Level Agreements with this Constituent.

Service Level Agreement (SLA)

An Agreement between an (IT) Service Provider and a Constituent. The SLA describes the IT Service, documents Service Level Objectives, and specifies the responsibilities of the IT Service Provider and the Constituent.

Underpinning Contract (UC)

An agreement between the Service Provider and a third party. This third party can be an external service provider, the Constituent or a Partner.

KPI (Key Performance Indicator)

A metric that is used to help manage a Process, Service or activity.Most of the KPI's concern Availability of Performance of a Process, Service or activity. For each KPI, a description of what it represents, how is it measured, calculated and evaluated is provided. A Service Level Objective is also associated.

Service Level Objective (SLO)

A commitment that is documented in a Service Level Agreement. Service Level Objectives are based on Service Level Requirements, and are needed to ensure that the IT Service quality is fit for purpose. Service Level Objectives are the target of the KPIs.

Availability of an environment or an application

Availability is usually calculated as a percentage of time the IT Service, the environment or the application is able to perform its agreed function. This calculation is based on the Agreed Service Window and Downtime.

Performance

The extent to which the available functionalities are performed efficiently. The concrete definition of Performance for a given Service can be found in the "Definition" section of the KPI for Performance.

Conformity

The extent to which a goal (e.g. Resolution Time) is achieved.

Service Desk

Point of contact for all the Service Requests. The Service Desk consists of the Contact Center, Supervision and Business and Integration Support.

Contact Center

Single point of contact for end-users and customers, first line.

Supervision

Second line of support with regards to IT operation matters. Nevertheless, the supervision is a privilege point of contact with major partner's Helpdesks.

Business and integration Support

The Service for integration support helps customers to integrate their service(s) into the eHealth environments. This support is given on both, Production and Acceptance, environments.

Roles and Responsibilities:

- Help the 1° line resolving issues about applications and services in Production (and Acceptance)
- Inform customers (only the restricted list) when the incidents are more technical
- Integration support (in Acceptance & Production) : act as "Gate Keeper"
- Update tickets and keep the 1° line support informed of the progress of each ticket
- Manage (update) the WebForm with new and to be deleted SAC's
- Manage all support documentation (Smals, eHealth & Partners)
- Populate the know-how database (FAQs,…) with regular upcoming incidents/problems
- Document Flow Validation Process
- Advanced reporting on the achievement of SLA for all incidents, and communicate these reports to the Service Management and Management Teams

Helpdesk / Self Service Portal

Single point of Contact is the area of Bureautica Services.

Support Request (SR)

Total set of Requests: Request for incident resolution, Information, Change and Support improvement

Request for Change (RFC)

A means of proposing a Change to any component of an IT Infrastructure or any aspect of an IT Service

Request for Incident resolution (INC)

Request for the resolution of an unplanned interruption to a Service or a reduction in the Quality or the Service Failure of a Configuration Item that has not yet impacted Service(for example : failure of one disk from a mirror set).

Request for Information (RFI)

Request for an answer to a Service-related question.

Request for Support Improvement

Request for improvement of the manner in which support is provided. This type of request is also referred to as a "complaint".

Release

A group of Changes that are tested, packaged and deployed into the IT Infrastructure at the same time.

IT Infrastructure Release

A Release specifically applicable to the IT infrastructure

Applicative Release

A Release specific to applications.

Incident

Any event deviating from the (expected) standard operation of a system.

Incident Management

The process that takes care of the handling of questions, wishes and disruptions.

Technical Incident

An Incident that results in unavailability, slowness or instability. The cause of these Technical Incidents can usually be found in the Infrastructure or the Software.

Applicative Incident

An Incident that results in functional errors. Some functionalities may be unavailable or performed/calculated incorrectly. A solution can only be brought here by adjusting the Application Software (via Patch or Release)

Security Incident

Incident that could affect the confidentiality of the data handled by/at the Service Provider. Some of these Incidents may be subject to GDPR regulation

Functional / Applicative question

A question that focuses on the understanding how the application works.

The application works correctly, but the End User does not know (exactly) how to use it.

Content question

A question that focuses on the use of the application in a specific case. What are the applicable rules/laws in this case?

The application works correctly, the End User knows the different possibilities and functionalities of the application, but he does not know how to introduce this concrete situation.

Impact

The extent to which the Constituent or User experiences (negative) influence from an Incident, Problem or Change that occurs.

The concrete details of the Impact in the event of an Incident can be found in paragraph 5.2.2.1.

Urgency

Measurement of the time after which an incident, problem or change has a significant impact on the business.

Priority

The Priority of an Incident is determined on the basis of Service Level and Impact. This Priority affects the order in which Incidents are handled within the Incident Management process.

The concrete determination of the Priority of an Incident can be found in paragraph 5.2.2.1.

Disaster

An unplanned situation that, due to its origin and/or size, has a significant influence on the availability (and/or performance) of one or more Services.

Infrastructure

All Hardware, Software, buildings, procedures and documentation.

Equipment / Hardware

All material components of the environment such as servers, storage, network components, cables, communication lines, PCs or printers.

Software

The set of programs required to make an environment function. This consists of System Software and Application Software.

System Software

Basic software like Operating Systems, Middleware of Databases.

Application Software

Software that has been developed to meet specific needs/wishes of the Constituent

Tenant

(Co) User of a (shared) IT environment in the context of Cloud Computing.

Multi-Tenant

Multi-tenant is a terms / Architecture used in Cloud Computing for the case where several Users use the same public or private Cloud. Each tenant's data is segregated and invisible to the other tenants.

Patch

Small piece of software used by the Software publisher to fix errors or perform updates.

3.2. Levels of Service

The measure of reliability and robustness of a Service. The Service Level is defined at the start of the Mission and is dependent on the installed infrastructure and used system software.

The I&S Governance Board can validate the requested level by analyzing the foreseen I&S infrastructure blocks.

Other factors may possibly influence the Service Level. There is no formal description of this influence.

The Service Level only has an influence on the Priority in Incident Management.

3.2.1. Summary of the conditions to join a particular Service Level

Service Level Best Effort

An SLA can have the Service Level Best Effort when for one or another reason (non-predefined) and independent of the used infrastructure only very limited guaranty can be offered.

Service Level Bronze

An SLA can have the Service Level Bronze when following conditions are met:

- The different infrastructure layers used have a level of at least Bronze.
- Service coordination is performed by Supervision/Back Office.
- There is at least Infrastructure monitoring provided.

Note: the Non-PROD environments usually fall under Bronze.

Service Level Silver

An SLA can have the Service Level Silver when following conditions are met, in addition to those of Bronze:

- The different infrastructure layers used have a Level of at least Silver. The can be achieved based on Silver level building blocks or through a combination of lower level building blocks that together meet the Silver level requirements.
- There is always some form of duplication of the infrastructure.
- An Acceptance environment is always provided.
- In addition to infrastructure monitoring, Application monitoring is also provided[3].

Service Level Gold

An SLA can have the Service Level Gold when following conditions are met, in addition to those of Silver:

- The different infrastructure layers used have a level of at least Gold. This can be achieved by using Gold level building blocks or by a combination of lower level building blocks that together meet the Gold level requirements.
- A Test environment and an Acceptance environment are always provided.
- Service coordination is performed by a dedicated Technical Coordinator (TC) or Service Delivery Manager.
- The Release Management Process applies to both Infrastructure and Application[1].

[3] If the Service contains Application Software

Service Level Platinum

- An SLA can have the Service Level Platinum when following conditions are met, in addition to those of Gold:
- The different Infrastructure Layers used have a level of at least Platinum. This can be achieved using Platinum level building blocks or a combination of lower level building blocks that together meet the Platinum level requirements.
- Service coordination is performed by a dedicated Technical Coordinator (TC) or Service Delivery Manager with backup and Business Duty Manager
- Demand Management (Capacity Management) is implemented
- A DRP test is performed twice a year, one of which is based on a “Datacenter down” scenario.
- A BCP (3rd Data Center) is required when no High Availability Infrastructure is implemented.
- Real time performance monitoring has been implemented.

3.2.2. Summary of the benefits of the different Service Levels

Service Level Best Effort

- Availability for Infrastructure Services: no formal objective
- Availability of Application Services: no formal objective
- Service Window: up to maximum Mon – Fri , 8:00 – 16:30
- Priority Incidents: maximum P5 (with impact HIGH)
- A Service Meeting can be scheduled annually
  Note:
  - There is no communication during the Incident Management process.

Service Level Bronze

- Availability for Infrastructure Services: SLO between 98% to 99%
- Availability of Application Services: SLO between 95% to 98%
- Service Window: up to maximum Mon – Fri , 8:00 – 16:30
- Priority Incidents: maximum P3 (with impact HIGH)
- General Infrastructure Release communication
- A Service Meeting can be scheduled annually

  Note:
  - There is no communication during the Incident Management process.
  - A maximum of 12 x 8 hours of planned downtime per year is foreseen. Other periods can also be agreed with the Constituent.

Service Level Silver

- Availability for Infrastructure Services: SLO between 99% to 99.5%
- Availability of Application Services: SLO between 98% to 99%
- Service Window: up to maximum Mon – Sun , 0:00 – 24:00
- Priority Incidents: maximum P2 (with impact HIGH)
- General Infrastructure Release communication
- A Service Meeting can be scheduled quarterly

  Note:
  - There is no communication during the Incident Management process.
  - A maximum of 12 x 8 hours of planned downtime per year is foreseen. Other periods can also be agreed with the Constituent.

Service Level Gold

- Availability for Infrastructure Services: SLO between 99.5% to 99.9%
- Availability of Application Services: SLO between 99% to 99.5%
- Service Window: up to maximum Mon – Sun , 0:00 – 24:00
- Priority Incidents: maximum P1 (with impact HIGH)
- Incident communication for Incidents with Business impact during Working Hours (email and SMS)
- Incident report (initial version) for Incidents with business impact within 2 Business Days
- Follow-up of the Incidents by the Incident Manager during working hours (Supervision outside working hours)
- General Infrastructure Release communication
- A Service Meeting can be scheduled monthly

Note:

- A maximum of 12 x 8 hours of planned downtime per year is foreseen. Other periods can also be agreed with the Constituent.

