

# *Defense Manpower Data Center*

---

Personnel Security & Assurance



## **Joint Personnel Adjudication System (JPAS) PKI Frequently Asked Questions (FAQs)**

**Document Version 2.1**

**08/15/2016**



This document is current as of August 15, 2016. The following set of responses to FAQs is provided in order to answer common questions regarding the Joint Personnel Adjudication System (JPAS) PKI logon procedures.

## Table of Contents

**Section 1: General Questions .....4**

1. What are the Regulations associated with the JPAS PK-enable deployment? ..... 4

2. What should I use to log into JPAS and when will the logon methods change? ..... 4

3. Is there any written requirement to remove username/password? ..... 5

4. Why is DMDC removing username/password? ..... 5

5. What if I am using my boss, friend or co-worker’s username/password or PKI credential to log onto JPAS? ..... 5

6. How will DMDC communicate upcoming deployments, modifications, and information regarding JPAS? ..... 5

7. What is an active JPAS account? ..... 6

8. How do I get a JPAS account? ..... 6

9. Will JPAS accounts be handled different (e.g. System Access Request (SAR), unlocking of accounts, account management) now that JPAS uses a smartcards? ..... 6

10. What if I am attempting to log in using my user ID and password and can’t? ..... 6

11. How do I know I’m logged in through CAC/PIV and not my user ID and password? ..... 6

12. Is a user ID and password required prior for logging in with a non-CAC? ..... 7

13. Will I have to register my non-CAC each time I log in? ..... 7

14. If I log in with a CAC/PIV card, will I be required to change my password? ..... 7

**Section 2: Common Access Card (CAC) and Public Key (PK) Enabling Questions .....7**

15. Who qualifies for a CAC? ..... 7

16. How do I login to JPAS with my DoD approved PKI credential (CAC, PIV, or other? ..... 8

17. I have inserted my non-CAC (PIV/PIV-I/Smart card) and clicked the ‘CAC/PIV Log In’ button and now I see a Self Registration screen. What should I do on this screen? ..... 8

18. Do I need to register my CAC? ..... 9

19. What do I do if I can't login using my CAC? ..... 9

20. What if I don’t qualify for a CAC? ..... 9

21. What Identity Credentials contain DoD approved PKI certificates? ..... 9

|  |  |           |
|--|--|-----------|
| 22.  | Can I access JPAS if I have other types of DoD approved PKI certificates? .....  | 10        |
| 23.  | What important dates should I remember when it comes to PK Enabling JPAS? .....  | 10        |
| 24.  | What should a Facility Security Officer (FSO) do if their organization did not acquire DoD approved PKI certificates by the January 21, 2012 PK Enabling deadline? .....     | 10        |
| 25.  | Smaller companies may not have an extensive IT infrastructure. Whom can they call to assist with the certificates and setting up the hardware? .....                         | 11        |
| 26.  | Does Industry need PKI certificates before requesting accounts via SAR?.....   | 11        |
| 27.  | How will DMDC validate Industry users for JPAS access when the PKI/Smartcards are issued - will the account manager screen require an update to add smartcard numbers? ..... | 11        |
| 28.  | How do I get a PKI certificate if I don't qualify for a CAC or my Agency doesn't issue PIVs? .....   | 11        |
| 29.  | Are there any questions I need to ask the ECA vendor when I first call them? .....   | 12        |
| 30.  | Can USB Tokens be used on DoD Government Furnished Equipment? .....  | 12        |
| 31.  | What do I do when the ECA PKI vendor offers me a thumb drive instead of a smartcard? .....   | 12        |
| 32.  | What hardware will I need to logon to JPAS using a smartcard? .....  | 13        |
| 33.  | What hardware will I need to logon to JPAS using a USB Token? .....  | 13        |
| 34.  | What software will I need to logon to JPAS using a smartcard/USB Token? .....  | 13        |
| 35.  | If I have a CAC do I need to purchase an additional certificate? .....   | 13        |
| 36.  | What if I forgot the PIN or Password for my credential? .....  | 14        |
| <b>Section 3: Technical Questions (when attempting to log on with CAC/PIV) .....</b> |  | <b>15</b> |
| 37.  | Why do I get "Internet Explorer cannot display the webpage?" .....   | 15        |
| 38.  | Why am I not able to choose a digital certificate or why don't I see a list of certificates? ...   | 15        |
| 39.  | How do I export my digital certificate? .....  | 15        |
| 40.  | Why do I get the PKI Authentication Failure screen and what does it mean? .....  | 16        |
| 41.  | Why does the browser not prompt me for my digital certificate and/or my PIN? .....   | 16        |
| 42.  | Must I always close all of my browser windows after logging out of JPAS? .....   | 17        |
| 43.  | Must I leave my CAC/PIV card inserted into my computer while I'm logged into JPAS? .....   | 17        |
| <b>Section 4: Defining Terms for PK-Logon .....</b>                                  |  | <b>17</b> |
| 44.  | What is a CAC? .....   | 17        |
| 45.  | What is a Smartcard? .....   | 17        |
| 46.  | What is a smartcard reader? .....  | 18        |
| 47.  | What is FIPS 201? .....  | 18        |
| 48.  | What is middleware? .....  | 18        |

|   |  |           |
|---|--|-----------|
| 49.   | What is JFT-GNO? .....                                   | 18        |
| 50.   | What is PKI? .....                                       | 19        |
| 51.   | How does Public and Private Key Cryptography work? ..... | 20        |
| 52.   | What is certificate authority? .....                     | 20        |
| 53.   | What is a public key certificate? .....                  | 21        |
| 54.   | What is HSPD-12? .....                                   | 21        |
| 55.   | What is cryptographic logon? .....                       | 21        |
| 56.   | What is a web browser? .....                             | 22        |
| <b>Section 5: List of Agencies who distribute PIVs to their employees .....</b> |  | <b>22</b> |

---

## Section 1: General Questions

### 1. What are the Regulations associated with the JPAS PK-enable deployment?

- a. For DoD or other Federal Agencies: Joint Task Force-Global Networking Operations (JFT-GNO) Tasking Order 07-15, Public Key Infrastructure (PKI) implementation, Phase 2 mandates widespread DoD PKI implementation for DoD information systems (including web-servers). Public Key (PK) enabling is further supported by DoD Directive 8500.01E, Information Assurance (IA), and DoD Instruction 8520.2, Public Key Infrastructure (PKI) and Public Key (PK) Enabling.
- b. For cleared contractors: This change in procedures to logon to JPAS constitutes notice by DoD as their Cognizant Security Agency in accordance with paragraph 2-200b, National Industrial Security Program Operating Manual (NISPOM) (DoD 5220.22-M).

