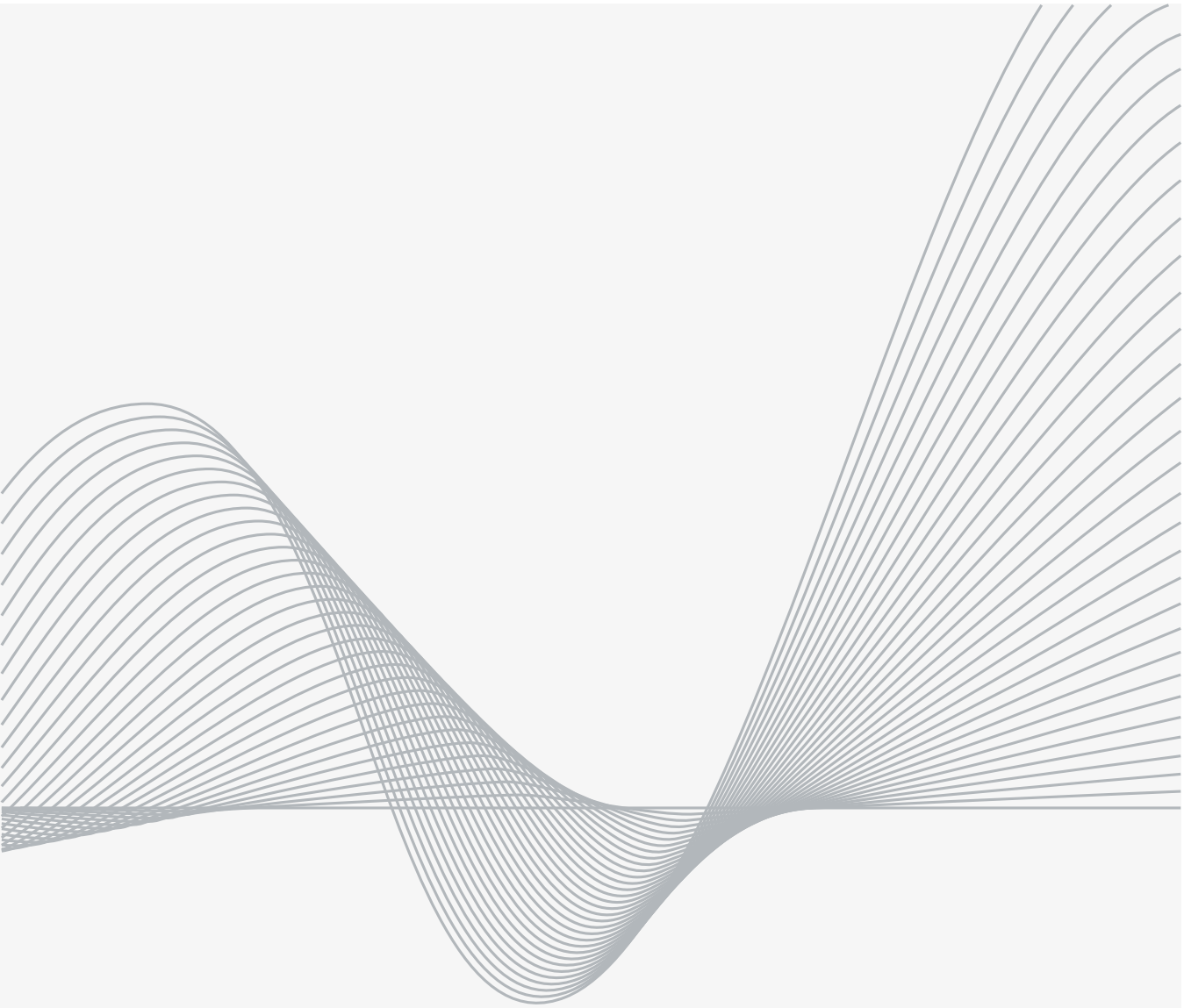
Service Level Agreement

Presto



Simac IDS ltd

2 Huddersfield Road
Stalybridge,
Greater Manchester
SK15 2QA

T: +31 (0)40 258 21 10
E: info@simac-ids.com

Company number: 11129016
VAT number: GB290711018

SIMAC-IDS.CO.UK

CUSTOMER – TBA

Service Level Agreement

Presto

Date:	2026
Reference:	TBA
Created by:	< Support >
Document version:	1.5
Document status:	Ready
Classification:	Public

