Instructions for Completing DD Form 2842

Department of Defense (DOD) Public Key Infrastructure (PKI) Certificate of Acceptance and Acknowledgement of Responsibilities (Subscriber)

Part 1. Certificate Acceptance by Subscriber

The following information will be completed by the Subscriber and verified by a Registration Official:

(Note: If the electronic version of this form is used, some blocks may be automatically filled. Only the remaining blocks require completion.)

Block a. Enter full name as Last Name, First Name, Middle Name.

Block b. Enter Social Security Number

Block c. Enter the identifying number provided by the Registration Official (i.e., EDIPI or UID)

Block d. Enter branch of service, major command, and duty station.

Block e. Enter 7 digit DSN telephone number or 10 digit commercial telephone number (i.e. *area code + 7 digit number*).

Block f. Enter current e-mail address

Read the Acknowledgement of Responsibilities, Liability, and Governing Law statements.

Blocks g (1) and (2) and Blocks h (1) and (2). In Block g (1) enter a descriptive name for a federal government-issued identification credential with a picture, for example *Military ID card* or *Passport*. Enter a unique identification number from that credential in Block g (2).

If a federal government identification credential with a picture is not available, two non-federal government-issued identification cards are required. At least one of the identification cards must show the Subscriber’s picture (for example, a drivers license). Enter a descriptive name for the first credential in Block g (1) and a unique identification number from that credential in Block g (2). Enter a descriptive name for the second credential in Block h (1) and a unique identification number from that credential in Block h (2).

Block i. The Subscriber must sign in this block. The signature should match the name provided in Block a. The Registration Official will indicate in this block if the Subscriber is incapable of signing**.** *(Note: For the electronic version of this form, the Subscriber’s signature will be automatically applied)*

Block j. Enter the current date in nine character form (YYYYMMMDD).

Part 2. Identity Verification by the Registration Official

The following information will be completed by the Registration Official at the time of Subscriber’s registration:

(Note: If the electronic version of this form is used, some blocks may be automatically filled. Only the remaining blocks require completion.)

Block a. Enter full name as Last Name, First Name, Middle Name.

Block b. Enter branch of service, major command, and duty station.

Block c. Enter 7 digit DSN telephone number or 10 digit commercial telephone number (i.e. *area code + 7 digit number*).

Block d. Enter current e-mail address

Block e. The Registration Official must sign in this block. The signature should match the name provided in Block a. *(Note: For the electronic version of this form, the Registration Official’s digital signature will be automatically applied)*

Block f. Enter the current date in nine character form (YYYYMMMDD).

The Registration Official will provide a copy of the form to the Subscriber.

SUBSCRIBER	**DEPARTMENT OF DEFENSE (DOD) PUBLIC KEY INFRASTRUCTURE (PKI) CERTIFICATE OF ACCEPTANCE AND ACKNOWLEDGEMENT OF RESPONSIBILITIES**

1. CERTIFICATE ACCEPTED BY

a. **NAME** *(Typed or printed) (Last, First, Middle Initial)*	b. **SSN** — —	c. **UNIQUE IDENTIFICATION** *(e.g., EDIPI, UID)*
d. **ORGANIZATION**	e. **TELEPHONE NUMBER** *(Include Area Code)*	f. **E-MAIL ADDRESS**

PRIVACY ACT STATEMENT

AUTHORITY: E.O. 9397.

PRINCIPAL PURPOSE(S): To collect social security number and other personal identifiers during the certification registration process, to ensure positive identification of the subscriber who signs this form.

ROUTINE USES: Information is used in the DOD PKI certificate registration process.

DISCLOSURE: Voluntary; however, failure to provide the information may result in denial of issuance of a token containing PKI private keys.

You have been authorized to receive one or more private and public key pairs and associated certificates. A private key enables you to digitally sign documents and messages and identify yourself to gain access to systems. You may have another private key to decrypt data such as encrypted messages. People and electronic systems inside and outside the DoD will use public keys associated with your private keys to verify your digital signature, or to verify your identity when you attempt to authenticate to systems, or to encrypt data sent to you. The certificates and private keys will be issued on a token, for example a Common Access Card (CAC), another hardware token, or a floppy disk. The certificates and private keys on your token are government property and may be used for official purposes only.

Acknowledgement of Responsibilities: I acknowledge receiving my PKI private keys and will comply with the following obligations:

- I will use my certificates and private keys only for official purposes;
- I will comply with the instructions described to me today for selecting a Personal Identification Number (PIN) or other required method for controlling access to my private keys and will not disclose same to anyone, leave it where it might be observed, nor write it on the token itself;
- I understand that if I receive key management (encryption/decryption) key pairs on my token, copies of the private decryption keys have been provided to the key recovery database in case they need to be recovered; and
- I will report any compromise (e.g., loss, suspected or known unauthorized use, misplacement, etc.) of my PIN or token to my supervisor, security officer, Certification Authority (CA), Registration Authority (RA), Local Registration Authority (LRA), Trusted Agent (TA), or Verifying Official (VO), immediately.

Liability: I will have no claim against the DoD arising from use of the Subscriber's certificates, the key recovery process, or a Certification Authority's (CA's) determination to terminate or revoke a certificate. The DoD is not 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 DoD CA.

Governing Law: DoD Public Key Certificates shall be governed by the laws of the United States of America.

g. IDENTIFICATION 1		h. IDENTIFICATION 2	
(1) TYPE *(DoD ID, Passport, etc.)*	(2) NUMBER	(1) TYPE *(DoD ID, Passport, etc.)*	(2) NUMBER

i. **SUBSCRIBER'S SIGNATURE** *(The signature provided may be a digital signature if a good fingerprint or other adequate biometric has been collected. Otherwise the subscriber must provide a handwritten signature.)*	j. **DATE SIGNED** *(YYYYMMMDD)*

2. REGISTRATION OFFICIAL PER CPS

I have personally verified the identity of the person above in accordance with the applicable CPS and have personally witnessed that person sign the form.

a. **NAME** *(Typed or printed) (Last, First, Middle Initial)*	b. **ORGANIZATION**
c. **TELEPHONE NUMBER** *(Include Area Code)*	d. **E-MAIL ADDRESS**
e. **REGISTRATION OFFICIAL'S SIGNATURE**	f. **DATE SIGNED** *(YYYYMMMDD)*

PREVIOUS EDITION IS OBSOLETE.

Reset

A copy of this form shall be provided to the Subscriber.