Service Level Agreement
Base Service: End to end encryption (E2EE)
Version 2016.01

This document is provided to you free of charge by the

eHealth platform

Willebroekkaai 38

38, Quai de Willebroeck

1000 BRUSSELS

Service Level Agreement

Base Service End to End Encryption (Addressed Messages)

Between

Service provider	**Service customer**
eHealth Platform	User Community
Quai de Willebroeck, 38	
B-1000 BRUSSELS	

To the attention of: the user community

Author:	Service Management
Date:	September, 2016
Version:	*2016.01*
Status:	Final
Type:	Public
Confidentiality:	
Language:	English
Exhibit of:	MSA

1. Table of Content

2. Document management

2.1. Document history

Version	Date	Author	Description of changes / remarks
2015.01	March 2015	eHealth Service Management	Update
2016.01	September 2016	eHealth Service Management	Update

2.2. Document references

ID	Title	Version	Date	Author
	Bestuur overeenkomst			
	Master Service Agreement	1.0		

2.3. Purpose of the document

The objective of this document is to define the Service Level Agreement for the set of *Base Service for End to End Encryption of addressed messages* proposed by the eHealth platform. It defines the minimum level of service offered on the eHealth platform, and provides eHealth's own understanding of service level offering, its measurement methods and its objectives in the long run.

This document contains a short description of the set of services offered by End to End Encryption. These services currently are centred only on the following functions[1] :

- Manage the encryption and decryption of addressed messages
- Manage the creation of asymmetric keys (public – private key pair), used for encrypting and decrypting addressed messages.

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

- Some of the dependencies on technical and/or functional components needed and used by the Web Services and other utilities offered by eHealth in the framework of the End to end Encryption service

[1] In order to use these functions, eHealth provides several products:
- utilities and libraries to be integrated in application software to be used by "external" Health Care Providers
- utilities and Web Services located on the eHealth platform and managed by the eHealth platform.

Their use and functions will be detailed further in the document.

- Some technical and/or functional components on which the Web Services and other utilities are dependent
- Measurements and KPIs intended to account for a certain number of performance indicators.

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

- A broad description of the business services offered by the eHealth platform to the applications which may want to make use of them
- Description of cross-sectional services offered on the eHealth platform, such as managing request for Certificates, i.a. Certificates used in the End to End Encryption Service for authentication of Health Care Partners
- Description of support services, including registering, managing and solving possible incidents with the End to end Encryption suite of services, managing changes, etc.
- Performance indicators related to those services.

2.4. Validity of the Agreement

This document is valid as long as the *Base Service for End to End Encryption of addressed messages* is part of the eHealth offering or is not significantly altered, in which case a new version of this document will be presented.

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

2.5. Service and Maintenance Windows

2.5.1. Service Level

By default, the priority for the support for this Basic Service (as described in the MSA) is GOLD. Nevertheless, objectives described below are valid only for the Production environment.

2.5.2. Service window

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

The following table summarises the eHealth service window.

Service Window								
		Day of the week (closing days of Service Provider = Sunday)						
		Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
Day period	00:00 – 07:00	🟩	🟩	🟩	🟩	🟩	🟩	🟩
	07:00 – 08:00	🟩	🟩	🟩	🟩	🟩	🟩	🟩
	08:00 – 16:30	🟩	🟩	🟩	🟩	🟩	🟩	🟩
	16:30 – 19:00	🟩	🟩	🟩	🟩	🟩	🟩	🟩
	19:00 – 20:00	🟩	🟩	🟩	🟩	🟩	🟩	🟩
	20:00 – 21:00	🟩	🟩	🟩	🟩	🟩	🟩	🟩
	20:00 – 24:00	🟩	🟩	🟩	🟩	🟩	🟩	🟩

Legend	
🟩	Timeslots where the Service must be available according to the SLA and where corrective actions will be taken to resolve detected Incidents.
🟢	Timeslots where the Service will be available provided there are no blocking Incidents. If these incidents do appear, no corrective action will be taken.
🟧	Timeslots where unavailability can occur.