Version	Date	By	Description
0.1	11-04-2016	Rob Geraedts	Initial document
0.2	13-04-2016	Alexi Muns/Rob Geraedts	Review
1.0	22-04-2016	Alexi Muns/Rob Geraedts	Final
1.1	02-02-2017	Rob Geraedts	Annotations
1.2	06-02-2018	Rob Geraedts	Review
1.3	17-02-2019	Rob Geraedts	Annotations
1.4	28-12-2021	Lars Teulings	Design Lay-out Change
1.5	08-01-2024	Christian van Deuren	Updates to services
1.6	14-01-2026	Judy Voykovic	Review

This document has been created with care and tailored for you. To prevent unlawful use, we would like to point out that nothing of this document may be reproduced and / or made public by means of print, photocopy, scan or any other way, without the prior written permission of Simac IDS ltd.

Table of contents

Table of contents 3
General 5
Introduction 5
Glossary 5
Presto in a SaaS environment 7
Production environment 7
Test/acceptance environment 7
Performance 7
User access 8
Security 8
Authorised access 8
Physical access security of the application server 9
Data backup and restore 9
Protection against internet attacks (DDoS) 10
Service Levels 11
Availability 11
Processes 11
Maintenance & incidents 12
Malfunctions and defects 12
Disaster Recovery 13
Out of scope cases 13
Test/acceptance environment issue prioritization 13
Fix process 14
Reporting issues/defects 14
Service Portal 14
Issue follow-up and process 14
Maintenance 15
General 15
Releases process 16
Warranty 16
Firmware 16

Hardware.....17
Special provisions.....17
Escalation Procedure.....18

CHAPTER 1

General

Introduction

This Service Level Agreement (SLA) is part of the contract for the use of the **Presto** software service. Presto is a student attendance registration and engagement monitoring & reporting system. Presto is offered as Software as a Service (SaaS).
The agreement is between

- Simac IDS (referred to as Supplier)

And

…… (referred to as Customer)

Wherever this document refers to *Presto*, it refers to the current version – V4.0 - and all future versions of Presto. In the remainder of this document, Presto will be referred to as the "Application"

This SLA covers the offering of the Application as Software as a Service.
This SLA also covers support on the reports that are provided within the Application.
This SLA also describes the quality of service and the way this is measured and reported.
This SLA is effective from the moment the Customer has taken the production environment into service.
This SLA has the same period of validity as the contract for the use of the Application.

Glossary

Adaptive maintenance	Update & version management and deployment.
Availability (of the system)	The system is available if it can be reached via the Internet to perform the tasks it is intended for. Availability does not consider any customer infrastructure.
Backup	Securing the database by creating a copy. If in contract, also storing the data on a co-location.
Corrective maintenance	Problem solving maintenance, also available during office hours (unless agreed upon otherwise).
Digibook observation	A registered attendance of a student via the DigiBook.
DTAP	Development, Test, Acceptance and Production environments
Force Majeure	An extraordinary event or circumstance beyond the control of the parties, such as a war, strike, riot, crime, hurricane, flood, earthquake, volcanic eruption, etc., energy failure at supplier premises or wider area, internet failure at internet exchange or provider.
Innovative Maintenance	Customer specific or generic continuous development of Presto.

