BaaS Service description

The BaaS Services are described below. The Parties acknowledge that the descriptions of the BaaS Services may need to be updated from time to time and the Parties undertake to keep updated service description available to the Parties, Customers and Users.

General Description of BaaS

SUNETS cloud-based backup service is based on IBM Tivoli Storage Manager (TSM) and Cristie's Bare Machine Recovery for TSM (TBMR). The service is delivered from secure data centers with high availability. Data doesn't need to leaves Sweden because data centers are physically located within the country and are directly connected to SUNET.
The service is flexible: the user can control which data to be backed up, how backups should be encrypted and how long they will be saved. Major focus of the service is to give the user control over both their data and their costs. Below is a summary of the main features;
Built on IBM TSM and Cristie's TBMR.
100% disk-based storage, which means very fast restore of backups, including the use of Cristie's TBMR.
Comprehensive support for databases and applications, such as MS SQL, MySQL, DB2, MS Exchange.

High security

- Role-based access control tied to SWAMID
- Backups are encrypted both in transit and on disk

High Availability

- Disaster Protection - Data is stored in different geographic location (different than the users campus)
- Replication - option to save data in two geographic locations (allows for protection against force majeure disasters in IPnett data centers)
- Redundant connection to Sunet

Clear pricing model and predictable costs, please see Appendix 3

Service pricing model is based on the amount of data stored in the BaaS system. This means that the user pays for exactly the amount of data that actually needs to be stored to a backup. Through a feature in TSM called de-duplication, each part of a file only stores once, even if it's used multiple times. This means that the actual storage requirements for backup in general is lower than the data stored in the systems that is being backed up. The effect of de-duplication is difficult to be estimated but it is not uncommon to have 40-70%.
TSM uses a technique called Incremental Forever, which means that the files are only backed up when they have changed. This causes that the amount of stored security copies further minimizes, which further reduces storage requirements and thus the cost.

Service performance guarantees

The service supports at a minimum a 5 Gbit/s aggregated encrypted restore throughput per each customer (e.g. a University). The service, being disk-based, has very good parallelism and supports higher throughput than any typical individual SUNET-connected university's aggregated bandwidth (20 Gbps).

High aggregated restore performance is achieved through parallelizing restore sessions. The performance of the customers backup clients (servers) (CPU, Memory, disk buses, network bandwidth, OS tuning) is naturally not within control of the service. The bottleneck is typically that of the customer's individual server and it is not certain that a single client system have the performance to achieve neither backup nor restore at these aggregated speeds.

Being disk-based, the service has a major advantage over tape based backup solutions in supporting a high count of parallel restore sessions without running out of tape drives, which typically only have 3-5 tape drives.

The service will not impose any artificial rate limiting on performance per customer. If the service and the customer have capacity to deliver faster than the minimum bandwidth, this extra performance will be available.

Service functionality

The service consists of two major parts – service portal and backup/restore software.
The *end user to sign up for service uses the service portal*. The service also provides a restful API that allows for easy automatic scripting of deployments. Service portal user account is automatically provisioned upon first use, based on federated identity attributes. TSM backup client credentials are managed via the service portal. When a user enables backups, a user account for the machine is automatically created in TSM.

The user workflow for the BaaS solution is:

- The user signs in to the service portal
- User selects backups
- User selects "*new"* and what extra properties they desire (e.g., application specific backup)
- All settings are automatically created in TSM, provided that the user is authorized.
- A link to the relevant TSM-software package as well as pre-generated configuration files are created and available for download
- User installs TSM on the desired target, and either uses the provided configuration file, or do their own modification.

Backup of hosted virtual machines are handled similar to customer hosted machines, although the user work flow may be simplified:

- User signs in to the service portal
- User creates machine, authorization checks are performed
- User checks box with "backup for this service", authorization checks are performed
- All TSM-settings are automatically created;
- The user gets a link to a TSM-bundle for the relevant platform and a pre generated config file.
- Alternatively, the machine is already created, and the users wants to add backup later, then the user will do this from the properties of an already created machine In the case of backup-as-a-service the user signs in to the portal, the steps to create a BaaS object is similar.

