LAWRENCE
LIVERMORE
NATIONAL
LABORATORY

LLNL-SR-814394

Enterprise Credentialing Service Statement of Work (SOW)

G. Lee, S. Ecklund

September 10, 2020

Disclaimer

This work performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory under Contract DE-AC52-07NA27344.

1 SCOPE OF WORK

1.1 Project Overview

The scope of this project includes providing professional services in support of the development and deployment of an Enterprise Credentialing Service for the Department of Energy (DOE) National Nuclear Security Administration (NNSA), which will be used for issuing and managing credentials used for authentication, digital signature, and encryption functions by users, applications, and devices in a closed computing environment. The Seller shall provide subject matter expertise for the design and deployment of the technologies and processes that comprise the Enterprise Credentialing Service, which will include a public key infrastructure (PKI) and a credential management system (CMS) that issues and manages PKI-based smartcard credentials. The Enterprise Credentialing Service will support approximately 17,000 users at 15 DOE NNSA sites and laboratories located across the continental United States.

The technology for the backend infrastructure of the Enterprise Credentialing Service will be deployed in datacenters at three geographically distinct locations: Sandia National Laboratory (SNL) in Albuquerque, New Mexico; Lawrence Livermore National Laboratory (LLNL) in Livermore, California; and NNSA Information Assurance Response Center (IARC) in Las Vegas, Nevada. SNL is expected to host the Development Environment and the Integration Environment. LLNL and IARC are expected to host the Production Environment, unless determined necessary by the LLNS' Technical Representative to complete a specific task assigned herein, the Seller is not anticipated to be physically present at the datacenters. The computing resources at the datacenters is expected to be accessible via any one of the three remote computing facilities located at SNL, LLNL, or DOE Headquarters located in Germantown, Maryland. In the event travel is determined necessary, the Seller shall be escorted when access is required to the remote computing facilities to assist and help facilitate the installation and configuration of the software technology, which will be performed by authorized DOE NNSA personnel.

1.2 Vendor Technology

The vendor technology for the PKI and CMS components of the Enterprise Credentialing Service will be:

- PKI
  - Vendor: Entrust Datacard
  - Product: Entrust Authority Security Manager
  - Purpose: Certification Authority (CA) for the PKI
- CMS
  - Vendor: HID Global
  - Product: ActivID Credential Management System
  - Purpose: Issue and manage lifecycle of PKI-based smartcard credentials
- Hardware Security Module
  - Vendor: nCipher
  - Product: nShield connect XC
  - Purpose: Protect all keys of the enterprise credentialing system and generate all private keys that will be provisioned onto PKI-based smartcards issued by the CMS
- Smartcard technology
  - HID Global ActivID Applet Suite v2.7.6 on Giesecke & Devrient Sm@rtCafé Expert 7.0
  - Certificate #45 on the FIPS 201 Approved Product List.

2 Project Objectives

The objective of this project is to obtain professional services to support:

1. The design and deployment of an Enterprise Credentialing Service that issues and manages PKI-based smartcard credentials and PKI certificates for devices and applications.

2. The deployment of an Enterprise Credentialing Service in a manner that is consistent with Committee on National Security Systems (CNSS) PKI policies and guidance (Section 11 Reference Documents).

3 Project Scope

3.1 The scope of this Statement of Work encompasses the Seller providing the highest quality of professional services to efficiently and effectively fulfill the project objectives cited above. Specifically, the Seller shall provide qualified personnel skilled in the use of PKI and CMS technology for the design and deployment of a comprehensive Enterprise Credentialing Service to be completed within the Project Schedule.

3.2 The Seller shall be directly responsible for ensuring the accuracy, timeliness and completeness of all assignments and the tasks performed herein.

3.3 The Seller shall demonstrate their knowledge and expertise of the Entrust and HID technologies by developing a solution architecture that incorporates these technologies as the foundational components of the Enterprise Credentialing Service. The Seller shall identify additional technology vendors to supplement the Entrust and HID technologies to meet the Technical Requirements of this SOW. If needed, all software and hardware will be procured separate from this SOW upon the Seller delivering the solution architecture document that identifies what technology(ies) are needed to meet the Technical Requirements of this SOW.