Service Level Platinum

- Availability for Infrastructure Services: SLO between 99.9% to 99.95%
- Availability of Application Services: SLO between 99.5% to 99.9%
- Service Window: up to maximum Mon – Sun , 0:00 – 24:00
- Priority Incidents: maximum P1 (with impact HIGH). In case of several Incidents at the same time, those for Platinum will be handled before those for Gold Services.
- Incident communication for Incidents with Business impact during Working Hours (email and SMS)
- Specific communication during crises periods (within and outside working hours): Instant communication Channel
- Incident report (initial version) for Incidents with Business impact within 1 Business Day
- Follow-up of the Incidents by the Incident Manager during working hours
- Business and Infrastructure Duty Manager available 24 hours a day during crisis periods
- Specific and detailed Release communication
- A Service Meeting can be planned according to the Client's wishes
- RPO can be reduced to 0
- RTO: to be determined per Service

Note:

- A maximum of 2 x 30 minutes of planned downtime per year is foreseen for the execution of the major releases. This can also be scheduled outside of Working Hours. Other periods can also be agreed with the Constituent.

3.3. Abbreviations

ASM	Algemene Samenwerkingsmodaliteiten
AZ	Availability Zone
BSM	Bijzondere Samenwerkingsmodaliteiten
CAB	Change Advisory Board
CI	Configuration Item
CoBRHA	Common Base Registry of Healthcare Actors
CSM	Chain Service Manager
DPO	Data Protection Officer
DRP	Disaster Recovery Plan
FD	Fault Domain
GDPR	General Data Protection Regulation
IN	Datacenter Industrielaan, Bruxelles
INC	Incident
I&S	IT Infrastructure, Operations, Services and support
KPI	Key Performance Indicator
P1, P2, P3, P4, P5 & P6	The different priority level
MTBF	Mean Time Between Failure
MTTR	Mean Time To Repair
MSA	Master Service Agreement
OLA	Operational Level Agreement
RFC	Request for Change
RFI	Request for Information
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SDM	Service Delivery Manager
SFPD	Datacenter Esplanade de l'Europe, Saint-Gilles
SLA	Service Level Agreement
SLM	Service Level Management
SLO	Service Level Objective
SPOC	Single point of contact
SIP	Service Improvement Plan
SR	Service Request
SSP	Self Service Portal

UC	Underpinning Contract
UP	Datacenter Quai de Willebroeck, Bruxelles
VAS	Value Added Services

3.4. RGPD

All the terms and conditions regarding the General Data Protection Regulation are described in the specific ASM (chapter 6) and are outside the scope of this MSA. Incidents relating to the GDPR are escalated to the DPO level (of the Constituent and the Service Provider).

3.5. Scope

This MSA applies to all Services delivered to the Constituent by the Service Provider and covered by an SLA from the same Service Provider within the framework of infrastructure and IT project and maintenance service offerings (see ASM, chapters 2.1 and 2.2). Other types of services described in the ASM such as staff training or the provision of specialized personnel (detachment) are not included in the scope.

4. Relationship management

To be able to manage the Service Delivery in an efficient and consistent way, the Constituent and the Service Provider agree to put in place a Relationship Management process. It describes the Relationship roles and the Steering meetings to be put in place.

4.1. Relationship roles

Following roles are defined for the management of the Services delivered in the scope of this MSA and related SLA. The specific names in following table will only be updated once a year.

Table 1. Roles

Role	Description	Service Provider	Constituent
Relationship Manager	Provides information about the Service capabilities of the Service Provider Assures the commercial relationship with the Constituent.	Mrs. D. Puttaert	Mr. M. Stuckens Emmanuel de Hemricourt de Grunne
Service Manager(s)	Is responsible for the quality of the delivered Services.	Mr. S. Akkermans	Mr. M. Stuckens
Service manager Integration VAS	Is responsible for the quality of the Integration of VAS	Mr. S. Akkermans Mr. N. Rogge Mr. S. Dahmane (back-up)	Mr. M. Stuckens
Program Manager	Is responsible for the overall management and coordination of the different subprojects in the health sector.	Mr. S. Akkermans	Mr. M. Stuckens
Development Manager	Is responsible for the development & maintenance of applications	Mr. S. Akkermans	Mr. M. Stuckens
Technical Project Manager	Responsible and SPOC for every infrastructure issue within the project.	Mr. S. Van Buggenhout	Mr. M. Stuckens
Service Delivery Expert Service Delivery	Assistant of Service Manager	See Technical Coordinator	Mr P. Heller Mrs. K. Guenter
Technical Coordinator	Release Manager I&S	Mr. S. Jans Mr. W. Biart Mr. J. Harhellier	Mr. H. De Clercq Mr. F. Libert
SLM	Formalizes the MSA, the SLA and related procedures SLA reporting	Mr. P. Hollande	Mr. M. Stuckens Mr P. Heller Mrs. K. Guenter

4.2. Steering meetings

Following meetings will be organized to discuss the quality of the services delivered in the scope of this MSA and the related SLA.

Table 2. Steering meetings

Meeting	Constituent	Service Provider	Frequency	Agenda
TOP TOP	• CEO (Frank Robben) • Service Manager • Program and development Managers	• Director ICT & Operational Services (Jean Luc Vanneste) • Relationship manager • Service Manager(s)	Monthly	• General evaluation of the delivered Services. • Budget follow-up • Discussion /follow-up of open issues • Discussion/follow-up of "Changes" within the Service
Account Management meeting	• Relationship manager(s) • Service Manager	• Relationship manager • Service Manager(s)	Monthly	• Budget follow-up • BSM follow-up • Invoicing follow-up
Service Management meeting	• Relationship manager • Service Manager • Development Manager • Service Delivery Expert	• Relationship manager • Service Manager •	Monthly or ad hoc	• Discussion/follow-up of the SLA results and evolution. • Follow-up of the Incidents • Planning of Planned interventions
Release Board	• Service Manager(s) • Service Delivery Expert • Development Manager	• Service Manager(s) • Technical Project Managers	Monthly or Ad hoc	• Approval of Major & Minor releases • Approval of Change exceptions
Operational Follow-up meeting	• CEO • Service Manager • Development & Program Managers • Security Resp • Legal Resp • Communications Resp	• Service Managers	Bi weekly	• Services follow-up • Development follow-up
Capacity meeting	• Service Manager • Service Delivery Expert • Service Delivery	• Capacity manager • Service manager • Technical Coordinators • Service Level management		• Status of the capacity • Evaluation for the next months (capacity needs)

Technical meetings	• Service manager • Technical experts	• Service manager • Technical Coordinators	Ad-hoc	• Discussions around Technical issues

4.3. Escalation procedure

4.3.1. Escalation approach

From time to time, issues will arise that cannot be resolved at the various levels of management within the Constituent and Service Provider teams. These issues may arise at a particular site or level. These issues may involve obligations of Party, performance, staff, etc.

Either party may decide an escalation is desirable when the current level of investigation doesn't bring the expected satisfaction, as well as in terms of reactiveness as in the received responses. In that case, either party can make use of the escalation process established.

It is the intent of both parties to resolve issues in a constructive way that reflects the concerns and collaboration interests of each party. Both parties' primary objective and intent is to have issues resolved by the appropriate levels of authority without the need for escalation. With this in mind, the following steps are to be followed:

4.3.2. Escalation process

Most escalations will be handled at the second escalation level by the Service Delivery Experts / Technical Coordinator. Prior to initiate the escalation to the next level, all parties engaged in attempting to resolve the issue, shall make sure that all attempts to resolve the issue have been taken.

Escalations to level 4 should be seen as an exception and should only be initiated if all options to resolve the problem are exhausted and a decision at the executive level is required.

Note that the ticket number created at the Contact Center should be used as reference for all communication regarding the issue and its escalation.

Escalation levels:

Lev	Role	Constituent	Service provider
1	SPOC	**Service Expert**	**Contact Center eHealth** 02-788.51.55. **Supervision** 02-787.59.65
2	Service Delivery Expert	**Service Expert** 02-891.86.31 Philippe.Heller@ehealth.fgov.be eHealth_Service_Management@ehealth.fgov.be back up Karin.guenter@ehealth.fgov.be 02-891.86.67	**Technical Coordinator** W. Biart +3227875760 wesley.biart@smals.be Kristof Camelbeke +3227874813 Kristof.Camelbeke@smals.be Joël Harhellier +3227874835 joel.harhellier@smals.be **On duty Manager** Ad hoc
3	Outsourcing Management	**Service Manager (and the eHealth CEO)** 02-891.86.17 0478-43.56.58 michel.stuckens@ehealth.fgov.be	**Service Manager** 02-787.54.08 0477-70.24.95 sven.akkermans@smals.be
4	Highest management level	**F. Robben** 02-741.84.01 0476-87.96.48 Frank.Robben@ehealth.fgov.be	**J-L. Vanneste** 02-787.58.20 0477-50.55.25 Jean-Luc.Vanneste@smals.be

4.4. Auditing the Service

When needed, eHealth may carry out an audit of one or more of the Services defined. The purposes of any such audit will be to assess the extent to which Smals has met the specification for the Service or Services being audited and to suggest ways in which these Services could be improved. Such audits will pay particular attention to the performance of Smals with respect to the listed indicators. The audits will also take account of the budget available. eHealth may be assisted, where necessary, by the appointment of independent experts.

The Management Committee may also request an audit of the methods and procedures used by eHealth and Smals to measure the values of the Service level parameters defined for the Services. The purpose of the audit will be to confirm the accuracy of eHealth's reports on the extent to which it has achieved the required levels of Service.

5. Service Management

- To be able to deliver all Services with a professional quality, Service Provider has put in place Service Management processes based on ITIL good practices.
- These Service Management processes will guarantee that the different Services are delivered in a consisting way and that the Service Objectives will be met.
- Key Performance Indicators necessary to measure and to report the quality of these processes will be described in the following chapters.

5.1. Service level standards

5.1.1. Service, Support and Maintenance Window

5.1.1.1. Service Window

The default Service Window for eHealth Services in Production environment is:

Service Window								
		Day of the week (closing days of the 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 – 17:30							
	17:30 – 20:00							
	20:00 – 24:00							

The default Service Window for eHealth Services on Acceptance, Integration and Test environments is:

Service Window								
		Day of the week (closing days of the 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 – 17:30							
	17:30 – 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.

