General Services Administration
Federal Acquisition Service
Authorized Federal Supply Schedule FSS Price List

On-line access to contract ordering information, terms and conditions, up-to-date pricing, and the option to create an electronic delivery order are available through GSA Advantage!®, a menu-driven database system. The INTERNET address GSA Advantage!® is: GSAAdvantage.gov.

Multiple Award Schedule (MAS)

Entrust Corporation

1187 Park PL
Shakopee, MN 55379
Phone: (952) 933-1223
Internet Address: https://www.entrust.com/

Contract Number: 47QTCA20D007M

Period Covered by Contract: March 20, 2020, through March 19, 2030

Pricelist current as of Modification #PO-0030, effective October 28, 2025

Business size: Other than Small

For more information on ordering, go to the following website: https://www.gsa.gov/schedules

Prices Shown Herein are Net (discount deducted)

CUSTOMER INFORMATION

1a. Table of awarded special item number(s) with appropriate cross-reference to item descriptions and awarded price(s).

SINs	Recovery	SIN Title
541519PKI	541519PKIRC	Public Key Infrastructure (PKI) Shared Service Providers (PKI SSP) Program
OLM	OLMRC	Order-Level Materials (OLM's)

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 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 Pricelist

2. Maximum order. $1,000,000

3. Minimum order. $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.. Does not apply to credit card orders

9. Foreign items (list items by country of origin). None

10a. Time of delivery. 30 Days

10b. Expedited Delivery. Contact Contractor

10c. Overnight and 2-day delivery. Contact Contractor

10d. Urgent Requirements. Contact Contractor

11. F.O.B. point(s). Destination

12a. Ordering address(es). : Same as company address

12b. Ordering procedures: See Federal Acquisition Regulation (FAR) 8.405-3.

13. Payment address(es).Same as company address

14. Warranty provision. Standard Commercial

15. Export packing charges, if applicable. Export packing is available outside the scope of this contract

16. Terms and conditions of rental, maintenance, and repair (if applicable). Not applicable

17. Terms and conditions of installation (if applicable). Not applicable

18a. Terms and conditions of repair parts indicating date of parts price lists and any discounts from list prices (if applicable). Not applicable

18b. Terms and conditions for any other services (if applicable). Not applicable

19. List of service and distribution points (if applicable). Not applicable

20. List of participating dealers (if applicable). Not applicable

21. Preventive maintenance (if applicable). Not applicable

22a. Special attributes such as environmental attributes (e.g., recycled content, energy efficiency, and/or reduced pollutants). Not applicable

22b. 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/. Not applicable

23. Unique Entity Identifier (UEI) number: HWMGGWPNM6Y3

24. Notification regarding registration in SAM.gov (formerly the Central Entrust has registered in the System for Award Management (SAM) database. The CAGE code is 1LDQ2

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.

