Application for Certificate (non-PIV)

Employees, contractors, and affiliates of NASA must agree to the terms of this agreement before receiving a NASA Operational Certificate Authority (NOCA)-assigned digital certificate. This applies to certificates assigned to the applicant or device certificates sponsored by the applicant. Applicants are bound to these terms 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 Registration Authority must be complete, accurate, and truthful. Notify the Super 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 NOCA 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 Super 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.

Cessation of Operation: If you no longer need your certificate or the device certificate, notify your Security Officer, Super Registration Authority, Local Registration Authority, or Trusted Agent to request revocation.

Export Laws: Notify your Super 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 revocation repositories, root certificates, and issuer certificates from Treasury repositories, i.e., pki.treas.gov (HTTP), ldap.treas.gov (LDAP), and ocsp.treas.gov (OCSP).

By clicking the "accept" button on your certificate request, you indicate your understanding and acceptance of the terms of this agreement. This agreement is applicable for the lifetime of the certificate.