2.5.3. Support Window

Support Window								
		Day of the week (Closing days of Service Provider = Sunday)						
		Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
Day period	00:00 – 07:00	🟧	🟧	🟧	🟧	🟧	🟧	🟧
	07:00 – 08:00	🟨	🟨	🟨	🟨	🟨	🟧	🟧
	08:00 – 16:30	🟩	🟩	🟩	🟩	🟩	🟧	🟧
	16:30 – 19:00	🟨	🟨	🟨	🟨	🟨	🟧	🟧
	19:00 – 20:00	🟨	🟨	🟨	🟨	🟨	🟧	🟧
	20:00 – 21:00	🟧	🟧	🟧	🟧	🟧	🟧	🟧
	20:00 – 24:00	🟧	🟧	🟧	🟧	🟧	🟧	🟧

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

2.5.4. Maintenance window & planned interventions

eHealth will strive for limiting as much as possible the impact and duration of the planned interventions. Today, eHealth is committed to make efforts so planned unavailability’s do not exceed one to a few hours per year.

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

2.5.5. Unplanned interventions

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

3. Service scope

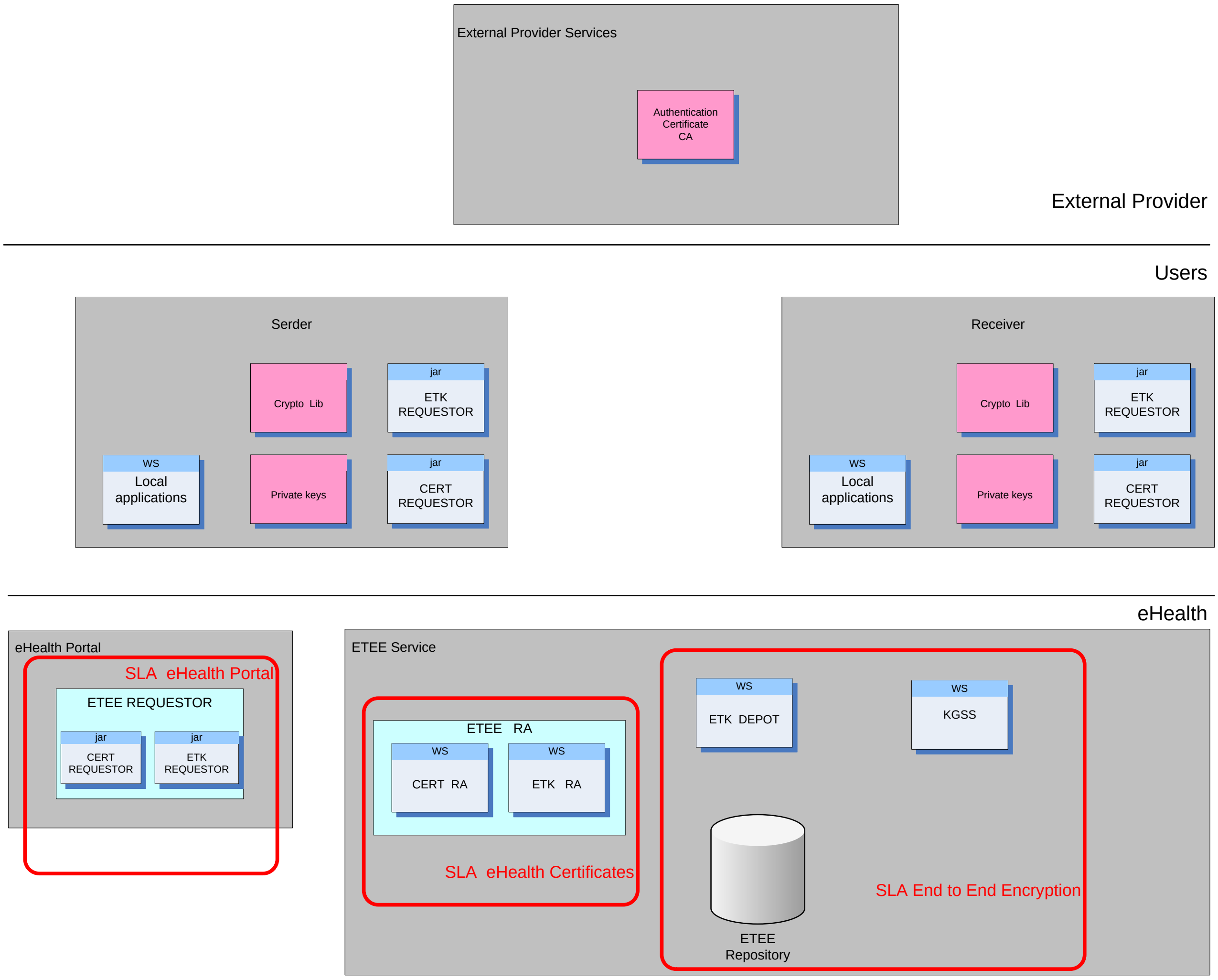
3.1. eHealth Service

3.1.1. General

Following table gives an overview of the different activities for Certificates, Tokens and Encryption and the SLA they can be found in.