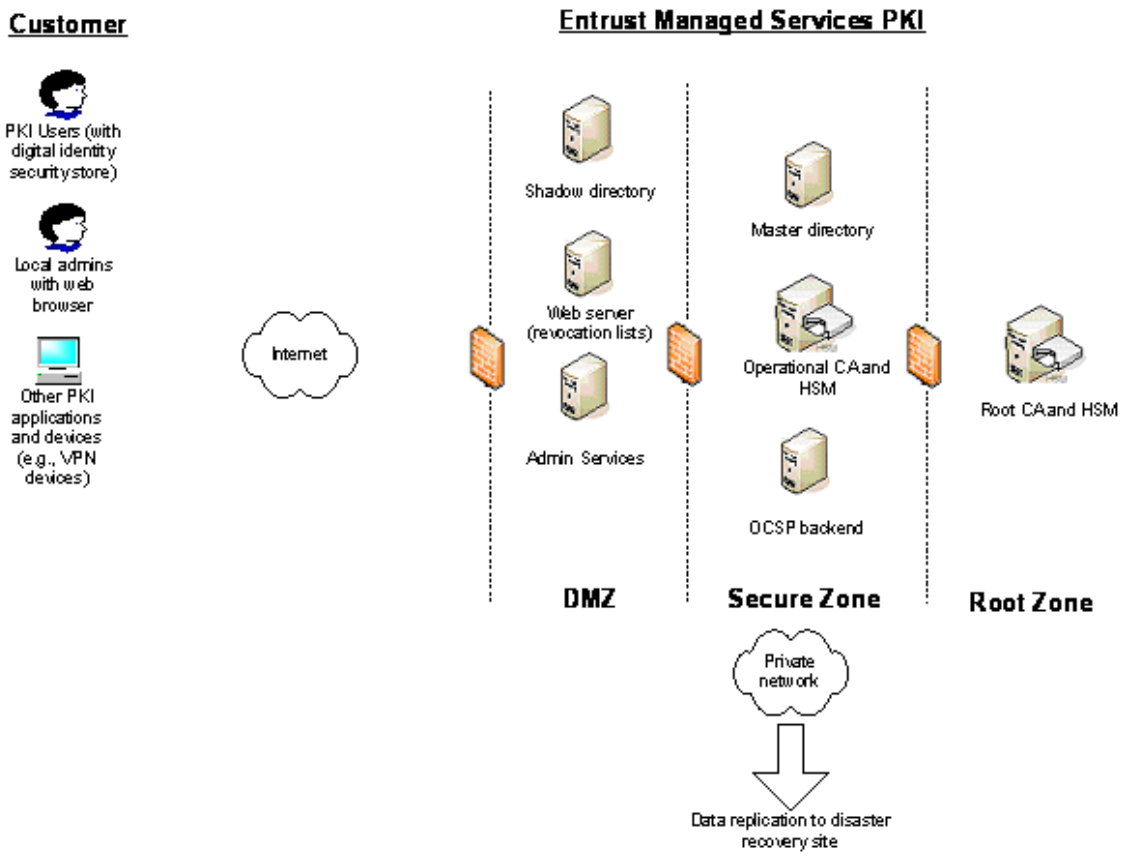
This CA is cross certified to the Federal Common Policy CA.

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.



MANAGED SERVICES PKI COMPONENTS – ENTRUST NETWORK

The primary data center for the Entrust Managed Services PKI is hosted at a CyrusOne data center in Carrolton, Tx. The facility is a state-of-the-art data center collocation facility, including perimeter fencing, redundant power services, on-premise 24/7 security guards, 24/7 staffed NOCC and security cameras for surveillance capabilities. Physical servers are secured within the cage in locked 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, carrier neutral CyrusOne Internet Exchange connectivity, efficient cooling and fire suppression systems.

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).

DERIVED CREDENTIAL ISSUANCE SERVICE

DERIVED CREDENTIAL ISSUANCE SERVICE DESCRIPTION

The Derived Credential Issuance Service (DCIS) is a service that performs life-cycle management for Derived PIV Credentials (DPC). DPCs are digital certificates that reside on mobile devices such as mobile phones and are issued through the use of a PIV Authentication certificate as both the mechanism of authentication and the source of information to create the new certificates (hence the term "derived"). DPCs consist of one or more of the following: a Derived Authentication certificate, a Derived Signature certificate, and/or Derived Encryption certificate. Customers whose PIV cards contain Encryption certificates issued by the Entrust Managed Services Federal SSP may be able to recover the key to their mobile devices depending on the technologies utilized to deliver certificates to the device. DPCs may be delivered directly to virtual smart cards (applets) installed on the mobile device, or they may be delivered to a Mobile Device Manager (MDM) that will deliver the credentials to a mobile device as part of a more comprehensive deployment.

DPCs are issued in compliance with *Federal Information Processing Standard (FIPS) Special Publication 800-157, Guidelines for Derived Personal Identity Verification (PIV) Credentials*. DCIS consists of two (2) main parts: the Derived Credential Management Service (DCMS), and the Derived Credential Administration Service (DCAS). DCMS is a mandatory system that interfaces with Certificate Authorities (CAs) and delivers certificates to mobile devices. DCAS is an optional (no cost) component that provides an administrative mechanism and interfaces that allow agencies to control the lifecycle of DPCs issued to agency users either manually or programmatically. Each of these two components are described below:

DCMS performs the majority of the work in the DCIS. DCMS is responsible for:

- implementing the policies required to conform to Federal requirements,
- ensuring the binding between the person and the certificates issued to the mobile device
- interfacing to the CA to request certificate issuance,
- deploying certificates to the mobile device or delivering certificate to an authorized Mobile Device Manager,
- performing a check seven (7) days after DPCs are issued to ensure that the PIV card used by the subscriber to request DPCs was not revoked within the seven (7) day period.