Leaves / explained absences	A registered date/time period that defines the absence of a student, together with a reason and description
MTBF	Mean Time Between Failure
Opening times / opening hours	The time between 08:00 and 17:00 hrs. UK time, in which the service desk is manned.
Patch	Temporary solution to fix an issue.
Performance	The response/reaction time of the system during normal operation.
Presto	Student Attendance registration and engagement monitoring & reporting system.
Preventive Maintenance	System clean-up maintenance for performance improvement and/or new study year.
Production environment	The environment that runs the customer's live system and database, that is used by students, academics and staff.
Recovery Point Objective (RPO)	The maximum targeted period in which data might be lost.
Recovery Time Objective (RTO)	The targeted duration of time within the system must be restored after a disaster or disruption.
Regular Scheduled maintenance	Maintenance activities that take place outside of office hours (unless agreed upon otherwise).
Resolution time	The time between registration of an incident by the customer and the solution that fixes the system degradation/disruption
Response time	The time between the registration of an incident by the customer and the start of the triage/investigation by a service engineer.
SAAS	Software as a Service.
Test/acceptance environment	A separate environment where all new features, links and/or interfaces are functionally tested with customer datasets and
	where new versions or features are accepted by the customer.
UAT	User Acceptance Test.
Work-around	Temporary solution to circumvent a problem.
Working day	An 8-hour period on Monday through Friday, except for public holidays. On Dutch public holidays, 2nd and 3rd level telephone support will be available.
Working hours	Hours within a working day, within opening hours.

CHAPTER 2

Presto in a SaaS environment

The staff of an educational institution has access to two Presto environments. Below is a description of both environments. For the remainder of this SLA, Presto production environment is assumed, unless specifically stated otherwise.

Production environment

This is the environment, where the “live” attendance is registered.
The production environment availability and response to issues is described in the chapter “Service Levels”.
The Application is available 24 hours a day, 7 days per week.
Regular maintenance (e.g., replacing hardware) or software updates based on Adaptive or Innovative maintenance will not be performed during *opening hours*, unless Supplier and Customer agree otherwise.
Any maintenance action will be communicated with the Customer at least 30 days in advance.
Maintenance will always be planned with the agreement of the Customer.

Corrective maintenance (solving critical or urgent disruptions) may take place during opening hours, after contacting and agreement with the Customer.
Disruptions that are less urgent, will be handled outside the opening hours.

The system’s availability will be monitored continuously. If the system should be disrupted in any way, an SMS and email alert system will make sure that the necessary persons are informed immediately to take action to start the correcting process. Furthermore, designated persons of the Customer will be notified according to the service levels described in the chapter Service Levels.

Test/acceptance environment

This environment is intended for performing tests and accepting new features/versions of the Application.
The test/acceptance environment will be kept up to date with respect to new versions.
This environment may also be used for training purposes. Supplier and Customer can make separate arrangements regarding keeping the data in the test/acceptance environment up to date.

As it is updated more often, the availability of the test/acceptance environment cannot be guaranteed according to the same service level as the production environment. Therefore, the service levels as described in the chapter “Service Levels” do not apply to this environment. Supplier will make the best effort to provide as high as possible availability.
Regular Scheduled Maintenance regarding connections to other, external systems will be performed in the standard service window of the Customer.

Performance

The response time of a web application depends on several things, like the web server response time, the quality of the (inter)network connection, the brand/version of the browser and the speed of the PC used.
The response time of a “card read” will mainly depend on the quality of the (inter)network connection. In uninterrupted situations (i.e., where there is unobstructed (inter)network, Supplier guarantees to respond

to a card read within 3 seconds. This will be guaranteed up to 40 card reads (40 readers) simultaneously. If over 40 cards are presented simultaneously, all cards will be scanned. Any readers that are unable to access the server immediately, due to heavy load, will store the scanned card until the reader is able to reach the server again. At this point, the card information will be synced. In offline mode, students can continuously scan cards. All card scans will be stored and synced later (normally after 1-2 minutes).

