

**AUTHORIZED FEDERAL ACQUISITION SERVICE  
INFORMATION TECHNOLOGY SCHEDULE PRICELIST  
GENERAL PURPOSE COMMERCIAL INFORMATION TECHNOLOGY  
EQUIPMENT, SOFTWARE AND SERVICES**

Special Item No. 132-61 Authentication Products and Services

Note: Contractor has been awarded all Special Item Numbers under the Cooperative Purchasing & Disaster Recovery Program.

**Entrust, Inc.**

Three Lincoln Centre

5430 LBJ Freeway, Suite 1250

Dallas, TX 75240

Phone: (972) 728-0447 Fax: (972) 728-0440

Internet Address: [www.entrust.com](http://www.entrust.com)

**Contract Number:**

**GS-35F-0332K**

**Period Covered by Contract:**

**March 31, 2010 through March 30, 2020**

General Services Administration

Federal Acquisition Service

**Pricelist current through Modification #PO-0086, dated September 27, 2015**

Products and ordering information in this Authorized FAS Information Technology Schedule Pricelist are also available on the GSA Advantage! System. Agencies can browse GSA Advantage! by accessing the Federal Acquisition Service's Home Page via the Internet at <http://www.gsa.gov/fas>

**INFORMATION FOR ORDERING ACTIVITIES  
APPLICABLE TO ALL SPECIAL ITEM NUMBERS**

- 1a. Table of awarded special item number(s) with appropriate cross-reference to item descriptions and awarded price(s).  
  
SIN 132-61- Public Key Infrastructure (PKI) Shared Service Providers (PKI SSP) Program
- 1b. Identification of the lowest priced model number and lowest unit price for that model for each special item number awarded in the contract. This price is the Government price based on a unit of one, exclusive of any quantity/dollar volume, prompt payment, or any other concession affecting price. Those contracts that have unit prices based on the geographic location of the customer, should show the range of the lowest price, and cite the areas to which the prices apply.  
See Attached Pricelist
- 1c. If the Contractor is proposing hourly rates, a description of all corresponding commercial job titles, experience, functional responsibility and education for those types of employees or subcontractors who will perform services shall be provided. If hourly rates are not applicable, indicate "Not applicable" for this item.  
See Attached Pricelist
2. Maximum order.  
  
SIN 132-61- \$1,000,000
3. Minimum order.  
  
SIN 132-61- \$100
4. Geographic coverage (delivery area).  
The Geographic Scope of Contract will be domestic and overseas delivery
5. Point(s) of production (city, county, and State or foreign country).  
United States
6. Discount from list prices or statement of net price.  
Government prices are net
7. Quantity discounts.  
None
8. Prompt payment terms.  
2% 10 days - NET 30 days from receipt of invoice or date of acceptance, whichever is later. Applied to SIN 132-61 ONLY. Does not apply to credit card orders
- 9a. Notification that Government purchase cards are accepted at or below the micro-purchase threshold.  
Government purchase cards are accepted at or below the micro-purchase threshold.
- 9b. Notification whether Government purchase cards are or are not not accepted above the micro-purchase threshold.  
Government purchase cards are accepted above the micro-purchase threshold.
10. Foreign items (list items by country of origin).  
None

- 11a. Time of delivery.  
132-61 30 Days
- 11b. Expedited Delivery.  
Contact Contractor
- 11c. Overnight and 2-day delivery.  
Contact Contractor
- 11d. Urgent Requirements.  
Contact Contractor
12. F.O.B. point(s).  
FOB Destination
- 13a. Ordering address(es).  
Entrust, Inc  
Attn: GSA Orders  
8300 Greensboro Drive, Suite 250  
McLean, Virginia 22102
- 13b. Ordering procedures: For supplies and services, the ordering procedures, information on Blanket Purchase Agreements (BPA's) are found in Federal Acquisition Regulation (FAR) 8.405-3.
14. Payment address(es).  
Entrust, Inc.  
PO Box 972894  
Dallas, Texas 75397-2894
15. Warranty provision.  
Standard Commercial
16. Export packing charges, if applicable.  
Export packing is available outside the scope of this contract
17. Terms and conditions of Government purchase card acceptance (any thresholds above the micro-purchase level).  
None
18. Terms and conditions of rental, maintenance, and repair (if applicable).  
Not applicable
19. Terms and conditions of installation (if applicable).  
Not applicable
20. Terms and conditions of repair parts indicating date of parts price lists and any discounts from list prices (if applicable).  
Not applicable
- 20a. Terms and conditions for any other services (if applicable).  
Not applicable
21. List of service and distribution points (if applicable).  
Not applicable