DPCs may be delivered directly to an Entrust smart credential applet on a mobile device, or they may be delivered to an authorized third-party Mobile Device Manager that is responsible for managing multiple functions of the device, including PKI credentials.

DCAS is a customer-facing service that provides interfaces that allow customers to control the issuance of DPCs or to revoke existing DPCs. Customers may submit lists of distinguished names for their users that:

- are authorizing to have DPCs from their organization
- have DPCs and that should be revoked
- have DPCs and that should be suspended

- have DPCs and that should be removed from suspension
- should be administrators / should no longer be administrators

DCAS supports a REST interface for web services that allows customers to integrate with an existing credential management system or human resources system. A client is also provided that permits smaller customers to administer the system manually. Errors and confirmation information are emailed back to the administrators for the organization.

Issuing DPCs

DPC issuance is governed by the *X.509 Certificate Policy For The U.S. Federal PKI Common Policy Framework* (Certificate Policy). This policy document is maintained the Federal PKI Policy Authority (FPKIPA). FPKIPA is a group of U.S. Federal Government Agencies (including cabinet-level Departments) chartered by the Federal CIO Council. FPKIPA owns this policy and represents the interest of the Federal CIOs.

Subscriber authentication is performed according to the Certificate Policy and the specific procedures will vary depending upon the assurance level the certificate is issued under. Currently, OMB Memorandum M-04-04, E-Authentication Guidance for Federal agencies, December 16, 2003 define four (4) levels of assurance for identity assurance. These levels vary from LOA-1 (no identity proofing required) through LOA-4 (Level 4 requires strong cryptographic authentication of all parties, and all sensitive data transfers between the parties. Either public key or symmetric key technology may be used. The token secret shall be protected from compromise through the malicious code threat). Derived PIV Credentials can be issued at identity assurance levels three or four (LOA-3 or LOA-4). The credential may reside on a hardware or software security token within the mobile device.

An LOA-3 Derived PIV Credential may be issued remotely or in person using the DCMS web portal to perform PIV Authentication using the following process:

1. an applicant presents the PIV Authentication certificate from his or her existing PIV Card to DCMS for derived credential issuance.
2. if the PIV Authentication certificate verifies,
3. and the PIV Authentication certificate has not been revoked,
4. then, DCMS will verify that the user's distinguish name has been uploaded to the system as a user permitted to be issued a credential, usually through DCAS.

If all of these steps are successful, then DPCs will be issued.

If the Applicant is requesting a LOA-4 Derived PIV Credential, then the applicant will appear in person before a Registration Authority and identify himself/herself using a biometric sample that can be verified against the applicant's PIV Card. The RA or LRA retains records of the verification.

DCMS will automatically re-check revocation status of the applicant's PIV Authentication certificate seven (7) calendar days following issuance of the Derived PIV Credential in order to detect the use of a compromised PIV Card to obtain a Derived PIV Credential.

KEY RECOVERY SERVICE (KRS)

KRS DESCRIPTION

KRS is a multi-tenant service designed to retrieve encryption keys which have been escrowed by an Entrust Certification Authority (CA) during the enrollment process of a 'managed' user. Tenants are separated in the system so that one tenant is unable to request or approve keys belonging to another tenant. Retrieved keys may be stored in software, in an encrypted PKCS #12-formatted file or on a hardware token.

The KRS enforces roles and group membership through cryptographic controls (issuance of dedicated PKI certificates) and with group and policy controls on the CA. In addition, certain policy controls, such as whether a Registration Authority (RA) is permitted to approve a request for a key whose certificate asserts a higher assurance policy that the RA's certificate, are set on the KRS computer server through configuration parameters.

KRS PROCESS

The process of requesting an escrowed key is as follows:

- A KR connects to the KRS using the KRS client, and provides sufficient information to identify a user (distinguished name, serial number, etc.)
- The KR is provided with a list of the user's keys that may be recovered. The KR checks the keys that are being requested. The KR submits the request to the KRS.
- The KRS notifies the KRAs via email that a transaction is pending. (KRS may be configured to notify a subset of KRAs, referred to as KRA1s, or all KRAs may be notified, and the transaction is handled on a first-come basis. In any event, the first KRA to service the transaction is called KRA1.)
- KRA1 logs in, opens the queue, and sees the transaction. KRA1 reviews the transaction and determines whether the transaction should be permitted according to government agency guidelines. KRA1 may approve the transaction, deny the transaction, cancel or ignore the transaction.
- If the transaction is approved by KRA1, KRA2 is notified that there is a pending transaction in the queue. KRA2 reviews the transaction and determines whether the transaction should be permitted according to government agency guidelines. KRA2 may approve the transaction, deny the transaction, cancel or ignore the transaction.
- If both KRA1 and KRA2 approve the transaction, an encrypted message is sent to the KR with instructions regarding how to complete the key recovery process and provide a password or PIN for key storage.