### 2. What should I use to log into JPAS and when will the logon methods change?

- a. Users will need three items to access JPAS as of **January 21, 2012**. These three items are:
  1. An Active JPAS account (account management policies have not changed).
  2. An Approved Active PKI Certificate on either a smartcard or USB token (both are considered hardware).
  3. Hardware and Software needed to read the PKI Certificate.
    - i. JPAS users will need a smartcard reader (hardware) and middleware (software) used to read the PKI certificate on the smartcard credential.
    - ii. USB Tokens will only require middleware to be installed to use the PKI certificate.

**3. Is there any written requirement to remove username/password?**

- a. *For DoD or Other Federal Agencies:* Joint Task Force-Global Networking Operations (JTF-GNO, now Cyber Command) Tasking Order 07-15, Public Key Infrastructure (PKI) implementation, Phase 2 mandates widespread DoD PKI implementation for DoD information systems (including web-servers). PK enabling is further supported by DoD Directive 8500.01E, Information Assurance (IA), and DoD Instruction 8520.2, Public Key Infrastructure (PKI) and Public Key (PK) Enabling.
- b. *For cleared contractors:* This change in procedures to logon to JPAS constitutes notice by DoD as their Cognizant Security Agency in accordance with paragraph 2-200b, National Industrial Security Program Operating Manual (NISPOM) (DoD 5220.22-M).

**4. Why is DMDC removing username/password?**

- a. *For DoD or Other Federal Agencies:* To be in full compliance with DoD Policy (JTF GNO Tasking Order 07-15, Public Key Infrastructure (PKI) implementation, Phase 2) and protect Personally Identifiable Information (PII) in JPAS.
- b. *For cleared contractors:* DoD as their Cognizant Security Agency has determined that this change in logon procedures shall occur in accordance with NISPOM paragraph 2-200b.

**5. What if I am using my boss, friend or co-worker's username/password or PKI credential to log onto JPAS?**

- a. It is a violation of DoD Regulations and CSA policy for cleared contractors to share a username and password or allow an individual to access another's JPAS account in any manner or form. Only the authorized account holder is permitted to access/use his/her JPAS account; combined or —company user accounts are not recognized or permitted. If you are not using your own account that you requested via submission of an authorized System Access Request (SAR) form, STOP USAGE IMMEDIATELY.

Any Account Manager, authorized or unauthorized user who violates JPAS security and account management policies will risk immediate forfeiture and TERMINATION of their JPAS account, regardless of any access requirements that may exist to support mission critical and job essential tasks. As such, when you select 'AGREE' when entering the JPAS system, you are agreeing to comply with all JPAS administration policies, to include the termination of JPAS access if usage terms are violated.

**6. How will DMDC communicate upcoming deployments, modifications, and information regarding JPAS?**

- a. Users can find information on JPAS by going to the JPAS Welcome Screen within the JPAS application in addition to the DMDC Personnel Security Assurance (PSA) JPAS web pages for alerts, notices, and user guide resources at <https://www.dmdc.osd.mil/psawebdocs>.

## **7. What is an active JPAS account?**

- a. Currently, an active JPAS account is an account that has been logged into in the past 30 days. An inactive JPAS account is an account that has not been logged into between 31 and 45 days. Your JPAS account will be deleted if you do not log into JPAS over the course of 45 days per DoD Regulations ([CYBERCOM TASKORD 13-0641](#)).
- b. If you are applying for a new account, the logon timer starts from the day the account is created in the system, NOT from the day you first register your PKI certificate. As a result if you do not register your certificate within 45 days of account creation, the account will be deleted and you will have to reapply.
- c. The 15-minute inactivity timeout rule will still apply.
- d. JPAS users using a PKI certificate (CAC, PIV, ECA PKI) may be asked to validate their PIN while they are actively using JPAS, this is not a timeout. This is used to reauthenticate the user.

## **8. How do I get a JPAS account?**

- a. Please see the [DMDC JPAS](#) web pages under Access Request to find out how to get a JPAS account. Please ensure that you have properly filled out the PSSARs in addition to having completed the mandatory trainings. To find out the Most Common PSSAR Reject Reasons, please visit the DMDC JPAS web pages.

## **9. Will JPAS accounts be handled different (e.g. Personnel Security System Access Request (PSSAR), unlocking of accounts, account management) now that JPAS uses a smartcards?**

- a. DMDC is not changing how accounts are managed at this time. DMDC is only changing login methods for JPAS accounts. Please see FAQ #2 in this document for further information. A JPAS user will still need to qualify, submit a PSSAR, complete mandatory trainings and be approved to receive a JPAS account.
- b. The process of unlocking accounts is still the same. A JPAS user will have to call the Call Center or having an Account Manager unlock the account.
- c. A user will have to remember their system generated username and password in order to self-register their non-CAC certificates.

## **10. What if I am attempting to log in using my user ID and password and can't?**

- a. As of January 21, 2012, users must use DoD approved PKI credentials to logon to JPAS. The username/password logon capability has been eliminated.

## **11. How do I know I'm logged in through CAC/PIV?**

- a. Look at the URL in the Address bar of the browser; it will begin with "https://jpasпки..." then login was not done successfully using approved PKI.

**12. Is a user ID and password required prior for logging in with a non-CAC?**

- a. Yes, you must have an active user ID and password prior to accessing JPAS as these are utilized on the self-registration page, where your JPAS account and PKI credential are correlated.
- b. You will only be required to input your User ID and password when registering a new certificate (e.g. when replacing an expired certificate)

**13. Will I have to register my non-CAC each time I log in?**

- a. No, if you have only **one** non-CAC JPAS will only present the Self Registration screen to users whose non-CAC is not already stored in JPAS.
- b. If you have more than one PKI credential for various roles, yes, you will need to register if the card is different from what was previous registered, or you have multiple non-CACs, or a combination of CAC and non-CAC.
  - 1. JPAS will store user ID association to only one certificate at a time.
  - 2. Due to a number of individuals supporting multiple contracts with multiple certificates, we have allowed a overwrite procedure that states if your certificate is not in the system then it will take you to the self-registration page. At the self-registration page, you will enter your username/password and it will then link that certificate to that username/password. This will occur every time you change or replace certificates.

