

Obtaining Future JPAS Logon Methods

PK-Enabling JPAS

Defense Manpower Data Center (DMDC)

Version 1.0

06/03/2011

This issue paper provides information for the Joint Personnel Adjudication System (JPAS) users on obtaining Public Key Infrastructure (PKI) certificates for future JPAS logon. All JPAS users will be required to obtain a Department of Defense (DoD) approved PKI certificate by January 2012.

This is a living document and will be updated as needed. Please see the Frequently Asked Questions (FAQ) in Attachment E for definition or explanation of technical terms.

Coordination of Document

This document was coordinated with and reviewed by members of the following organizations: Office of the Under Secretary of Defense for Intelligence (OUSDI) Security Directorate, Defense Security Service (DSS), Defense Human Resource Activity (DHRA) Common Access Card (CAC) Policy Office, Department of Defense Chief Information Office (DoD CIO), External Certificate Authority Public Key Infrastructure (ECA PKI) vendors, Industry Representatives, and Defense Manpower Data Center (DMDC).

Version Tracking

DATE	VERSION #	DESCRIPTION OF CHANGES
6/3/2011	1.0 (Released)	First Published Version After Coordination

1: Background

The Joint Personnel Adjudication System (JPAS) logon procedures are being updated to provide additional security and privacy protection of clearance data and personally identifiable information (PII). These changes are pursuant to Department of Defense (DoD) regulations mandating improved security by restricting access to only users with cryptographic logon. The change to logon procedures will occur by January 2012.

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.”

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: Important Dates to Remember

Phase 1 – Common Access Card (CAC)-enabled JPAS deployed on **January 15, 2011.**

Phase 2 – PK-enabled JPAS will be deployed in **July 2011.**

Phase 3 – Username and password will be removed in **January 2012.**

3: Implementation Plan

Users will need three items to access JPAS by January 2012. These three items are:

1. An active JPAS account;
2. An approved active PKI Certificate; and,
3. Hardware and Software needed to read the PKI certificate (See Attachment B – “Potential Hardware and Software”).

While DMDC is able to provide general guidance on the JPAS logon methods to both Government and cleared industry JPAS users, each Department/Agency/company likely has different policies, procedures, hardware, and software. If the JPAS user does not already have an existing active PKI Certificate on a smartcard, the user will have to go through its organization’s internal procedures. These procedures include contacting the Security, IT or Human Resource office within the users’

Department/Agency/company to obtain the hardware and software necessary to log into JPAS before January 2012. This will take time and is not an “overnight” process. On average, this process may take approximately 4 weeks.

In addition to an active JPAS account, there will be four PKI methods authorized for continued access:

1. The DoD CAC;
2. Other Federal Agency’s Personal Identity Verification (PIV) cards;

3. Medium Token Assurance or Medium Hardware Assurance PKI certificate on a smartcard issued via the External Certification Authority (ECA) PKI Program; or,
4. Other DoD approved PKI certificates that are cross-certified with the Federal Bridge Certification Authority at medium-token or higher which are on a smartcard.

Software certificates residing on or in a workstation file, CD, fob, or thumb drives are not acceptable. Only approved hardware certificates (e.g., smartcards) will be accepted.

If you do not qualify for a CAC or PIV, you will most likely need to pursue the third PKI option: Medium Token Assurance or Medium Hardware Assurance Certificate on a smartcard via the ECA PKI Program. This is the option that many cleared companies in the National Industrial Security Program will plan for and procure. Please coordinate internally to see which method is right for Department/Agency/company.

In July 2011, DMDC will be deploying the Phase 2 logon procedures for JPAS. This will allow users to use other Federal Agency's PIV cards, PKI certificate on a smartcards issued by ECA, other DoD approved PKI certificates on smartcards, or a username/password to logon to JPAS. During the months of June and July, DMDC will be conducting a test pilot with a select number of cleared companies. These companies have already been identified. A test pilot will include testing the use of an approved DoD PK certificate on a smartcard to log into JPAS. DMDC will also continue working to ensure technical issues are resolved prior to terminating the username /password capability currently scheduled in January 2012.