The process of daily backups could lead to some temporary delay of the system. Therefore, backups will be created at night-time, between 01:00 hrs. and 06:00 hrs. UK Time.
During the day, incremental backups of the database are made and stored on the database server itself. The incremental backups are small, and they do not decrease system performance.

The performance of the test/acceptance environment may differ from that of the production environment.

User access

The Application can be accessed through any computer with an Internet connection that is equipped with a modern Internet browser. Supplier supports the following browser brands:

- Google Chrome
- Mozilla Firefox
- Microsoft Edge
- OSX Safari

Regarding browser software versions, Supplier will support at least the current major version of the browsers listed above. If other Internet browsers or older versions of the brands above are used, the Application may be less secure or suffer from lower performance.
Supplier aims to support any new version of before mentioned browser brands, within 6 months after their release.
Supplier cannot keep track of the support for all past browser versions. Supplier can make a special effort to support other/older browser at additional cost.

CHAPTER 3

Security

Authorised access

With respect to the access to (personal) data stored in the Application, the following applies:

- Users of the application must identify themselves by means of a username and a password. Additionally, extra security can be applied by introducing tokens.
- Users are limited to 3 consecutive failed login attempts. After 3 failed attempts, the user account will be blocked.
- Every login attempt is logged within the system. For analysis purposes, the log file is kept for a minimum of 2 years and a maximum of 5 years. Customer will inform Supplier of Supplier's and/or UK law requirements on retention of logging information, so Supplier can configure the system accordingly.

- All communication between the server and the user PC is encrypted by default, using industry standard encryption methods.
- To assure an acceptable security level, the Customer will make sure that all users use passwords that are considered to be “strong”. For a password to be considered as “strong” it should:
    - Be at least 8 characters long
    - Contain at least 1 lower case letter
    - Contain at least 1 upper case letter
    - Contain at least 1 digit or symbol

Customer and Supplier already agreed on the use of AD with LDAPS. Login credentials, password security level and the block/unlocking process are handled in the AD.

Physical access security of the application server

The following security measures and protocols apply to the physical access security of the application server:

- Only system administrators of the hosting company have access to the physical server room containing the servers that the Application is installed on. Every system administrator has an electronic key that allows access to the server room. When system administrator roles change (e.g. people leaving the company), the access by this electronic key will be blocked immediately.
- Employees of the hosting company are bound to a non-disclosure agreement with the Supplier.
- The hosting company always holds an up-to-date list of all personnel that has access to the server room.
- The hosting company has instructions and procedures in place that describe to their employees how to manage personal data from others.
- The hosting company manages the total security of their premises and uses the services of a professional security company to manage and enforce this.
- Supplier will audit the hosting company procedures once every calendar year.

Data backup and restore

All Application data is stored in a database. To prevent possible data loss and for the purpose of disaster recovery, a backup procedure is in place:

- A full backup of the system database is made every night between 01:00 hrs. and 06:00 hrs. UK Time. This backup is stored at a separate, external hosting company.
- During the day, incremental backups of the database are made and stored on the database server itself. The incremental backups are small, and they do not decrease system performance.
- Once every quarter (3 months) the Suppler performs a full backup – restore cycle on the test/application environment. This is to test that the system can be quickly restored in case of a major failure or disruption.
- Restoring the system, using a backup, as a result of support or maintenance activities by the Supplier are free of charge.
- On request of the Customer, the Supplier can restore a specific situation using a backup file. Restoring a backup on customer request is always a specific case that will be planned between Customer and Supplier. These actions will be charged. A cost estimation or fixed offer will be

made in advance. On-demand restore actions will only be done if/when the action will not interfere with the service of other customers of the Supplier.

- Supplier can achieve an RTO of <= 8 hrs. The RTO can be achieved when an incident is reported within the Service Desk opening hours.
- Supplier can achieve an RPO of <= 8 hrs. The RPO can be achieved when an incident is reported within the Service Desk opening hours.