22. List of participating dealers (if applicable).  
Not applicable
23. Preventive maintenance (if applicable).  
Not applicable
- 24a. Special attributes such as environmental attributes (e.g., recycled content, energy efficiency, and/or reduced pollutants).  
Not applicable
- 24b. If applicable, indicate that Section 508 compliance information is available on Electronic and Information Technology (EIT) supplies and services and show where full details can be found (e.g. contractor's website or other location.) The EIT standards can be found at: [www.Section508.gov/](http://www.Section508.gov/).  
Not applicable
25. Data Universal Number System (DUNS) number.  
799454061
26. Notification regarding registration in SAM.gov (formerly the Central Contractor Registration) database.  
Entrust has registered in the System for Award Management (SAM) database. The CAGE code is 1LDQ2

**TERMS AND CONDITIONS APPLICABLE TO  
AUTHENTICATION PRODUCTS AND SERVICES  
(SPECIAL ITEM NUMBER 132-61)**

**1. ORDER**

- a. Agencies may use written orders, EDI orders, blanket purchase agreements, individual purchase orders, or task orders for ordering authentication products and services under this contract. Blanket Purchase Agreements shall not extend beyond the end of the contract period; all services and delivery shall be made and the contract terms and conditions shall continue in effect until the completion of the order. Orders for tasks which extend beyond the fiscal year for which funds are available shall include FAR 52.232-19 (Deviation – May 2003) Availability of Funds for the Next Fiscal Year. The purchase order shall specify the availability of funds and the period for which funds are available.
- b. All task orders are subject to the terms and conditions of the contract. In the event of conflict between a task order and the contract, the contract will take precedence.
- c. When placing an order, ordering activities may deal directly with the contractor or ordering activities may send the requirement to the Program Management Office to received assisted services for a fee.

**2. PERFORMANCE OF SERVICES**

- a. The Contractor shall commence performance of services on the date agreed to by the Contractor and the ordering activity.
- b. The Contractor agrees to render services only during normal working hours, unless otherwise agreed to by the Contractor and the ordering activity.
- c. The ordering activity should include the criteria for satisfactory completion for each task in the Statement of Work or Delivery Order. Services shall be completed in a good and workmanlike manner.
- d. Any Contractor travel required in the performance of the Services under SIN 132-61 must comply with the Federal Travel Regulation or Joint Travel Regulations, as applicable, in effect on the date(s) the travel is performed. Established Federal Government per diem rates will apply to all Contractor travel. Contractors cannot use GSA city pair contracts.

**3. STOP-WORK ORDER (FAR 52.242-15) (AUG 1989)**

- a. The Contracting Officer may, at any time, by written order to the Contractor, require the Contractor to stop all, or any part, of the work called for by this contract for a period of 90 days after the order is delivered to the Contractor, and for any further period to which the parties may agree. The order shall be specifically identified as a stop-work order issued under this clause. Upon receipt of the order, the Contractor shall immediately comply with its terms and take all reasonable steps to minimize the incurrence of costs allocable to the work covered by the order during the period of work stoppage. Within a period of 90 days after a stop-work is delivered to the Contractor, or within any extension of that period to which the parties shall have agreed, the Contracting Officer shall either-
  - (1) Cancel the stop-work order; or
  - (2) Terminate the work covered by the order as provided in the Default, or the Termination for Convenience of the Government, clause of this contract.
- b. If a stop-work order issued under this clause is canceled or the period of the order or any extension thereof expires, the Contractor shall resume work. The Contracting Officer shall make an equitable adjustment in the delivery schedule or contract price, or both, and the contract shall be modified, in writing, accordingly, if-
  - (1) The stop-work order results in an increase in the time required for, or in the Contractor's cost properly allocable to, the performance of any part of this contract; and
  - (2) The Contractor asserts its right to the adjustment within 30 days after the end of the period of work stoppage; provided that if the Contracting Officer decides the facts justify the action, the Contracting Officer may receive and act upon the claim submitted at any time before final payment under this contract.
- c. If a stop-work order is not canceled and the work covered by the order is terminated for the convenience of the Government, the Contracting Officer shall allow reasonable costs resulting from the stop-work order in arriving at the termination settlement.
- d. If a stop-work order is not canceled and the work covered by the order is terminated for default, the Contracting Officer shall allow, by equitable adjustment or otherwise, reasonable costs resulting from the stop-work order.