It is recommended that JPAS users currently without access to one of the four PKI methods to start the process of obtaining these certificates as soon as possible.

4: JPAS Accounts

Current JPAS Users: A current JPAS user can continue using their username/password for access until January 2012, at which time username/password will no longer be authorized. After January 2012, an approved DoD PKI certificate on a smartcard will be needed to access JPAS.

Potential JPAS Users: A potential JPAS user must meet the JPAS account requirements, submit a signed System Access Request (SAR) Form to their Service or Agency, and be approved to receive a JPAS account. At this time, a potential JPAS user does not need an active PKI certificate on a smartcard prior to submitting a SAR to obtain a JPAS account. However, the potential JPAS user will need both a JPAS account and an active PKI certificate on a smartcard to log into JPAS by January 2012.

Note that the current account process and procedures will not change, only the logon method will change. A user will need both an active JPAS account and the approved DoD PKI certificate on a smartcard. In order to find out more information on getting a JPAS account, please go to:

- <https://www.dmdc.osd.mil/psawebdocs/> and select JPAS, the General FAQs link is under the FAQ section in the left-hand column and/or,
- Attachment A - "How Do I Get A JPAS Account".

For any current user or potential JPAS user utilizing PKI logon methods, it is required to have an active JPAS account in addition to one of the PKI certificates.

5: Obtaining Additional Hardware and Software

JPAS users will need a smartcard reader and the smartcard middleware (software) associated with reading a PKI certificate. Since each Department/Agency/company has different procedures, please refer to your IT Support Staff for guidance on procuring the necessary hardware and software. Some Departments/Agencies/companies already have the smartcard middleware associated with reading a PKI certificate installed on a smartcard so there will be no need to obtain middleware. If your Department/Agency/company does not have the associated middleware, the Department/Agency/company will need to obtain the middleware.

The ECA PKI providers may direct/provide their consumers to specific smartcard readers and/or smartcard middleware that work best with their product. As a Government agency, DMDC cannot specifically state which smartcard reader/smartcard middleware to purchase. DMDC can only direct you to the GSA Schedule. Please see Attachment B – “Potential Hardware and Software”.

6: 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, or other approved DoD PKI on a smartcard).
2. Obtain a smartcard reader, smartcard reader driver, and (if necessary) smartcard middleware
 - a. Installation of smartcard readers and smartcard middleware is the responsibility of the Department/Agency/company that controls the workstation configuration.
 - b. Plug in the smartcard reader to the Personal Computer (PC).
 - c. Install the smartcard reader driver on the PC.
 - i. Either this should come bundled with the smartcard reader or the PKI provider should include instructions to locate the site where the driver can be obtained.
 - ii. If necessary, install smartcard middleware on the PC.
3. Simply insert the smartcard into the smartcard reader and logon to JPAS by selecting “*CAC Log in*”. In July 2011, this button will read “*CAC/PKI Log in*”.
4. JPAS will prompt first time users to register their cards within JPAS.

7: Obtaining PKI Certificates

JPAS Users WITH existing approved DoD PKI Certificates:

For those military, civilian, and contractor personnel who already have one of the four authorized types of PKI certificates, software, and hardware, no additional action is needed.

JPAS Users WITHOUT existing approved DoD PKI Certificates:

For those without an approved DoD PKI, please go through your Departments/Agencies/companies internal procedures such as contacting your Security, IT or Human Resource office to determine if you qualify. The decision regarding which authorized credential to use is up to the JPAS user, the organization the JPAS user supports, and their employer. Below is basic guidance on obtaining PKI medium hardware certificates on a smartcard that are authorized for JPAS access.

1. **CAC Issuance:** Eligible populations include Active Duty/Reserve service members, DoD civilian employees, and DoD contractors that are under DoD contract and sponsored by a DoD Service or Agency (Directive Type Memorandum (DTM) 08-003). Not all of DoD Industry

personnel are eligible for CACs. DoD Contractors may obtain CACs if their government sponsor deems it necessary and if they fulfill one of the three requirements:

- a. Be active duty, reservist, or a DOD civilian.
- b. The user must work on-site at a military or government installation.
- c. User is a DoD contractor that works on GFE equipment.