If the user selects that backups should be encrypted and that the user should be the only one in control of the key, a warning message is displayed, informing the user of the importance of keeping the key under their control and that neither Customer IT nor IPnett can be of assistance to restore the data should they lose control of it.
A configuration file is created together with the TSM package for the relevant platform and is available for download. The user can select a key or have one generated from the interface, or, probably most commonly, decide the key on designated target machine.

A user identified as an administrator (based on identity federation attributes) has extended privileges and can access objects inside their own domain, even if they did not create these. This is to prevent IT from ending up in a loose-loose situation where important IT-systems have been created without involving IT, and a DR situation has occurred, perhaps after the original creator have changed roles, or quit a department.
The backup/restore software is based on IBM Tivoli Storage Manager – TSM. TSM clients need to be installed on each node that desires backup functionality. The client then authenticates against the server by username and password in an established TLS-tunnel. TSM will use a disk storage backend.

Service functionality changes
IPnett reserves the right to increase the list of supported platforms without prior notification. The support for EOL platforms and applications will be done on a best effort basis, and may require professional services to work around limitations of the platform.

IPnett will not in any way compromise or risk customer privacy due to the need for legacy clients. This may result in legacy clients needing professional services, or using dedicated servers for legacy clients.

IPnett will assist with migration paths and workarounds for legacy clients.

As of 2014-11, the service has full support for the following platforms:

OS	Latest TSM version	BaaS Support Level
AIX v6.1	7.1	AIX 64-bit: Full (With required minimum level of xIC.rte and xlsmp.rte filesets.)
AIX v7.1	7.1	AIX 64-bit: Full
HP-UX 11i v3	7.1	Itanium: Full
Linux RHEL 6	7.1	x86_64: Full i686: Full Power: Full zSeries: Full
Linux RHEL 7	7.1.1	x86_64: Full i686: Full Power: Full zSeries: Full
Linux SLED 11	7.1	x86_64: Full
Linux SLES 11		x86_64: Full Power: Full
Mac OS X 10.10	7.1.1	x86_64: Full
Mac OS X 10.9	7.1	x86_64: Full
Mac OS X 10.8	7.1	x86_64: Full
Solaris 11	7.1	x86_64: Full (with 7.1.1) SPARC: Full
Solaris 10	7.1	x86_64: Full (with 7.1.1) SPARC: Full
Windows Server 2012 R2 (6.3)	7.1	x86_64: Full i686: Full
Windows Server 2012 (6.2)	7.1	x86_64: Full i686: Full
Windows Server 2008 R2 (6.1)	7.1	x86_64: Full i686: Full
Windows Server 2008 (6.0)	7.1	x86_64: Full i686: Full

Windows 8.1 (6.2)	7.1	x86_64: Full i686: Full
Windows 8 (6.2)	7.1	x86_64: Full i686: Full
Windows 7 (6.1)	7.1	x86_64: Full i686: Full

As of 2014-11, the service has best effort support for at least the following platforms:

OS	**Latest TSM version**	**BaaS Support Level**
Linux RHEL 6.4 and newer	6.2	i686: Limited - workaround #1
Linux RHEL 6.3 and older	6.2	i686: Limited - workaround #2
Linux RHEL 5.3 or later	6.4	x86_64: - Limited - workaround #2 Power: Limited - workaround #2
Linux RHEL 5.3 or later	6.2	i686: - Limited - workaround #2 Power: Limited - workaround #2
Linux RHEL 4	5.5	i686: - Limited -workaround #2
Linux SLES 10	6.4	x86_64: Limited - workaround #2 Power: Limited - workaround #2 zSeries: Limited - workaround #2
Mac OS X 10.7	6.4	x86_64: Limited - workaround #1
SunOS 5.10	6.2	i686: Limited - workaround #1
SunOS 5.11	6.2	i686: Limited - workaround #1
Windows Vista (6.0)	6.4	x86_64: Limited - workaround #1 i686: Limited - workaround #1
Windows Server 2003 R2 (5.2)	6.3	i686: Limited - workaround #1
Windows Server 2003 (5.2)	6.3	x86_64: Limited - workaround #1 i686: Limited - workaround #1
Windows XP Professional (5.1)	6.2	x86_64: Limited - workaround #1 i686: Limited - workaround #1

Support Levels

Full
Full support means that Sunet BaaS service works according to specification. E.g. means in this context that IBM encryption libraries are sufficiently new to support TLS 1.2, and to all the functionality of the service is in the backup client.

