Symantec User Authentication
Service Level Agreement

Overview and Scope

This Symantec User Authentication service level agreement ("**SLA**") applies to Symantec User Authentication products/services, such as Managed PKI (MPKI), Validation & ID Protection (VIP), and such other User Authentication solutions as identified by Symantec from time to time, each a "**User Authentication Service**". This SLA should be read in connection with the applicable Services Description or Statement of Service for the User Authentication Service in question. The service level described in a current published Service Description or Statement of Service will govern over this SLA, if there is any conflict between such documents.

This SLA applies to new or renewal Service Periods of User Authentication Service, performed on or after the SLA Version date indicated in this document. For Customers with User Authentication Services purchased before such SLA Version date, the prior service level agreements shall apply until the expiration of their current annual Service Period, such that this SLA shall apply commencing on the next annual Service Period. This SLA document is organized as follows:

- **Technical Support SLA information**
- **Service Performance SLA information**
- **Definitions**

Technical Support SLA

Customer Administrators

Customer may nominate named Customer Administrators authorized to interact with Symantec for purposes of reporting problems with User Authentication Services, requesting technical support, and collaborating with Symantec Technical Support in the resolution of reported problems. The number of such Customer Administrators varies by level of support (Bronze, Gold, Platinum) included in the purchased Service, as specified below.

Customer shall identify, and may also from time to time change, its Customer Administrators using Symantec's then current Technical Support processes.

Severity Levels

Customers are responsible for determining the severity level of each problem logged with Symantec Technical Support. The Severity Level reflects the potential impact to your business. The response times associated with Symantec's provision of technical support to Customer in connection with the User Authentication Services will be based in part on classification of reported problems by severity level as follows:

Severity Level	Impact or Significance of Problem
Severity 1 **(Critical Events)**	Severity 1 problems include any events that have a ***major*** adverse impact on the operations of the system and on end users' use of the User Authentication Service(s), such as the problem types described below. A customer cannot classify a problem as Severity 1, and Symantec will not classify an issue as a Severity 1 problem, unless a Customer Administrator with immediate access to the affected system(s) and related information contacts Symantec by telephone to request support. ○ System or application unavailability that prevents critical transactions from being processed ○ Online application outages that significantly impact the online availability of the User Authentication Service(s) ○ Telecommunications interruptions that lead to a major disruption of the User Authentication Service(s) ○ Consistent degradation of availability that significantly impairs the utility of the User Authentication Service(s)
Severity 2 (High Importance Events)	Severity 2 problems include any events (other than Severity 1 problems) that have a ***moderate*** adverse impact on the operations of the system and on end users' use of the User Authentication Service(s), such as: ○ Errors that disable only certain nonessential functions of the User Authentication Service(s) and may result in degraded operations, including without limitation, errors that cause significant transaction processing delays ○ Intermittent degradation of availability that moderately impairs the utility of the User Authentication Service(s)
Severity 3 (Medium Importance Events)	Severity 3 problems include any events (other than Severity 1 or 2 problems) that have a ***minor*** impact on the operations of the system and on end users' use of the User Authentication Service(s).

Technical Support Response Time – Symantec will use commercially reasonable efforts to perform the following activities:

For Bronze Service: Symantec will provide telephone and email support to up to two (2) Customer Administrator(s), as follows:

(i) for Severity 1 problems, 24 hours a day, 7 days a week, 52 weeks a year, and

(ii) at Customer's option, for Severity 2 and 3 problems, as follows:

- From 5:00 am - 6:00 pm Pacific Standard Time, Monday through Friday, 52 weeks a year, excluding United States national holidays and Scheduled Down Time periods.
- From 8:00 am – 6:00 pm CET, Monday through Friday, 52 weeks a year, excluding Ireland national holidays and Scheduled Down Time periods
- From 8:30 am to 5:00 pm AEST, Monday through Friday, 52 weeks a year, excluding Australian national holidays, Melbourne and Victoria holidays, and Scheduled Down Time periods

(iii) During the regional business hours above, Bronze Service Customers may contact their appropriate regional User Authentication Symantec Technical Support center, based on Customer location as indicated in the Customer's service order (and not based on location of Customer Administrator(s)).

For Gold and Platinum Service: Symantec will provide technical telephone and email support to up to two (2) Customer Administrator(s) for Gold service, or five (5) Customer Administrators for Platinum service, 24 hours a day, 7 days a week, 52 weeks a year for Severity 1, 2, and 3 problems.