To find out more information:

- a. On the CAC, you can visit <http://www.cac.mil/>.
- b. On the DTM 08-003, you can visit <http://www.dtic.mil/whs/directives/corres/pdf/DTM-08-003.pdf>.

2. **PIV Issuance:** Each Federal Agency is responsible for issuing PIV cards to qualifying employees and contractors.¹ Please use your internal procedures such as contacting your Security, IT or Human Resource office to get additional information on determining qualifications for a PIV from your Federal Agency and an explanation of the process for obtaining a PIV as it varies from Agency to Agency.

Please see Attachment C – “Agencies Who Distribute PIVs To Their Employees” for a listing of Department/Agencies who current issue PIV cards. This attachment also contains a list of known Department/Agencies that do not distribute PIV cards.

If you do not qualify for a CAC and your Department/Agency does not issue PIV cards, you will need to obtain an ECA PKI certificate on a smartcard or other DoD approved PKIs that are cross-certified at the Federal Bridge Certification Authority. Whether the PKI is an ECA certificate or another DoD approved and cross-certified PKI, a Medium Token Assurance certificates or a Medium Hardware Assurance certificate on a smartcard are acceptable.

The option that most cleared companies will take is the Medium Token Assurance Certificate on a smartcard or a Medium Hardware Assurance Certificate on a smartcard provided by an ECA PKI Provider. However, many of the larger cleared companies have other DoD approved PKIs that are cross-certified at the Federal Bridge.

3. **ECA PKI Program:** The DoD established the ECA Program 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 “smart card” qualifies. Please refer to <http://iase.disa.mil/pki/eca/> for more information.

If you do not qualify for either a CAC or PIV, coordinate with your company to obtain a **Medium Token Assurance Certificate on a smartcard** or a **Medium Hardware Assurance Certificate on a smartcard** from one of the three DoD ECA currently approved vendors listed below:

[IdenTrust, Inc.](#)

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

Email: helpdesk@identrust.com

Phone: 888.882.1104

[Operational Research Consultants, Inc.](#)

¹ Homeland Security Presidential Directive-12 (HSPD-12) stipulates that personnel requiring regular access for more than 180-days to a Federally-controlled information system or facility shall be issued a PIV Card.

Web Site: <http://www.eca.orc.com/>
Email: ecahelp@orc.com
Phone: 800.816.5548

VeriSign, Inc.

Web Site: <https://eca.verisign.com/>
Email: eca-support@verisign.com

Please Note: There is a fee associated with an ECA Certificate. Please pay close attention to each individual vendor's instructions on how to obtain an ECA PKI certificate on a smartcard.

Only approved **Medium Token Assurance Certificate** or a **Medium Hardware Assurance Certificate** on smartcards will be accepted.

What is Medium Token Assurance: On the DISA ECA PKI website, <http://iase.disa.mil/pki/eca/>, it states this level is intended for applications handling sensitive medium value information, with the exception of transactions involving issuance or acceptance of contracts and contract modifications. Private keys associated with Medium Token Assurance level certificates must be generated and stored in hardware tokens. Identity proofing must be done in-person, but can be performed by an ECA Registration Authority, Trusted Agent, Notary, or Authorized DoD Employee (outside the US). Medium Assurance has been mapped to DoD Medium Assurance and Federal Bridge Medium Hardware Assurance.

What is Medium Hardware Assurance: On the DISA ECA PKI website, <http://iase.disa.mil/pki/eca/>, it states this level is intended for all applications operating in environments appropriate for medium assurance but which require a higher degree of assurance and technical non-repudiation. Private keys associated with Medium Hardware Assurance level certificates must be generated and stored in hardware tokens. Identity proofing must be done in-person by an ECA Registration Authority or Trusted Agent. Outside the US, an ECA Registration Authority or Trusted Agent must participate in the identity proofing process in addition to an Authorized DoD Employee. Medium Assurance has been mapped to DoD Medium Assurance Hardware and Federal Bridge Medium Hardware Assurance. Please see FAQs for additional questions and answers.