Limited- Workaround 1
"Limited - workaround 1" means that IBM's support for the platform is best effort. It also means that support for TLS version 1.2 is missing in the encryption library. Workaround is to run the client over a TCP <-> SSL proxy on localhost, preferably *stunnel*, which uses the OpenSSL encryption library.
TSM version 6.3 and above supports client-side dedup.
TSM version 6.2.x and below leaves deduplication to the server instead, which is fully functional.

Limited- Workaround 2
In addition to the limitations of "Limited - workaround 1" here is also required backports of more modern versions of the packages stunnel and OpenSSL with support for TLS 1.2.

Other operating systems and OS versions may be supportable using professional services. IPnett will provide guidance for methods to achieve backups from unsupported platforms.

The service supports the following applications:

Microsoft Exchange:

- Microsoft Exchange Server 2010 SP2, and later maintenance levels: Standard or Enterprise Editions

- Microsoft Exchange Server 2013 CU2 and later CU and maintenance levels: Standard or Enterprise Editions Note: This is toleration level support. Exploitation of new features available with Microsoft Exchange Server 2013 is not available in this fix pack release.

- Microsoft Exchange Server 2007 SP3, and later Service Pack levels: Standard or Enterprise Editions - Using older but supported client.

- Microsoft Exchange Server 2010 SP1, and "Update Rollup 2 for Exchange Server 2010 (KB242517) and later rollup and later Service Pack levels: Standard or Enterprise Editions - Using older but supported client.

- Microsoft Exchange Server 2003 SP2 - Using older but supported client. IBM will likely drop the support for this client in the near future.

Microsoft SQL server:
The following application levels are supported for the x86 platform:

- Microsoft SQL Server 2008 SP3, and later maintenance levels: Standard or Enterprise Editions

- Microsoft SQL Server 2012, and later maintenance levels: Standard, Business Intelligence, or Enterprise Editions

- Microsoft SQL Server 2008 SP1, and later Service Pack levels: Standard x64 or Enterprise x64 Editions - Using older but supported client.

- Microsoft SQL Server 2008 R2 SP1, and later Service Pack levels: Standard, Enterprise, or Data Center Editions - Using older but supported client.

- Microsoft SQL Server 2005 SP3, and later Service Pack levels: Standard or Enterprise Editions - Using older but supported client.

The following application levels are supported for the x64 platform:

- Microsoft SQL Server 2008 SP3, and later maintenance levels: Standard x64 or Enterprise x64 Editions

- Microsoft SQL Server 2008 R2 SP2, and later maintenance levels: Standard, Enterprise, or Data Center Editions

- Microsoft SQL Server 2012, and later maintenance levels: Standard, Business Intelligence, or Enterprise Editions

- Microsoft SQL Server 2008 SP1, and later Service Pack levels: Standard x64 or Enterprise x64 Editions - Using older but supported client.

- Microsoft SQL Server 2008 R2 SP1, and later Service Pack levels: Standard, Enterprise, or Data Center Editions - Using older but supported client.

- Microsoft SQL Server 2005 SP3, and later Service Pack levels: Standard or Enterprise Editions - Using older but supported client.

Oracle:

The following application levels are supported for the 64-bit AIX platform:

- 64-bit Oracle 11gR2: Standard or Enterprise Server, and later maintenance levels of 11gR2

The following application levels are supported for the 64-bit HP Itanium platform:

- 64-bit Oracle 11gR2: Standard or Enterprise Server, and later maintenance levels of 11gR2

The following application levels are supported for the 64-bit Linux x86_64 platform:

- 64-bit Oracle 11gR2: Standard or Enterprise Server, and later maintenance levels of 11gR2

- 64-bit Oracle 12c: Standard or Enterprise Server, and later maintenance levels of 12c

The following application levels are supported for the 64-bit Linux on System z platform:

- 64-bit Oracle 11gR2: Standard or Enterprise Server, and later maintenance levels of 11gR2

The following application levels are supported for the 64-bit Solaris SPARC platform:

- 64-bit Oracle 11gR2: Standard or Enterprise Server, and later maintenance levels of 11gR2
- 64-bit Oracle 12c: Standard or Enterprise Server, and later maintenance levels of 12c