Protection against internet attacks (DDoS)

The Application is provided as SaaS and the service is accessed via the Internet. Unfortunately, nowadays Internet servers more and more suffer from Internet attacks. Most common attacks nowadays are called “Distributed Denial of Service” or DDoS attacks. Especially banks and government web sites have been subject of attack, lately.
These attacks are targeted to overload a server or web page, by making tens or hundreds of thousands requests to a server every second. As servers are normally not capable of handling so many requests, they become overloaded. This means that normal operation (the service they were designed for) stops. A DDoS attack normally does not expose any data to unauthorized people. It is merely a disruption of the service itself. Nevertheless, during a DDoS attack, the service could become temporarily unavailable.

Although Supplier will take all measures within their power to prevent any unauthorized access to Customer’s data, avoiding a DDoS attack is almost impossible.
To minimize the effect of a possible DDoS attack, Supplier can offer a separate service that actively monitors the Application server connection. If a DDoS threat is detected, this service will reroute the internet traffic and then attempt to filter out the “normal” Application service traffic from the DDoS traffic. This would then result in a situation where normal operation can continue instead of it being blocked completely by the DDoS traffic.
To be able to filter the traffic, extensive systems have to be put in place, resulting in a serious increase in cost. To be able to offer a filter system at an affordable price, a solution was designed that:

A. Only kick-in when necessary
B. Is shared with other Customers

The service, “NaWas” is available as standard. It has proven to knockoff most common (small to medium) DDoS attacks. It is however no insurance that it can handle all (especially very big) DDoS attacks.

CHAPTER 4

Service Levels

In case of an incident or disruption of the Application, Supplier will do everything within their power to restore normal operation within the shortest possible time, in the most efficient way.

Availability

The Presto system is available 24/7 365 days a year (excluding any planned maintenance). The system will have an availability of 99,9%, during opening hours.

Processes

To categorize the service levels, this SLA distinguishes two processes in the Application: •

Primary process

This process includes the following Application functions:

○ (card) Scanning ○

Explained absences ○

DigiBook observations

- Secondary process

  This process includes the following Application functions:

  - Assess
  - Managing
  - Report
  - Administration

The SLA distinguishes 3 incident priorities:

Priority	Cause
Critical	• As a result of a disruption of the **Primary** Process, use of the Application is not possible for more than 10% of the users.
Urgent	• As a result of a disruption of the **Primary** Process, use of the Application is not possible for less than 10% of the users. • As a result of a disruption of the **Secondary** Process, use of the Application is not possible for the specific Secondary process functions.
Routine	• As a result of a disruption, the availability and use of the Application is not impaired immediately.

Based on the 3 priorities, the following service levels will be used

Priority	Response time	Status reports	Fix available	Final solution
Critical	< 15 min. (phone) for 98% of incidents	Continuously, at least every 2-3 hours.	< 8 working hrs. for 98% of incidents	< 2 working days
Urgent	< 4 working hrs. for 98% of incidents	Per incident	< 16 working hrs. for 98% of incidents	< 6 working days
Routine	< 8 hrs. for 98% of incidents	N/A	N/A	< 10 working days

- Response times are valid on working days. An exception is made for *force majeure* situations.
- With incidents, every "change" or information item is logged in the service portal and this will result in an email being sent out to the registered service email address of the Customer.
- Any action that needs to be taken, will be done in consultation with the Customer.

Maintenance & incidents

Maintenance of the Application includes:

1. Corrective maintenance
2. Preventive maintenance
3. Adaptive maintenance
4. New versions (fixed intervals)

Any change or update to the Application will be made available to the Customer. Any change or update will be made available in the Test/Acceptance environment first. The supplier will inform the Customer about any implications that the change might have for the Customer, as far as the Supplier can foresee them. Every change will be accompanied by appropriate release notes. Planning for the production will be made in consultation with the Customer.