5.1.1.2. Support Window

Support for eHealth Basic Services **in Production** environment is accessible through the Contact Center

The default Support Window of the Contact Center is:

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

Legend	
	Timeslots for which the eHealth Contact Center is available for the End-Users with a second line support for Infrastructure (HW, OS, Middleware and DB) only.
	Timeslots for which the eHealth Contact Center is available for the End-Users with a second line support, including Application Support.
	Timeslots for which the eHealth Contact Center is unavailable for the End-Users. The End-User will have the possibility to record a voice message or send a webrequest that will be treated on the next Working day.

The default Support Window of the Supervision is:

Support Window Supervision								
		Day of the week (Closing days of the 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 – 17:30							
	17:30 – 20:00							
	20:00 – 24:00							

Legend	
	Timeslots for which the Supervision team is only reachable through guard duty for a second line support (stand-by)
	Timeslots for which the Supervision team is available for a second line support

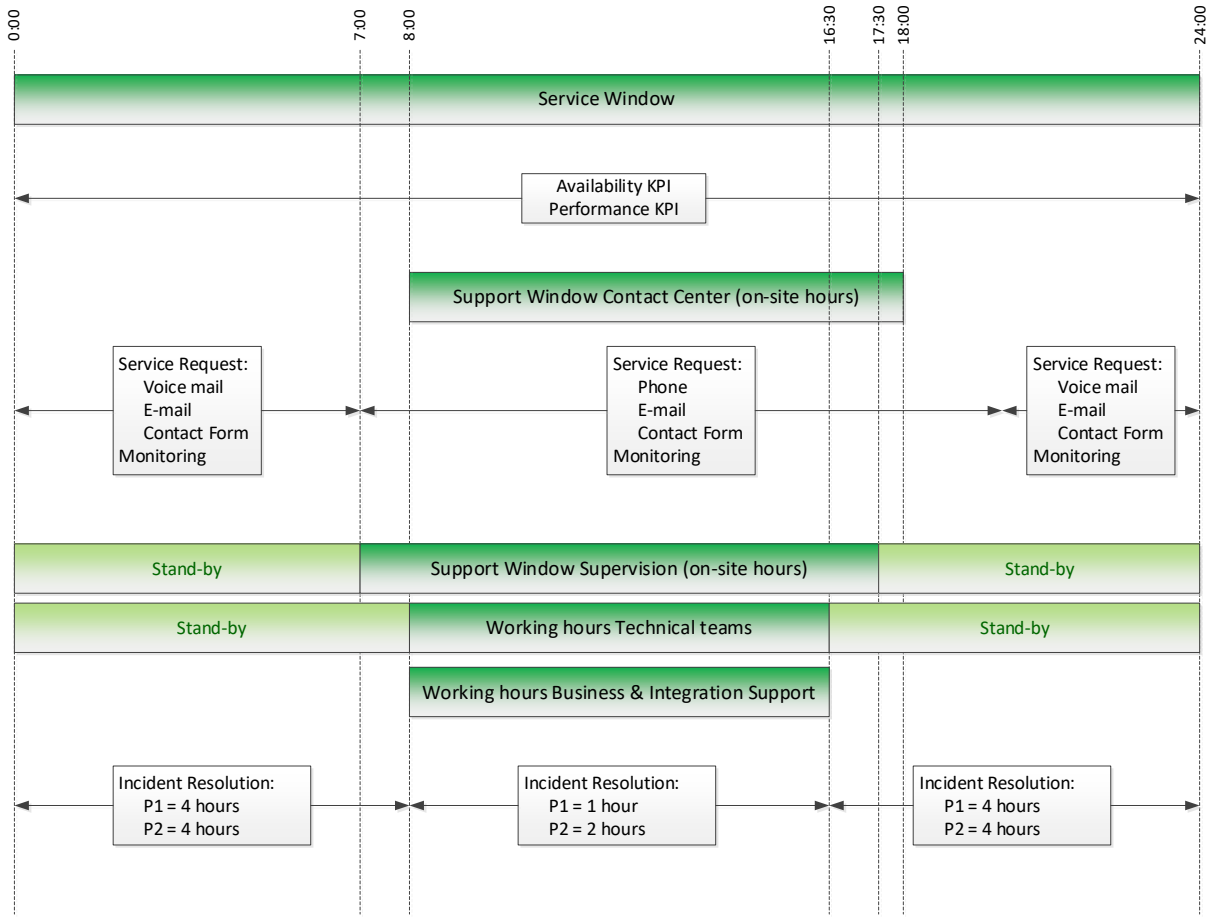
Support for eHealth Services **in Acceptance environment** is accessible through the Contact Center

Support for eHealth Services **in Integration and Test environments** is accessible through the Business & Integration Support.

The default Support Window is:

Support Window Acceptance and Test environments								
		Day of the week (Closing days of the 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 – 17:30							
	17:30 – 20:00							
	20:00 – 24:00							

Following chart illustrates the relations between Service Window, Support Window, Working hours and their related deliverables and/or KPI's



Remark: P1 Incidents logged between 5:00am and 8:00am on working days will be resolved by 9:00am and P2 Incidents logged between 6:00am and 8:00am on working days will be resolved by 10:00am

Service Window and Support Window will be specified in each separate SLA (at least if not default).

Maintenance Window will also be specified in each SLA.

Changes on the Production environment can only be performed during the Maintenance Window, unless specified otherwise and agreed upon by both parties.

Changes & release requiring modifications to the Constituent system or their users system, Service Provider will be subject to terms & conditions of the release policy.

5.1.1.3. Maintenance Window

- **Maintenance window for Production environment**

During the Major Releases, a downtime of maximum 30 minutes is authorized.

Other maintenance windows can be defined in agreement with the Constituent (e.g. Major upgrade of DB's).

This downtime will not be taken into account when calculating the Availability of the different Services.

5.1.2. Service Level Criticality

Service Level Criticality are defined per Service and per logical environment

Service Level criticality is defined in the specific SLA's. However, following levels are defined as standard:

Production environment	PLATINUM
Acceptance environment	SILVER
Bug Fix environment	SILVER
System Integration environment	BRONZE
Development environment	BRONZE
Partner Integration environment	BRONZE

5.2. Incident management

5.2.1. Definition

- The Incident management process points to the activities needed to restore a normal service operation as quickly as possible and to minimize the impact on business operations, thus ensuring that the best possible levels of service quality and availability are maintained.

5.2.2. Implementation of Incident management

- This chapter describes the way Service Provider has implemented Incident Management. This document contains the main information needed by the Constituent to be able to communicate and interact efficiently with the Service Provider and vice versa. The complete description of the incident management process is available on request but is not a part of this MSA.

5.2.2.1. Priorities at Supervision

- On Incident assignation, the Priority is calculated based on the Service level criticality and the Impact of the situation.
- By default, the Business Importance Level on eHealth service in production is Platinum. Specific Service Level for each basic service is specified in the respective SLA's
- In case of conflicting data (in MSA and SLA) about the Business Importance Level of a Service, the SLA data prevail.
- The impact is defined based upon the following table. When the situation changes over time, Impact and Priority will be adapted accordingly.

Impact	Situation
High	• The incident affects all end-users
Medium	• The incident affects a group of end-users
Low	• The incident affects one or a limited number of end-users
None	• No degradation of the Service

- The priority at Supervision is calculated as follows:

Business Importance Level		Impact			
		HIGH	MEDIUM	LOW	NONE
	GOLD / Platinum	Priority 1 (P1)	Priority 2 (P2)	Priority 4 (P4)	Priority 6 (P6)
	SILVER	Priority 2 (P2)	Priority 3 (P3)	Priority 5 (P5)	Priority 6 (P6)
	BRONZE	Priority 3 (P3)	Priority 4 (P4)	Priority 6 (P6)	Priority 6 (P6)

Please note that a Priority 1 or 2 incident shall be raised in case of lack of compliancy to the KPI within the calculation window.

5.2.2.2. Detection, Response, Reaction and Resolution targets

- See Ch. 5.2.6. for Incident Management KPI's
- When the resolution process requires an intervention of the End User, the time needed to perform these interventions, will not be reported as Resolution time of the Service Provider (Status = "Waiting For").
- Interventions performed outside Working Hours can take longer as those within Working Hours. (See Ch. 5.2.6. KPI for Incident management).

5.2.3. Incident Reporting

Incident management depends mainly on the following:

- The PABX, phone logs every incoming call;
- Service Now logs and support the management of incident by the Contact Center;
- Service Now logs and support the management of incident by the Supervision. It is thus the second line incident management tool;
- Infrastructure and other monitoring tool

5.2.4. Graphical overview of Incident lifecycle

5.2.4.1. Supervision

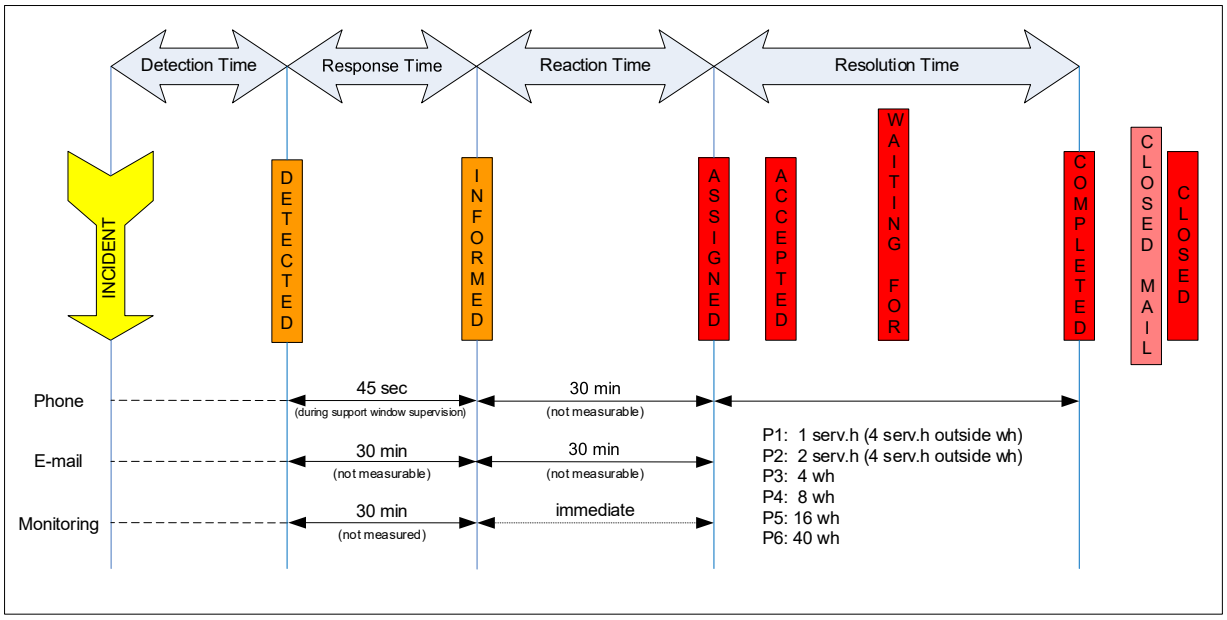
Statuses in the Service Management tool at Supervision