Activity	Needed for/when:	Covered by SLA
Download ETEE Requestor	Request Certificates and Tokens	eHealth Portal
Download the Encryption Library	Local encryption	eHealth Portal
Creation of Certificate Including the transfer of the Certificate to the End-user to create an ETK	Authentication	eHealth Certificates
Request an ETK (Token) Only the Publication of the ETK	E2E Encryption enabling	eHealth Certificates
ETK Depot – Get the Public ETK of a Known Recipients	E2E Encryption to a Known Recipients	E2E Encryption
KGSS – Get Symmetric key for an Unknown Recipients	E2E Encryption to a Unknown Recipients	E2E Encryption
Revocation of Certificate	Certificate or ETK has to be terminated	eHealth Certificates
Consult Certificates		eHealth Certificates But not measured in that SLA
Renewal of Certificates (and ETK)		eHealth Certificates

Or in a graphical presentation:

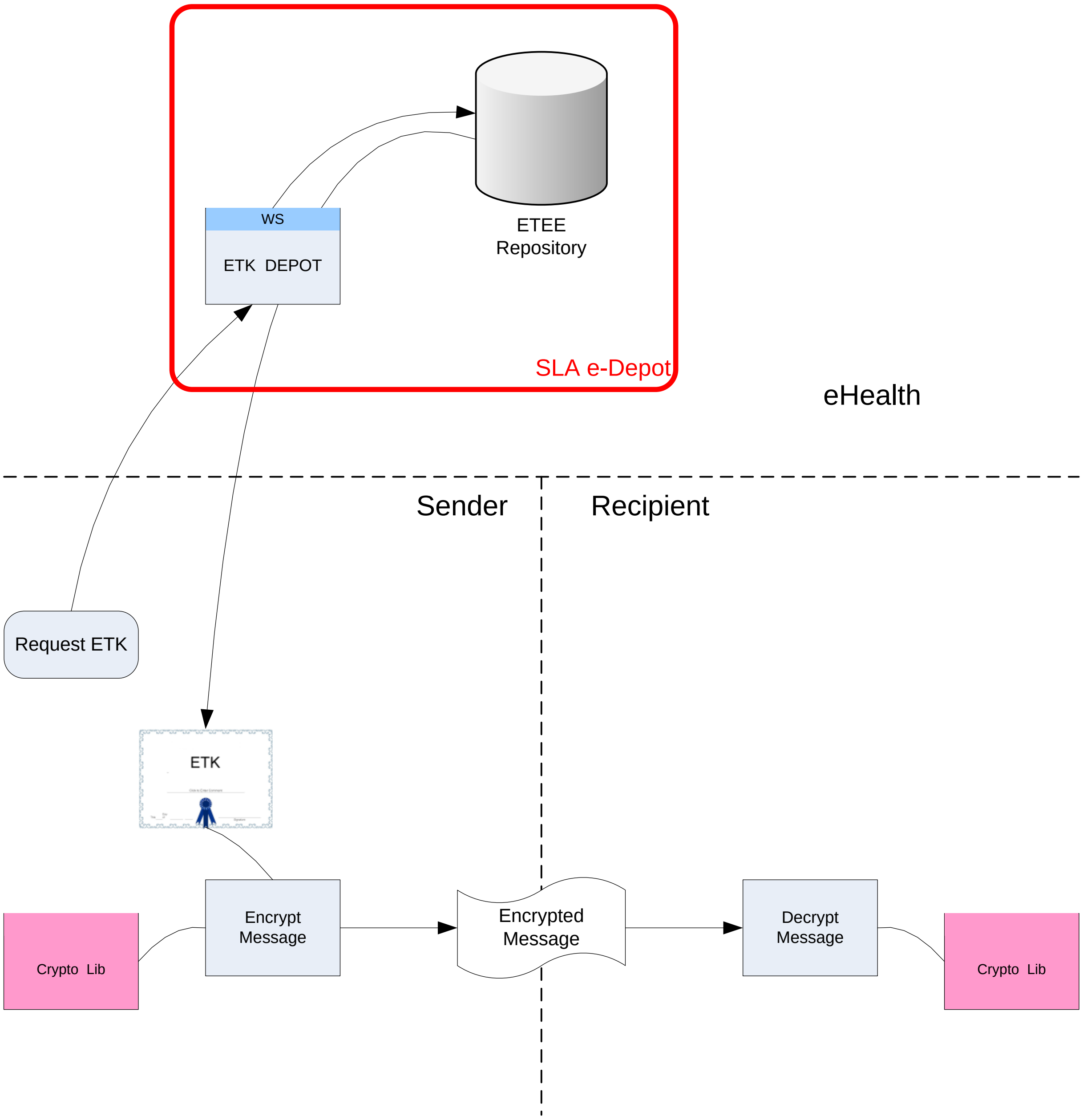


3.1.1.1. *Encryption / decryption for Known Recipients*

Before sending an encrypted message to a Known Recipient, the sender needs to get the public key of this addressee. This is done by using the web service "ETK Depot"[2]. He can then encrypt the message locally and send it to the Recipient.

The Recipient owns the Private key, with which he can decrypt the message locally.

The scope of "ETK Depot" only covers the request and download of the Public ETK.

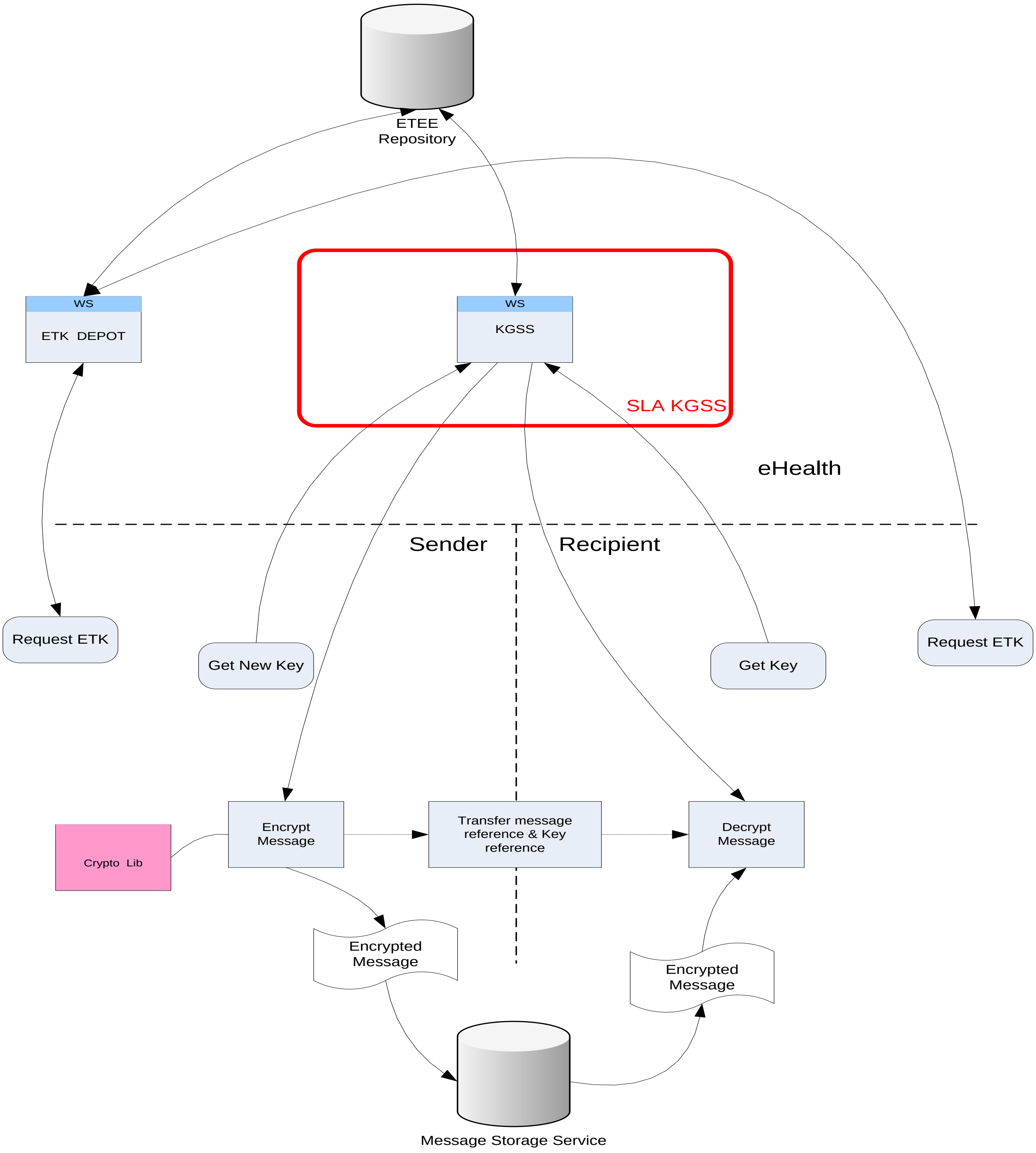


[2] Attention: This needs to be done for every message sent.