Any new release is proposed to the customer. Together with the customer, it is decided if and when to install the update. A new version update could be marked as "mandatory" by the Supplier, due to e.g. security issues.

Service of the Application includes:

1. Phone or service portal support for incidents or questions
2. Documentation for the Application

Malfunctions and defects

Any issue (malfunction or defect) that is reported by the Customer will be registered by the Supplier, if it meets the following criteria:

- The issue is demonstrable and reproducible, and
- The issue occurs in the operational (Production) environment of the Customer

If the issue occurs in the Test/Acceptance environment, the Customer will discuss the priority with the Supplier.

Disaster Recovery

The standard offering is 99,9% availability. For immediate Disaster Recovery, Supplier have backups and snapshots available, to restore the system. If Customer wishes to go to a higher level of availability, a redundant server solution can be offered, raising the availability to 99,95%.

Out of scope cases

Supplier will register all support requests. Not all requests, however, are part of the SLA. For example:

- Questions regarding the Customers wish to develop their own reports
- Questions about system configuration that is described in the Application documentation
- Questions about Customer specific configurations or features, outside of the standard Application configuration options

On request (by an authorized contact of the Customer) Supplier can offer to handle these requests at extra cost.

Test/acceptance environment issue prioritization

In consultation between Customer and Supplier, reported issues/defects in of the test/acceptance environment will be classified into priority categories that indicate the priority in which they will we handled and/or followed up. Priority categories have defined response and repair times. Supplier will solve the issue within the response/repair time of the specified category, in at least 85% of the cases. Supplier continuously strives to increase this percentage.

Next to issues and defects, the Customer may also contact Supplier with questions regarding the use of the Application. Questions regarding the use of the Application, for which the Application documentation does not provide enough information, will also be classified using the same priority categories.
If a Customer's question arises from insufficient knowledge of the Application, although this knowledge is presumed to be known, Supplier has the right to lower the priority of the question and/or defer the follow-up of the question. Supplier will then contact the Customer to discuss action to be taken to raise the Customer's knowledge level.

Priority		Response time (Working hrs. / working days)	Recovery time (Working days)
1	A feature/function cannot be used.	< 6 working hours	< 3 working days
2	A decrease of the performance is observed. The response to a "click" on a function of the Primary Process should not take longer than 5 seconds.	2 working days	Patch*

*) The solution will basically be delivered via a patch, if the defect has been reported at least 20 working days before the delivery date of a release. Supplier may also decide to offer, for the sake of efficient maintenance, the solution in a future patch or release in consultation with the users.

Temporary fixes by means of work-arounds or problem avoiding restrictions will always be accompanied by appropriate documentation by the Supplier. In case serious issues/defects cannot be fixed within the designated time, the Supplier will immediately inform the Customer. If issues/defects can also influence other customers, those will be informed immediately too.

Fix process

Supplier will continuously share information about the progress of fixing the issue/defect. Additionally, once every quarter, Supplier will sit down with the Customer to discuss current issues. In the first 3 months after production start, this interval will be once every month.

In some cases, fixing of issues/defects is not covered by the SLA:

- Issues that arise from improper use of the Application by the user
- Issues that can be traced back to the Customer (user(s)) not following Suppliers binding opinion regarding the use of the Application. Issues will be treated “per situation”. Users are at least expected to follow the users’ manuals and “behave” as they have been taught in the training that the supplier has provided.

Reporting issues/defects

Service Portal

Issues scan be reported to the Supplier’s service portal. With a personal login, designated employees of the Customer can login to the Service (web) Portal and report an issue. The issue report form will guide the customer through a series of questions to help clarify the circumstances of the issue/event. The Customer will receive an automatic confirmation of the reported issue. The Customer can see the reported issue in the portal. As soon as the Customer’s Support department picks-up the issue, the Customer is notified by email. All communication regarding a reported issue should be done in the Service Portal. Both Customer and Supplier can view all communication there.