The following application levels are supported for the 32-bit Windows x86 platform:

- 32-bit Oracle 11gR2: Standard or Enterprise Server, and later maintenance levels of 11gR2

The following application levels are supported for the 64-bit Windows x64 platform:

- 64-bit Oracle 11gR2: Standard or Enterprise Server, and later maintenance levels of 11gR2
- 64-bit Oracle 12c: Standard or Enterprise Server, and later maintenance levels of 12c

Additional Operating Environments

The following additional operating environments are supported:

- Oracle Real Application Clusters as supported with the level of Oracle used in your environment
- Solaris 10 and 11 global zones as supported by the Oracle database used in your environment
- Solaris 10 and 11 non-global (local) zones as supported by the Oracle database used in your environment

DB2:

DB2 has native support for backup to TSM.

Sharepoint:

SharePoint is supported using 3rd party software, either "DocAve" from AvePoint Inc. It is not included in the base service based on native TSM, but included as separate item in the Service Catalogue.

MySQL / PostgreSQL / Sybase ASE / OpenEdge 4 GL / Sybase IQ / Ingres / Interbase / Firebird:

MySQL is supported through a 3rd party client from Repostor AB. Repostor also provide clients for PostgreSQL, Sybase ASE, OpenEdge 4 GL, Sybase IQ, Ingres and Interbase/Firebird.
It is not included in the base service based on native TSM, but includes as separate items in the Service Catalogue.

Calculation of Availability

Downtime is defined as the actual time that a service or a product is not performing as agreed, and/or is not available to customer for normal use. Any period where the response time is noticeably slower than it would be in an optimized and fully operative technical environment, shall also be considered as Downtime. For the avoidance of doubt, downtime that is not automatically measured, for instance that is documented by analyzing the reasons for Incidents reported shall also be considered as Downtime.

Downtime is permitted in all agreed maintenance windows, provided however that Provider has made reasonable efforts to limit the downtime during the agreed maintenance window.

Provider uses maintenance windows to maintain infrastructure platforms and the operational environment. Such maintenance windows shall be announced 5 working days in advance. One maintenance window per service/month can be accepted, and each maintenance window shall be limited to as few hours as necessary, and shall be scheduled to such weeks/hours that has as little negative impact on Provider and Customers businesses as possible.

Exceptionally, in case of external and sever security threats not under Provider's control, Provider may request additional maintenance windows, for instance to install hot-fixes or security patches which could not have been installed by Provider during any preceding maintenance window. Such requests shall not be withheld without reasonable cause.

Exceptional maintenance windows may also be agreed between the Parties in Change Orders.

Provider shall give customer prior written notice at least 5 working days in advance of any expected downtime, or as soon as possible. Further, Provider shall give customer written notice immediately in case of unexpected downtime.

The equation for calculating the uptime of an agreed measure range is:

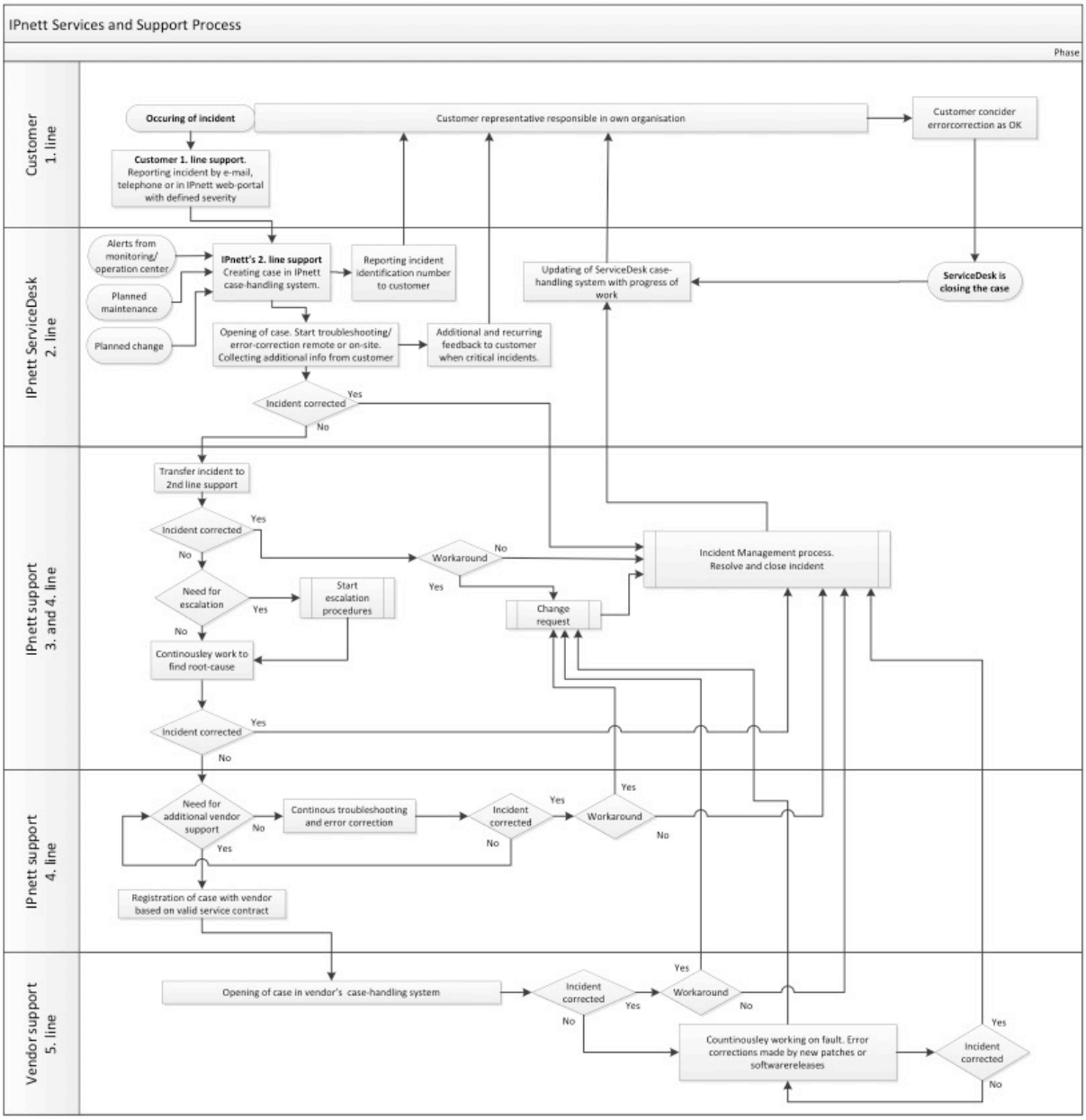
The SLA time and Downtime is entered as minutes in the formula. Uptime is expressed as a percentage with one decimal place. Agreed maintenance windows are not regarded as Downtime.

$$Uptime\ [\%] = \frac{100\ \% * (\text{SLA time in minutes} - \text{Downtime in minutes})}{\text{SLA time in minutes}}$$

Service	Guarantee	Delivery/ measurement	Calculation	Penalty
IaaS BaaS AaaS XaaS	99,9 % 24/7/365	Delivery at NREN connection point. Monitoring and measurement at Datacenter	As described under chapter "Calculation of availability" above	Calculation is based on total monthly fee for the service 99,9 < 5% 99,8 < 10% 99,6 < 15% 99,4 < 20% 99,2 < 25% 99,0 < 30%

Support process
Sunet Customers IT department (e.g. University IT Department) reports incidents to IPnett via web, e-mail or phone. Critical incidents shall always be recorded by phone in addition to other channels. The Customer applies severity level to the incident, which determines further treatment of the incident. Below is the contact details and a table describing the support process applicable for the BaaS:

Web: https://rt.cloud.IPnett.se
e-mail: baas@cloud.IPnett.se
Phone: +46 8 22 11 88