**14. If I log in with a CAC/PIV card, will I be required to change my password?**

- a. No, you will not be required to change your password; however, you may be asked to re-enter your PKI PIN after a period of time. This allows the application to reauthenticate the user.

**Section 2: Common Access Card (CAC) and Public Key (PK) Enabling Questions**

**15. Who qualifies for a CAC?**

- a. Eligible populations include Active Duty service members, DoD civilian employees, and DoD contractors that are under DoD contract *and* sponsored by a DoD Service or Agency (DoD Instruction 1000.13). Not all of DoD Industry personnel are eligible for CACs. DoD Contractors may obtain CACs if their government sponsor deems it necessary and fulfill one of the three requirements:
  - 1. Be active duty, reservist, or a DOD civilian.
  - 2. The user must work on site at a military or government installation.
  - 3. User is a DoD contractor that works on GFE equipment.
- b. JPAS Industry users do not automatically qualify for a CAC. There must be a requirement for access to a Government facility or network.
- c. To find out more information:
  - 1. On the CAC, you can visit <http://www.cac.mil/>.

2. On the DoDI 1000.13, you can visit [http://www.dtic.mil/whs/directives/corres/pdf/100013\\_vol1.pdf](http://www.dtic.mil/whs/directives/corres/pdf/100013_vol1.pdf)
3. For a non-official DoD source but has good information you can also visit [http://en.wikipedia.org/wiki/Common\\_Access\\_Card](http://en.wikipedia.org/wiki/Common_Access_Card).

#### 16. How do I login to JPAS with my DoD approved PKI credential (CAC, PIV, or other)?

##### a. First Time PKI JPAS Access Procedures:

1. Obtain an active JPAS account and an active PKI Certificate on a smartcard (CAC, PIV card, ECA PKI Certificate on a smartcard/token, or other approved DoD PKI on a smartcard/token).
2. Obtain a smartcard reader, smartcard reader driver, and smartcard middleware (if necessary)

Note: Installation of smartcard readers and smartcard middleware is the responsibility of the Department/Agency/company that controls the workstation configuration.

- i. Plug in the smartcard reader to the Personal Computer (PC).
- ii. Install the smartcard reader driver on the PC.
  - a. This should either come bundled with the smartcard reader or the PKI provider should include instructions to locate the site where the driver can be obtained.
  - b. If necessary, install smartcard middleware on the PC.
3. Simply insert the smartcard into the smartcard reader and logon to JPAS by selecting “*CAC/PIV Log in*”.
4. JPAS will automatically validate the CAC using the EDI PI.
5. If you have a CAC and receive a DEERS Identifier is Missing error means that your EDI PI is not on your JPAS record. This occurs once a month on the day of your birth. For example, if you were born on the 15th of the month, every 15th your record is sent to DEERS to obtain the EDI PI.
6. If you are logging on with a Federally Issued PIV, DoD ECA certificate, or another DoD approved credential, you will be taken to a self-registration screen
  - a. This screen will ask for your username and password, input this information
  - b. Your PKI credential will now be correlated with your JPAS account

#### 17. I have inserted my non-CAC (PIV/PIV-I/Smart card) and clicked the ‘CAC/PIV Log In’ button and now I see a Self Registration screen. What should I do on this screen?

- c. JPAS will display a new Self Registration screen to allow users to associate (or register) their non-CAC to their active JPAS user ID and password. Enter your JPAS user ID and password and click the “**Register**” button, then you will be taken into your JPAS account.
- d. JPAS will display a new Self Registration screen if your non-CAC is different from what was previous registered, or you have multiple non-CACs, or a combination of CAC and non-CAC (common amongst users supporting multiple contracts). The Self

Registration screen allows users to associate their non-CAC to their active JPAS user ID and password. Enter your JPAS user ID and password and click the “**Register**” button, then you will be taken into your JPAS account. You will be prompted to re-register your non-CAC each time you switch between certificates.

#### 18. Do I need to register my CAC?

- a. No; however, if there is a data mismatch between DEERS and JPAS regarding your Name, SSN and DOB fields, you will receive an Error message and you will have to ensure your personal data is correct in both databases.

#### 19. What do I do if I can't login using my CAC?

- a. If you receive one of these errors, please follow the instructions listed below:
  1. If you receive an ‘X509 error’, please close all browser (e.g. Internet) windows even those not associated with JPAS. The incorrect login or time-out is still active in your Internet browsing history.
  2. If you receive a ‘cannot find DEERS Identifier’, you will receive this error if you have received a new CAC or are part of Industry. It takes about 30 days for the DEERS Identifier to populate JPAS. Please try back at a later time to see if you are still receiving this error. Ensure your PII (full name, SSN, is consistent between DEERS and your JPAS account.

#### 20. What if I don't qualify for a CAC?

- a. The use of other DoD approved PKI certificates (e.g. PIV cards, ECA PKI cards, or other DoD approved PKI cards) for JPAS access will be authorized.

#### 21. What Identity Credentials contain DoD approved PKI certificates?

- a. CAC Cards: The Common Access Card (CAC) is a United States Department of Defense (DoD) smart card issued as standard identification for active-duty military personnel, reserve personnel, civilian employees, other non-DoD government employees, state employees of the National Guard, and eligible contractor personnel. For more information on CAC, please visit the following web sites:
  - CAC web site at <http://www.cac.mil/>.
  - On the DoDI 1000.13, you can visit [http://www.dtic.mil/whs/directives/corres/pdf/100013\\_vol1.pdf](http://www.dtic.mil/whs/directives/corres/pdf/100013_vol1.pdf)
- b. PIV Cards: Personal Identity Verification (PIV) Card required to be issued to all US Federal employees and contractors under HSPD-12 (as well as FIPS 201<sup>1</sup>). Each Federal Agency is responsible for issuing PIV cards to qualifying employees and contractors.<sup>2</sup> Please use your internal procedures such as contacting your Security, IT

---

<sup>1</sup> FIPS 201-1 “Personal Identity Verification of Federal Employees and Contractors,” <http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.201-2.pdf>

<sup>2</sup> Homeland Security Presidential Directive-12 (HSPD-12) stipulates that personnel requiring regular access for more than 120-days to a Federally-controlled information system or facility shall be issued a PIV Card.

or Human Resource office to get additional information on determining qualifications for a PIV from your Federal Agency. Your Agency will explain the process for obtaining a PIV card as it varies from Agency to Agency.