Within the time stated in the priority matrix the issue will be picked-up by a service engineer.
During opening hours, Critical issues can also be reported by phone, via +31 (0)40-2582126. Service Engineers of the Supplier are available during opening hours, on Working Days.

Issue follow-up and process

When an issue is reported, the supplier will respond according to the description of the SLA levels in section 4.1. The initial report will be done by the customer, via the supplier’s service portal. Customer will get an automatic email confirming the receipt of the issue report.
As soon as the issue is picked-up by a service engineer, Customer and Supplier’s service department will communicate via the service portal. In the portal, all communication and information on the issue is gathered.

Issues will normally we fixed within the time frames that Customer and Supplier have agreed upon. As soon as 50% of the fixing time has passed, Supplier will inform the Customer about the status of the solution and the expected remaining time before the solution can be implemented.

CHAPTER 5

Maintenance

General

Supplier will maintain the Application actively. Supplier will strive to implement any official (governmental) changes in laws or legislations, within the term that the UK government has set it to be into force. However, to be able to do so, supplier will require customer's information on new or changed regulations.

Supplier will actively inform the Customer about:

- Known issues in the Application
- Changes
- Releases
- Patches

The Customer is expected to actively monitor any information, received from the Supplier (by email, phone, Internet or otherwise) and relay this information to the appropriate employees and/or departments of the Customer. The Customer will immediately inform the Supplier in case of any change of contact persons or contact person contact details (e.g. phone numbers or email addresses).

Supplier distinguishes the following types of maintenance: •

Regular Scheduled maintenance
Maintenance activities that take place outside of office hours (unless agreed upon otherwise).

- Corrective maintenance
  Problem solving maintenance, also available during office hours (unless agreed upon otherwise).
- Preventive Maintenance
  System clean-up maintenance for performance improvement and/or new study year.
- Adaptive maintenance
  Update & version management and deployment.
- Innovative Maintenance
  Customer specific or generic continuous development of Presto.

Supplier will ensure that the Customer receives information about upcoming new versions, updates, patches etc. In consultation with the Customer, the Supplier will make newly released software available in the Customer's test/acceptance environment.
Exception to this procedure may be patches, as result of blocking issues or defects to the primary process. In consultation with the Customer, the Supplier may implement them directly on the Production environment.

The Supplier will actively inform the Customer about changes and their impact, by means of Release Notes.

Releases process

Customers of the Application will deliberate with the Supplier about (new) functions and features to be included in the next release. A release calendar s kept and distributed among all Customers of the Application.
When a new release is pending, the Supplier will go through a release acceptance process. Supplier will execute internal acceptance tests and will create the appropriate release documentation. In case of major updates and/or patches that have considerable impact, the Supplier will deliberate with the Customers of the Application to find the most appropriate release date and time. Lead time numbers are indicative. Supplier will always consult the Customer before planning a release.

The release process steps are listed below:

Step	By	Lead time
Announcement of an update, through the release calendar **Announcement of a patch**	Supplier	
Accepted to deploy the release or patch, on the test/acceptance environment	Customer	
Deploy to test/acceptance environment	Supplier	1 week
User Acceptance Test (UAT)	Customer	1 week
Solve remaining issues (if any)	Supplier	1 week
User Acceptance Test	Customer	1 week
Accepted for deployment to Production environment	Customer	
Release to Production environment	Supplier	1 week

CHAPTER 6

Warranty

Firmware

Supplier guarantees that, for the term of this SLA:

- When used for the intended purpose, any system firmware will keep the functionality and will keep operating according to the properties and specification as agreed upon and/or described at the time the SLA was entered.
- There will be no security measures or security functions built into the firmware, other than those described in the documentation.
- The firmware is free of any alien artifacts like viruses, worms etc.

Any new firmware release is proposed to the customer. Together with the customer, it is decided if and when to install the update.

