Veteran Affairs (VA) – PKI Subscriber Agreement

YOU MUST READ THIS VA PKI SUBSCRIBER AGREEMENT BEFORE APPLYING FOR, ACCEPTING, OR USING A VA PUBLIC KEY CERTIFICATE. IF YOU DO NOT AGREE TO THE TERMS OF THIS SUBSCRIBER AGREEMENT, DO NOT APPLY FOR, ACCEPT, OR USE THE VA PUBLIC KEY CERTIFICATE. BY SUBMITTING AN APPLICATION FOR A VA PUBLIC KEY CERTIFICATE, YOU DEMONSTRATE YOUR KNOWLEDGE AND ACCEPTANCE OF THE TERMS OF THIS SUBSCRIBER AGREEMENT.

THIS VA PKI SUBSCRIBER AGREEMENT will become effective on the date you submit your VA Public Key Certificate application to your designated Registration Authority (RA) (the authority responsible for identifying and authenticating the identity of VA Public Key Certificate applicants). By submitting a Certificate application you are requesting that the VA Certification Authority (CA) (the authority that issues and manages VA Public Key Certificates) issue a VA Public Key Certificate to you and you are expressing your agreement to the terms of this Subscriber Agreement.

VA Agency-Wide PKI Policy is governed by the X.509 Certificate Policy for VA PKI. VA Public Key Certificate Management Procedures (i.e., issuance, use and revocation of Certificates) are described in the VA Certification Authority (CA) Certification Practice Statement (CPS).

Within the VA PKI domain, each PKI user is both a Subscriber (an entity whose name appears as the subject of a public key certificate) and a Relying Party (an entity who uses a public key certificate to authenticate a digital signature or encrypt communications to the certificate subject).

You have been authorized to receive one or more digital credentials (PKI certificates) associated with private and public key pairs. PKI certificates are being provided on portable media and you will need to transfer these certificates into approved VA storage, e.g., browser of your workstation, desktop, laptop, etc. At a minimum, these key pairs enable you to electronically identify yourself to VA systems. Additionally these key pairs enable you to digitally sign documents and messages and perform encryption/decryption functions.

IN THIS CA DOMAIN, PURSUANT TO THE VA CA CPS, **EACH PKI USER, AS SUBSCRIBERS, MUST:**

- accurately represent myself in all communications with the VA issuing authorities, to include sponsor, authorizing official, enrollment officials, and issuance officials;
- Use Certificates exclusively for authorized VA business, consistent with the X.509 Certificate Policy for VA PKI and the VA CA CPS;
- Take reasonable precautions to protect his/her private keys and key tokens (if applicable) from loss, disclosure, modification, or unauthorized use;
- Protect his/her user password, by not writing it down and not disclosing his/her password to others. If a subscriber is concerned about not remembering the password, he/she may store a written copy in secure, locked container or drawer;
- Within 8 hours notify the appropriate authority upon suspicion of loss or compromise (e.g. suspected or known unauthorized use, misplacement, etc.) of my certificate private key;
- I understand that my digital certificates may be placed on “suspension” per requirements of VA and/or Division. I understand that a suspension of the digital certificates will be for a maximum of 7 days before it becomes permanently revoked and must be re-issued.
- Within 48 hours advise the appropriate Registration Authority (RA) if any changes in my

registration information and will respond to notices from the RA concerning my digital certificates;

- Inform the RA when he/she no longer requires the Certificate, for reasons including job transfer, extended leave, resignation or termination of employment; and
- Upon the termination of my relationship with the U.S. Government or upon demand by the appropriate authority, I will surrender the digital certificates for revocation.
- Abide by the statement below:

I, _____, declare under penalty of perjury, pursuant to 28.U.S.C. section 1746, that the information provided is true and complete to the best of my knowledge.

EACH PKI USER, AS RELYING PARTIES MUST:

- restrict use and reliance on Certificates issued by the VA CA to appropriate uses for those Certificates, in accordance with the X.509 Certificate Policy for VA PKI and in accordance with the VA CA CPS;
- verify Certificates, including checking the Certificate Revocation Lists (CRLs) and Authority Revocation Lists (ARLs), taking into account any critical extensions to confirm certificate validity.); and
- Use and rely on Certificates only if a valid certificate chain is established between the Relying Party and the certificate subject.