**4. INSPECTION OF SERVICES**

The Inspection of Services–Fixed Price (AUG 1996) (Deviation – May 2003) clause at FAR 52.246-4 applies to firm-fixed price orders placed under this contract. The Inspection–Time-and-Materials and Labor-Hour (MAY 2001) (Deviation – May 2003) clause at FAR 52.246-6 applies to time-and-materials and labor-hour orders placed under this contract.

**5. RESPONSIBILITIES OF THE ORDERING ACTIVITY**

Subject to security regulations, the ordering activity shall permit Contractor access to all facilities necessary to perform the requisite services.

**6. INDEPENDENT CONTRACTOR**

All services performed by the Contractor under the terms of this contract shall be an independent Contractor, and not as an agent or employee of the ordering activity.

**7. ORGANIZATIONAL CONFLICTS OF INTEREST**

a. Definitions.

“Contractor” means the person, firm, unincorporated association, joint venture, partnership, or corporation that is a party to this contract.

“Contractor and its affiliates” and “Contractor or its affiliates” refers to the Contractor, its chief executives, directors, officers, subsidiaries, affiliates, subcontractors at any tier, and consultants and any joint venture involving the Contractor, any entity into or with which the Contractor subsequently merges or affiliates, or any other successor or assignee of the Contractor.

An “Organizational conflict of interest” exists when the nature of the work to be performed under a proposed ordering activity contract, without some restriction on ordering activities by the Contractor and its affiliates, may either (i) result in an unfair competitive advantage to the Contractor or its affiliates or (ii) impair the Contractor’s or its affiliates’ objectivity in performing contract work.

b. To avoid an organizational or financial conflict of interest and to avoid prejudicing the best interests of the ordering activity, ordering activities may place restrictions on the Contractors, its affiliates, chief executives, directors, subsidiaries and subcontractors at any tier when placing orders against schedule contracts. Such restrictions shall be consistent with FAR 9.505 and shall be designed to avoid, neutralize, or mitigate organizational conflicts of interest that might otherwise exist in situations related to individual orders placed against the schedule contract. Examples of situations, which may require restrictions, are provided at FAR 9.508.

**8. INVOICES**

The Contractor, upon completion of the work ordered, shall submit invoices for products and/or services. Progress payments may be authorized by the ordering activity on individual orders if appropriate. Progress payments shall be based upon completion of defined milestones or interim products. Invoices shall be submitted monthly for recurring services performed during the preceding month.

**9. PAYMENTS**

For firm-fixed price orders the ordering activity shall pay the Contractor, upon submission of proper invoices or vouchers, the prices stipulated in this contract for service rendered and accepted. Progress payments shall be made only when authorized by the order. For time-and-materials orders, the Payments under Time-and-Materials and Labor-Hour Contracts at FAR 52.212-4 (MAR 2009) (ALTERNATE I – OCT 2008) (DEVIATION I – FEB 2007) applies to time-and-materials orders placed under this contract. For labor-hour orders, the Payment under Time-and-Materials and Labor-Hour Contracts at FAR 52.212-4 (MAR 2009) (ALTERNATE I – OCT 2008) (DEVIATION I – FEB 2007) applies to labor-hour orders placed under this contract.

**11. INCIDENTAL SUPPORT COSTS**

Incidental support costs are available outside the scope of this contract. The costs will be negotiated separately with the ordering activity in accordance with the guidelines set forth in the FAR.

**12. APPROVAL OF SUBCONTRACTS**

The ordering activity may require that the Contractor receive, from the ordering activity's Contracting Officer, written consent before placing any subcontract for furnishing any of the work called for in a task order.

**13. DESCRIPTION OF AUTHENTICATION PRODUCTS, SERVICES AND PRICING**

## DELIVERING SECURITY BENEFITS OF PKI FROM INDUSTRY LEADER

Entrust Managed Services PKI is a hosted certificate service that enables customers to quickly and easily request and manage user, application and device certificates over the Internet. The install, operation, maintenance, and monitoring of the PKI are handled by Entrust out of state-of-the-art secure facilities. With certificates users can secure applications such as Microsoft Office, Microsoft Outlook, remote access VPN and Adobe PDFs.