- Section 4 of this document lists the Agencies who distribute PIVs.
- c. **ECA Credentials:** This is designed to provide contractors a venue to procure DoD approved certificates. Only PKI certificates that have completed Joint Interoperability Test Command testing and received DoD approval for use on DoD systems are authorized for JPAS access – do not assume a corporate smartcard qualifies. These need to at a Medium Token Assurance or Medium Hardware Assurance certificate level. For more information, please visit the following web site:
- DISA’s ECA PKI at <http://iase.disa.mil/pki/eca/>.
- d. **PIV-Interoperable (PIV-I) Credentials:** Non-Federally issued PKI certificates issuers that have completed Joint Interoperability Test Command testing and received DoD approval for use on DoD systems are also authorized for JPAS access. For more information, please visit the following web site:
- Complete list of DoD approved external PKI providers are available at: [http://jitc.fhu.disa.mil/projects/pki/pke\\_lab/partner\\_pki\\_testing/partner\\_pki\\_status.aspx](http://jitc.fhu.disa.mil/projects/pki/pke_lab/partner_pki_testing/partner_pki_status.aspx)  
<http://iase.disa.mil/pki-pke/interoperability/index.html>
  - See question 28 for further information regarding “other” DoD approved credential providers

## **22. Can I access JPAS if I have other types of DoD approved PKI certificates?**

- a. Yes. DMDC has authorized the use of DoD approved PKI certificates other than CACs for JPAS as long as they meet the specifications outline in these FAQs and in the “Obtaining Future JPAS Logon Methods” document. Question 28 (below) also covers the entities that offer these credentials for sale.

## **23. What important dates should I remember when it comes to PK Enabling JPAS?**

- a. Username and Password were removed on **January 21, 2012**.
- b. If you do not have DoD approved PKI certificates for logon to JPAS, you have 90 days from the date of your last logon before your account is deleted for inactivity. Please use this period to complete the purchase of your credentials.

## **24. What should a Facility Security Officer (FSO) do if their organization did not acquire DoD approved PKI certificates by the January 21, 2012 PK Enabling deadline?**

- a. If an FSO does not have a PKI certificate, the FSO can no longer access JPAS. See 24.b for information on account deletion due to inactivity.
- b. If an FSO’s account is deleted due to inactivity after not logging on within 90 days of your previous logon, you will need to go through the Special Access Request (SAR) process again.

**25. Smaller companies may not have an extensive IT infrastructure. Whom can they call to assist with the certificates and setting up the hardware?**

- a. The PKI providers have Call Centers that are able to assist various users, including those with no technical background. The PKI provider's Call Centers are able to answer all questions and walk their customers through their processes.
- b. The JPAS Call Center does NOT answer questions regarding the PK-Enabling Initiative
- c. There is a Troubleshooting Guide on the DMDC JPAS web pages.
- d. [https://www.dmdc.osd.mil/psawebdocs/docRequest//filePathNm=PSA/appId=560/app\\_key\\_id=1559jsow24d/siteId=7/ediPnId=0/userId=public/fileNm=PKI+Technical+Troubleshooting+Guide+Master.pdf](https://www.dmdc.osd.mil/psawebdocs/docRequest//filePathNm=PSA/appId=560/app_key_id=1559jsow24d/siteId=7/ediPnId=0/userId=public/fileNm=PKI+Technical+Troubleshooting+Guide+Master.pdf)

**26. Does Industry need PKI certificates before requesting accounts via SAR?**

- a. A potential JPAS user does not need an active PKI certificate on a smartcard or token prior to submitting a SAR to obtain a JPAS account. As of January 21, 2012, a potential JPAS user will need both an active JPAS account in addition to an active PKI certificate to logon to the application. In the near future, potential JPAS users will need Certificate of JPAS Training prior to obtaining a JPAS account.

**27. How will DMDC validate Industry users for JPAS access when the PKI/Smartcards are issued - will the account manager screen require an update to add smartcard numbers?**

- a. The Account Manager will not be required to update or add smartcard numbers to their JPAS user's account. Each user will be required to register their own certificate with their valid JPAS username/password the first time they logon. This will link the certificate on the smartcard to their active JPAS account.

**28. How do I get a PKI certificate if I don't qualify for a CAC or my Agency doesn't issue PIVs?**

- a. If you do not qualify for either a CAC or PIV, coordinate with your company to obtain a FIPS 140-2 compliant **Medium Token Assurance Certificate on a smartcard or USB Token** or a **Medium Hardware Assurance Certificate on a smartcard** from one of the three DoD ECA currently approved vendors listed below or go to <http://iase.disa.mil/pki/eca/> for more information.

IdenTrust, Inc.

Web Site: <http://www.identrust.com/jpas/index.html> (*JPAS Specific*) or

<http://www.identrust.com/certificates/eca/index.html>

Email: [ECAsales@IdenTrust.com](mailto:ECAsales@IdenTrust.com)

Phone: (866) 299-3335

Operational Research Consultants, Inc. (also provides NFI services)

Web Site: <http://www.eca.orc.com/>

Email: [ecahelp@orc.com](mailto:ecahelp@orc.com)

Phone: (800) 816-5548

- b. Alternately, multiple Non-Federal Issuers (NFI) have been approved for PKI/cryptographic usage within DoD they include all of the Category II listed providers at the following website: <http://iase.disa.mil/pki-pke/interoperability/index.html>

Entrust Managed Services NFI

Website: <https://www.entrust.com/products/cloud/pki/>

POC: (888) 690-2424

Exostar, LLC

Website: [www.exostar.com](http://www.exostar.com)

POC: [stacey.leggat@exostar.com](mailto:stacey.leggat@exostar.com) (703) 793-7719

SureID, Inc. (formerly Eid Passport, Inc.)