3.4 For the Enterprise Credentialing Service, DOE NNSA will have dedicated Dell servers with Hypervisors running VMware ESXi 6.7.x in each of the datacenters. The Seller shall identify in the solution architecture document (Phase 2 - Architecture and Design) the minimum number of dedicated Dell servers that are needed in the production datacenters in order to achieve the Performance and Availability requirements in this SOW. The Seller shall identify in the solution architecture the PKI and/or CMS components (if any) that cannot be installed and operated on Hypervisors, and LLNS in concert with LANL will coordinate the logistics with the respective datacenters.

3.5 The Enterprise Credentialing Service will be in a closed computing environment that adheres to the policies and guidelines of the Committee on National Security Systems (CNSS). The Seller shall demonstrate their CNSS knowledge and expertise by developing a solution architecture and incorporating best practices that are in accordance with CNSS Policy No. 25 and CNSS Instruction No. 1300. As part of this SOW, the Seller shall develop and provide the requisite certification and registration practice statements (CPS/RPS) (**Phase 3 – PKI Governance Documentation**) in accordance with CNSS Instruction No. 1300. LLNS in concert with LANL, in conjunction with the DOE NNSA policy authorities will work with the Seller to ensure the CPS and RPS documentation meets DOE NNSA operational needs within the CNSS policy constraints.

4 Definitions

4.1 Key Terms

The following defines key terms as they are used in this SOW.

Term	Definition
Credential Management System (CMS)	The software technology that provisions and manages the life cycle of PKI-based smartcard credentials. In this SOW, the CMS base technology will be HID ActivID CMS.
Development Environment	All testing and vetting of the solution will be done in the certification test lab (CTL) at SNL in Albuquerque, NM. The Development Environment instance will be a discrete implementation to vet the solution architecture and modify, as necessary.
DOE Root Certification Authority (DOE Root CA)	The dedicated root CA that will be established as part this SOW. While the CA will be deployed and configured in accordance with CNSS Policy No 25 and CNSS Instruction No 1300, it will not be directly certified and chain to the CNSS Root Certification Authority.
Enterprise Credentialing Service	The comprehensive service that will result upon the execution of this SOW. The Enterprise Credentialing Service by DOE NNSA to issue and manage credentials used for authentication, digital signature, and encryption functions by users, applications, and devices in a closed computing environment. It will include a Public Key Infrastructure (PKI) and a Credential Management System (CMS).
Non-Person Entity (NPE)	Any hardware device, application, software, web server, etc. that is not a "person" and uses PKI certificates.
Production Environment	This is the production capability deployed in datacenters at two geographically separate sites - Primary site at LLNL in Livermore, California; Secondary site at IARC in Las Vegas, Nevada.
Public Key Infrastructure (PKI)	The technology, policies and processes that are implemented to issue and manage the life cycle of digital certificates and public/private key pairs. In this SOW, the PKI base technology for the certification authority will be Entrust Authority Security Manager.
Integration Environment	Co-located in the CTL at SNL, the Integration Environment instance will reflect the target configuration as it would be deployed in production based on the work done in the Development Environment. The Integration Environment shall mirror what is deployed and operational in production to facility quality control. The DOE NNSA security team will assess the security in this environment prior to approving deployment and/or changes to the production capability.

4.2 Acronyms

Acronym	Definition
CA	Certification Authority
CMS	Credential Management System
CNSS	Committee on National Security Systems
CPS	Certification Practice Statement
CTL	Certification Test Lab
DOE	Department of Energy
HSM	Hardware Security Module
IARC	NNSA Information Assurance Response Center
LANL	Los Alamos National Laboratory
LLNL	Lawrence Livermore National Laboratory
LLNS	Lawrence Livermore National Security LLC
LRA	Local Registration Authority
NNSA	National Nuclear Security Administration
NPE	Non-person entity
PKI	Public Key Infrastructure
RPS	Registration Practice Statement
RA	Registration Authority
SNL	Sandia National Laboratory

5 Project Breakdown

Phase 1 - Initial Kick off and Project Assessment

Objectives: Conduct an initial project kickoff meeting and a requirements review to assess DOE NNSA's business requirements and perform a gap analysis with the SOW requirements cited herein including all Reference Documents.	
Key Activity: ♦ Project Kickoff meeting and detailed work completion plan covering all Phases of the SOW? ♦ Requirements review session with Seller, LLNS, LANL, and relevant DOE stakeholders (e.g. Enterprise Architecture, Information Security Officer, etc.)	
Seller Deliverables: ♦ Gap Analysis ♦ Work completion plan ♦ Updated Requirements Document (if needed)	
Total Estimated Hours	

This phase is deemed complete upon review and acceptance of all Seller Deliverables by LLNS.