During such hours, incoming technical support calls will be answered by an automated call system. Symantec will provide a call system option for a customer to speak directly to a trained customer support representative. 80% of the time that this option is selected (as measured on a rolling 90-day basis), customers will speak to a trained customer support representative within 120 seconds of selecting that option.

Target Response Times. Symantec's target Response Times for callbacks and email support, broken out by Service type and Severity Level, are provided in the Table below. Note that **"Response Time"** means the amount of time that elapses between the Customer's report of a software or service problem to Symantec and Symantec's response acknowledging the report and indicating that a response to the problem has been initiated. The following are goals and not commitments.

Severity Level **(During hours outlined above)**	**Bronze Service Response Time Goals**	**Gold Service Response Time Goals**	**Platinum Service Response Time Goals**
Severity 1 (Customer must initiate by telephone)	Within 1 hour	Within 1 hour	Within 30 minutes
Severity 2 (Customer may initiate by telephone or email*)	Within 6 business hours	Within 6 hours	Within 2 hours
Severity 3 (Customer may initiate by telephone or email*)	Next business day	Within 8 hours	Within 8 hours
*The turnaround time for email requests could be longer than for telephone requests			

Maintenance and Service Version

Bronze, Gold and Platinum Support include a maintenance plan under which Symantec will provide Software upgrades, bug-fixes, patches, error corrections and enhancements which are developed by Symantec and made available to Symantec's customers for these offerings on an if and when available basis. SYMANTEC WILL PROVIDE SUCH MAINTENANCE PLAN AND CUSTOMER SUPPORT AS PROVIDED IN THIS SLA ONLY FOR THE THEN CURRENT RELEASE OF THE SERVICES OR SOFTWARE AND THE IMMEDIATELY PRECEDING MAJOR RELEASE AT ANY GIVEN TIME.

Problem Management and Escalation Process

A specified level of Technical Support representative is assigned to every escalation to oversee the case from a holistic viewpoint. The Technical Support representatives handling escalations are responsible for evaluating your situation, facilitating the issue at a global level, and acting as advocates on your behalf.

Problem Escalation. Severity 1 and 2 problems will be internally escalated as described below:

Severity 1:

- *Hour 0 through Hour 1:* For non-system wide issues related to Symantec's back-end systems*,* Symantec's Technical Support Manager and, if required, Symantec's Backline Maintenance and Escalation Manager, or their equivalents, are notified of the problem and are actively working on the problem. For system-wide issues related to Symantec's back-end systems, Symantec Production Services Manager, or equivalent, is also notified and actively working on the problem.
- *Hour 2 through Hour 4:* For non-system wide issues related to Symantec's back-end systems, Symantec's Director of Technical Support or equivalent is notified and involved in the problem resolution as may be required. For system-wide issues related to Symantec's back-end systems, the Vice President of Production Services and Vice President of Technical Support or equivalent are also notified and involved in the problem resolution as may be required.
- *Hour 5:* Symantec's Vice President of Technical Support or equivalent is notified for non-system wide issues related to Symantec's back-end systems.

Severity 2:

- *Hour 0 through Hour 72:* Symantec will work to resolve the problem and will attempt to provide a solution within 72 hours after problem identification. If Symantec does not develop a plan within the first 72 hours after the problem is reported, for resolution of the problem within the 10 day period following the 72-hour window, and provided the problem is not due to Customer's fault, then at Customer's explicit request Symantec will escalate the problem in accordance with the Severity 1 escalation procedures described above.

Technical Support Contact Information and Telephone Numbers can be found at:
https://www.symantec.com/contactsupport

Service Performance SLA

Symantec MPKI, VIP, and other User Authentication Services

The SLA information below describes Symantec's standard Service Performance SLA terms for Customers of our Bronze Service level, and certain additional Service Performance SLA commitments for Customers who purchase Symantec's premium SLA packages ("Gold Service" and "Platinum Service"), as applicable:

Service Availability

- **Up Time Measurement.** Up Time is calculated on a rolling 90-day basis as a percentage equal to (i) the total number of minutes in any such 90-day period that Symantec's systems are available and capable of receiving and processing data from customers, divided by (ii) the total number of minutes in such period.
- **Up Time Percentage.** Symantec's Up Time percentage throughout each such 90-day period will be no less than:
  - For Managed PKI: Ninety-nine percent (99%) for Bronze and Gold Service, and no less than ninety-nine and one-half percent (99.5%) for Platinum Service.
  - For VIP (including VIP credential provisioning, VIP Manager, VIP Self-Service Portal and VIP Intelligent Authentication): Ninety-nine percent and one-half percent (99.5%). For VIP credential validation only, Symantec's Up Time percentage will be no less than ninety-nine point nine-five percent (99.95%).
- **Scheduled Down Time.** Symantec will notify Customer via electronic mail of Scheduled Down Time and anticipated impact to User Authentication Service specific functionality not less than thirty (30) hours in advance of the planned downtime window. Scheduled Down Time will not exceed four (4) hours in any single calendar week.