The firmware updates are done with a maximum of once a year. In case of an update, the Supplier would require remote access to your reader network (VPN or equivalent) to perform the update.
A firmware update consists of making a network connection to a reader and then send a new firmware version to it. The update process is normally done either 1-by-1 or in small batches.

Hardware

Hardware warranty on all material and manufacturing defects is 1 year.
The warranty period starts as soon as the device is installed and configured in the Application. In case of a warranty claim, the Supplier will either repair the device or replace the device with an equivalent replacement device.

It is common practice to hold a buffer stock of pre-configured devices, to swap if needed. Supplier advises Customer to have 1% of devices as “swap” buffer stock.
In case of a reported hardware failure by the Customer, Supplier will send a new device to Customer within 1 week. Customer can send the defective device back to Supplier.

The MTBF, based on current figures (1-2017) of the supplier, is 5 years. The technical lifetime of the devices is expected to be 7-10 years.

Special provisions

Third party hardware, as well as operating systems or other (third party) software is no part of this agreement, unless stated otherwise.
The following occurrences, issues and defects are not covered by this agreement:

- Any disturbance or defect that was caused by operating errors or by use of the system for purposes other than which it is intended / suitable for. This also includes any damage caused by the use of the system in a way it is not intended for and/or suitable for, e.g., power surges, mechanical shocks, water damage, submerging in liquids etc.
- Disturbances of defects caused by problems with the network or power infrastructure.
- Unnecessary on-site visits by employees of the Supplier or their third-party partners, after customer’s request.
- Damages due to moving equipment or maintenance/repairs to equipment performed by others than those authorized by the Supplier.
- Repairs to fix defects or decreased system quality that were caused by hardware or software components that were not delivered by the Supplier, or, caused by bad power supply and/or telecommunication connection.
- Any damage due to negligence, accidents, burglary, theft, assault and vandalism, sabotage, strikes, demonstrations, or other violence
- Any cost for services requested by the Customer
- Any the errors that in whole or in part are the result of incorrect, careless, or incompetent use and/or use for other than normal (business) purposes, external causes (for example, moisture, incorrect mains voltage, lightning, static electricity, etc.) or caused by products that have been modified, damaged or opened by parties other than the Supplier.

CHAPTER 7

Escalation Procedure

Any request for support should be reported via the Supplier's service portal. With a personal login, designated employees of the Customer can login to the Service (web) Portal and report an issue. The service portal will generate an automatic confirmation of the reported issue. The Customer can see the reported issue. As soon as the Customer's Support department picks-up the issue, the Customer is notified by email. All communication regarding a reported issue should be done in the Service Portal. Both Customer and Supplier can view all communication there.

- The Service Portal is available 24/7. Telephone support for the 1st escalation level is available during opening hours, on working days.
- Telephone support for the 2nd escalation level is available during opening hours and, on basis of best effort, from 07:00 to 22:00 hrs. CET on working days.
- Telephone support for the 3rd escalation level is available during opening hours, on working days.

If the Customer feel that they do not get the desired result from their requests, the following escalation procedure is defined:

Supplier:

1st escalation level (default):

Helpdesk employee: central telephone number of the helpdesk.

- Service portal https://simac-ids.atlassian.net/servicedesk/customer/portal/2
- Urgent: Phone +31 (0)40-2582126 (opening hours / working days)

2nd escalation level:

Manager Support

- Email support@simac-ids.com
- Telephone +31 (0)40-2582110

3rd escalation level:

Director: Har Heuberger

- Telephone +31 (0)40-2582110

Customer:

1st escalation level

Functional Application administrator: ……

- Email …..
- Telephone …..

2nd escalation level ……..:

……

- Email .....
- Telephone .....

3rd escalation level

Director: .....

- Email .....
- Telephone .....

Thus, agreed upon and signed:

Date	Date.....
Place	Place .....
Name:	Name: H.J.M.L. Heuberger
Title:	Title: Director
.....	Simac IDS