Status	Meaning
Assigned	• When a SR is created and transferred to a Group Coordinator
Accepted	• When a Group Member accepts a SR
Completed	• When the Incident is solved. The solution is implemented
Waiting For	• When waiting for action or information of the Constituent or a 3rd party managed by the Constituent
Closed	• When the caller confirms that the Incident is solved
Closed mail	• When the caller is unreachable, a mail is sent to inform him of the implemented solution

Other statuses

Status	Meaning
Detected	• phone: the user calls the Supervision • e-mail: the e-mail is received in the mailbox of the Supervision • monitoring: initial detection of potential error (first test failure)
Informed	• phone: Supervision picks up the phone • e-mail: the e-mail is opened by Supervision • monitoring: confirmation that the error is considered as an issue (e.g. after several retrials)

Timeline within Supervision



5.2.4.2. Contact Center

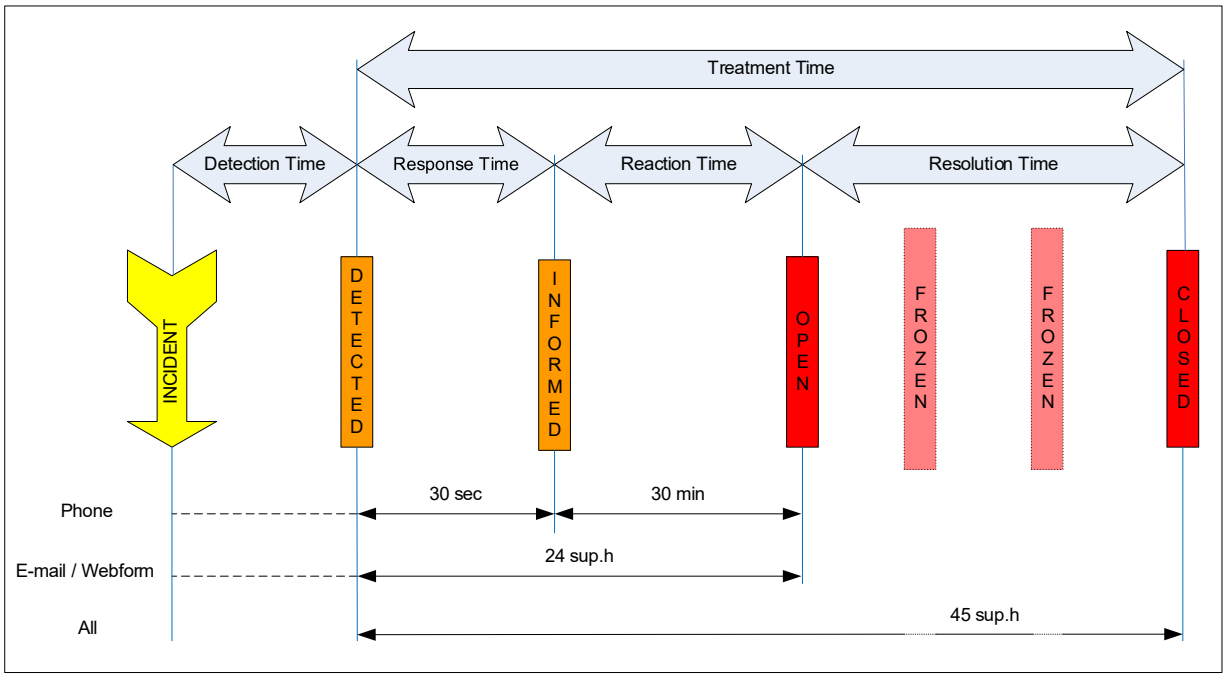
Statuses in the Service Management tool at Contact Center

Status	Meaning
Open	• When a SR is created and transferred to a Group Coordinator
Closed	• When the Incident is solved by all parties involved in solving the issue. At this point, the solution has already been implemented and the client informed of this solution.
Frozen	• When waiting for action or information of the End User

Other statuses

Status	Meaning
Detected	• phone: the user calls the Contact Center • e-mail/webform: the e-mail is received in the mailbox of the Call Center
Informed	• phone: Call Center picks up the phone • e-mail/webform: not applicable

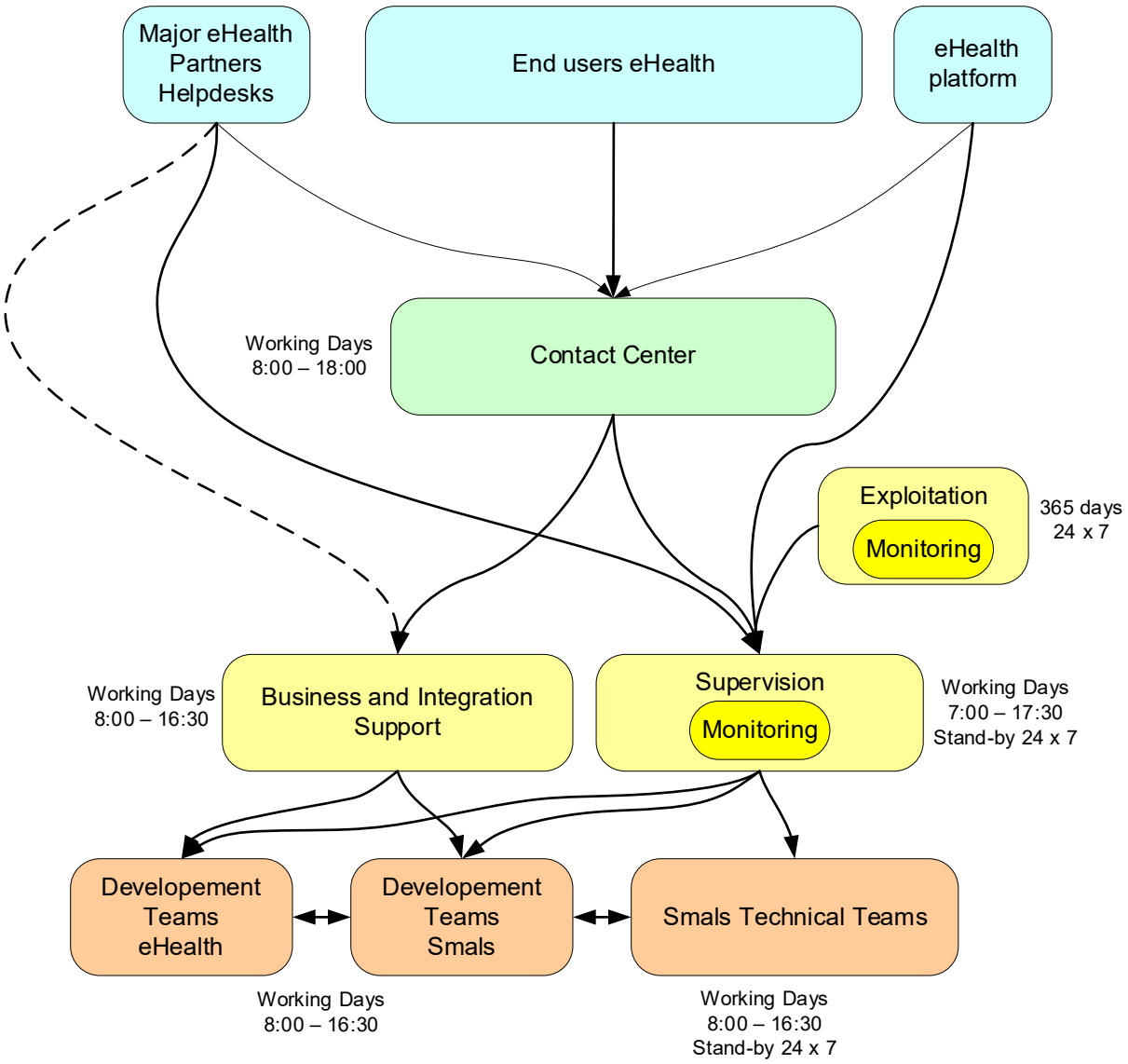
Timeline within Contact Center



In case of major Technical Incident, the Supervision team is contacted immediately after creation of the ticket (status “opened”).

