Application for non-PIV Certificate

Employees, contractors, and affiliates of the Department of the Treasury must agree to the terms of this agreement to receive a Treasury-issued digital certificate. This applies to certificates assigned to the applicant or device certificates sponsored by the applicant. Applicants are bound to the terms of this document for the lifetime of the certificate.

Restricted Use: These certificates are the property of the United States Government. Illegal or unauthorized use of these certificates is punishable by law. ***This certificate must never be used to protect classified data***.

Sponsors: Sponsors submit applications in behalf of devices such as Web servers, Microsoft Domain Controllers, routers or other devices. Sponsors are liable for the proper use of the certificate. Sponsors provide a fully qualified host name, a group email address for the administration team, and other information about the device. The email address allows the CA to contact administrators.

Use of Approved Encryption Algorithms: Acceptable encryption algorithms in order of preference are AES-256, AES-192, AES-128 or 3DES, as specified in the NIST Federal Information Processing Standard (FIPS) Publication 140.

Accuracy of Representation: Information submitted to the CA must be complete, accurate, and truthful. Notify your Registration Authority, Local Registration Authority or Trusted Agent of changes to information contained in the certificate.

Protection of Private Keys: Subscribers must follow the directions contained in the CA's Certificate Policy and Registration Practice Statement to protect the private keys associated with the certificate.

Notification of Forgotten Password, Profile Loss, Disclosure, or Compromise: Upon actual or suspected loss, disclosure, or compromise of a private cryptographic key, unused activation codes, or a cryptographic profile's password, notify your Registration Authority, Local Registration Authority, or Trusted Agent ***immediately***.

Non-Transference of License: You may not transfer your certificate or software to any other person.

Revocation: If you no longer need a certificate, or it has been compromised, notify your Treasury Security Officer, Registration Authority, Local Registration Authority, or Trusted Agent as soon as possible requesting revocation.

Export Laws: Notify your Registration Authority, Local Registration Authority, or Trusted Agent if you have business requirements involving encryption for someone outside the United States or a foreign national within the United States.

Revocation Data: Subscribers to Treasury maintained CAs must use Certificate Revocation Lists (CRL), root certificates, and issuer certificates from Treasury repositories, i.e., pki.treas.gov (HTTP), ldap.treas.gov (LDAP), and ocsp.treas.gov (OCSP).

Your signature on the next page indicates your understanding and acceptance of the terms of this agreement by signing below. This agreement is applicable for the lifetime of the certificate.

Applicant Phone Number(s):

Applicant Work Address:

Common name:
CN is required to be a DNS SAN CN=

Email Address:
(Group Email for devices)

Additional SubjectAltName(s):
(optional)

Examples include: MS GUID (domain controllers), DNS name(s), IP address(es), and User Principal Name.

Certification Authority:

○ TOCA Production
○ TOCA Development

Certificate Type:

○ Web Server
○ Web Server with Client and Server OIDs
○ Device or Server (3-Year Certificate for Non-Web Servers Only)
○ Domain Controller
○ RA Credential

Action:

○ Create New Certificate
○ Perform Key Recovery
○ Revoke Certificate

Reason:

Special Instructions (optional): ______________________________

______________________ ______________________ ______________________
Name (Printed) Date Digital Signature (PIV)

Email the completed and digitally signed form to your Bureau RA.

(This section is to be completed by the Registration Authority)

Do not write below this line.

Identify Proofing

Date: ______________________

Applicant's Identification #1: ______________________

Applicant's name as it appears on ID#1: ______________________

Applicant's Identification #2: ______________________

Applicant's name as it appears on ID#2: ______________________

Registration Authority (RA) Name: ______________________

RA's Digital Signature (PIV): ______________________

(Identity verification: (1) PIV credential used to digitally sign this application or (2) a Federally issued credential and a State issued credential recorded by the RA)