Website: [www.sureid.com](http://www.sureid.com)

POC: [fedgov@sureid.com](mailto:fedgov@sureid.com) (503) 924-5300

Verizon Business NFI

Website: <http://www.verizonenterprise.com/products/security/>

POC: (877) 297-7816

### **29. Are there any questions I need to ask the ECA vendor when I first call them?**

- a. Be sure to ask "Do you provide the PKI Medium Token or Medium Hardware certificates on FIPS 140 compliant devices?"
- b. "What are the timelines associated with your credential issuance?"
- c. "What is your PIN/Password reset policy?"

### **30. Can USB Tokens be used on DoD Government Furnished Equipment?**

- a. Yes, FIPS 140-2 USB tokens can be used on DoD Government Furnished Equipment. While there is a DoD Policy prohibiting USB Memory Drives, it does not prohibit using the USB interface to connect a smartcard reader or a FIPS 140-2 validated USB token.

### **31. What do I do when the PKI vendor offers me a thumb drive instead of a smartcard?**

- a. The PKI certificate needs to be generated directly on the FIPS 140 compliant device. FIPS 140 compliant Medium Token Assurance USB Tokens are acceptable. Please contact your IT department to ensure all internal policies and procedures of your organization will be followed prior to purchasing any PKI related equipment.

### 32. What hardware will I need to logon to JPAS using a smartcard?

- a. [A Computer](#) – Each JPAS user will be required to have a Pentium computer, 133 MHz (minimum), 128 MB RAM and a Web browser with 128-bit security encryption, and a Public Key Infrastructure (PKI) certificate/token (currently, 128 bit SSL is used until PKI becomes available). This is an existing JPAS requirement and this requirement has not changed.
- b. [A SmartCard Reader](#) – GSA HSPD-12 Approved Products List is the source for identifying which smartcard readers are authorized for use with the approved PKIs.
- c. Please refer to the FIPS 201 Approved Products List for smartcard readers, referred to as "Transparent Readers," located at: <http://www.idmanagement.gov/approved-products-list>. Simply click drop down on the top row to display the list.

### 33. What hardware will I need to logon to JPAS using a USB Token?

- a. Additional hardware will not be required as long as the computer has a USB interface that is available. Additional middleware will be required.

### 34. What software will I need to logon to JPAS using a smartcard/USB Token?

- a. [Step One](#): Please see your company or agency's IT staff to ensure your Department/Agency/company has existing smartcard middleware. Many Department/Agency/company already have existing smartcard middleware within their infrastructure. If your Department/Agency/company's IT staff confirms that the Department/Agency/company does not have existing smartcard middleware, then please go to Step Two.
- b. [Step Two](#): Your Department/Agency/company does not have existing smartcard middleware so your Department/Agency/company will need to obtain it. [GSA HSPD-12 Approved Products List](#) is the source for identifying which smartcard middleware is authorized for use with the approved PKIs. There are over a dozen authorized PIV Middleware, ranging from DoD's widely used ActivClient to Gemalto's SafesITe FIPS201 Client API. Many approved PKI vendors have the option of bundle deals to include the necessary hardware and software.

Please refer to the FIPS 201 Approved Products List for the smartcard middleware, referred to as 'PIV Middleware' located at: <http://www.idmanagement.gov/approved-products-list>. Simply click Category on the top row to alphabetically sort the list of products. Then scroll down to the list of "PIV Middleware" for the complete listing.

The PKI providers may direct/provide their consumers to specific smartcard readers and/or middleware that work best with their product.

### 35. If I have a CAC do I need to purchase an additional certificate?

- a. DMDC and the Common Access Card (CAC) Policy Office have listened to the concerns and have taken into consideration the request that anyone issued a CAC can use it to logon to JPAS. The CAC serves as verification of identity for an individual; however,

you must still have an active JPAS account to logon to the application. A CAC with ANY affiliation (Military, Civilian, Contractor) can be used to logon to JPAS independent of affiliation. Anyone that has been issued a valid CAC may use it to logon to JPAS.

- b. JPAS will allow users to utilize CAC and multiple PKI certificates as an authentication mechanism. A CAC utilizes the Electronic Data Interface Personnel Identifier (EDIPI) to correlate access to a JPAS account. The PKI certificate utilizes a separate parsed Object Identifier (OID) which is linked to an individual JPAS user's account. If a user has multiple PKI certificates, they will have to self-register their certificate each time they switch certificates. If a user uses a CAC and a PKI certificate, then both could be used to access JPAS. The validation process is different in order to capture how the user is logging in - CAC vs PKI certificate
- c. If you have not been issued a CAC for your job functions, you will need to acquire a PKI certificate. See question #16 for clarification of who qualifies for a CAC.
- d. Examples common across industry: Multiple use cases have been developed for several scenarios regarding the CAC and its intended purpose when it comes to JPAS access, they are as follows.
  - i. A contractor has received a CAC for the expressed purpose of base access on contract XYZ, the same contractor is also a Facility Security Officer (FSO) for his/her company. That contractor **may** use their CAC from contract XYZ to facilitate access to JPAS in fulfillment of their duties as an industry FSO.
  - ii. Similar to the example in (i) a Reservist or National Guardsman is a CAC holder and they also work as a Facility Security Officer (FSO) for their full time employment with an industry company. They are authorized to use their Reservist/NG CAC for their responsibilities as an industry FSO even if they do not use the Reservist/NG CAC for JPAS access in their Reservist role.
  - iii. An individual is a specific JPAS consultant hired by several companies to act as an FSO for their various employees. This JPAS consultant has a CAC for one of its contracts for base access only. The consultant may use the CAC for their role as an FSO for each of the various companies.

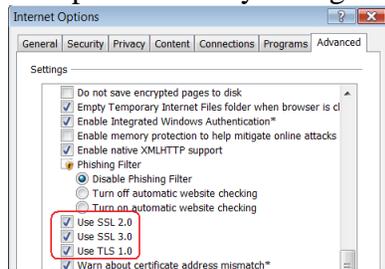
### 36. What if I forgot the PIN or Password for my credential?