IPnett Services and Support Process
Phase
Customer 1. line
IPnett ServiceDesk 2. line
IPnett support 3. and 4. line
IPnett support 4. line
Vendor support 5. line
Occuring of incident
Customer representative responsible in own organisation
Customer concider errorcorrection as OK
Customer 1. line support. Reporting incident by e-mail, telephone or in IPnett web-portal with defined severity
Alerts from monitoring/ operation center
Planned maintenance
Planned change
IPnett's 2. line support Creating case in IPnett case-handling system.
Reporting incident identification number to customer
Updating of ServiceDesk case-handling system with progress of work
ServiceDesk is closing the case
Opening of case. Start troubleshooting/ error-correction remote or on-site. Collecting additional info from customer
Additional and recurring feedback to customer when critical incidents.
Incident corrected
Yes
No
Transfer incident to 2nd line support
Incident corrected
Yes
No
Workaround
No
Yes
Incident Management process. Resolve and close incident
Need for escalation
Yes
Start escalation procedures
No
Change request
Continousley work to find root-cause
Incident corrected
Yes
No
Need for additional vendor support
No
Yes
Continous troubleshooting and error correction
Incident corrected
Yes
No
Workaround
Yes
No
Registration of case with vendor based on valid service contract
Opening of case in vendor's case-handling system
Incident corrected
Yes
No
Workaround
Yes
No
Countinousley working on fault. Error corrections made by new patches or softwarereleases
Incident corrected
Yes
No

If the incident is not solved and SLA is exceeded or SLA level is in risk being exceeded, escalation routines will be initiated.

The escalation routines shall be initiated if:

- It is not started eligible debugging of enrolled incidents within defined response time (table 2) related to escalation level 1 (table 1).
- Customer has not received necessary feedback about the status of ongoing error correction within defined response time (table 2) related to escalation level 2 (table 1).
- Incidents are not corrected or that solution time is not set within defined response time (table 2) related to escalation level 3 and 4 (table 1).

Each party have the responsibility to perform escalation within his own organization.

Table 1

Escalation level	Customer representative	IPnett representative
1	Product Owner SUNET	Julie-Renate Huse, Support Manager Phone: +47 67 20 10 42
2	Product Owner SUNET	Irene Hortman, Technical Manager Phone: +47 67 20 10 41
3	COO SUNET	Halvor Holmen, CTO Phone: +47 67 20 10 40
4	CEO SUNET	Marius Brekke, CEO Phone: +47 67 20 10 25

Table2

Category	Incident correction to be started within	Definition	IPnett incident handling	Response time / escalation level			
				1	2	3	4
Critical incident P1	SLA	Incidents that cause loss of service or continuous instability of mission-critical functionality and have no workaround. The Incident causes or may cause a material adverse effect on Customer's business or material parts of the operational services are unavailable.	IPnett is working continuous 24/7 with the Incident until it is resolved or a satisfactory "work-around" is established. There is regular feedback to the Customer on the progression of the error handling. IPnett's management will create a dialogue with the manufacturer's support department. If necessary, IPnett will require on-site assistance from the manufacturer.	SLA	SLA + 30 min.	SLA + 60 min	SLA + 2 hours
Major incident P2	SLA	Incidents that are impairing, but not causing loss of service or loss of mission-critical functionality. Intermittent issues that affect mission-critical functionality. The Incident causes or may cause an adverse effect on Customer's business or a critical function does not work, or work with response times that are inferior to the agreed.	IPnett is working continuous 24/7 with the Incident until it is resolved or a satisfactory "work-around" is established. IPnett will inform the Customer regarding progression of the Incident handling. IPnett's management will create a dialogue with the manufacturer's support department. If necessary, IPnett will require on-site assistance from the manufacturer.	SLA	SLA + 60 min.	SLA + 2 hours	SLA + 4 hours
Minor incident P3	SLA	All other incidents	IPnett is working with the Incident during normal business hours until it is resolved or a satisfactory "work-around" is established. IPnett's management will create a dialogue with the manufacturer's support department if necessary.	SLA	SLA + 1day	SLA +5 days	n.a.

Table 3 (definition of service levels)

Service Level / Description	Service Level (equal to or less than)	Critical Service Failure (equal to or less than)	Service Credit (paid where incident Service Level exceeds SLA Service Level)
Critical/P1 Resolution time	4h from incident start or notification by the Customer	24 hours total time per month	For every incident that exceeds the Service Level a value of 10% of the monthly charges on a calendar month.
Major/P2 Resolution time	24h from incident start or notification by the Customer	72 hours total time per month	For every incident that exceeds the Service Level a value of 10% of the monthly charges shall be paid. Values shall be measured on a calendar month.
Minor/P3 Resolution time	3 Business days from incident start or notification by the Customer	No value	None