Instructions for Completing the AMS System Account and Certificate Request Form

Please select your requirement for the type of credential to be issued using the toggle provided at the top of the page.

SECTION 1 – Requestor Information (Requestor)

Fill in your First Name, Last Name, Email address, OPDIV (dropdown or type if not listed), HHS ID and Affiliation (dropdown) information. Additionally, if a specific AMS account name is required, please provide.

SECTION 2 – Account Details (Requestor)

This section is used to request access to specific applications with various roles, provided AMS integrates with those applications; both of these details are optional, but recommended.

Additionally, please provide the justification for the service/system account. This field is required and please provide a level of detail to fully communicate the use case and why a standard user account cannot be leveraged.

SECTION 3 – Agreement (Requestor)

PIV Holder – Please select your completion status regarding the HHS Annual IT Security Awareness training and read the attestation regarding the information provided on the form. If you agree, insert the signature of the Requestor

Left click the signature field
In the 'Sign Document' dialog, ensure the –S certificate from your PIV is selected, and click 'Sign'
Enter your PIV PIN, and save the document when prompted

If the requestor also requires a software certificate for the account then must also digitally sign page 2.

Once all information in sections 1-3 is complete, the requestor can click the "Email to Supervisor" button to generate an email with the form attached. Please be sure to add the recipient email address before sending.

SECTION 4 – ISSO Approval (Application ISSO)

The ISSO of the target system will fill out their contact information and provide a date when the AMS system account should expire (if none is provided account expiration will align to requestor PIV expiration) and will subsequently digitally sign, attesting to the requestor's need for the account and related credentials.

Once all information and a signature in section 4 is complete, the supervisor can click the "Email to PERSEC" button to generate an email with the form attached. Be sure to address to the specific OPDIV PERSEC office email if needed (HHS HSPD-12 office is currently the default email).

Section 5 – Personnel Security Approval (PERSEC)

Once the form is received, PERSEC specialists will validate the requestor has signed the Rules of Behavior, and will also confirm that an appropriate background investigation has been scheduled or completed to support an AMS system account, providing their digital PIV signature once complete.

Once all attestation and signatures are complete in section 5, the PERSEC specialist can then email to the PMO for approval. Clicking the "Email to PMO" button will generate an email with the completed form attached and pre-addressed.

Section 6 – PMO Approval (AMS PMO)

If the PMO approves of the account creation, they will digitally sign. Clicking the "Email to AMS" button will generate an email with the completed form attached and pre-addressed to the Tier III helpdesk for processing.

Section 7 - AMS Internal Use Only, do not fill out

HHS PKI Subscriber Agreement
(Only required if requesting Bot/Software Certificate)

Part A: Requestor Data

This information will auto populate provided it is input in Sections 1 and 4

1. **Legal name:** Type in Requestor's name
2. **OPDIV:** From the drop down menu select the requestor's OPDIV
3. **Organization:** Type in the Requestor's OPDIV (this field is optional)
4. **Primary Email Address:** Type in Requestor's Primary Email address
5. **Phone:** Type in Requestor's phone number
6. **Sponsor:** Type in the Requestor's Sponsor.

    - **Sponsor** – A Subscriber's supervisor, administrative officer, contracting officer, contracting officer's technical representative, program manager, etc., who authorizes the Subscriber to receive software certificates and is also responsible to validate that the subscriber is an active employee by the respective OpDiv.

7. **Phone**: Type in the sponsor's phone number.
8. **Sponsor Email Address**: Type in the sponsor's email address

Part B: Acknowledgement of Responsibilities

Read the responsibilities that are expected from a Software Certificate Requestor

Part C: Requester Signature

PIV Holder –

1. Left click the signature field
2. In the 'Sign Document' dialog, ensure the –S certificate from your PIV is selected, and click 'Sign'
3. Enter your PIV PIN, and save the document when prompted
4. Date is optional with digital signature
5. Click the 'Save and Email' button at the bottom of the form
6. You will be required to save you form to a location of your choosing
7. Your default email application will open a new message with your form attached and addressed to the PKI Helpdesk. If you are using an Outlook client, click the OPTIONS ribbon and then the digital signature icon
8. Select the 'Send' button and input your PIV PIN when prompted

AMS System Account Request Form

Credential Type: ○ **UserID/Password** ○ **Software Certificate (Bot)** ◉ **No Selection**

SECTION 1 Requetor Info

First Name:

Last Name:

Email (Primary SMTP):

Contact Number:

OPDIV: Select

HHS ID (10-digit # on back of PIV):

Affiliation (Contractor/Federal): Select

Requested AMS System Account Name (Bot Name):

SECTION 2 Account Detail

Application(s) (Optional):