Pre-Production Environment for VIP

- Customer will have access to the Symantec pre-production environment as applicable to the VIP User Authentication Service(s) provided for a period of 60 days after the start date of Bronze and Gold Service, and for a period of one (1) year after the start date of Platinum Service.
- No other provision of this SLA will be applicable to pre-production environment availability or performance.

Additional Terms for Platinum Service Customers

Managed PKI Service Performance

For Platinum Service only, the Managed PKI Services (if applicable) will be provided in accordance with the following Service Performance standards, as applicable (excluding any additional latency resulting from use of the Managed PKI Services in conjunction with other User Authentication Services), which standards reflect average performance for customers over any calendar month:

- 90% of all Customer Administrator approvals of a digital certificate will occur within 10 seconds
- 90% of all Customer Administrator revocations of a digital certificate will occur within 5 seconds
- 90% of all Customer Administrator requests for a CRL will occur within 5 seconds
- 90% of all end user requests for a digital certificate will occur within 5 seconds
- 90% of all end user pickups of approved digital certificates will occur within 5 seconds
- 90% of all end user revocations of his/her own digital certificate will occur within 5 seconds
- 99% of all of the above requests or actions will occur within 2 minutes

Customer Relationship Manager

For eligible Platinum Service customers only, Symantec will designate a qualified Symantec employee to serve as Customer Relationship Manager for the coordination of implementation activities, and management of problem resolution and escalation efforts. The Customer Relationship Manager also will be available to conduct support service reviews at Customer's request once every calendar quarter. The eligibility is determined by the then-current Symantec policy and based on customers' annual spending for support. The current annual spending requirement is USD $12,500 or 15% of the applicable User Authentication Service annual fee, whichever is greater.

Reports

For Platinum Service only, Symantec will make available to Customer monthly reports, detailing the following for the monthly period covered by the report:

- the total percentage of Up Time; and
- the number of Scheduled Down Time periods; and
- the percentage of Scheduled Down Time periods completed within the scheduled window specified in the notice provided by Symantec; and
- severity level classifications and current resolution status for reported problems, upon request, and
- for Managed PKI Services only, actual Service Performance figures corresponding to the standards specified in this SLA (aggregated across all Managed PKI Service customers).

Definitions

Capitalized terms that are not otherwise defined in this SLA have the meanings given below.

"AEST" means Australian Eastern Standard Time **(**GMT +10:00)

"CET" means Central European Time (GMT +01:00)

"Customer Administrator" means a named, trusted individual of Customer who is designated by Customer to Symantec as its administrator with respect to the relevant Service(s), and who Customer authorizes to interact with Symantec on technical problems with the Service.

"GMT" means Greenwich Mean Time

"PKI" means Public Key Infrastructure

"PST" means Pacific Standard Time (GMT -08:00)

"Scheduled Down Time" means periods of scheduled unavailability of the Symantec system and User Authentication Service, in order to perform routine service maintenance, upgrades, and testing.

"**Services Order Term**" is Customer's committed period of User Authentication Services, which may be more than 12 months depending on Customer's order.

"Service Performance" means the amount of time that elapses between the arrival of data sent by Customer at Symantec's back-end system and the transmission from Symantec's back-end system of the corresponding response or automated action initiated by Symantec in connection with the relevant User Authentication Service. "**Service Performance**" refers only to the performance of Symantec's back-end system, and does not include the system availability, performance, or response delay of any third party.

"**Service Period**" is each annual period within a Services Order Term**.**

"Up Time" means the percentage of time that Symantec's systems are available and capable of receiving and processing data from Customer in connection with the applicable User Authentication Services. Scheduled Down Time is not considered downtime for the purpose of this SLA. Unless otherwise specified, "Up Time" refers only to availability of Symantec's systems, and does not include the system availability or performance of any party.

"VIP" means Validation & ID Protection.