- a) This depends on the specific type of credential you are dealing with:
  - a. For a DoD CAC, you have 3 attempts to enter a correct PIN, if you fail the 3<sup>rd</sup> attempt your credential will be locked; in order to unlock you will need to visit a DEERS/RAPIDS station to unlock and subsequently use
  - b. For a Federal PIV, a similar procedure will be necessary as with the CAC
  - c. For ECA and other DoD approved PKI credentials this process can vary from issuer to issuer.
    - i. Note: some issuers do not conduct a PIN/Password reset and will require the purchase of a separate credential, please be forewarned and ask the what the vendor's SOP is prior to purchase
    - ii. The JPAS team is currently in the process of coordinating to ascertain their procedures and educate JPAS users

## Section 3: Technical Questions (when attempting to log on with CAC/PIV)

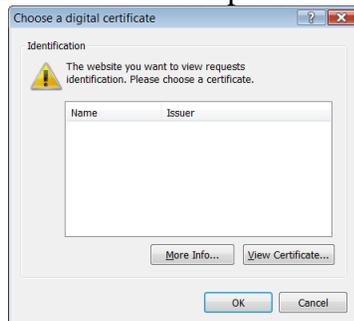
### 37. Why do I get “Internet Explorer cannot display the webpage?”

- a. Because this is an HTTPS (secure) address, be sure SSL and TLS protocols are enabled. Go to the browser’s Menu bar and click **Tools > Internet Options > Advanced** tab, and check under the security section as shown below.
- b. It is also possible that you might have a cross certificate error



### 38. Why am I not able to choose a digital certificate or why don't I see a list of certificates?

- a. This means that the Certificate Authority (CA) for the user digital certificate in question has not been installed or is no longer considered valid by DMDC. Export (Install) your digital certificate to resolve. If this does not work, contact the JPAS Help Desk.
- b. Also ensure that your middleware is installed properly and your hardware is connected to the computer



### 39. How do I export my digital certificate?

- a. For Internet Explorer complete the following steps to export a certificate:
  1. Open Internet Explorer.
  2. From the Menu bar, select **Tools > Internet Options**.
  3. The Internet Options dialog box appears.
    - i. Click the **Content** tab.
    - ii. Click the **Certificates** button.
      - a. The Certificates dialog box appears.

1. Ensure the **Personal** tab is selected (this should be the default tab). The tab lists your certificates and lets you choose a certificate for export.
  - i. Select the certificate to export.
  - ii. Click the **Export** button.
  - iii. The Certificate Export Wizard appears.
  - iv. Select the “**No, do not export the private key**” button.
  - v. Select the “Base-64 encoded X.509 (.CER).”
  - vi. In the File name field, enter the path and filename to which you want to export the certificate.
2. After completing the wizard, locate the exported file and append **.txt** (i.e.: mycertificate.cer.txt) to the end of the filename. Changing the file extension to txt allows you to e-mail the certificate without it being blocked by most e-mail applications.

#### 40. Why do I get the PKI Authentication Failure screen and what does it mean?

- a. This may happen for several reasons, but the most common is that revocation checking has determined your digital certificate to be invalid. If this continues to happen, contact the issuer of the CAC/PIV card to determine whether it has been revoked. If it has not, try again later, or contact the JPAS Help Desk.
- b. This could also mean that the DMDC OCSP is not configured properly with your providers’ Credential Revocation List (CRL) distribution point, please export your certificate given the instructions above and attach to the following email:  
[dmdc.contactcenter@mail.mil](mailto:dmdc.contactcenter@mail.mil)

#### 41. Why does the browser not prompt me for my digital certificate and/or my PIN?

- a. There are several possible reasons:
  1. Operating System  
Logging in to a computer with a CAC/PIV card, enables what is called “single-sign on.” Thus allowing the operating system to cache the PKI information and forward it to applications when required. For this type of configuration, it is recommended to never leave CAC/PIV cards inserted when you are physically not present at the computer.
  2. Browser Cache  
A user is not fully logged out of JPAS until all browser windows have been closed. Simply closing browser tabs or currently active browser windows is not secure enough. Leaving a browser tab or window open allows the browser to recall a previously used digital certificate and PIN from its cache. Browser cache is stored memory and is not fully erased until all browsers have been closed. Failing to close all browser windows after logging out of JPAS would allow someone else the chance to log in with your credentials.

3. Your trusted root certification authority does not match any provided in the JPAS Approved Certification Authorities (ACA, “hint list”), could be a cross certificate error

**42. Must I always close all of my browser windows after logging out of JPAS?**

- a. Yes, please always close your browser once you have logged out of JPAS.

**43. Must I leave my CAC/PIV card inserted into my computer while I’m logged into JPAS?**

- a. The CAC/PIV card is only needed for authentication purposes, to prove you are who you say you are, and during random reauthentications during your session.
- b. However, once you have successfully logged in to JPAS with a CAC/PIV card it is recommended that you do not remove your card. Removing the CAC/PIV card may cause your computer to become automatically locked by the operating system.

## **Section 4: Defining Terms for PK-Logon**

**44. What is a CAC?**

- a. The Common Access Card (CAC) is a United States Department of Defense (DoD) smart card issued as standard identification for active-duty military personnel, reserve personnel, civilian employees, other non-DoD government employees, state employees of the National Guard, and eligible contractor personnel.

The CAC is used as a general identification card as well as for authentication to enable access to DoD computers, networks, and certain DoD facilities. It also serves as an identification card under the Geneva Conventions. The CAC enables encrypting and cryptographically signing email, facilitating the use of PKI authentication tools, and establishes an authoritative process for the use of identity credentials.

**45. What is a Smartcard?**

- a. A smartcard, chip card, or integrated circuit card (ICC), is any pocket-sized card with embedded integrated circuits. There are two broad categories of ICCs. Memory cards contain only non-volatile memory storage components, and perhaps dedicated security logic. Microprocessor cards contain volatile memory and microprocessor components. The card is made of plastic, generally polyvinyl chloride, but sometimes acrylonitrile butadiene styrene or polycarbonate. Smartcards may also provide strong security authentication for single sign-on (SSO) within large organizations.
- b. Though not an official DoD source, for more information you can also visit <http://en.wikipedia.org/wiki/Smartcard>.

#### 46. What is a smartcard reader?

- a. A card reader is a data input device that reads data from a card-shaped storage medium. Historically, paper or cardboard punched cards were used throughout the first several decades of the computer industry to store information and write programs for computer system, and these were read by punched card readers. More modern card readers are electronic devices that use plastic cards imprinted with barcodes, magnetic strips, computer chips or other storage medium.
- b. Though not an official DoD source, for more information you can also visit [http://en.wikipedia.org/wiki/Card\\_reader](http://en.wikipedia.org/wiki/Card_reader).