DMDC's preference is a Medium Hardware Assurance certificate on a smartcard. However due to the very limited site locations for the Trusted Agents, DMDC is allowing *Medium Token Assurance certificates on a smartcard*. In order for a JPAS user to obtain a Medium Token Assurance Certificate or a Medium Hardware Assurance Certificate on a smartcard, the JPAS user's identity must be vetted. The Medium Token Assurance Certificate and Medium Hardware Assurance Certificate have different vetting process.

- **Medium Token Assurance Certificate Identity Vetting:** Only requires a notary to validate the identity of the JPAS user. Please follow the ECA vendor's procedures and forms for identity vetting using a notary.
- **Medium Hardware Assurance Certificate Identity Vetting:** Requires a Trusted Agent or a Trusted Correspondent/Local Registration Authority Officer to validate the identity of JPAS user. Please follow the ECA vendor's procedures and forms for identity vetting using a Trusted Agent or a Trusted Correspondent/Local Registration Authority Officer. Please see below for the differences between a Trusted Agent and Trusted Correspondent/Local Registration Authority Officer.

- A Trusted Agent is an ECA vendor representative (e.g. IdenTrust, ORC, VeriSign representative) that performs the identity vetting at a company location. The locations of the Trusted Agents are listed on the webpages of the individual vendors.
- A Trusted Correspondent/Local Registration Authority Officer enables organizations to have digital certificates issued to employees, officers and agents by performing the identity vetting process themselves in-house. Training and an application will allow a selected individual within a company to perform the identity vetting process for others within a company that needs to purchase the Medium Hardware Assurance Certificates. The Trusted Correspondent/Local Registration Authority Officer must go through the Trusted Agent identity vetting process then apply to become a Trusted Correspondent/Local Registration Authority Officer. Please contact each vendor for the vendor's policies and procedures to become a Trusted Correspondent.

Please see Attachment D – “ECA PKI Web Site” for screen shots of the web sites and helpful hints. Questions regarding costs and implementation should be directed to one of the three DoD ECA currently approved vendors as the answers depend on numerous decisions companies need to make (i.e., number to purchase, expiration dates, technical capabilities, etc.). **Do not purchase the certificates or associated equipment without first coordinating and consulting with your supervisor and/or company.**

4. **Other DoD Approved PKI**

PKI certificates that have completed Joint Interoperability Test Command testing and received DoD approval for use on DoD systems are also authorized for JPAS access. A complete list of companies that may provide their employees these PKIs is located at http://jitc.fhu.disa.mil/pki/pke_lab/partner_pki_testing/partner_pki_status.html

8: FAQs Available

Additional information and frequently asked questions can be found at:

- Attachment E – “Frequently Asked Questions”
- <https://www.dmdc.osd.mil/psawebdocs/> under JPAS and JPAS PKI FAQs in the left-hand column.
- Operational Research Consultants, Inc. web site at <http://www.eca.orc.com/help.html>
- VeriSign, Inc. web site at <https://knowledge.verisign.com/support/eca-support/index.html>
- IdenTrust, Inc. web site at http://www.identrust.com/certificates/eca/eca_faqs.html

Attachment A: How do I get a JPAS account?

1. Military Users

MAJCOM Account Managers: To obtain a JPAS account, you will need to contact an established JPAS Account Manager or POC within your organization or military branch. If there is not yet an appointed JPAS Account Manager within your organization, or if you do not know who this person is, then please refer to the JPAS POC Listing on the DMDC JPAS User [Web site](#) to locate a JPAS POC for your organization. This person will then assist you in setting up your account. To request an account, you will need to complete a JPAS System Access Request (SAR). To obtain this form, access the DMDC JPAS User [Web site](#). Then, click on the "Access Request" link on the left side menu bar. Submit this completed form to your JPAS Account Manager or POC, who will then create your account.

Users and Non-Primary Account Managers: To get a JPAS account, you will need to contact an established JPAS Account Manager or POC within your organization or military branch. If there is not yet an appointed JPAS Account Manager within your organization, or if you do not know who this person is, then please refer to the JPAS POC Listing on the JPAS Web Site to locate a JPAS POC for your organization. This person will then assist you in setting up your account. To request an account, you will need to complete a JPAS System Access Request (SAR). To obtain this form, access the DMDC JPAS User [Web site](#). Then, click on the "Access Request" link on the left side menu bar. Submit this completed form to your JPAS Account Manager or POC, who will then create your account.