Phase 2 - Architecture and Design

This phase may commence upon completion of Phase 1.

Objectives: This phase focuses on developing the solution architecture, as it will be deployed in the Production Environment. The solution architecture document is critical for LLNS in concert with LANL obtaining approval from the DOE NNSA engineering design review board to commence with Phase 6. It is expected that the solution design will be updated and refined during deployment of the technology in the Development Environment at SNL in Phase 6.	
Key Activity: ♦ Collaborate on technical requirements and design alternatives ♦ Identify software and hardware (if any) that needs to be procured independent of this SOW, including the number of Dell servers and Hypervisors needed to deploy the design in Production Environment ♦ Develop solution architecture ♦ Develop test plan ♦ Virtual technical meetings, as mutually agreed upon	
Seller Deliverables: ♦ Solution architecture ♦ Test Plan ♦ List of software and hardware to include make, model and amount needed ♦ Recommended number of Dell servers and Hypervisors needed to deploy the design in Production Environment	
Total Estimated Hours	

This phase is deemed complete upon review and acceptance of all Seller Deliverables by LLNS.

Phase 3 – PKI Governance Documentation

This phase may commence upon completion of Phase 1.
This phase may be performed concurrently with Phase 2 and all subsequent phases.

Objectives: This phase focuses on developing the foundational PKI governance documentation that demonstrates the Enterprise Credentialing Service adheres to the requisite CNSS polices, specifically CNSS Policy No. 25 and CNSS Instruction No. 1300. While DOE NNSA follows CNSS, the certification and approval of the PKI governance documentation by the CNSS PKI Governing Body is not in scope of this SOW; however, the PKI governance documentation will be submitted to and coordinated with the appropriate DOE NNSA policy organization for approvals.	
Key Activity: ♦ Develop the DOE Root Certification Authority CPS in accordance with CNSS Instruction No. 1300. Under this SOW, DOE NNSA is not expecting to submit the CPS to CNSS for approval and certification; however, the CPS is expected to conform with CNSS Instruction No. 1300 as though it would be submitted to CNSS. ♦ Develop CPS for each issuing CA subordinate to the DOE Root Certification Authority in accordance with CNSS Instruction No. 1300 ♦ Develop RPS for issuance of PKI-based smartcard credentials and Non-Person Entity certificates	

♦ Virtual technical meetings, as mutually agreed upon	
Seller Deliverables: ♦ DOE Root Certification Authority CPS ♦ CPS for each issuing CA subordinate to the DOE Root Certification Authority that is established under this SOW ♦ RPS for issuance of PKI-based smartcard credentials ♦ RPS for Non-Person Entity certificates	
Total Estimated Hours	

This phase is deemed complete upon review and acceptance of all Seller Deliverables by LLNS.

Phase 4 - Off-card Key Generation Integration

This phase may commence upon completion of Phase 1.
This phase may be performed concurrently with Phase 2 and all subsequent phases.

Objectives: This phase focuses on activities needed to ensure the HID ActivID CMS is able to support the issuance of PKI-based smartcard credentials with all private keys generated off-card by the HSM. It is expected that HID ActivID CMS already supports off-card generation of private keys associated with encryption certificates. Per the Technical Requirements in this SOW, the private keys for authentication and signing certificates shall also be generated off-card by the HSM, which is a requirement that may require modifications and/or customizations to the HID ActivID CMS software.	
Key Activity: ♦ Assess what must be done with the HID ActivID CMS to support off-card key generation of all private keys ♦ Develop and document the enhancements to the HID ActivID CMS ♦ Virtual technical meetings, as mutually agreed upon	
Seller Deliverables: ♦ All custom source code and middleware that is developed as result of this SOW, except for code that is integrated within the HID ActivID CMS and made available via the licensed product. ♦ Configuration documentation	
Total Estimated Hours	

This phase is complete upon verification that off-card key generation for all private keys is supported during Phase 6.

Phase 5 - Training and Standard Operating Procedures (SOPs)

This phase may commence upon completion of Phase 2.
This phase may be performed concurrently with Phase 3 and all subsequent phases.