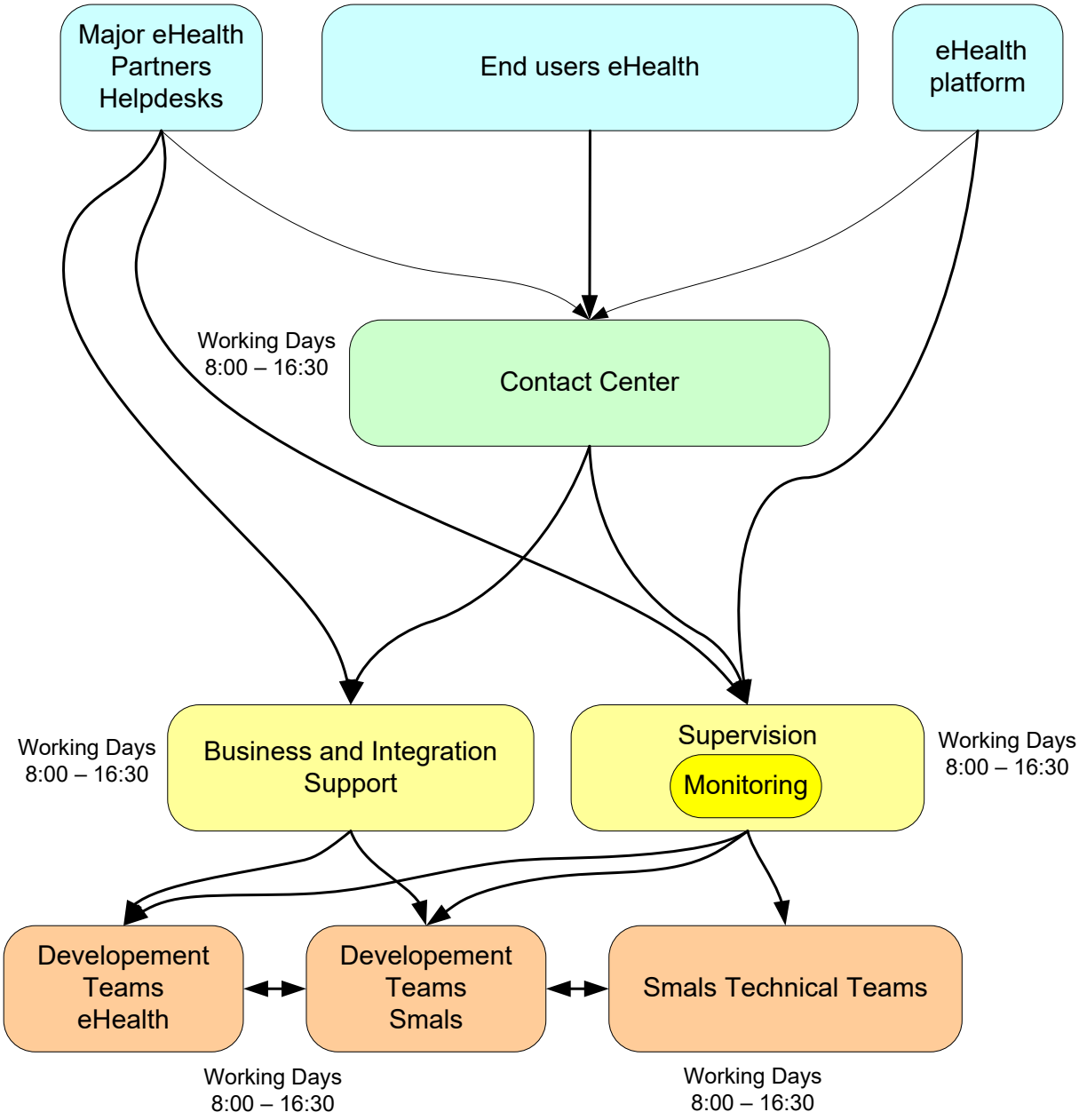
5.2.5. Incident (Service Request) Flow

5.2.5.1. Production environment

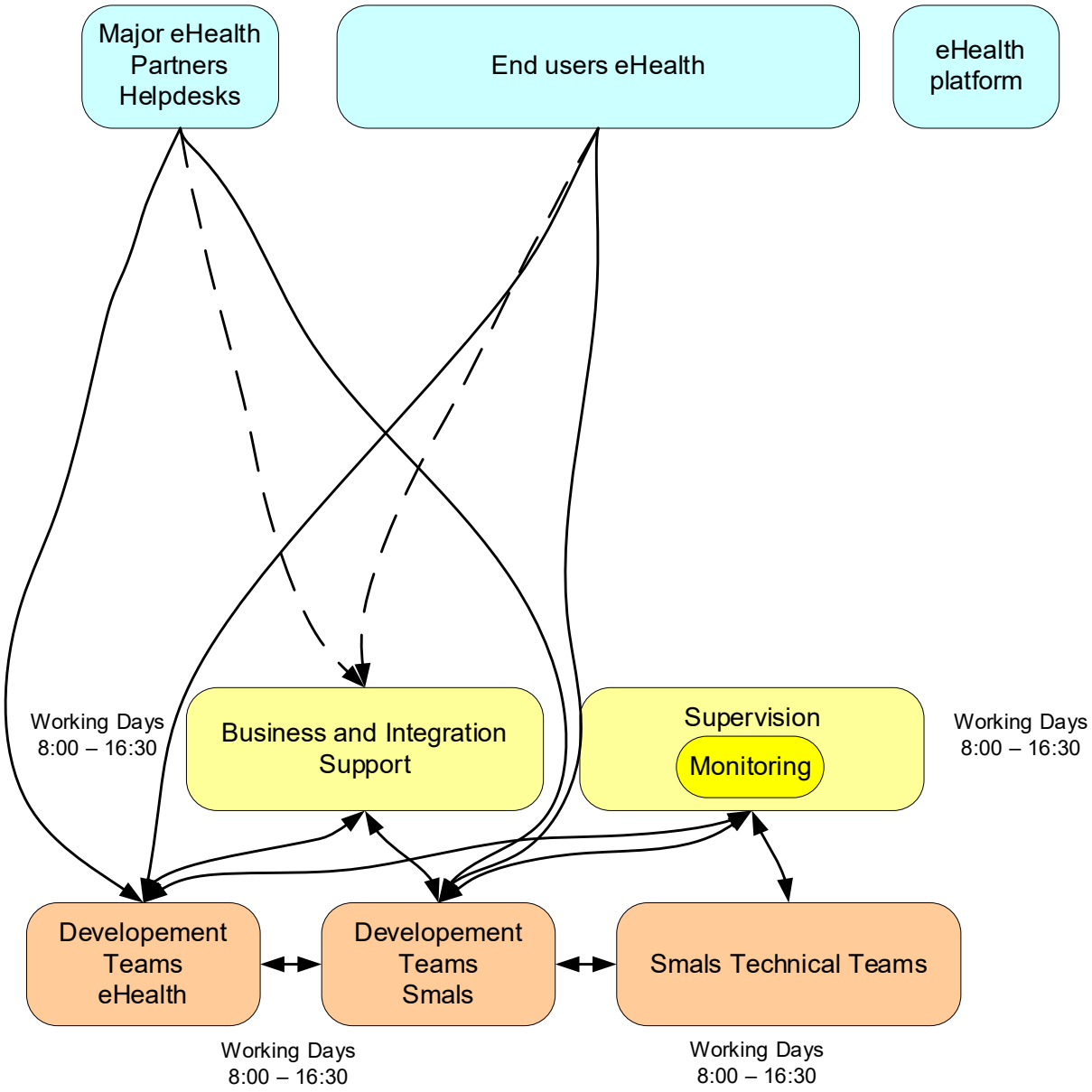


An additional channel (secured chat – signal) is added in case of incident for ease of follow up and exchange of information. The session can be initiated by the Service Provider or the Constituent.

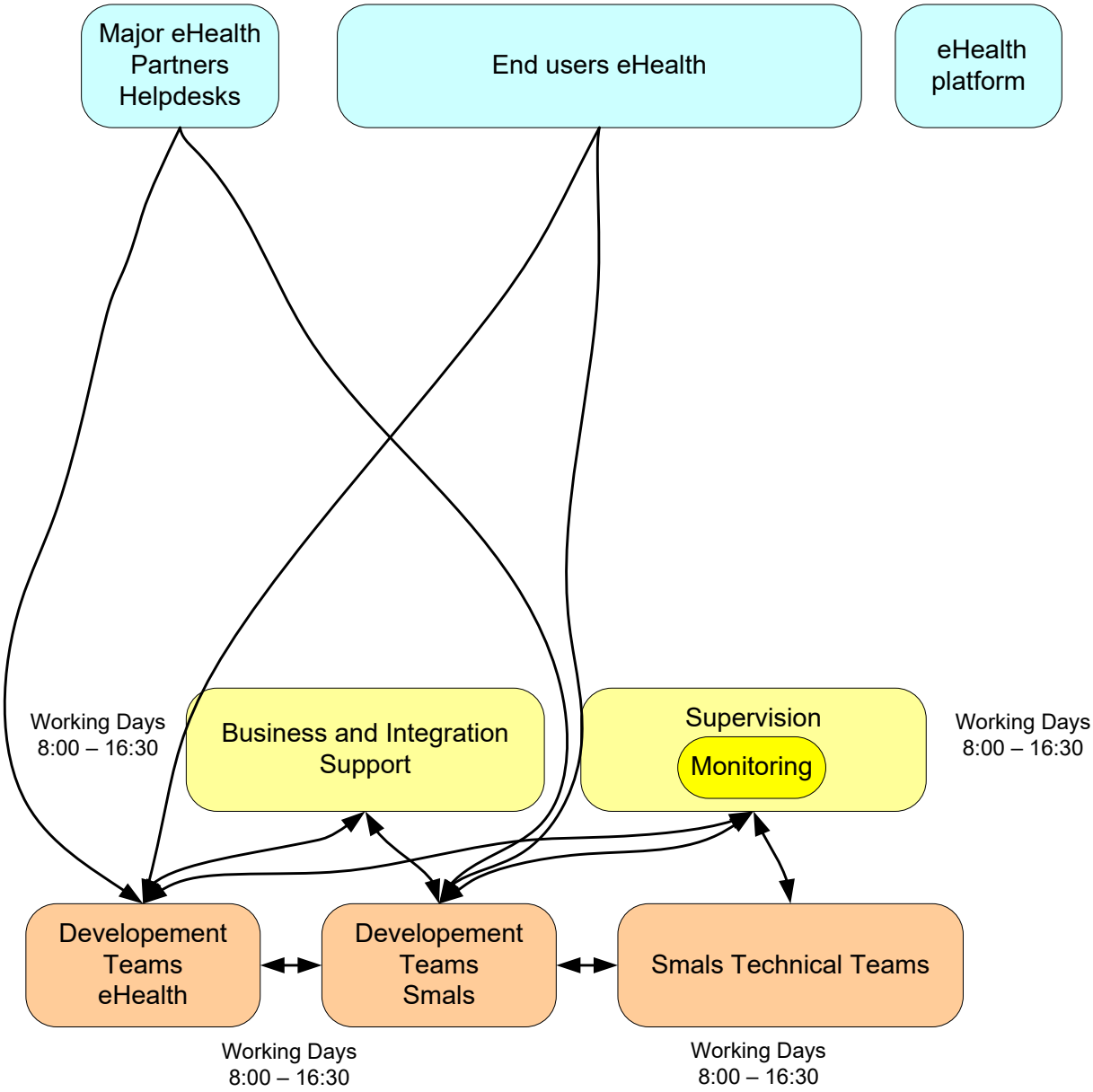
5.2.5.2. Acceptance environment



5.2.5.3. Integration environment



5.2.5.4. Other environments



5.2.6. KPI for Incident management

- ***Measuring method & Calculation***
  - The KPI's mentioned hereunder and in the following chapters are, unless specified otherwise, related to the processing of technical Incidents and are therefore seen in the perspective of the Supervision part of the Service Desk.
  - The definition is most of the time seen as a timeframe delimited by two statuses in the Service Management tool.
  - The measuring method and calculation is based on a ratio of the "Defined Performance" and the maximum possible Performance