Entrust's knowledge and experience as a technology provider within the Federal PKI environment is unsurpassed. Entrust has assisted in writing global PKI standards and US Federal PKI policy and has deployed our mature, industry-leading solutions throughout the US Federal government and in government agencies around the world. Entrust has longstanding relationships and technical interoperability with various leading smart card, card management system and OCSP vendors that are in use within the Federal agencies today.

The US Federal government has been a leader in the use of public key infrastructure (PKI) and has played a major role driving the maturity of PKI. Over the years, the Federal government has promulgated and refined policy related to the implementation of PKI aimed at maximizing the value that this technology brings to Federal agencies. Thus the General Services Administration (GSA) created the Shared Service Provider (SSP) program. Through an SSP, an agency can purchase digital certificates in an outsourced model.

The Entrust Managed Services SSP has been designed to meet US Federal Common policy and standards requirements while providing the same high level of technology and services that have positioned Entrust as a leader in PKI across the Federal Government. Entrust is pleased to have joined the ranks of providers under this program.

### **Entrust Managed Services Federal SSP**

The Entrust Managed Services Federal SSP is for employees of the US Federal Government, or their contractors where a US Federal department has sponsored their contractor.

This CA is cross certified to the Federal Common Policy CA.

## ENTRUST MANAGED SERVICES PKI SOLUTION OVERVIEW

Entrust's Managed Services Federal SSP includes the following services:

- Generation and storage of all CA signing keys and database encryption keys in FIPS 140-3 Hardware Security Modules
- Issuance of x.509 digital certificates for use in supported hardware or supported software
- Storage/recovery of keys, update/renewal/revocation of certificates
- Setup and operation of environment in accordance with US Federal PKI policy
- Auditor witnessed CA key generation and annual audits of service practices
- Disaster recovery and business continuity services
- Web based enrolment, admin and management
- Online Certificate Status Protocol (OCSP) services
- VPN Secured communications with the Entrust PKI

The diagram below illustrates the Entrust Managed Services Federal SSP technical architecture.

## Customer

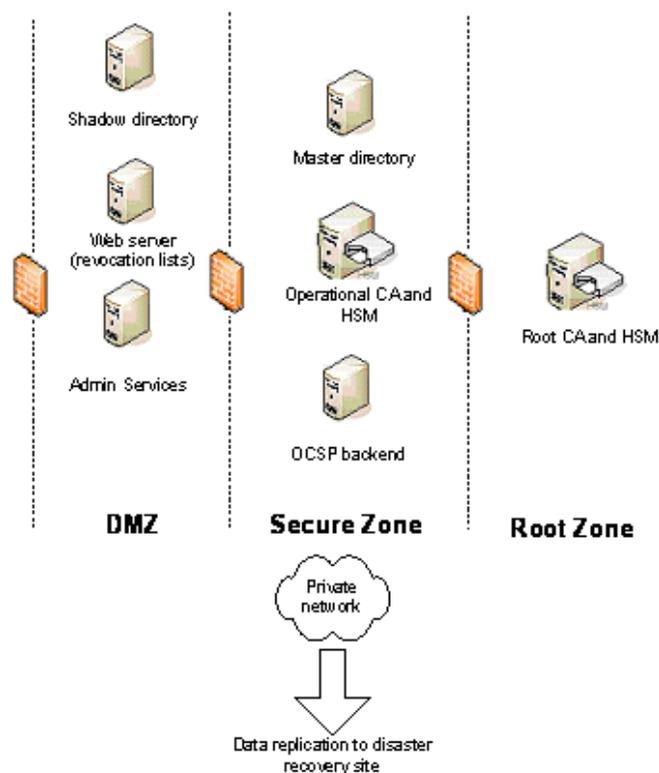
PKI Users (with digital identity security store)

Local admins with web browser

Other PKI applications and devices (e.g., VPN devices)



## Entrust Managed Services PKI



### MANAGED SERVICES PKI COMPONENTS – ENTRUST NETWORK

The primary data center for the Entrust Managed Services PKI is hosted at a Savvis data center in Sterling, Va. The facility is a state-of-the-art data center collocation establishment, including steel-reinforced walls, on-premise security guards and security cameras for surveillance with digital recorders and pan-tilt-zoom (PTZ) capabilities. The Managed Services PKI is located within a secure cage within the data center and fully enclosed with a custom designed roof structure and secured sub-floor. Physical servers are secured within the cage in locked computer cabinets with specially designed sub-section security panels to restrict access to the specific security zones within the cabinets to authorized administrators. Entrust Managed Services PKI infrastructure is separated into distinct “zones” with the most secure zone containing critical components that require the highest level of protection including the CAs. The premises are monitored 24 hours a day and 7 days a week using CCTV systems and motion detectors. Access to the CAs is limited to those authorized personnel required to perform Entrust’s obligations. Access is controlled through the use of electronic access controls, mechanical locksets and deadbolts. The secure facilities also include conditioned power, efficient cooling and fire suppression.