If the KR or the KRAs cancel the transaction, the process terminates and the request is logged and archived. All requests have a 'time-to-live' validity period during which time the KRAs are expected to process the request. If the KRAs fail to act within this period, the request will expire and the requester will be notified that the request has expired.

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.

DERIVED CREDENTIAL ISSUANCE SERVICE

Additional legal clauses for inclusion with Fed SSP terms in Entrust GSA

DEFINITIONS

"Certificate Policy" means a policy document which addresses electronic transactions performed during certificate management. A certificate policy describes all aspects associated with the generation, production, distribution, accounting, compromise, recovery and administration of digital certificates.

"DCAS Administrator" means an individual, system or process responsible for performing the tasks of adding revoking or removing Subscribers from the DCIS.

"DCMS Administrator" means an individual responsible for performing the tasks of adding revoking or removing Subscribers from the DCIS. DCMS Administrators are only necessary if DCAS is not being used by the agency.

"Derived Credential Administration Service" or "DCAS" means a customer-facing service that interfaces with customers to control the issuance of DPCs or to revoke existing DPCs. DCAS is used when a Mobile Device Manager is not used; otherwise the Mobile Device Manager usually performs these operations.

"Derived Credential Issuance Service" or "DCIS" means a service that performs life-cycle management for Derived PIV Credentials.

"Derived Credential Management Service" or "DCMS" means a system that interfaces with Certificate Authorities ("CAs") and delivers digital certificates to mobile devices.

"Derived PIV Credentials" or "DPC" are digital certificates that reside on mobile devices such as mobile phones and are issued through the use of a PIV authentication certificate as both the mechanism of authentication and the source of information to create the new certificates.

"Mobile Device Manager" or "MDM" means a third-party system that administers mobile devices such as mobile phones and tablets. MDM systems are systems that allows IT administrators to control, secure and enforce policies on smartphones, tablets and other endpoints. MDM is a core component of enterprise mobility management (EMM)

which also includes mobile application management, identity and access management and enterprise file sync and share.

APPOINTMENT AND RESPONSIBILITIES FOR DCIS

(a) **Derived Credential Issuing Service**. Provided that You have purchased the Derived Credential Issuance Service and paid the applicable fees, Entrust will provide the Derived Credential Issuance Service as part of the Entrust Managed Services Federal SSP, in compliance with the Certificate Policy. The Derived Credential Issuance Service provides the ability to issue digital certificates derived from existing PIV cards (one or more of the following: Derived Authentication digital certificates, Derived Signature digital certificates, Derived Encryption digital certificates). If You have PIV cards which contain encryption digital certificates issued by the Entrust Managed Services Federal SSP, You may not be able to recover the key to Your mobile devices depending on the technologies utilized to deliver the digital certificates to the device.

(b) **DCMS Administrator**. You will appoint one (1) or more of your employees to serve as a DCMS Administrator who is authorized to request DPC issuance, revocation, suspension, or release from suspension. Two (2) initial DCMS Administrators will be added by administrators. You may elect to add additional administrators.

(c) **DCAS Administrator.** You will appoint one (1) or more of your employees to serve as DCAS Administrator(s). It is the responsibility of the DCAS Administrator to add the distinguished names of all Subscribers who are permitted to receive DPCs. DCAS Administrators may add additional DCAS Administrators. Additional DCAS Administrator credentials may be assigned to processes or systems that manage automated lifecycle management for credentials.

KEY RECOVERY SERVICE (KRS)

Additional legal clauses for inclusion with Fed SSP terms in Entrust GSA

DEFINITIONS

"Certificate Policy" means a policy document which addresses electronic transactions performed during certificate management. A certificate policy describes all aspects associated with the generation, production, distribution, accounting, compromise, recovery and administration of digital certificates.

"Key Recovery Officer" or "KRO" means an individual responsible for performing identity and validation tasks for trusted roles in the KRS. KROs are identified by each government agency and it is the government agency's responsibility to add and/or remove other Trusted Roles in KRS for that specific government agency.