5.2.6.1. Incident detection phase by Service Provider

Monitoring tools Availability		
Goal of the KPI	• Evaluate the availability of the Monitoring tools	
Definition	• Monitoring is considered to be available when the logfile is updated with the results of the different measurements.	
Measuring method	• The availability of the Monitoring tools are measured with the Monitoring tool. The amount of valid (OK or Not OK) results for the application monitoring is compared with the expected amount of results	
Calculation	$Availability = \frac{Amount\ of\ valid\ results}{Amount\ of\ expected\ results}$	
Calculation window	• Monthly	
Objective	Committed	Target
	Min 99,9%	Min 99,9%

5.2.6.2. *Incident Response phase*

- The incident response phase objective is to limit the time between incident identification by a specific tool or end user and the moment the service desk initiate its take up. This set of KPI's gives an indication of the speed of Response by the service desk on new incident.
- The incident response time is the time between the detection of an incident and the moment the service desk respond to the event.
- There are three major inputs for the service desks (the monitoring, the mail & the contact form, and the phone). As described in the "Incident (Service Request) Flow" chapter, Incidents can be notified either to the Contact Center or to the Supervision.
- Currently, the response time is only measured on the performance of the Contact Center and the Supervision with regard to phone call. This SLA assumes also that for each service request initiated by phone if require a ticket for an incident is opened at the same time.

Contact Center availability		
Goal of the KPI	• Evaluate the availability of the Contact Center	
Definition	• "Availability Contact Center" is measured by checking its response time.	
Measuring method	• The PBX records timestamps for incoming calls and for phone pick-up.	
Calculation	• The difference between above mentioned parameters is calculated for each incoming call • The percentage of phone pick-up performed within X sec is calculated	
Calculation window	• Monthly	
Objective	• 30 seconds	
Conformance	Committed	Target
	Min 80%	Min 90%

Supervision availability		
Goal of the KPI	• Evaluate the availability of the Supervision Service desk	
Definition	• "Supervision Availability" is measured by checking its response time.	
Measuring method	• The PBX records timestamps for incoming calls and for phone pick-up.	
Calculation	• The difference between above mentioned parameters is calculated for each incoming call • The percentage of phone pick-up performed within X sec is calculated	
Calculation window	• Monthly	
Objective	• 45 seconds (during availability timeslot within Support Window of Supervision)	
Conformance	Committed	Target
	Min 80%	Min 90%

Abandoned call rate in the Contact Center		
Goal of the KPI	• Evaluate the rate of the abandoned calls in the Contact Center	
Definition	• "Abandoned call rate in the Contact Center" is measured by checking the amount of abandoned calls (hanged up calls without answer) in relation with the total amount of incoming calls.	
Measuring method	• The PBX records for incoming calls.	
Calculation	• The percentage of phone calls hanged up without answer regarding the total amount of incoming calls	
Calculation window	• Monthly	
Conformance	Committed	Target
	N/A (depends on the caller too)	Max 10%

Abandoned call rate in the Supervision		
Goal of the KPI	• Evaluate the rate of the abandoned calls in the Supervision	
Definition	• "Abandoned call rate in the Supervision" is measured by checking the amount of abandoned calls (hanged up calls without answer) in relation with the total amount of incoming calls.	
Measuring method	• The PBX records for incoming calls.	
Calculation	• The percentage of phone calls hanged up without answer regarding the total amount of incoming calls	
Calculation window	• Monthly	
Conformance	Committed	Target
	N/A (depends on the caller too)	Max 10%

5.2.6.3. Incident Reaction phase

<table>
<tr><th colspan="4">Incident Reaction time at Contact Center for phone calls</th></tr>
<tr><td>Goal of the KPI</td><td colspan="3">• Measure whether the Incidents are registered (a ticket is created) and are assigned within the committed timeframes.
• This KPI gives an indication of the speed of Incident registration and assignment / dispatching.</td></tr>
<tr><td>Definition</td><td colspan="3">• The time between the answer of the call and the creation of a ticket and its assignment to a group for resolution (status “Open”) this includes the communication time with the end user to understand the incident/request, set the right priority and identify to whom it should be assigned.</td></tr>
<tr><td>Measuring method</td><td colspan="3">• All “Incidents assigned within the committed timeframe” are filtered and listed.
• All “Incidents” are filtered and listed.
• This is done for the Incidents registered during the Calculation window.</td></tr>
<tr><td>Calculation</td><td colspan="3">• Ratio of the above mentioned parameters</td></tr>
<tr><td>Calculation window</td><td colspan="3">• Monthly reporting, yearly evaluation</td></tr>
<tr><td rowspan="2">Objective</td><td rowspan="2">Reaction time at Contact Center for phone calls</td><td colspan="2">Compliance</td></tr>
<tr><td>Committed</td><td>Target</td></tr>
<tr><td></td><td>30 minutes within the Support Hours</td><td>Min 80%</td><td>Min 95%</td></tr>
<tr><td>Remark</td><td colspan="3">This measure is currently limited to the measure related to incident notified by phone call at the Contact Center.</td></tr>
</table>

<table>
<tr><th colspan="4">Incident Response & Reaction time at Contact Center for webform and mail</th></tr>
<tr><td>Goal of the KPI</td><td colspan="3">• Measure whether the Incidents (or requests) are registered (a ticket is created) and are assigned within the committed timeframes.
• This KPI gives an indication of the speed of Incident registration and assignment / dispatching.</td></tr>
<tr><td>Definition</td><td colspan="3">• The time between the receipt of the e-mail and the creation of a ticket and its assignment to a group for resolution (status “Open”).</td></tr>
<tr><td>Measuring method</td><td colspan="3">• All “Incidents assigned within the committed timeframe” are filtered and listed.
• All “Incidents” are filtered and listed.
• This is done for the Incidents registered during the Calculation window.</td></tr>
<tr><td>Calculation</td><td colspan="3">• Ratio of the above mentioned parameters</td></tr>
<tr><td>Calculation window</td><td colspan="3">• Monthly reporting, yearly evaluation</td></tr>
<tr><td rowspan="2">Objective</td><td rowspan="2">Response & Reaction time at Contact Center for Webform and mail</td><td colspan="2">Compliance</td></tr>
<tr><td>Committed</td><td>Target</td></tr>
<tr><td></td><td>24 Support Hours</td><td>Min 80%</td><td>Min 90%</td></tr>
<tr><td>Remark</td><td colspan="3">This measure is currently limited to the measure related to incident notified by webform/mail at the Contact Center.</td></tr>
</table>

<table>
<tr><th colspan="4">Callback Requested at Contact Center - Response & Reaction time</th></tr>
<tr><td>Goal of the KPI</td><td colspan="3">• Measure whether Callbacks Requested are Responded (recalled) within the committed timeframes.
• This KPI gives an indication of the speed of Recalls handling.</td></tr>
<tr><td>Definition</td><td colspan="3">• The time between the receipt of the Callback request on the phone mailbox and the Recall.</td></tr>
<tr><td>Measuring method</td><td colspan="3">• All “Incidents assigned within the committed timeframe” are filtered and listed.
• All “Incidents” are filtered and listed.
• This is done for the Incidents registered during the Calculation window.</td></tr>
<tr><td>Calculation</td><td colspan="3">• Ratio of the above mentioned parameters</td></tr>
<tr><td>Calculation window</td><td colspan="3">• Monthly reporting, yearly evaluation</td></tr>
<tr><td rowspan="3">Objective</td><td rowspan="2"></td><td colspan="2">Compliance</td></tr>
<tr><td>Committed</td><td>Target</td></tr>
<tr><td>Callback Requested During Contact Center hours – First contact Call back
6 Support Hours</td><td>Min 80%</td><td>Min 90%</td></tr>
<tr><td>Callback Requested Outside Contact Center hours – First contact Call back
Recalled before end of the next working day</td><td>Min 80%</td><td>Min 90%</td></tr>
<tr><td>Remark</td><td colspan="3">n/a</td></tr>
</table>

<table>
<tr><th colspan="4">Incident Response & Reaction time at 2nd line support for webform and mail</th></tr>
<tr><td>Goal of the KPI</td><td colspan="3">• Measure whether the Incidents (or requests) are registered (a ticket is created) and are assigned within the committed timeframes.
• This KPI gives an indication of the speed of Incident registration and assignment / dispatching.</td></tr>
<tr><td>Definition</td><td colspan="3">• The time between the receipt of the e-mail and the creation of a ticket and its assignment to a group for resolution (status “Open”).</td></tr>
<tr><td>Measuring method</td><td colspan="3">• All “Incidents assigned within the committed timeframe” are filtered and listed.
• All “Incidents” are filtered and listed.
• This is done for the Incidents registered during the Calculation window.</td></tr>
<tr><td>Calculation</td><td colspan="3">• Ratio of the above mentioned parameters</td></tr>
<tr><td>Calculation window</td><td colspan="3">• Monthly reporting, yearly evaluation</td></tr>
<tr><td rowspan="3">Objective</td><td rowspan="2">Response & Reaction time at 2nd line support for Webform and mail</td><td colspan="2">Compliance</td></tr>
<tr><td>Committed</td><td>Target</td></tr>
<tr><td>1 work day</td><td>Min 80%</td><td>Min 90%</td></tr>
<tr><td>Remark</td><td colspan="3">This measure is currently limited to the measure related to incident notified by webform/mail at the Contact Center.</td></tr>
</table>