3.1.1.1. Encryption / decryption for Unknown Recipients

The process of sending encrypted messages to unknown recipients, is a sequence of encrypted communications both between known and unknown recipients (e.g.: to be able to communicate with the KGSS – the web service that provides the symmetric keys for unknown recipient – an ETK for known recipients is needed).

Only the transactions with the KGSS are in the scope of this Service.



3.2. Business criticality

The business criticality of the “register an ETK” functionality is **Bronze** as a single user should register an ETK only once every 3 years. Nevertheless, the eHealth platform monitors the performance and availability of this service in order to react on any strange behaviour

The business criticality of the “request for ETK of addressee” is **Gold** as it supports every encryption.

3.3. Interdependencies

The services covered by this Service Level Agreement are functionally dependent upon services offered by the CA.

The encryption web service depends on the Certification eHealth basic service to ensure that only authorised entities can have access to the service.

3.4. Service Objectives - Overview

Service	KPI	SL ID	Condition	Measure based on	Limit	Service Window	Objective Committed	Objective Target
ETK Depot	Availability ETK Depot	ETD1	Test script passes	Fictitious request		Mo – Su 0:00 – 24:00	99,5%	99,9%
	Performance – Response time for ETK Depot	ETD2	Response time ≤ 1 sec	Real transactions		Mo – Su 0:00 – 24:00	98%	99%
KGSS	Availability KGSS	ETK1	Test script passes	Fictitious request		Mo – Su 0:00 – 24:00	99,5%	99,9%
	Performance – Response time for KGSS “Get Key” and “Get New Key”	ETK2	Response time ≤ 1 sec	Real transactions		Mo – Su 0:00 – 24:00	90%	95%

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

3.5. Service Objectives – Details Services concerned with registering an ETK

3.5.1. Availability ETK Depot

<table>
<tr><th colspan="5">Objectives</th></tr>
<tr><td>Definition</td><td colspan="4">• The ETK Depot service is considered to be available when the following test is correctly executed:
○ Look-up a nonexistent record
○ Returning the corresponding Error message
○ If the Error message is as expected, the test was successful
• Planned interventions executed within the Maintenance Window are not recorded as unavailable time.</td></tr>
<tr><td>Measuring method</td><td colspan="4">• The availability of the different functionalities is measured by executing the test scripts every 10 minutes. When the script is executed with as result a Status “OK”, the test “passed”.
• When the script is executed with an other result, the test “failed”</td></tr>
<tr><td>Calculation</td><td colspan="4">$Availability = \frac{\sum Passed\ Tests\ x\ 100}{\sum Total\ Tests} \%$
○ Total Tests = Total number of tests launched within corrected timeframe
○ Passed Tests = Total number of tests that resulted in a status “OK” within the same timeframe
○ Corrections are applicable on tests that are not taken into account because they were caused :
▪ by a Validated Authentic Source or partner application out of scope of this SLA
▪ by a failing monitoring tool</td></tr>
<tr><td>Reporting and evaluation period</td><td colspan="4">• The availability is calculated and reported monthly. Corrective actions are initiated when appropriate.
• The formal evaluation however is done on a yearly basis.</td></tr>
<tr><td rowspan="3">Service Level Objectives</td><th rowspan="2">Functionality</th><th rowspan="2">Service Window</th><th colspan="2">Service Level Objective</th></tr>
<tr><th>Committed</th><th>Target</th></tr>
<tr><td>ETK Depot</td><td>Mon – Sun 0:00 – 24:00</td><td>99,5%</td><td>99,9%</td></tr>
</table>