"Key Recovery Practices Statement" means a policy document which addresses the protection and recovery of key management private keys (i.e. decryption keys) held in escrow. Such policy document describes all aspects associated with the storage and recovery of key management certificates.

"Key Recovery Service" or "KRS" means the hardware, software and policy functions, systems and subsystems that interface with the Entrust Shared Service Provider (SSP) Certification Authorities (CAs) in order to retrieve escrowed encryption keys. KRS enforces the policies described in the Key Recovery Practices Statement (KRPS) as identified in the Certification Authority's Certificate Practices Statement (CPS).

"Key Recovery Agent" or "KRA" means an individual who, using a two-party control procedure with a second KRA, is authorized to interact with the KRS and approve the extraction of requested escrowed keys.

"Key Requestor" or "KR" means an individual who wishes to recover a user's escrowed private key(s). These keys may be recovered for: (a) investigative / forensic purposes, (b) in circumstances where the user is not available to access data previously encrypted, or (c) to respond to court orders. The KR originates the request for one or more specific keys, and receives the keys if extraction is approved.

"Trusted Role" means individuals trusted to perform actions on Your behalf within the Key Recovery Service. Trusted Roles includes Key Recovery Officers, Key Requestors and Key Recovery Agents.

APPOINTMENT AND RESPONSIBILITIES FOR KRS

(a) **Key Recovery Service**. Provided that You have purchased the Key Recovery Service and paid the applicable fees, Entrust will provide the Key Recovery Service as part of the Entrust Managed Services Federal SSP, in compliance with the Certificate Policy and the Key Recovery Practices Statement. The Key Recovery Service provides the ability to recover encryption keys which have been escrowed by the Entrust Certification Authority. Entrust will rely solely on the request submitted by the Key Requestor and on the approvals of the Key Recovery Agents to release the requested keys to the Key Requestor. You are solely responsible for the use and/or disposition of any and all recovered escrowed keys. Notwithstanding anything to the contrary in this Contract, Entrust and its affiliates will have no responsibility or liability to You, Your employees and/or Your subcontractors regarding the use and/or disposition of any and all recovered escrowed keys.

(b) **Key Recovery Officer**. You will appoint one (1) or more of your employees to serve as a Key Recovery Officer with responsibility for performing identification and validation of Your employees who are authorized to act as Key Requestors and Key Recovery Agents. The functions performed by the Key Recovery Officer are set forth in the Key Recovery Practices Statement and include (i) verifying the identity of an applicant for a Trusted Role in the KRS, (ii) adding the applicant to the KRS system, and (iii) promptly removing Trusted Roles when they no longer require access. You will promptly notify Entrust of any changes to the identity of the person(s) who are designated as Key Recovery Officers. Key Recovery Officers will not fulfill any other Trusted Role within the Key Recovery Service.

(c) **Key Requestor(s)**. You will appoint one (1) or more of your employees to serve as the Key Requestor. It is the responsibility of the Key Requestor ensure that all key requests are in compliance with the Certificate Policy, Key Recovery Practices Statement and with organizational policies. The Key Requestor is responsible for the storage, utilization and destruction of recovered escrowed keys in a manner compliant with the Certificate Policy, Key Recovery Practices Statement and with organizational policies. The Key Requestor shall maintain written records that track the disposition of recovered escrowed keys and provide all documentation to Entrust or to a third-party auditor retained by Entrust for review upon request. Key Requestors will not fulfill any other Trusted Role within the Key Recovery Service.

(d) **Key Recovery Agent(s).** You will appoint at least two (2) employees to serve as Key Recovery Agents. Key Recovery Agents are responsible for reviewing key recovery requests, determining that the requests are appropriate and in compliance with the Certificate Policy, Key Recovery Practices Statement and with organizational policies. If the request is in compliance, the Key Recovery Agent will approve the requests in a timely manner. Key Recovery Agents may reject a request if the request does not comply with the Certificate Policy, Key Recovery Practices Statement, or with organizational policies. Key Recovery Agents will not fulfill any other Trusted Role within the Key Recovery Service.

(e) **Key Recovery Records**. You are responsible for maintaining a records outside of the KRS system which records the location of storage, usage, disposition and/or destruction of the recovered escrowed keys. These records shall be made available to Entrust or a third-party auditor retained by Entrust for review upon request.

ENTRUST CORPORATION'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