5.2.6.4. Incident Resolution phase

<table>
<tr><th colspan="6">Incident Resolution time at Supervision</th></tr>
<tr><td>Goal of the KPI</td><td colspan="5">• Measure whether the Incidents are solved within the committed timeframes.
• This KPI gives an indication of the speed of Incident resolution.</td></tr>
<tr><td>Definition</td><td colspan="5">• The time between the first assignment to a group for resolution (status “Assigned”) and the moment that an answer is communicated or a solution is implemented (status “Completed”).</td></tr>
<tr><td>Measuring method</td><td colspan="5">• Per priority, all “Incidents completed within the committed timeframe” are filtered and listed.
• All “Incidents” are filtered and listed.
• This is done for the Incidents “completed” during the Calculation window.</td></tr>
<tr><td>Calculation</td><td colspan="5">• Ratio of the above mentioned figures</td></tr>
<tr><td>Calculation window</td><td colspan="5">• Monthly reporting, yearly evaluation</td></tr>
<tr><td rowspan="8">Objective</td><td rowspan="2">Priority</td><td rowspan="2">Resolution time for Incidents registered during Working Hours</td><td rowspan="2">Resolution time for Incidents registered outside Working Hours</td><td colspan="2">Compliance</td></tr>
<tr><td>Committed</td><td>Target</td></tr>
<tr><td>P1</td><td>1 Service Hour</td><td>4 Service Hours</td><td rowspan="6">Min 80 %</td><td rowspan="6">Min 90 %</td></tr>
<tr><td>P2</td><td>2 Service Hours</td><td>4 Service Hours</td></tr>
<tr><td>P3</td><td>4 Working Hours</td><td>4 Working Hours</td></tr>
<tr><td>P4</td><td>1 Working Day</td><td>1 Working Day</td></tr>
<tr><td>P5</td><td>2 Working Days</td><td>2 Working Days</td></tr>
<tr><td>P6</td><td>5 Working Days</td><td>5 Working Days</td></tr>
<tr><td>Remark</td><td colspan="5">The current reporting on resolution time cannot distinguish incident resolution period under the responsibility of the service provider and one under the responsibility of a third party or a partner (identified by the status).
Therefore, a global reporting on resolution time including the “waiting for” period has been implemented. When the indicator exceeds the committed value, the service provider further investigates on the influence of “waiting for” period.
Refer to ch. 5.1.1.2 for more details on Resolution time for P01 and P02 outside Working Hours.</td></tr>
</table>

<table>
<tr><th colspan="4">Incident Treatment time at Call Center</th></tr>
<tr><td>Goal of the KPI</td><td colspan="3">• Measure whether the Incidents (or requests) are handled and solved within the committed timeframes.
• This KPI gives an indication of the speed of Incident resolution.</td></tr>
<tr><td>Definition</td><td colspan="3">• The time between the receipt of the e-mail or the call (“Detection time”) and the moment that an answer is communicated or a solution is implemented (status “Closed”).</td></tr>
<tr><td>Measuring method</td><td colspan="3">• All “Incidents completed within the committed timeframe” are filtered and listed.
• All “Incidents” are filtered and listed.
• This is done for the Incidents “Closed” during the Calculation window.</td></tr>
<tr><td>Calculation</td><td colspan="3">• Ratio of the above mentioned figures</td></tr>
<tr><td>Calculation window</td><td colspan="3">• Monthly reporting, yearly evaluation</td></tr>
<tr><td rowspan="2">Objective</td><td rowspan="2">Treatment time at Call Center</td><td colspan="2">Compliance</td></tr>
<tr><td>Committed</td><td>Target</td></tr>
<tr><td></td><td>45 Support Hours</td><td>Min 80 %</td><td>Min 90 %</td></tr>
<tr><td>Remark</td><td colspan="3">The reporting on resolution at Call Center distinguishes incident resolution period under the responsibility of the service provider and one under the responsibility of the End User (identified by the status). This last period is excluded from the Treatment time.</td></tr>
</table>

<table>
<tr><th colspan="4">Incident Treatment time at 2nd line support</th></tr>
<tr><td>Goal of the KPI</td><td colspan="3">• Measure whether the Incidents (or requests) are handled and solved within the committed timeframes.
• This KPI gives an indication of the speed of Incident resolution.</td></tr>
<tr><td>Definition</td><td colspan="3">• The time between the receipt of the e-mail or the call (“Detection time”) and the moment that an answer is communicated or a solution is implemented (status “Closed”).</td></tr>
<tr><td>Measuring method</td><td colspan="3">• All “Incidents completed within the committed timeframe” are filtered and listed.
• All “Incidents” are filtered and listed.
• This is done for the Incidents “Closed” during the Calculation window.</td></tr>
<tr><td>Calculation</td><td colspan="3">• Ratio of the above mentioned figures</td></tr>
<tr><td>Calculation window</td><td colspan="3">• Monthly reporting, yearly evaluation</td></tr>
<tr><td rowspan="2">Objective</td><td rowspan="2">Treatment time at 2nd line support</td><td colspan="2">Compliance</td></tr>
<tr><td>Committed</td><td>Target</td></tr>
<tr><td></td><td>5 work days</td><td>Min 80 %</td><td>Min 90 %</td></tr>
<tr><td>Remark</td><td colspan="3">The reporting on resolution at 2nd Line distinguishes incident resolution period under the responsibility of the service provider and one under the responsibility of the End User (identified by the status). This last period is excluded from the Treatment time.</td></tr>
</table>

Reopened Incidents at Supervision		
Goal of the KPI	• Measure whether the closed Incidents were indeed really solved. • This is a KPI that measures the quality of the Incident management process.	
Definition	• An Incident is considered to be “Reopened” when the status goes from the status “Closed ” or “Closed mail” back to the status “Assigned”.	
Measuring method	• All “Reopened Incidents” are filtered and listed.(can be done only within 28 days) • All “Incidents” are filtered and listed. • This is done for the Incidents “closed” during the Calculation window.	
Calculation	• Ratio of the above mentioned parameters	
Calculation window	• Monthly with data of the last 3 months	
Objective	Committed	Target
	Max 10 %	Max 5%

5.3. Change management

- This chapter describes how Changes are handled.
- The “Change Management” procedures contain guidelines to evaluate the risks of the planned Changes, to minimize the possible impact on the End-users and to prepare one or more “roll-back” scenarios.

5.3.1. Category of Changes

- All changes to Infrastructure and Applications can be classified in one of following categories:
    - Emergency Changes
    - Standard Changes
    - Normal Changes
- “*Emergency Changes*” are Changes related to the resolution of an Incident (technical or security) with impact for the End-users. They are collected in Emergency Releases. The administrative part of the “Change Management” (creation of change, …) is postponed after the Incident resolution, all this in order to reduce the implementation time of the “Change”.
- “*Standard Changes*” are Changes with a limited or no impact for the End-users and with controlled risk. For those “changes” there is a template that contains the necessary procedures (predefined “work orders”) and which is accepted by both the Service Provider and the Constituent.
- “*Normal Changes*” are Changes for which the risk and impact for the End-users have to be evaluated. They are collected in releases (major, minor or emergency). The decision to perform the Change is taken by the eHealth Release Board via a CAB or an eCAB meeting.

5.3.2. Approval and information concerning the Changes

- “*Emergency Changes*” are executed with a formal approval of the release board via an eCAB (Emergency Change Advisory Board) meeting which can be replaced by phone/mail communication. During the “Service meetings”, they are reported and commented (“Incident management”).
- The “*Standard Changes*” are neither announced nor reported at the moment of implementation. During the “Service meetings”, they are reported and commented (“Change management”).
- For the “*Normal Changes*”, the implementation of a Change that may have any impact on the End-user will be approved by the eHealth Release Board. This discussion can, depending on the risk, the impact, the urgency and/or the availability of representatives, be done by phone or during a formal meeting. For changes concerning infrastructure and applications shared with other clients, they can be part either of an eHealth release or of another client release.
-

5.3.3. KPI for Change management

Nonstandard and Emergency changes executed without an approval by the Release Board		
Goal of the KPI	• Measure whether Nonstandard and Emergency Changes are executed correctly (with a Release Board validation)	
Definition	• All Nonstandard and Emergency Changes have to be executed with a validation of the Release Board. The Nonstandard and Emergency Changes being executed without an approval of the Release Board are considered as "Nonstandard and Emergency Changes executed an approval by the Release Board"	
Measuring method	• All "Nonstandard and Emergency Changes without an approval by the Release Board" are filtered and listed. This is done based on the presence (or the lackt) of the status "Waiting for CAB" in the history of the changes • All "Nonstandard and Emergency Changes" are filtered and listed.	
Calculation	• Ratio of the above mentioned parameters	
Calculation window	• Monthly with data of the last 3 months	
Objective	Committed	Target
	Max 20%	Max 5%
Remarks	• This KPI should also include changes related to project	

Requests for Change executed in time		
Goal of the KPI	• Check whether the Requests for Change initiated by eHealth are executed in time	
Definition	• Requests for Change initiated by eHealth executed before or at the "Requested date" mentioned in the RfC.	
Measuring method	• For all Requests for Change, the "Requested date" and the "Execution date" are extracted from the Service Management tool	
Calculation	• Requests for Change executed in time are calculated by comparing the "Requested date" and the "Execution date" • Requests for Change executed in time are compared to the total number of Requests for Change and the ratio is calculated.	
Calculation window	• Monthly with data of the last 3 months	
Objective	Committed	Target
	Min 80%	Min 90%
Remarks	• For standard change, the request date should be a delivery date agreed at each request	

Number of Emergency Changes (Bug Fix implementation)		
Goal of the KPI	• As the implementation of Emergency Changes can endanger the stability of the environment, the goal is to keep the number to a minimum.	
Definition	• Emergency Changes as defined in Ch.5.3.1.	
Measuring method	• Manual registration of the Emergency Changes	
Calculation	• List the Emergency Changes per Calculation window	
Calculation window	• Monthly reporting, yearly evaluation	
Objective	Committed	Target
	As both the Constituent and the Service Provider can request Emergency Changes, no formal objective will be defined	Max 5 Emergency Changes per Calculation Window

5.4. Release Management

- For the description of this process, reference is made to the Release Management Process (general principles) and the specific Release Policy for eHealth.
- Both Service Provider and Constituent will respect the specifications in the above mentioned documents (Release Management process and Release Policy for eHealth).

5.4.1. Category of Releases

- The different Release categories are listed hereafter for information purposes. The formal definitions are available in the Release Management process description.