Objectives: This phase is for developing training materials and standard operating procedures (SOPs) for the various roles to administer and operate the Enterprise Credentialing Service. The SOPs should reinforce but in more friendlier and usable format than the CPS documentation that is being developed in Phase 3.	
Key Activity:	

♦ Develop training materials ♦ Develop SOPs ♦ Virtual technical meetings, as mutually agreed upon	
Seller Deliverables: ♦ Training materials and SOPs for role holders ♦ SOPs for administrators	
Total Estimated Hours	

This phase is deemed complete upon review and acceptance of all Seller Deliverables by LLNS.

Phase 6 - Deployment of Development and Integration Environments

This phase may commence upon written approval by the LLNS' Technical Representative

Objectives: Deploy the technology (software and hardware, if any) in the datacenter at SNL. Two instances will be deployed: a Development Environment and a Integration Environment. The Development Environment will be a discrete implementation to vet the solution architecture and modify, as necessary. The Integration Environment will reflect the target configuration as it would be deployed in production. The Integration Environment is expected to be a mirror of what is deployed and operational in production. In this phase, the DOE NNSA security team will assess the solution that is deployed, and security issues and concerns must be addressed or mitigated.	
Key Activity: ♦ Install, configure, and test the solution (e.g., software, hardware, configurations) in Development Environment per the solution architecture and test plan ♦ Install, configure, and test the solution (e.g., software, hardware, configurations) in Integration Environment, which will use the same physical hardware as Development Environment but on separate Hypervisors ♦ Provide consulting services as it relates to the key generation ceremonies for the non-production DOE Root Certification Authority ♦ Provide consulting services as it relates to the master key generation ceremonies for the smartcard token (i.e., Giesecke & Devrient Sm@rtCafé Expert 7.0) and the CMS. The same master key will used in Production Environment as part of Phase 7. ♦ Address/mitigate security issues identified by the DOE NNSA security team ♦ Update/revise solution architecture	
Seller Deliverables: ♦ Final solution architecture ♦ Executed test plan / results	
Total Estimated Hours	

This phase is complete when LLNS, have proof that the Enterprise Credentialing Service in the Integration Environment achieves the Technical Requirement in this SOW.

Phase 7 - Deployment in Production Environment

This phase may commence upon written approval by the LLNS' Technical Representative.

Objectives: The focus of this phase is to deploy the solution into the production datacenters in LLNL and IARC as it is deployed in the Integration Environment at SNL. In this phase, the DOE NNSA security team will assess the solution that is deployed, and security issues and concerns must be addressed or mitigated.	
Key Activity: ♦ Install, configure, and test the solution (e.g., software, hardware, configurations) in Development Environment at LLNL per the solution architecture and test plan ♦ Install, configure, and test the solution (e.g., software, hardware, configurations) in Development Environment at IARC per the solution architecture and test plan ♦ Address/mitigate security issues identified by the DOE NNSA security team ♦ Update/revise solution architecture	
Seller Deliverables: ♦ Final solution architecture ♦ Executed test plan / results	
Total Estimated Hours	

This phase is complete when LLNS, have proof that the Enterprise Credentialing Service in the Production Environment achieves the Technical Requirement in this SOW.

Phase 8 – On-going Support

This phase may commence upon written approval by the LLNS' Technical Representative.

Objectives: Provide on-going support for the deployed Enterprise Credentialing Service in the Development, Quality, and Production environments.	
Key Activity: ♦ Troubleshooting and problem resolution ♦ Assist with enhancements to improve the architecture, performance, sustainability, and usability ♦ Assess updates, hotfixes, and patches of PKI and CMS technology stacks to determine their applicability and impact to the current deployed solution and to provide technical support, as needed	
Seller Deliverables: ♦ Documentation, as needed	
Total Estimated Hours	

6 Project Schedule and Documentation

The overall project time is 15-months as shown in Table 1 below

Table 1. Project Schedule

< Recommend a Gantt chart or simple project schedule be included as follows: >

Enterprise Credentialing Service SOW	**Target Completion**	***Completion TimeLine – CY2020-2021***														
		Sept	Oct	Nov	Dec	Jan	Feb	Mar	Apr	May	June	July	Aug	Sept	Oct	Nov
Phase 1 - Initial Kick off and Project Assessment	Sep 30, 2020															
Phase 2 - Architecture and Design	Oct 30, 2020															
Phase 3 – PKI Governance Documentation	Apr 30, 2021															
Phase 4 - Off-card Key Generation Integration	Nov 30, 2020															
Phase 5 - Training and Standard Operating Procedures (SOPs)	Jan 29, 2021															
Phase 6 - Deployment of Development and Integration Environments	Jan 29, 2021															
Phase 7 - Deployment in Production Environment	Mar 31, 2021															
Phase 8 – On-going	POP															

All documentation developed in support of this SOW will be treated as Official Use Only (OUO). Information, which would classify the documents at Secret or higher, will be excluded from documentation.