The following components are managed within the Entrust hosted infrastructure:

#### Certification Authority (CA)

The CA issues digital certificates for use by users subscribed to the Managed Services PKI. The CA is operated according to a certificate policy (CP) and certificate practices statement (CPS) which meet US Federal Common policy and standards requirements.

#### Online Certificate Services Protocol (OCSP) Server

The OCSP Server works in conjunction with an OCSP responder to provide certificate status information. This represents an alternative to using certificate revocation lists or CRLs stored in a directory or on a Web server.

#### Administration Services

Entrust provides a Web portal for facilitating secure registration and administration of Digital IDs. The registration model is based on delegated registration where the customer Registration Authority enrolls the customer Local

Registration Authorities (LRAs) who then enrolls and manages end-user subscribers.

Administration Services provides administrators and managers with flexible options to allow distribution of administrative functions throughout the organization, ranging from in-person authentication to an LRA to bulk enrollment using shared secrets. Administration functions and roles can be delegated to ensure appropriate coverage on a global basis. Queued approval and authorization processes allow organizations to ensure the appropriate level of approval is applied to registration and administrative Digital ID issuance and management transactions.

Administrators and end-users can access this portal using digital certificates stored within a Web browser; there is no requirement for software to be installed on the desktop in order for Administrators to quickly and easily request and manage user certificates online.

### **Master Directory**

Entrust hosts and maintains a directory with all PKI relevant entries. Optionally, Entrust Managed Services PKI can publish user data to an existing and compatible customer LDAP directory.

### **Shadow Directory**

A shadow directory can be accessed by users to encrypt data for other users and to obtain certificate status information. Entrust Managed Services PKI supports scalable CRL Distribution Points, full CRLs and OCSP.

### **Secure Communications**

Entrust hosts a VPN for securing communications between the customer network and the hosted service.

## MANAGED SERVICES PKI COMPONENTS – CUSTOMER NETWORK

Users, devices and applications make use of a digital identity to secure applications such as Microsoft Office, user remote access wireless and VPN authentication, and email communications.

This section describes a number of components that are available for use within the customer network:

### **Entrust Entelligence Security Provider**

Entrust Entelligence Security Provider on user's desktops provides:

- Strong Enterprise Security  
Protects users' digital identities and enforces centrally controlled security policies to help prevent unauthorized access to sensitive information. Strong, certificate-based authentication ensures only authorized users, machines and devices are permitted access to your assets, networks and other information.
- Integrated Secure Email  
The platform works seamlessly with Microsoft® Outlook®, which improves the performance and ease of use of secure email.
- Signature and Encryption  
Allows users to protect sensitive data by digitally signing and encrypting files for themselves or others.
- Transparent Management  
Automate the entire lifecycle management of user digital identities; including automatic certificate updates prior to expiration without human intervention, preventing business interruption due to expired certificates

### **Entrust Authority Auto-enrollment Server**

Entrust Authority Auto-enrollment Server fully automates enrollment of users and devices through Microsoft Windows network.

### **Smartcards or Tokens**

End-user or Administrator certificates may be stored on smart cards or USB tokens for additional security of the

private keys.

**Entrust Authority Enrollment Server for VPN**

Entrust Authority Enrollment Server for VPN enables automatic population of certificates in VPN devices using Simple Certificate Enrollment Protocol (SCEP).

---

**SERVICE PLAN  
FOR FEDERAL BRIDGE TRUSTED CERTIFICATES (“Plan”)**

Background:

Entrust provides managed services for PKI and operating as a Certification Authority under the Federal PKI Policy Authority Shared Service Provider (SSP) program, including issuing, managing, revoking, and renewing certificates, as well as other related services.

Where You have purchased either a shared service provider (“SSP”) service or a dedicated service provider (“DSP”) service from Entrust, the parties wish to enter into an agreement pursuant to which You may operate as a registration authority and perform certain activities related to the processing and verification of information contained in certificate applications and sending certificate requests related to the issuance of certificates.

This Plan sets out the scope of services that will be provided by Entrust, and also sets out Your role as a registration authority.