Major release

- Contains
  - nonstandard changes, new application and infrastructure deployments
  - Changes on the eHealth Backend Core
  - Modifications to libraries
  - Modifications to Weblogic descriptors

Minor release

- Contains all Changes that can't wait until the following Major Release to meet specific business needs approved by the Release Board. This includes:
  - Deployment / modifications of simple pipes (pass through)
  - Deployment / modifications of complex pipes without impact on the eHealth Backend Core

Emergency Release (at any time)

- Changes that can't wait until next Major or Minor Release due to a bug that has high production and/or business impact
- Release process will be followed although some process steps will be simplified to meet the urgency for deployment

5.4.2. Generic Release Timeline

Release Process Timeline, Next-Release Calendar can be found on :
https://www.ehealth.fgov.be/ehealthplatform/fr/service-releases-management

5.4.3. KPI for Release Management

Number of bugfixes after Major and Minor Release deployment		
Goal of the KPI	• Evaluate the quality of the Release by evaluating the additional amount of bugfixes after the release.	
Definition	• Bugfixes identified to be linked to (succeeding) a Release	
Measuring method	• Manual registration of the Emergency changes linked to a Release	
Calculation	• List the Emergency changes linked to a Release per Calculation window	
Calculation window	• Monthly with data of the last 3 months	
Objective	Committed	Target
	As both the Constituent and the Service Provider can cause bugs, no formal objective will be defined	Max 5 Bug Fixes per Calculation Window

Respect of the release calendar	
Goal of the KPI	• A correct planning is important to offer all the partners the opportunity to test extensively their part of the eHealth solution.
Definition	• Number of reschedules per year. The schedules taken into account are: ○ Content Freeze ○ Code Freeze ○ beginning of the yellow phase (start of integration tests with partners) ○ production date.
Measuring method	• Manual registration of the reschedules
Calculation	• Number of reschedules per year taken out of the list of schedules and their applied date.
Calculation window	• Monthly with data of the last 3 months
Objective	• As both the Constituent and the Service Provider can request reschedules, no formal objective will be defined. The number of reschedules will only be reported

Respect of the compliance against Freeze period	
Goal of the KPI	• A correct planning is important to offer all the partners the opportunity to test extensively their part of the eHealth solution. This includes compliance against Freeze Periods.
Definition	• Number of accepted demands not respecting freeze periods.
Measuring method	• Manual registration of the defined demands
Calculation	• Number of accepted demands per year
Calculation window	• Monthly with data of the last 3 months
Objective	• As both the Constituent and the Service Provider can request reschedules or demands for exception on freeze, no formal objective will be defined. The number of demands will only be reported

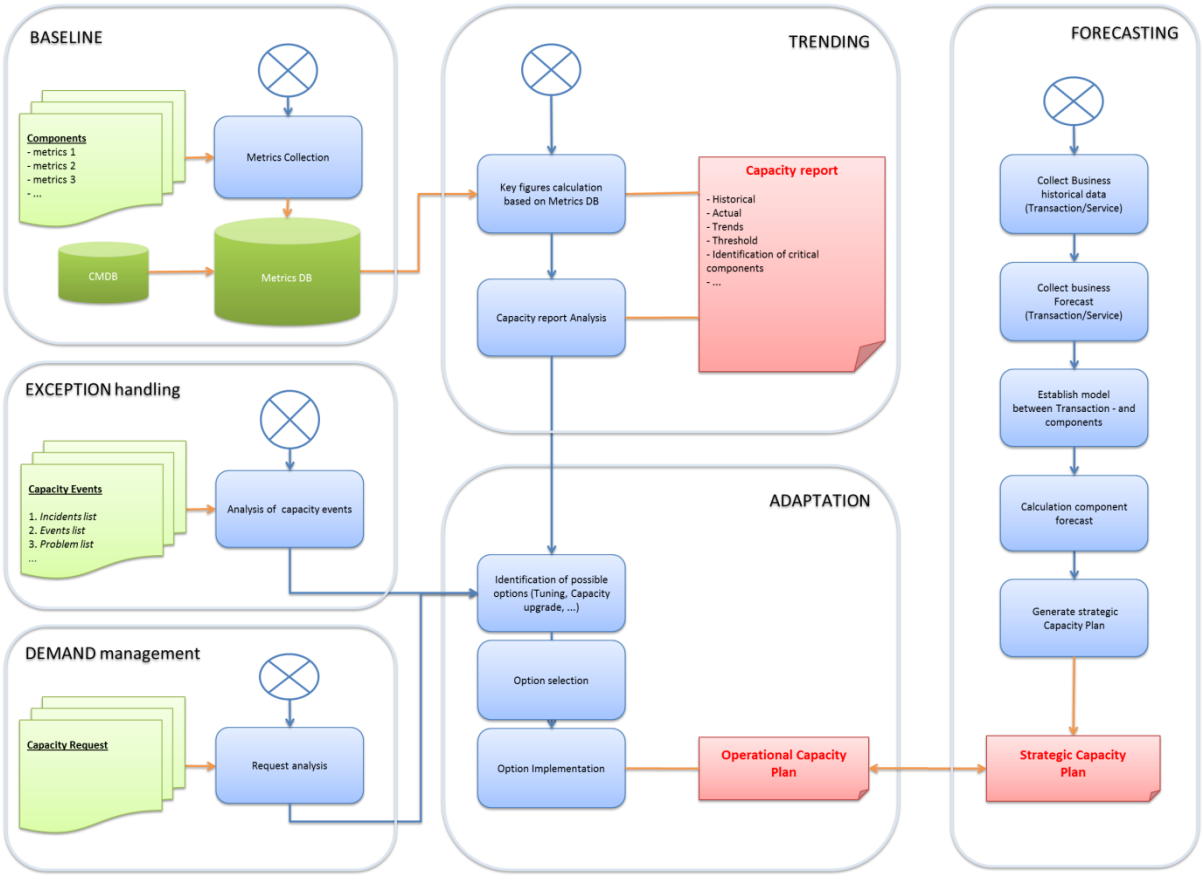
5.5. Capacity Management

Goals

- Prevent incidents related to capacity issues
- Manage the capacity of the infrastructure
- Manage the Business Forecast

A monthly meeting is organised for the follow up of the capacity.

Following activities will be covered by the Capacity Management.



5.5.1. Baseline: Centralized Collection of the infrastructure's usage

- Gathering of metrics from the monitoring tools
- Aggregation of the data and calculation of some key indicators

5.5.2. Trending: Analysis of the evolution of the resources usage

- Based on historical data
- Trend computation
- Capacity reporting
- Identification of under/over capacity components
- Analyse of Capacity reports by technical teams

5.5.3. Adaptation: Definition of the required adaptations to cope with the needed capacity

- Based on capacity analysis, incidents or new requests
- Analysis possible options to cover Capacity need
- Adaptation of the Operational Capacity Plan

5.5.4. Exception handling: Analysis of the capacity incidents/events to take the necessary measures to prevent their new occurence

- Early detection of capacity events
- Periodical review with technical teams

5.5.5. Demand Management: Management of new capacity request

- Management of the requests
- Improvement of the evaluation of the capacity needs

5.5.6. Forecasting: Definition of a Strategic Capacity plan

- Based on business forecasts
- Identification of the historical business data and future needs (amount of transactions)
- Modelling transactions <-> resource needs
- Definition of the Strategic Capacity Plan

5.6. Service Level Management

5.6.1. Service Review

During the lifetime of the agreement, Service review meetings will be held on a monthly basis. The date of these meetings will be agreed between both Service Manager of the Service Provider and the Management Committee.

5.6.2. SLA Reporting

The goal of SLA measurements and SLA reporting is to share a common understanding between the user community and eHealth on the Services delivered over the last period.

This will enable both:

- to compare the actual performance against the agreed upon KPI's and other criteria,
- to have a clear view on the development and the trends of this performance.

This information will allow the Management Committee to manage this performance.

eHealth supplier shall provide detailed supporting information for each report to eHealth in machine-readable form suitable for use on a personal computer. The data and detailed supporting information shall be eHealth's Confidential Information, and eHealth may access such information online and in real-time, where technically feasible, at any time during the Term.

5.7. Financial Management

Covered in the BSM

5.8. Overview of KPI

Process	KPI			SLO	Committed Service Level	Target Service Level
Incident Management	Monitoring tools Availability				Min 99,9%	Min 99,9%
	Contact Center	Phone	Availability (Response time)	30 sec	Min 80%	Min 90%
			Abandoned call rate		N/A	Max 10%
			Reaction time	30 min within sup.h	Min 80%	Min 95%
		Mail/Webform	Response & Reaction time	24 sup.h	Min 80%	Min 95%
		CallBack	Response & Reaction time for requests during CC working hours	6 sup.h	Min 80%	Min 90%
			Response & Reaction time for requests outside CC working hours	End of next working day	Min 80%	Min 90%
		All	Incident Treatment time	45 sup.h	Min 80%	Min 90%
	Supervision	Phone	Availability (Response time)	45 sec	Min 80%	Min 90%
			Abandoned call rate		N/A	Max 10%
		All	Resolution time	According to priority	Min 80%	Min 90%
			% Reopened Incidents	(3 months view)	Max 10%	Max 5%
	2nd Line	Mail	Response & Reaction time	1 work day	Min 80%[4]	Min 95%
			Incident Treatment time	5 work days	Min 80%	Min 95%
			Number of tickets opened	(monthly view)	N/A	N/A

[4] Only if amount of tickets is big enough for evaluation

Process	KPI	SLO	Committed Service Level	Target Service Level
Change Management	Non Standard and Emergency Changes executed without a CAB	(3 months view)	Max 20%	Max 5%
	Requests for Change executed in time	(3 months view)	Min 80%	Min 90%
	Number of Emergency Changes (Bug Fix implementation)	(Monthly view)	N/A	Max 5 Emergency Changes
Release Management	Number of Bug fixes after Major and Minor Release Deployment	(3 months view)	N/A	Max 5 Bug fixes
	Respect of the release calendar	(3 months view)	N/A	N/A
	Respect of the compliance against Freeze period	(3 months view)	N/A	N/A

Reporting is produced monthly.

Additional reporting is provided by the Contact Center team self on weekly basis.

Attachment 01 – Service Structure