CERTIFICATES MAY BE USED ONLY FOR PURPOSES RELATED TO VA BUSINESS AND ARE SUITABLE FOR PROVIDING CONFIDENTIALITY, AUTHENTICATION, NON-REPUDIATION AND DATA INTEGRITY FOR VA INFORMATION UP TO AND INCLUDING SENSITIVE BUT UNCLASSIFIED. CERTIFICATES ARE NOT TO BE USED FOR CLASSIFIED INFORMATION.

The VA reserves the right to refuse to issue or revoke any VA Public Key Certificate.

THIS AGREEMENT SHALL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH UNITED STATES FEDERAL LAW. VA PUBLIC KEY CERTIFICATES ARE DEEMED GOVERNMENT SUPPLIED EQUIPMENT, AND AS SUCH, ALL PKI USERS, AS SUBSCRIBERS AND/OR RELYING PARTIES, ARE BOUND BY U.S. FEDERAL LAW GOVERNING THE USE OF GOVERNMENT PROVIDED EQUIPMENT.

AS A SUBSCRIBER AND/OR RELYING PARTY, YOU AGREE TO USE THE VA PUBLIC KEY CERTIFICATE AND ANY RELATED VA PKI SERVICES ONLY IN ACCORDANCE WITH THIS SUBSCRIBER AGREEMENT, THE VA CA CPS AND THE X.509 CERTIFICATE POLICY FOR THE VA PKI.

I Agree

_____ _____

PKI Subscriber Signature Date

PKI Software Certificates Request Form

SECTION 1

First Name:

Last Name:

Email (Primary SMTP):

Affiliation (Contractor/Federal): Contractor

SECTION 2

Sponsor (e.g., First line Supervisor (VA Employee), Program Manager(PM), VA ISO/TA, or Administrative Officer(AO)/COTR responsible for contractor) Name, Signature and Date:

(Printed Name) (Signature) (Date)

SECTION 3

Subscriber's Signature and Date: I declare that under the penalty of perjury in accordance with 28.U.S.C. 1746 that the information provided is true and complete to the best of my knowledge.

(Sign in the presence of the Registrar or Notary Public) (Date)

SECTION 4
Notary * use only

Notary Public: _____
I hereby certify that on this _____ day of _____, 20__,
in the city of _____ and in the county of
_____ , _____
personally appeared before me the signer and subject of the above form, who signed or attested the same in my presence, and presented one valid government-issued form of photo ID as proof of his or her identity and a second form of ID if the valid government-issued ID does not have a serial number.
My Commission Expires In: _____
Street Address of Branch or Office: _____
Name of Organization Employing Notary:
_____

This section is not used for VA Employees!

SECTION 5
Notary Public seal here

SECTION 6

Trusted Agent/ISO/LRA/Registrar's or Notary's Name, Signature and Date: I declare under penalty of perjury, pursuant to 28 U.S.C. section 1746, that I have verified the identity of the applicant above.

(Printed Name) (Signature) (Date)

SECTION 7
Trusted Agent/ISO/LRA/Registrar's or Notary's * use only

Government Issued ID #1 (Photo Required)

Exact Name Listed on ID

Expiration Date (If Available)

Identification Type

Issuing Authority

Government Issued ID # 2

Exact Name Listed on ID

Expiration Date (If Available)

Identification Type

Issuing Authority

SECTION 8
Photocopy or paste digital Picture here
PHOTO ONLY

The information collected herein is intended for internal use only for the purpose of issuing a PKI soft certificate to the individual. The information on this form shall not be shared with any organization outside of VA. You have the right not to provide any data element, although that may prevent VA from issuing your PKI soft certificate.

You will need to be proofed by either your local Trusted Agent (VA Employees) or by a notary (non-VA Employees).

A trusted agent can be found by visiting the Information Security SharePoint Portal through the VA Intranet website.