2. DoD Agency Users

Agency Primary Account Managers: If you are going to be the Primary or Alternate Account Manager for a new* agency, the DoD Security Services Center (JPAS Call Center) will create your account. To request an account, you will need to submit 2 items to the DoD Security Services Center (JPAS Call Center). First, create a Letter of Appointment (LOA) on your agency's letterhead indicating that these two individuals will be the Primary and Alternate account managers for your agency. Your agency's director must sign the letter. Second, a JPAS System Access Request (SAR) must be completed for each manager. To request an account, you will need to complete a JPAS System Access Request (SAR). To obtain this form, access the DMDC JPAS User [Web site](#). Then, click on the "Access Request" link on the left side menu bar. Submit this completed form to your JPAS Account Manager or POC, who will then create your account.

A SAR must be completed for each manager and signed by your agency's director. Upon completion of the SAR and the LOA, please submit them to the DoD Security Services Center (JPAS Call Center). Instructions on where to submit your paperwork can be found on the DoD Security Services Center (JPAS Call Center) contact information is located at https://www.dmdc.osd.mil/psawebdocs/docPage.jsp?p=JPAS&fileNm=POCs_DoD_Security_Services_Center.htm. DoD Security Services Center (JPAS Call Center) will notify you with your account information.

*Current agencies will follow the procedures for users and non-primary account managers below.

Users and Non-Primary Account Managers: To obtain a JPAS account, you will need to contact an established JPAS Account Manager or POC within your agency. If there is not yet an established Account Manager within your agency, or if you do not know who this person is, please contact the DoD Security Services Center (JPAS Call Center) to locate an Account Manager or POC for your agency*. DoD Security Services Center (JPAS Call Center) contact information is located at https://www.dmdc.osd.mil/psawebdocs/docPage.jsp?p=JPAS&fileNm=POCs_DoD_Security_Services_Center.htm. To request an account, you will need to complete a JPAS System Access Request (SAR). To obtain this form, access the DMDC JPAS User [Web site](#). Then, click on the "Access Request" link on the left side menu bar. Submit this completed form to your JPAS Account Manager or POC, who will then create your account.

*There may be circumstances in which the Call Center cannot determine who your account manager is.

3. Industry Users

Company Account Managers: If you are going to be the Primary for your company, the DoD Security Services Center (JPAS Call Center) will create your account. To request an account, you will need to submit 2 items to the DoD Security Services Center (JPAS Call Center). First, create a Letter of Appointment (LOA) on your company's letterhead indicating that you will be the Primary account manager for your company. A Corporate Officer or Key Management Personnel (KMP) must sign the letter. Second, a JPAS System Access Request (SAR) must be completed for each manager. To request an account, you will need to complete a JPAS System Access Request (SAR). To obtain this form, access the DMDC JPAS User [Web site](#). Then, click on the "Access Request" link on the left side menu bar. Submit this completed form to your JPAS Account Manager or POC, who will then create your account.

A SAR must be completed and signed by a Corporate Officer or KMP. The signature for the nominating official must be the same as the signature for the appointment letter. Upon completion of the SAR and the LOA, please submit them to the DoD Security Services Center (JPAS Call Center). Instructions on where to submit your paperwork is located on the DoD Security Services Center (JPAS Call Center) web site located at https://www.dmdc.osd.mil/psawebdocs/docPage.jsp?p=JPAS&fileNm=POCs_DoD_Security_Services_Center.htm. Once the accounts have been created, the DoD Security Services Center (JPAS Call Center) will notify you with your account information.