#### 47. What is FIPS 201?

- a. FIPS 201 (Federal Information Processing Standards Publication 201) is a United States federal government standard that specifies Personal Identity Verification (PIV) requirements for Federal employees and contractors. In response to HSPD-12, the NIST Computer Security Division initiated a new program for improving the identification and authentication of Federal employees and contractors for access to Federal facilities and information systems. FIPS 201 was developed to satisfy the technical requirements of HSPD 12 approved by the Secretary of Commerce, and issued on February 25, 2005. FIPS 201 together with NIST SP 800-78 (Cryptographic Algorithms and Key Sizes for PIV) are required for U.S. Federal Agencies but do not apply to US national security systems. The SmartCard Interagency Advisory Board has indicated that to comply with FIPS 201 PIV II US government agencies should use smart card technology.
- b. Though not an official DoD source, for more information you can also visit [http://en.wikipedia.org/wiki/FIPS\\_201](http://en.wikipedia.org/wiki/FIPS_201).

#### 48. What is middleware?

- a. Software that provides a link between separate software applications. Middleware is sometimes called plumbing because it connects two applications and passes data between them. Middleware allows data contained in one database to be accessed through another. This definition would fit enterprise application integration and data integration software. ObjectWeb defines middleware as: "The software layer that lies between the operating system and applications on each side of a distributed computing system in a network.
- b. Though not an official DoD source, for more information you can also visit <http://en.wikipedia.org/wiki/Middleware>.

#### 49. What is JFT-GNO?

- a. Joint Task Force-Global Network Operations (JTF-GNO) was a subordinate command of United States Strategic Command whose mission is to: direct the operation and defense of the Global Information Grid (GIG) across strategic, operational, and tactical boundaries in support of the US Department of Defense's full spectrum of war fighting, intelligence, and business operations.
- b. Its primary responsibilities are:

1. Identifying and resolving computer security anomalies that affect the GIG's ability to support Secretary of Defense (SECDEF) elements, Joint Staff, Supported Combatant Commands and the "warfighter".
  2. Identifying significant threats to the GIG. Developing, disseminating and implementing countermeasures to these threats in a timely manner via Information Assurance Vulnerability Messages (IAVM).
  3. Assessing the incidents reported by Combatant Command, service, and agency (CC/S/A) computer network defense (CND) and Regions individually and cumulatively for their impact on the "warfighter's" ability to carry out current and future missions.
  4. Coordinating the response actions taken by the CC/S/A CND service providers (CNDSP).
  5. Identifying emerging technologies and their associated threats in order to integrate migrations and response actions into current CND posture.
- c. Though not an official DoD source, for more information you can also visit [http://en.wikipedia.org/wiki/Joint\\_Task\\_Force-Global\\_Network\\_Operations](http://en.wikipedia.org/wiki/Joint_Task_Force-Global_Network_Operations).

## 50. What is PKI?

- a. Public Key Infrastructure (PKI) is a set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates. In cryptography, a PKI is an arrangement that binds public keys with respective user identities by means of a certificate authority (CA). The user identity must be unique within each CA domain. The binding is established through the registration and issuance process, which, depending on the level of assurance the binding has, may be carried out by software at a CA, or under human supervision. The PKI role that assures this binding is called the Registration Authority (RA). For each user, the user identity, the public key, their binding, validity conditions and other attributes are made unforgeable in public key certificates issued by the CA. The term trusted third party (TTP) may also be used for certificate authority (CA). The term PKI is sometimes erroneously used to denote public key algorithms, which do not require the use of a CA.
- b. Though not an official DoD source, for more information you can also visit [http://en.wikipedia.org/wiki/Public\\_key\\_infrastructure](http://en.wikipedia.org/wiki/Public_key_infrastructure)
- c. Another explanation of PKI (public key infrastructure) states that it enables users of a basically unsecure public network such as the Internet to securely and privately exchange data and money through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority. The public key infrastructure provides for a digital certificate that can identify an individual or an organization and directory services that can store and, when necessary, revoke the certificates. Although the components of a PKI are generally understood, a number of different vendor approaches and services are emerging. Meanwhile, an Internet standard for PKI is being worked on.
- d. The public key infrastructure assumes the use of public key cryptography, which is the most common method on the Internet for authenticating a message sender or encrypting a message. Traditional cryptography has usually involved the creation and sharing of a secret key for the encryption and decryption of messages. This secret or

private key system has the significant flaw that if the key is discovered or intercepted by someone else, messages can easily be decrypted. For this reason, public key cryptography and the public key infrastructure is the preferred approach on the Internet. (The private key system is sometimes known as symmetric cryptography and the public key system as asymmetric cryptography.)

- e. A public key infrastructure consists of:
  1. A certificate authority (CA) that issues and verifies digital certificate. A certificate includes the public key or information about the public key.
  2. A registration authority (RA) that acts as the verifier for the certificate authority before a digital certificate is issued to a requestor.
  3. One or more directories where the certificates (with their public keys) are held.
  4. A certificate management system.

### 51. How does Public and Private Key Cryptography work?

- a. In public key cryptography, a public and private key are created simultaneously using the same algorithm (a popular one is known as RSA) by a certificate authority (CA). The private key is given only to the requesting party and the public key is made publicly available (as part of a digital certificate) in a directory that all parties can access. The private key is never shared with anyone or sent across the Internet. You use the private key to decrypt text that has been encrypted with your public key by someone else (who can find out what your public key is from a public directory). Thus, if I send you a message, I can find out your public key (but not your private key) from a central administrator and encrypt a message to you using your public key. When you receive it, you decrypt it with your private key. In addition to encrypting messages (which ensures privacy), you can authenticate yourself to me (so I know that it is really you who sent the message) by using your private key to encrypt a digital certificate. When I receive it, I can use your public key to decrypt it. Here's a table that restates it:

| To do this   | Use whose          | Kind of key |
|--|--------------------|-------------|
| Send an encrypted message                                    | Use the receiver's | Public key  |
| Send an encrypted signature                                  | Use the sender's   | Private key |
| Decrypt an encrypted message                                 | Use the receiver's | Private key |
| Decrypt an encrypted signature (and authenticate the sender) | Use the sender's   | Public key  |

### 52. What is certificate authority?

- a. In cryptography, a certificate authority or certification authority (CA) is an entity that issues digital certificates. The digital certificate certifies the ownership of a public key by the named subject of the certificate. This allows others (relying parties) to rely

upon signatures or assertions made by the private key that corresponds to the public key that is certified. In this model of trust relationships, a CA is a trusted third party that is trusted by both the subject (owner) of the certificate and the party relying upon the certificate. CAs are characteristic of many public key infrastructure (PKI) schemes.