7 Technical Requirements

1. At a minimum, the PKI must include:
    a. An offline DOE Root Certification Authority;
    b. An online issuing CA for issuing PKI certificates (authentication, signing and encryption) to users on smartcards;
    c. A separate online issuing CA for issuing Non-Person Entity (NPE) PKI certificates to webservers, applications and devices;
    d. An nCipher nShield connect XC HSM;
    e. A key escrow repository for storing private encryption keys and certificates; and
    f. A PKI directory service for publishing public encryption certificates and certificate revocation lists (CRLs).
2. At a minimum, the PKI service must provide the following:
    a. The solution must issue PKI certificates at various assurance levels and encoding specific x509 certificate policy identifiers (OIDs) to distinguish one certificates issuing at various policy levels. DOE/NNSA will provide policy OIDs that map to the respective policy OIDs in the CNSSI 1300.

b. CRLs must be posted to a PKI directory that can be retrievable via an http URL.
c. As encryption certificates are issued, the public key must be made available in a PKI directory for lookups by email clients and the private key shall be escrowed (and recoverable) in a key escrow server.
d. All CA signing keys shall be protected by the HSM.
e. Digital signature certificates shall be issued, at a minimum, with the SHA-256 signature algorithm.
f. RSA key length shall be, at a minimum, 2048 modulus.
g. The encryption algorithm shall be, at a minimum, AES-256.
h. A PKI certificate enrollment capability:
    i. For authorized users to request and/or renew NPE PKI certificates; and
    ii. For authorized registration authorities (RAs) or local registration authorities (LRAs) to issue and manage the NPE PKI certificates.
i. The PKI solution must send automated notifications, at configurable and varying thresholds (e.g., 90 days, 45 days, etc.) to inform PKI subscribers, other than smartcard credentials managed by the CMS, when PKI certificates are about to expire.
j. The PKI must generate and send alerts to authorized PKI administrators:
    i. Certificates issued by the PKI, other than those associated with smartcard credentials managed by the CMS, are about to expire and have not been renewed or updated.
    ii. Authorized PKI role holders (RAs, LRAs, etc.) who have not accessed the PKI solution to perform an action.

3. At a minimum, the CMS service must provide the following:
    a. The CMS shall support full life cycle management of smartcard credentials to include, but not limited to issuance, revocation, replacement, PIN Reset, and certificate update.
    b. The CMS shall support and use GlobalPlatform Secure Channel Protocol version 3.0 for provisioning and managing smartcard credentials.
    c. The CMS shall support off-card generation of private keys via the FIPS 140-2 Level 3 HSM for all PKI certificates issued on smartcard tokens, including authentication, digital signature, and encryption certificates.
        i. Only the private keys for encryption certificates shall be stored in the key escrow repository of the enterprise PKI.
    d. The CMS shall issue and manage, at a minimum, two (2) separate smartcard credentials for a single identity: 1 primary for general usage, 1 secondary for privileged/administrator usage.
    e. The CMS shall support a distributive provisioning model where the smartcard credentials are issued and managed at the respective credential subscriber's site.
    f. The CMS solution shall employ technical controls to ensure that no single person or CMS role holder or person can:
        i. Issue (or provision) a smartcard credential on behalf of a credential subscriber without the knowledge and consent of the credential subscriber;
        ii. Update a subscriber's smartcard credential with new PKI keys and certificates with the knowledge and consent of the credential subscriber;
        iii. Reset the PIN or passcode of a subscriber's smartcard credential without the knowledge and consent of the credential subscriber.
    g. The CMS solution shall provide a user portal interface that allows a subscriber to:
        i. Provision a smartcard credential that is assigned to the subscriber;
        ii. Update their smartcard credential with new PKI keys and certificates;

iii. Reset the PIN or passcode of their smartcard credential whenever it is locked or when the subscriber has forgotten the current PIN or passcode.