Users and Non-Primary Account Managers: To obtain get a JPAS account, you will need to contact an established JPAS Account Manager or POC within your company. If there is not yet an established Account Manager within your company, or if you do not know who this person is, please contact the DoD Security Services Center (JPAS Call Center) to located an Account Manager or POC for your company. The DoD Security Services Center (JPAS Call Center) contact information is located on the DMDC JPAS User Support Web Pages under Contact

Customer Service. The URL is

https://www.dmdc.osd.mil/psawebdocs/docPage.jsp?p=JPAS&fileNm=POCs_DoD_Security_Services_Center.htm . To request an account, you will need to complete a JPAS System Access

Request (SAR). To obtain this form, access the DMDC JPAS User [Web site](#). Then, click on the "Access Request" link on the left side menu bar. Submit this completed form to your JPAS Account Manager or POC, who will then create your account.

Submit the completed SAR form to your JPAS Account Manager or POC, who will then create your account.

Attachment B: Potential Hardware and Software

The ECA PKI providers may direct/provide their consumers to specific smartcard readers and/or smartcard middleware that work best with their product. As a Government agency, DMDC cannot specifically state which smartcard reader/smartcard middleware to purchase. DMDC can only direct you to the GSA Schedule.

You will need two hardware items in order to logon to JPAS. These are:

1. **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.
2. **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.

Please refer to the FIPS 201 Approved Products List for smartcard readers, referred to as "Transparent Readers," located at: <http://fips201ep.cio.gov/apl.php>. Simply click Category on the top row to alphabetically sort the list of products. Then scroll down to the list of "Transparent Reader" for the complete listing.

You will need smartcard middleware if you do not already have it.

1. **Step One:** Please see your company or agency's IT staff to ensure your Department/Agency/company does not have existing smartcard middleware. Many Department/Agency/company 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.
2. **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.

The type of smartcard middleware depends on the users' OS, browser, and PKI. You will need to work closely with your Department/Agency/company's IT department to ensure the smartcard middleware you obtain is compliant with your Department/Agency/company IT infrastructure. For example, Department of Justice may have their own preferred smartcard middleware for their systems while a contractor using one of the ECA PKI medium hardware certificates on a token uses a different one via Firefox.

Please refer to the FIPS 201 Approved Products List for the smartcard middleware, referred to as 'PIV Middleware' located at: <http://fips201ep.cio.gov/apl.php>. 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.

Attachment C: Agencies Who Distribute PIVs To Their Employees

Below are links to many Federal agencies' PIV policies/offices. Since each agency has its own policy and procedure for distributing a PIV, please check with your associated agency below. If you do not qualify for a CAC and your agency does not distribute PIVs, you will need to get a ECA PKI. DoJ, DHS and DoT allow sub-organizations to issue their own PIV cards, FAA for example, while others may have their PIV info posted on their agency's intranet sites. Finally, over a dozen smaller Executive offices utilize GSA's USAccess for PIV issuance. Your Personnel Security or Human Resources office can provide information on determining qualification for a PIV from your Federal agency and explain the process for obtaining it as it varies from agency to agency.

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

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

Farm Credit System Insurance Corporation:

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

Federal Communications Commission:

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

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/>

These are the listings 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

Department of Health and Human Services

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

Attachment D: ECA PKI Web Sites

[DISA ECA PKI Program](#)

The screenshot shows the 'ECA PKI Program' website. At the top, there is a navigation bar with 'IA News', 'What's New', and 'Consent Notice'. The main heading is 'ECA PKI Program'. Below this, there is a purple box with 'IMPORTANT NOTES:' containing three paragraphs of text. To the left is a 'Subject Matter Links' menu with a red arrow pointing to 'Obtain an ECA Certificate'. To the right, there is an illustration of a padlock and computers, followed by the 'External Certification Authority Program:' section, which describes the DoD's ECA program. At the bottom, a small line of text reads: 'The DoD PKI Program Management Office (PMO) has designated the ECA'.

Information Assurance Support Environment
Your 'One-stop-shop' for IA Information

IA News What's New Consent Notice

ECA PKI Program

IMPORTANT NOTES:

The AKO/DKO web portal does not currently allow ECA certificates to be used for certificate login or access into CAC protected areas.

All DoD PKI relying parties must update their certificate trust list to only include both the current 1024 bit and the newly issued 2048 bit ECA Root and Subordinate CA certificates.

The IASE web site does NOT currently accept ECA certificates for entry into the PKI-protected area.