1. DEFINITIONS.

“Applicant” means an individual who is a person who has applied for a Certificate through LRA Web Site, but which has not yet been issued a Certificate, or a person that currently has a Certificate or Certificates and that is applying for renewal of such Certificate or Certificates or for an additional Certificate or Certificates through LRA Web Site.

“Certificate” means a digital certificate issued by the software used to operate the Certification Authority through the LRA Web Site.

“Certificate Application” means, in the case where Subscribers are not devices, the application form and information submitted by an Applicant when applying for the issuance of a Certificate.

“Certification Authority” means a certification authority operated by or for Entrust under the Federal PKI Policy Authority Shared Service Provider (SSP) program.

“Effective Date” means the date that the Order is accepted by Entrust.

“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 Entrust Certification Authority.

“Local Registration Authority” means a person that is responsible for the identification, review and verification of information provided by Applicants or Subscribers, but which does not sign or issue Certificates, Certificate revocation lists (“CRLs”), or other revocation information.

“LRA Guide” means the document available from Entrust, as updated from time to time, that sets out amongst other things the minimum verification practices to be used by a Registration Authority or Local Registration Authority to confirm the accuracy of all contents that are included in a Certificate. The LRA Guide may also incorporate an applicable certificate policy from Entrust regarding the Services and Certificates.

“LRA Web Site” means the worldwide web site that will be used to interact with prospective Applicants for the Certificate subscription process and for ongoing processing (such as digital certificate revocation) for Certificates issued to Subscribers through the LRA Web Site.

“Order” means Your purchase order to Entrust that is accepted by Entrust for SSP services or DSP services, as applicable.

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

“Services” means the SSP or DSP services and licenses provided by Entrust to You and Subscribers under this Plan for the duration of time that has been purchased by You. Where no duration is specified, the duration shall be deemed to be one year from the Effective Date.

“Subscriber” means a person who is issued a Certificate. Subscribers may also include sponsors of devices.

“Subscriber Agreement” means the agreement entered into between each Subscriber (or a person who is a sponsor for device Certificates) and Entrust as set out in the LRA Guide.

“You” or “Your” means the U.S. Government Agency or entity who has purchased the Services from Entrust.

## 2. APPOINTMENT AND RESPONSIBILITIES.

(a) Appointment. Subject to this Plan and for the duration of the Services, Entrust hereby grants You a non-exclusive, non-transferable license under the Entrust Certification Authority to (i) in the case where You have purchased SSP or DSP services, to act as a Registration Authority for prospective Applicants and Subscribers; and (ii) distribute Certificates under the Subscriber Agreement to Subscribers who You will cause to comply with, subject to the maximum annual quantity of Subscribers that You have purchased licenses for.

(b) Registration Authority. You will appoint one or more of Your employees (“Registration Authorities”) who will serve as the initial authority responsible for performing identification and authentication of additional employees who will administer Applicants. The functions performed by the Registration Authority are set forth in the LRA Guide and include: (i) providing Entrust with documentation identifying the initial and ongoing Local Registration Authorities (LRAs); (ii) creating verification records for each Local Registration Authority, together with copies of any supporting documents set forth in the LRA Guide; (iii) distributing the activation data required to complete the certificate enrollment process for the Local Registration Authorities; (iv) providing Entrust with digitally signed documentation for any requested changes to the baseline certificate contents; and (v) providing Entrust documentation for any requested modifications to the security policies enforced through the Entrust Certification Authority. You will promptly notify Entrust of any changes to the identity of the person(s) who are designated as Registration Authorities.

(c) Local Registration Authority. You will appoint additional employees to serve as Local Registration Authorities who will administer Subscribers. The functions performed by each Local Registration Authority are detailed in the LRA Guide and will include: (i) receiving Certificate Applications from Applicants; (ii) creating verification records for each Applicant and any supporting documents set forth in the LRA Guide; (iii) approving or rejecting Certificate Applications based on information which is accurately confirmed and verified following procedures no less stringent than are set out in the LRA Guide; (iv) instructing Entrust from time to time to issue, renew, and revoke Certificates using the procedures set out in the LRA Guide; (v) providing Entrust with accurate information to be included in each Certificate; (vi) reviewing each Certificate created by Entrust for You to ensure the accuracy of the content of each Certificate; and (vii) collecting reported compromises of any Certificates and promptly instructing Entrust to update the CRL. You will promptly notify Entrust of any changes to the identity of the person(s) who are designated as Local Registration Authorities.