- b. Though not an official DoD source, for more information you can also visit [http://en.wikipedia.org/wiki/Certificate\\_authority](http://en.wikipedia.org/wiki/Certificate_authority).

### 53. What is a public key certificate?

- a. In cryptography, a public key certificate (also known as a digital certificate or identity certificate) is an electronic document which uses a digital signature to bind a public key with an identity — information such as the name of a person or an organization, their address, and so forth. The certificate can be used to verify that a public key belongs to an individual. In a typical public key infrastructure (PKI) scheme, the signature will be of a certificate authority (CA). In a web of trust scheme, the signature is of either the user (a self-signed certificate) or other users ("endorsements"). In either case, the signatures on a certificate are attestations by the certificate signer that the identity information and the public key belong together. For provable security this reliance on something external to the system has the consequence that any public key certification scheme has to rely on some special setup assumption, such as the existence of a certificate authority.
- b. Though not an official DoD source, for more information you can also visit [http://en.wikipedia.org/wiki/Public\\_key\\_infrastructure](http://en.wikipedia.org/wiki/Public_key_infrastructure).

### 54. What is HSPD-12?

- a. There are wide variations in the quality and security of identification used to gain access to secure facilities where there is potential for terrorist attacks. In order to eliminate these variations, U.S. policy is to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy by establishing a mandatory, Government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors (including contractor employees). This directive mandates a federal standard for secure and reliable forms of identification.
- b. Though not an official DoD source, for more information you can also visit [http://www.dhs.gov/xabout/laws/gc\\_1217616624097.shtm#0](http://www.dhs.gov/xabout/laws/gc_1217616624097.shtm#0).

### 55. What is cryptographic logon?

- a. Until modern times cryptography referred almost exclusively to encryption, which is the process of converting ordinary information (called plaintext) into unintelligible gibberish (called ciphertext).[2] Decryption is the reverse, in other words, moving from the unintelligible ciphertext back to plaintext. A cipher (or cypher) is a pair of algorithms that create the encryption and the reversing decryption. The detailed operation of a cipher is controlled both by the algorithm and in each instance by a key. This is a secret parameter (ideally known only to the communicants) for a

- specific message exchange context. A "cryptosystem" is the ordered list of elements of finite possible plaintexts, finite possible ciphertexts, finite possible keys, and the encryption and decryption algorithms which correspond to each key. Keys are important, as ciphers without variable keys can be trivially broken with only the knowledge of the cipher used and are therefore useless (or even counter-productive) for most purposes. Historically, ciphers were often used directly for encryption or decryption without additional procedures such as authentication or integrity checks.
- b. Though not an official DoD source, for more information you can also visit <http://en.wikipedia.org/wiki/Cryptography>.

#### **56. What is a web browser?**

- a. A web browser is a software application for retrieving, presenting, and traversing information resources on the World Wide Web. An information resource is identified by a Uniform Resource Identifier (URI) and may be a web page, image, video, or other piece of content.[1] Hyperlinks present in resources enable users to easily navigate their browsers to related resources. Although browsers are primarily intended to access the World Wide Web, they can also be used to access information provided by web servers in private networks or files in file systems. The major web browsers are Windows Internet Explorer, Mozilla Firefox, Apple Safari, Google Chrome, and Opera.

### **Section 5: List of Agencies who distribute PIVs to their employees**

Department of State:

<http://www.state.gov/documents/organization/121534.pdf>

Department of Treasury:

<http://www.treasury.gov/about/role-of-treasury/orders-directives/Pages/td71-12.aspx>

Department of Housing and Urban Development:

<http://www.hud.gov/offices/adm/hudclips/forms/files/pivform.pdf>

Department of Veterans Affairs:

<http://www.va.gov/pivproject/>

Department of Labor:

<http://www.dol.gov/oasam/doljobs/DOL-PIV-Card-Policy.htm>

Department of Interior:

[www.doi.gov/hspd12/docs/PIV\\_Guide\\_v1\\_final.doc](http://www.doi.gov/hspd12/docs/PIV_Guide_v1_final.doc)

Department of Commerce:

<http://www.osec.doc.gov/osy/hspd-12/applicants.html>

Department of Energy:

<http://www.hss.energy.gov/HSPD12/guidance/n2064.pdf>

Department of Agriculture:

<http://hspd12.usda.gov/index.html>

General Services Administration:

<http://www.gsa.gov/portal/content/103401>

Farm Credit Administration:

[http://www.fca.gov/home/policies\\_notices/personal\\_identity.html](http://www.fca.gov/home/policies_notices/personal_identity.html)

Farm Credit System Insurance Corporation:

<http://fcsic.gov/FCSIC%20PIVC.html>

Federal Communications Commission:

<http://www.fcc.gov/hspd-12/>

Health and Human Services

<http://www.hhs.gov/ocio/securityprivacy/pglandreports/hspdreport.html>

Institute of Museum and Library Services:

<http://www.ims.gov/about/hspd12.shtm>

NASA:

<http://itcd.hq.nasa.gov/PIV.html>

USAccess via GSA:

<http://www.fedidcard.gov/>

**This is the list of agencies where the PIV is currently not being distributed:**

Department of Justice: Each bureau has its own process

Department of Homeland Security: Each bureau has its own process

Department of Transportation

Department of Education

Federal Energy Regulatory Commission

Federal Housing Finance Administration

Federal Labor Relations Authority

Federal Maritime Commission

Federal Reserve Board

International Boundary and Water Commission JMF

National Archives

National Endowment for the Arts

National Transportation Safety Board

National Mediation Board

US Official of Special Counsel

Securities and Exchange Commission Version