3.5.2. Performance ETK Depot

<table>
<tr><th colspan="2">Objectives</th></tr>
<tr><td>Definition</td><td>• The performance of the ETK Depot Service refers to its response time. Response time meaning the time needed to execute a request. This request can be
○ Deliver an ETK to a requestor
• Attention: The response time does not include:
○ The time needed to deliver the information over the Internet
○ The time needed to process the information at the End Users premises.</td></tr>
<tr><td>Measuring method</td><td>• This response time is measured on the Reverse Proxies. Both start time (request received) and stop time (answer sent to the End User) are measured and stored in a database.
• Measuring is done on real transactions, and only on those having a “stop time” within the measuring period.</td></tr>
<tr><td>Calculation</td><td>• All response times are calculated: Stop time – Start time for every request.
• The percentage that meets the target is calculated based on following formula:
$$Performance = \frac{\sum Tests\ meeting\ the\ target\ \ x\ 100}{\sum Total\ Tests}\%$$</td></tr>
<tr><td>Reporting and evaluation period</td><td>• The performance is calculated and reported monthly. Corrective actions are initiated when appropriate.
• The formal evaluation however is done on a yearly basis.</td></tr>
<tr><td>Service Level Objectives</td><td>
<table>
<tr><th rowspan="2">Functionality</th><th rowspan="2">Target</th><th colspan="2">Service Level Objective</th></tr>
<tr><th>Committed</th><th>Target</th></tr>
<tr><td>Performance ETK Depot</td><td>1 sec</td><td>98%</td><td>99%</td></tr>
</table>
</td></tr>
</table>

3.5.3. Availability KGSS

<table>
<tr><th colspan="5">Objectives</th></tr>
<tr><td>Definition</td><td colspan="4">• The KGSS service is considered to be available when the following test is correctly executed:
○ Execute a wrongly formatted request “Get New Key”
○ Check the returned Error message
○ If the Error message is as expected, the test was successful
• Planned interventions executed within the Maintenance Window are not recorded as unavailable time.</td></tr>
<tr><td>Measuring method</td><td colspan="4">• The availability of the different functionalities is measured by executing the test scripts every 10 minutes. When the script is executed with as result a Status “OK”, the test “passed”.
• When the script is executed with an other result, the test “failed”</td></tr>
<tr><td>Calculation</td><td colspan="4">$$Availability = \frac{\sum Passed\ Tests\ x\ 100}{\sum Total\ Tests}\%$$
○ Total Tests = Total number of tests launched within corrected timeframe
○ Passed Tests = Total number of tests that resulted in a status “OK” within the same timeframe
○ Corrections are applicable on tests that are not taken into account because they were caused :
▪ by a Validated Authentic Source or partner application out of scope of this SLA
▪ by a failing monitoring tool</td></tr>
<tr><td>Reporting and evaluation period</td><td colspan="4">• The availability is calculated and reported monthly. Corrective actions are initiated when appropriate.
• The formal evaluation however is done on a yearly basis.</td></tr>
<tr><td rowspan="3">Service Level Objectives</td><th rowspan="2">Functionality</th><th rowspan="2">Service Window</th><th colspan="2">Service Level Objective</th></tr>
<tr><th>Committed</th><th>Target</th></tr>
<tr><td>KGSS</td><td>Mon – Sun 0:00 – 24:00</td><td>99,5%</td><td>99,9%</td></tr>
</table>

3.5.4. Performance KGSS

<table>
<tr><th colspan="2">Objectives</th></tr>
<tr><td>Definition</td><td>

- The performance of the KGSS Service refers to its response time. Response time meaning the time needed to execute a request. This request can be
  - Respond to a “Get Key” request
  - Respond to a “Get New Key” request
- Attention: The response time does not include:
  - The time needed to deliver the information over the Internet
  - The time needed to process the information at the End Users premises.

</td></tr>
<tr><td>Measuring method</td><td>

- This response time is measured on the Reverse Proxies. .Both start time (request received) and stop time (answer sent to the End User) are measured and stored in a database.
- Measuring is done on real transactions, and only on those having a “stop time” within the measuring period.

</td></tr>
<tr><td>Calculation</td><td>

- All response times are calculated: Stop time – Start time for every request.
- The percentage that meets the target is calculated based on following formula:

$$Performance = \frac{\sum Tests\ meeting\ the\ target\ \ x\ 100}{\sum Total\ Tests}\%$$

</td></tr>
<tr><td>Reporting and evaluation period</td><td>

- The performance is calculated and reported monthly. Corrective actions are initiated when appropriate.
- The formal evaluation however is done on a yearly basis.

</td></tr>
<tr><td>Service Level Objectives</td><td>
<table>
<tr><th rowspan="2">Functionality</th><th rowspan="2">Target</th><th colspan="2">Service Level Objective</th></tr>
<tr><th>Committed</th><th>Target</th></tr>
<tr><td>Performance “Get Key” and “Get New Key”</td><td>1 sec</td><td>90%</td><td>95%</td></tr>
</table>
</td></tr>
</table>