Entrust Managed PKI Americas
Service Levels and Support

These service levels and support provisions are incorporated into the Entrust Managed PKI Americas Agreement ("Plan") between Entrust and You ("Customer"). Capitalized Terms not defined herein have the meanings given to them in the Plan. Entrust may revise these service levels and support provisions by posting a new version at https://www.entrust.com/legal-compliance/terms-conditions/entrust-managed-pki . Such new version will become effective on the date it is posted except that if the new version significantly reduces Customer's rights, it will become effective sixty (60) days after being posted. If Customer objects in writing during that sixty (60) day period, the new version will become effective upon renewal of Customer's subscription.

1. Service Levels

a. Targets

Entrust will use commercially reasonable efforts to achieve the service level targets set out below (each, a "Service Level Target").

Applicable components/functions	Target
Certificate Validation services (OCSP, CRLs)	99.9% Uptime
Certificate issuance	99.5% Uptime
Test components (including test CAs) All components of Offerings provided for evaluation purposes	n/a

b. Calculation of Uptime

"Uptime" is calculated for each calendar month by subtracting the percentage of Downtime during such month from 100%.

"Downtime" means, subject to the exclusions below, an interruption of five (5) minutes or more during which the ability of ten percent (10%) or more of all users to access one or more of the components or functions listed in Section 1.a above is substantially impaired.

c. Maintenance Windows and Other Exclusions from Downtime

"Maintenance Windows" are the time frames during which Entrust may perform scheduled routine system maintenance. The Maintenance Windows will not exceed 12 hours per month. Entrust will use commercially reasonable efforts to provide 7 days advance notice of the Maintenance Windows.

Unavailability due to any of the following is excluded from Downtime:

i. any Maintenance Windows;
ii. suspension or termination of the Services in accordance with the terms of the Plan;
iii. implementation of critical / emergency security patches in accordance with a relevant risk/vulnerability assessment;
iv. factors outside of Entrust's reasonable control, including any Force Majeure event, and internet accessibility problems beyond Entrust's ISP environment; and
v. Customer's and/or any third party's networks, software, equipment, or other technology or

service.

d. Notice of Default

In order to receive a Service Level Credit (as defined below), Customer must provide written notice to Entrust within thirty (30) days of the end of the month in which the failure occurred if Customer believes Entrust has failed to meet any Service Level Target ("Service Level Default"). Upon receipt of such notice, Entrust will verify the accuracy of details provided by Customer against its service logs to determine, acting reasonably, whether a Service Level Default has or has not occurred, and will provide details relating to the cause of the Service Level Default to Customer within thirty (30) days from the date of notification. Customer's failure to provide the notice required in this Section will disqualify Customer from receiving a Service Level Credit.

e. Service Level Credit

Customer will be entitled to receive the Service Level Credit for a confirmed Service Level Default.

"Service Level Credit" means an amount equal to five percent (5%) of the Monthly Fee for the calendar month in which a Service Level Default occurs, where "Monthly Fee" means the subscription fees paid to Entrust for the Services divided by the number of months in the applicable subscription term.

The total aggregate amount of the Service Level Credit to be issued by Entrust to Customer for all Service Level Defaults that occur in a single calendar month will be capped at five percent (5%) of the Monthly Fee for such calendar month. Service Level Credits can only be applied against the renewal subscription fees due to Entrust for the Services and any unused Service Level Credits are forfeited upon termination or non-renewal of the Plan. For clarity, Entrust is not required to issue refunds or make payments against such Service Level Credits under any circumstances, including upon termination of this Plan. The Service Level Credit is Customer's sole and exclusive remedy for any Service Level Default.

2. Support

a. Definitions

"First Line Support" will be the provision of a direct response to Local Registration Authorities, Subscribers and Applicants with respect to inquiries concerning the performance, functionality or operation of the Certification Authority.

"Second Level Support" means: (i) diagnosis of problems or performance deficiencies of the Certification Authority; (ii) a resolution of problems or performance deficiencies of the Certification Authority; and (iii) a direct response to Customer's trained support representative with respect to the problems and their resolution.

b. Support Services

Customer will be responsible for providing First Line Support. During the term of the Plan, Entrust will provide Customer with Second Level Support to Customer's trained support representative. The following sets out the scope of such services:

i. Hours of Operation. Telephone support by an Entrust technical support specialist will be accessible from 8:00 AM until 8:00 PM Eastern time, Monday through Friday (certain holidays excluded). On call telephone support is available 24x7x365 for Severity 1 incidents. E-mail support will be accessible 24 hours a day, 7 days a week, however, email is only monitored during our normal working hours. Extranet web support will be available 24 hours a day, 7 days a week, however, the extranet web support system is only monitored during our normal working hours.

ii. Classification. When Customer reports a problem or incident, Entrust will, in consultation with Customer, first classify the problem or incident according to its severity and nature. Severity 1 and 2 issues are limited to incidents that occur on a "Production System" (i.e. active users outside of a test lab environment). The incident will then be logged in Entrust's problem tracking system and classified into one of the following categories below:

Severity 1: Critical error which completely disables the Certification Authority in production use for which no work-around exists;

Severity 2: Either a critical error for which a work-around exists or a non-critical error that significantly affects the functionality of the Certification Authority in production use; and

Severity 3: Isolated error which does not significantly affect the functionality of the Certification Authority in production use.

iii. Basic Response Times. Entrust will use commercially reasonable efforts to provide an initial call back response to Customer within one (1) hour of Entrust's receipt of notice of an incident reported by telephone. Entrust will use commercially reasonable efforts to provide an initial response to Customer within one (1) business day of Entrust's receipt of an incident reported by e-mail. Incidents will be handled according to the level of severity. For Severity 1 and Severity 2 incidents, Entrust will advise Customer periodically at reasonable intervals as to the progress made by Entrust in diagnosing and/or correcting any reported error, defect or nonconformity.

Severity 1: Entrust will make commercially reasonable efforts to resolve and correct a Severity 1 error, defect or nonconformity within twenty-four (24) hours from notification. If related to the Certification Authority, the resolution and correction will be implemented through a work around or currently available Certification Authority release. If changes are required to the Certification Authority, Entrust will make commercially reasonable efforts to resolve and correct a Severity 1 error within five (5) continuous days from notification.

Severity 2: Entrust will make commercially reasonable efforts to resolve and correct a Severity 2 error, defect or nonconformity within five (5) continuous business days from notification. Such resolution and correction may be provided to Customer as a Certification Authority fix or work-around.

Severity 3: Entrust will make commercially reasonable efforts to resolve and correct a Severity 3 error within twenty-one (21) continuous business days from notification. In the event of a Severity 3 incident involving the Certification Authority, Entrust may include any Certification Authority error corrections in the next upgrade of the software used by Entrust.