Application Role(s) (Optional):

System Account Justification:

SECTION 3 Agreement

I have completed the Annual IT Security Awareness Training: ○ Yes ○ No

I accept the responsibility for the system to which I am granted access and will not exceed my authorized level of access. I understand that my access may be revoked or terminated for non-compliance with Department of Health and Human Services (HHS) security policies or with the latest AMS System Account Guideline. I accept responsibility to safeguard the information contained in this system from unauthorized or inadvertent modification, disclosure, destruction, and use. I understand and accept that my use of the system may be monitored as part of managing the system, protecting against unauthorized access and verifying security problems. I agree to notify the appropriate organization that issued my system account when access is no longer required. I agree to follow the guidance provided by the latest 'AMS System Account Guidelines

Email to ISSO

(Digital Signature)

SECTION 4 ISSO Approval

Verification:
By signing below, the Supervisor is confirming the need for an AMS System Account as well as confirming that the information presented in the User Information section of this form is accurate and complete for the individual to whom the account is issued.

Supervisor Name: **Contact Number:**

Email (Primary Government): **Acct Expiration:**

Email to PERSEC

(Digital Signature)

SECTION 5 Personnel Security Approval

Select the appropriate checkbox below to verify that the applicant has signed the application Rules of Behavior.
Note: The signature page for the application Rules of Behavior must be signed and submitted back to the Authorizing Agent along with this completed AMS System Account Request Form. ○ Yes ○ No

Confirm that favorably adjudicated fingerprints have cleared and required investigation has been initiated/ completed. Note: AMS Tier 1/2 Help Desk Roles, Role Assignment Services role, PIV Exception role and Search HHSID role require Level - 5 Public Trust and AMS Super Administrator Role requires Level - 6. ○ Yes ○ No

Email to PMO

(Digital Signature)

SECTION 6 PMO Approval

By my signature below, I approve of this AMS system account request and authorize the AMS team to provision the account.

Email to AMS

(Digital Signature)

SECTION 7 Internal Use Only

AMS System Identifier (Bot Use Only):

Additional Information (Accounts, Roles, Notes):

PKI Subscriber Agreement

You have been authorized to receive one or more digital credentials (PKI certificates) associated with private and public key pairs. If you are receiving a smart card, these PKI certificates are contained on your card. If you are not receiving a card, these PKI certificates are being provided on portable media or via web-portal and you will need to intall these certificates into approved HHS storage, e.g., your workstation, desktop, laptop, etc. At a minimum, these key pairs enable you to electronically identify yourself for systems access. Additional key pairs may enable you to digitally sign documents and messages and perform encryption/decryption functions.

Part A: Requester Data

Legal name (Last Name, First Name, Middle Initial)			
OPDIV: Select	Organization (optional):	Primary Email Address:	Phone:
Sponsor:	Phone:	Sponsor Email Address:	

Part B: Acknowledgement of Responsibilities

By my signature below, I acknowledge receiving my smart card and/or digital certificates and will comply with the following obligations:

- I will accurately represent myself in all communications with the HHS issuing authorities, to include sponsor, authorizing official, enrollment officials, and issuance officials;
- I will comply with the instructions described to me today for selecting a Personal Identification Number (PIN), password, or other required method for controlling access to my private keys and will not disclose the same to anyone, leave it where it might be observed, nor write it on the token itself;
- I will protect the contents of my PIV card at all times, by treating my PIV card as valuable personal property and keeping my PIN from disclosure as described above;
- I understand that if I receive key management (encryption/decryption) key pairs on my token, copies of the private keys have been provided to the key recovery database in case they need to be recovered; however, if I make additional copies of my certificates and private keys, I am responsible for protecting these copies and will store and protect them according to approved HHS policies and procedures;
- I will immediately notify the appropriate authority (see email address below) upon suspicion of loss or compromise (e.g. suspected or known unauthorized use, misplacement, etc.) of my PIV card, disclosure of my PIN, and/or other suspected key compromise;
- I understand that my PIV card and/or digital certificates may be placed on “suspension” per requirements of HHS and/or OPDIV. I understand that a suspension of the PIV card and/or digital certificates will be for a maximum of 7 days before it becomes permanently revoked and must be re-issued;
- I will promptly 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; and
- Upon the termination of my relationship with the U.S. Government or upon demand by the appropriate authority, I will surrender the PIV card and/or the digital certificates for revocation.

Please use the following email for all software certificate request form and other software certificate operations (e.g. revocation, renewal requests, etc.)

USHHSPKIHelpdesk@deloitte.com

Part C: Requester Signature

(Applicant Signature) _____ (Date, optional w/ digital signature) _____

Save and Email **Clear Form**