h. The CMS solution shall send automated notifications, at configurable and varying thresholds (e.g., 90 days, 45 days, etc.) to inform users their smartcard credential is about to expire.

i. The CMS solution shall generate and send alerts to authorized CMS administrators:
   i. Users with smartcard credentials about to expire and have not been renewed or updated;
   ii. Authorized role holders who have not accessed the CMS solution to perform an action.

j. The CMS solution shall provide an automated mechanism for credential subscribers to acknowledge receipt and rules of use upon being issued a smartcard credential via the CMS.

k. Technical and security controls shall be employed to ensure only authorized smartcards via established supply chain controls can be issued and managed by the enterprise CMS solution.

l. The CMS shall have a smartcard inventory mechanism:
   i. To ensure only smartcards procured through the approved supplied chain mechanism are issued and managed by the CMS.
   ii. To track smartcards from manufacturer via a centralized distribution process to the respective DOE/NNSA sites for credential issuance

m. The CMS solution shall provide reports and statistics associated with the life cycle of smartcards being managed.

n. The Seller shall assist with the key ceremony activities to establish custom manufacturer keys for the smartcard as part of the supply chain control processes.

4. If a Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG) is available for any component of the solution, it shall be employed.
5. The Enterprise Credentialing Service shall have automated mechanisms to support transactions and communications between the central authorities (e.g., CMS administrators, central registration authority) and the operators and roles (e.g., local registration authorities, credential activators, PIN reset operators, etc.) at the respective sites.

7.1 Performance and Availability Requirements

The Seller shall provide Professional Services to achieve the below Performance and Availability Requirement as follows:

1. Availability of service: .99997
2. Concurrent RA sessions: 30 (2 RAs at 15 sites)
3. Smartcards issued per day: 1000
4. Concurrent PIN reset sessions: 60 (4 pin reset operators at 15 sites)
5. NPE certificates issued per day: 20

8 Place of Performance

Unless otherwise authorized by the LLNS' Technical Representative, the Seller shall perform all work at its facility utilizing remote technologies and web conferencing tools.

Notwithstanding the above the majority of the work performed during Phase 6 and 7 may require in-person access to one of the three remote computing facilities in one of three (3) authorized DOE/NNSA remote computing locations: SNL in Albuquerque, New Mexico; LLNL in Livermore, California; or DOE Headquarters in Germantown, Maryland. Only DOE NNSA authorized personnel are permitted to touch

the actual computing resources in the remote computing facility; however, the Seller's project personnel are expected to be present and provide "over-the-shoulder" assistance during the performance of Phase 6 and 7. In the event of an excusable delay, the DOE NNSA may provide a virtualized "over-the-shoulder" capability to allow the Seller's project personnel to participate virtually from their own facility via web conferencing technology.

LLNS in concert with LANL will coordinate with the SNL, LLNL, and IARC on logistics and DOE NNSA personnel needed to perform (if any) installation and configuration at the respective physical datacenters.

9 Hours of Work

The Seller shall be available between the hours of 7:00 am – 4:30 pm MT, Monday – Friday, excluding government facility closures, Federal, LLNL Holidays. Exceptions to these work hours of work will be mutually agreed upon by the LLNS' Technical Representative and the Seller. Overtime work is NOT authorized. The Seller shall not be reimbursed for any stand-by time or support.

10 Travel

As authorized, domestic travel is anticipated to attend project meetings, conferences, demonstrations, and working groups, which are considered necessary for the completion of the work.

Anticipated Travel is as follows:

From	Destination	# of Trips	Duration Per Trip (Days)
City of Seller	Albuquerque, NM	2	5
City of Seller	Livermore, CA	3	5
City of Seller	Las Vegas NV	1	5

The Seller shall use only the minimum number of travelers and rental cars to accomplish the task(s) delineated herein. Travel shall be scheduled during regular business hours (e.g. 7am to 4:30 PM), whenever possible.

11 Reference Documents

(Under this section list all attachments, references, and technical exhibits that will be useful for the Seller to submit an appropriate proposal and to ensure proper performance.)

ID	Reference
CNSS Policy No. 25	CNSS Policy No. 25 "National Policy for Public Key Infrastructure in National Security Systems"
CNSS Instruction No. 1300	CNSS Instruction No. 1300 "Instruction for National Security Systems Public Key Infrastructure x.509 Certificate Policy under CNSS Policy No. 25"