(d) Security Measures. Commercially reasonable physical and procedural security controls will be implemented by Entrust to control access to the Entrust Certification Authority hardware and software. The Entrust Certification Authority host computer will have access control, CCTV systems and motion detectors. Access to the host computer will be limited to those authorized personnel required to perform such services. Access will be controlled through the use of electronic access controls, mechanical locksets, and deadbolts. The zone will be monitored 24 hours a day and 7 days a week by security staff, other personnel, or electronic means. Access control records will be maintained and audited periodically. Maintenance and service personnel will be properly escorted and supervised. You will operate the Registration Authority in an environment with appropriate physical, personnel, and electronic security measures. Physical security requirements for the Registration Authority include maintenance of the communication workstation(s) in a physically-secure room. Access to the room for the Registration Authority must be restricted to a limited number of named persons. Persons employed by or contracted to work on behalf of You must be checked to ensure they have appropriate skills, knowledge, and backgrounds (including any security clearance requirements imposed by law or Government policy) to operate in a trusted and secure environment.

(e) Certificate Services. Entrust will issue, renew, and revoke Certificates in accordance with the instructions received by Entrust from the Registration Authority or Local Registration Authority, which Entrust will be entitled to rely upon (collectively the “Certificate Services”). 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). Pager support is available 24 hours per day, 7 days per week. 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 You report a problem or incident, Entrust will, in consultation with You, 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 You 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 You 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 You 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 You 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 Entrust Certification Authority, Entrust may include any Entrust Certification Authority error correction in the next upgrade of the software used by Entrust.

(f) **Verification Records.** You will keep complete and accurate records (the "LRA Records") with respect to Your validation of Certificate Applications as contemplated by the LRA Guide. Upon request from Entrust, You will provide such LRA Records to Entrust so that Entrust and/or Entrust's independent auditor can confirm You followed the established procedures as set out in the LRA Guide. Alternatively, Entrust will have the right to appoint an independent auditor reasonably acceptable to You, under appropriate non-disclosure conditions, to audit LRA Records not more than once per year to confirm Your compliance with the verification requirements. For greater certainty, the above right to audit will be limited to those records on file with You that pertain to Your compliance with this Plan.

(g) **Your Responsibilities.** DSL, cable or another high speed Internet connection is required for proper transmission of the Certificate Services. You are responsible for procuring and maintaining the network connections that connect the Certification Authority, including, but not limited to, "browser" software that supports protocol used by Entrust, including Secure Socket Layer (SSL) protocol or other protocols accepted by Entrust, and to follow logon procedures for services that support such protocols. Entrust is not responsible for notifying You of any upgrades, fixes or enhancements to any such software, or for any compromise of data transmitted across computer networks or telecommunications facilities (including but not limited to the Internet) which are not provided or operated by Entrust or its subcontractors (which in this context shall not include internet service providers, telecommunication providers or other such internet access providers (an "ISP")) to provide the Certificate Services. Entrust assumes no responsibility for the reliability or performance of any connections as described in this paragraph for any such external infrastructure. You shall authorize access to and assign unique user names to Subscribers. As between the parties, You will be responsible for the confidentiality and use of passwords and for any misuse of such passwords. You agree not to access

the Certificate Services by any means other than through the interfaces that are provided by Entrust or otherwise contemplated in the LRA Guide. You shall not do any "mirroring" or "framing" of any part of the Certificate Services, or create Internet links to the Service which include log-in information, user names, passwords, and/or secure cookies. You undertake that (i) all information relevant to the issuance of a Certificate has been validated and is accurate in accordance with the minimum standards in the LRA Guide; (ii) any Certificate Applications approved by You has been authorized by the person named as the subject of the Certificate or by the person who owns and controls the device named as the subject of the Certificate; (iii) Your instructions respecting the issuance, renewal, and revocation of Certificates will be accurate, complete, and may be relied upon by Entrust; (iv) Entrust has the right to use any trademark, service mark, trade name, or other information (including personal information) provided to Entrust by You for inclusion in any Certificate hereunder; (v) if You learn that any Subscriber has compromised a private key corresponding to the public key in such Certificate then You will promptly notify Entrust of such compromise so that Entrust can revoke such Certificate; (vi) You will cause Your Registration Authorities, Your Local Registration Authorities, and any Subscribers to comply with the requirements of this Plan and the Subscriber Agreement; and (vii) You will use Certificates exclusively for lawful and authorized purposes; and (vii) You will not reverse engineer or interfere with the technical implementation of the Services or knowingly compromise the security of any of Entrust's systems. Where Certificates are issued to devices at Your request, You are responsible for ensuring that the devices You intend to use with Certificates support and are interoperable with the Certificates.

