

U.S. Government Printing Office Public Key Infrastructure End User Subscriber Agreement

You have been authorized to receive one or more public key certificates and private keys. The private keys will enable you to digitally sign documents and identify yourself to gain access to systems, or to decrypt data. Other employees will use the public key to verify your signature or to encrypt data to be sent to you. Your certificates may also be used to verify your identity when you attempt to authenticate to systems. A Government Printing Office (GPO) Registration Authority (RA) or your local Trusted Agent (TA) will provide you with the necessary instructions to generate your public and private keys and download your certificates. These items are government property and may only be used for official purposes.

As an End User subscriber, I agree that my use and reliance on the GPO public key certificates is subject to the terms and conditions set out below, as well as the provisions of the GPO CP, CPS, and applicable law.

Acknowledgement of Responsibilities: I acknowledge receiving instructions and shared secrets necessary to generate my public and private keys and download my certificates and will comply with the following obligations:

- I will not disclose the instructions or shared secrets (any information created as part of the registration process) to anyone or leave them where they might be observed.
- I will keep a copy of this Subscriber Agreement in my personal records.
- I will use my certificates and private keys only for official purposes.
- I will be the sole possessor of my private keys,
- I will not back up my private keys,
- I will create or store my private keys only onto approved devices and applications.
- I will comply with the supplied guidelines for selecting a strong password,
 - At least eight characters;
 - At least one numeric character;
 - At least one uppercase character;
 - At least one lowercase character;
 - At least one special character; and
 - No repetition of the previous 12 passwords.

- I will not disclose my password or PIN to anyone or leave it where it might be observed,
- If I record the password or PIN protecting my private keys, I will protect the written password or PIN from disclosure by sealing it in an envelope and storing it in a locked cabinet or desk, and store the password or PIN separately from the token containing my private keys.
- I will take all reasonable measures to prevent the loss, disclosure, modification or unauthorized use of any issued tokens.
- I will promptly notify my local Trusted Agent or the GPO Registration Authority of any known or suspected private key, certificate, token, or password compromise.
- I will promptly notify my local Trusted Agent or the GPO Registration Authority, if information in my certificate changes (name, e-mail address, organization).
- I will promptly notify my local Trusted Agent or the GPO Registration Authority, and surrender any smartcards or tokens, if I leave the organization for which the certificate was issued.
- I acknowledge that, when the GPO issues me the information permitting me to generate a certificate, the GPO will keep a copy of my private key corresponding to the public key of my encryption certificate, and the GPO will not disclose this key except with my consent, or where required by law.
- I acknowledge that I am responsible for all use of the GPO certificates bearing my name or identification.
- I acknowledge that I may ask for my certificate to be revoked at any time.

- (For Sponsors, representing devices that have been issued tokens) I will inform my local Trusted Authority or the GPO Registration Authority if responsibility for the device that has been issued a certificate/token is changed.

Operations: The password used to secure my GPO certificates is unknown to the GPO and there is no mechanism for the GPO to find the password. In the event of a lost password, as in the event of the loss of my private key(s), the GPO can recover only the private key corresponding to the public key contained in the encryption certificate and authorize the generation of a new digital signing public/private key pair.

GPO may revoke certificate(s) at any time without notice if—

- Identifying information in the certificate becomes invalid;
- A violation of this Subscriber Agreement or the requirements set forth by the GPO Certificate Policy has occurred or is suspected; or
- The private keys have been or are suspected of having been compromised, including being lost, stolen, or destroyed in a fashion where there is potential for compromise or loss of control.

Software: Certificate holder must honor any copyright, patent and licensing agreements with respect to any software provided by the GPO, and will not tamper with, alter, destroy, modify, reverse engineer, or decompile such software in any way.

The GPO PKI software includes cryptographic software subject to export controls under the Export Administration Regulations (15 CFR chapter VII, subchapter C). Anyone receiving the software by downloads or otherwise may not export the software without a license issued by the United States Department of Commerce, Bureau of Export Administration (BXA) under laws relating to the control of certain exports, re-exports, and activities.

Downloading, installing or using the GPO supplied Software indicates that the user represents and warrants that they are not located in, under the control of, or a national or resident of any country to which the export of the Software or related information would be prohibited by the laws of the United States. At this time these countries include Afghanistan, Cuba, India, Iran, Iraq, Libya, Montenegro, North Korea, Pakistan, Serbia, Sudan and Syria.

Liability: A Subscriber or Relying Party will have no claim against the GPO arising from use of the Subscriber's certificate or a CA's determination to terminate or revoke a certificate. In no event will the GPO be liable for any losses, including direct or indirect, incidental, consequential, special, or punitive damages, arising out of or relating to any certificate issued by a GPO CA.

Terms of Agreement: This Agreement constitutes a 3-year renewable contract, which may be (i) terminated by the subscriber at any time with proper notice as set forth in the GPO Certificate Policy or (ii) terminated by the GPO at anytime without notice. If any provision of this Agreement is declared by a court to be invalid, illegal, or unenforceable, all other provisions shall remain in full force and effect. The GPO reserves the right to refuse to issue certificates. The GPO reserves the right to cancel this program at any time. GPO certificates will be used to access records and systems on a U.S. Government computer system and unauthorized use or use beyond the purpose authorized may be subject to criminal penalties under the Computer Fraud and Abuse Act 18 U.S.C. § 1030(c). The GPO Public Key Infrastructure, including the use of, or reliance on certificates issued by a GPO Certificate Authority, shall be governed by the laws of the United States of America.

Requests for issuance of certificates or revocation of certificates shall be sent to your local Trusted Agent or the GPO Registration Authority, located at:

PKI Registration Authority – IT Security Division
US Government Printing Office
732 North Capitol St. NW
Washington, DC 20401

Token Receipt:

Not Issued on Token

USB Token

Serial Number _____

Smartcard

Serial Number _____

Other

Serial Number _____

Certificate/Token Acceptance: I understand that once I obtain and use my certificates that I have accepted the responsibility of fulfilling a Trusted User role and have accepted the terms and conditions of this Subscriber Agreement and will comply with the provisions of the GPO CP, CPS, and applicable law.

Agency: _____

Name: _____

Email: _____ Telephone Number: _____

(Signature) - *Must be signed in the presence of the RA/TA* Date: _____

Witness: I have personally witnessed the Subscriber apply the signature above, and personally verified the identity of the person receiving the instructions and shared secrets for creating his/her certificate by using the identity credentials described below.

Name: _____ Date and Time: _____ @ _____

PKI Role: _____ (PA / MU / SO / RA /TA/LRA)

(Signature)

Telephone Number: _____