(h) Additional Items. During the term of this Plan, Entrust warrants to You that the Certificate Services will comply with its applicable Certification Practice Statement, as amended from time to time, and will not introduce any material errors in the information supplied by You in any Certificate as a result of a failure to exercise reasonable care in creating the Certificate. You expressly acknowledge that Entrust reserves the right to revoke any Certificates if Entrust reasonably determines that there has been a security compromise or a security compromise is possible, or as otherwise permitted in the Subscriber Agreement or in this Plan. Any software made available for use with the Service ("Software") is a "commercial item" as that term is defined at FAR 2.101, consisting of "commercial computer software" and "commercial computer software documentation" as such terms are defined in FAR 12.212, and is provided to the U.S. Government only as a commercial end item. Government end users acquire the rights set out in this Agreement for the Software consistent with: (i) for acquisition by or on behalf of civilian agencies, the terms set forth in FAR 12.212; or (ii) for acquisition by or on behalf of units of the Department of Defense, the terms set forth in DFARS 227.7202. Use of this Software and related documentation is further restricted by the terms and conditions of this Agreement.

# ***ENTRUST, INC.'S AUTHORIZED GSA PRICING***

## **ENTRUST FEDERAL SHARED SERVICE PROVIDER UNDER FEDERAL BRIDGE POLICY**

The Entrust Managed Services FED SSP has been designed to meet US Federal Common policy and standards requirements while providing the same high level of technology and services that have positioned Entrust as a leader in PKI across the Federal Government. Entrust is pleased to have joined the ranks of providers under this program.

This offering provides certificates that are trusted under the Federal Bridge program. There is no requirement for US government departments to have in-house expertise in PKI or Security Policy as Entrust manages the PKI under the Federal Bridge policy framework.

### **Hosted components include:**

- CA (Entrust Authority Security Manager + associated Database)
- HSM for storage of CA keys
- PKI Directory
- Entrust Authority Administration Services
- Entrust Authority Enrollment Server for Web
- OCSP Service

### **Customer components (at customer location) available:**

- Entrust Authority Enrollment Server for VPN
- Entrust Authority Auto-Enrollment Server

### ***Entrust Managed Services Federal SSP***

The Entrust Federal Shared Service Provider (Fed SSP) is a hosted PKI offering for employees of the US Federal Government, or their contractors where a US Federal department has sponsored their contractor. The hosted Federal SSP CA is subordinate to the Entrust Federal Root CA, which in turn is cross-certified with the Federal Common Policy CA.

### **Certificates it is able to offer are:**

- PIV
- User, Device, Server

<b>SIN</b>	<b>Product Description</b>	<b>GSA Price</b>
	<b>Entrust Managed Services (Fed SSP)</b>	
	The Entrust Federal Shared Service Provider (Fed SSP) is a hosted PKI offering for employees of the US Federal Government, or their contractors where a US Federal department has sponsored their contractor. The hosted Federal SSP CA is subordinate to the Entrust Federal Root CA, which in turn is cross-certified with the Federal Common Policy CA. Certificates it is able to offer are: <ul style="list-style-type: none"><li>•PIV</li><li>•User, Device, Server</li></ul>	
132-61	Up to 100 (per entity)	\$66.64
132-61	101 – 500 (per entity)	\$20.70
132-61	501 – 1000 (per entity)	\$14.11
132-61	1001 – 5000 (per entity)	\$7.10
132-61	5001 – 10,000 (per entity)	\$5.99
132-61	10,001 – 50,000 (per entity)	\$5.04
132-61	50,001 – 100,000 (per entity)	\$3.53

SIN	Product Description	GSA Price
132-61	100,001 – 250,000 (per entity)	\$2.47
132-61	251,000 – 500,000 (per entity)	\$2.12
132-61	Over 500,000 (per entity)	\$1.81

**OCSP proof files download**

This optional service provides download access to OCSP signed validation proof lists for use with OCSP responders located within the customer environment. It is for US government departments that have requirements for OCSP validation within their own network.

SIN	Product Description	GSA Price
132-61	Annual fee for up to 5 downloads per day.	\$8,463.48