Subject Matter Links:

- Obtain an ECA Certificate
- Updates
- Upcoming Changes/Capabilities
- Users/Subscribers
- Certificate Types
- Assurance Levels
- Relying Parties/Applications
- Documents
- Policy Change Process
- FAQ
- Contact Us

External Certification Authority Program:

The DoD has established the External Certification Authority (ECA) program to support the issuance of DoD-approved certificates to industry partners and other external entities and organizations. The ECA program is designed to provide the mechanism for these entities to securely communicate with the DoD and authenticate to DoD Information Systems.

The DoD PKI Program Management Office (PMO) has designated the ECA

The screenshot shows the 'Obtain an ECA Certificate' website page. The main heading is 'Obtain an ECA Certificate'. To the left is a 'Subject Matter Links' menu with a red arrow pointing to 'Obtain an ECA Certificate'. The main content area explains that ECA certificates are obtained directly from vendors and lists three approved vendors: Operational Research Consultants, Inc. (ORC), Verisign, Inc., and IdenTrust, Inc. (formerly DST). Each vendor entry includes a URL, email address, and phone number.

PROGRAM

Obtain an ECA Certificate

Subject Matter Links:

- Obtain an ECA Certificate
- Updates
- Upcoming Changes/Capabilities
- Users/Subscribers
- Certificate Types
- Assurance Levels
- Relying Parties/Applications
- Documents
- Policy Change Process
- FAQ
- Contact Us

ECA Home Page

ECA Certificates are obtained directly from the vendors.

You may purchase an ECA Certificate from one of the approved vendors below:

- Operational Research Consultants, Inc. (ORC)
<http://www.eca.orc.com/>
Email: ecahelp@orc.com
Phone: 800.816.5548
- Verisign, Inc.
<https://eca.verisign.com/>
Email: eca-support@verisign.com
Phone: 650.426.3224
- IdenTrust, Inc. (formerly DST)
<http://www.identrust.com/certificates/eca/index.html>
Email: helpdesk@identrust.com
Phone: 888.882.1104

The screenshot shows the IdenTrust website's 'EXTERNAL CERTIFICATE AUTHORITY (ECA)' page. The navigation bar includes Home, Company, Solutions, Certificates, Partner, Library, and Support. Below the navigation, there are links for 'BEFORE YOU BUY', 'CERTIFICATE CENTER', 'AFTER YOU BUY', 'TRUSTID', 'ACES', and 'ECA'. The main content area is titled 'EXTERNAL CERTIFICATE AUTHORITY (ECA)' and includes a breadcrumb 'Certificates > ECA'. A section titled 'WHAT IS ECA?' explains that as part of an overall program to provide a stronger and more secure authentication mechanism for accessing Department of Defense (DoD) Information Systems, the DoD may require contractors to have DoD PKI ECA Certificates. A section titled 'CERTIFICATE OFFERING AND PRICING' lists two options: 'Get Information about each certificate type, price and validity' and 'Purchase a new certificate or Renew an existing certificate'. A section titled 'WHICH CERTIFICATE DO I NEED AND HOW DO I GET ONE?' lists five certificate types, each with a 'BUY' button and a 'Step-by-Step Process' link. A red arrow points to the 'BUY' buttons. The right sidebar contains sections for 'SALES CONTACT', 'CUSTOMER SUPPORT', 'ECA CERTIFICATE PRICING', and 'HOW TO BUY'.

EXTERNAL CERTIFICATE AUTHORITY (ECA)

Certificates > ECA

WHAT IS ECA?

As part of an overall program to provide a stronger and more secure authentication mechanism for accessing Department of Defense (DoD) Information Systems, the DoD may require contractors to have DoD PKI ECA Certificates. A notification sent by your DoD System Owner should indicate the specific DoD PKI ECA certificate required to access their application.

CERTIFICATE OFFERING AND PRICING

- Get Information about each certificate type, price and validity
- Purchase a new certificate or Renew an existing certificate

WHICH CERTIFICATE DO I NEED AND HOW DO I GET ONE?

IdenTrust offers the following DoD PKI ECA Digital Certificates. By selecting a certificate, you will be taken to a webpage that will provide more information on how to purchase, what identification and forms you will need to complete and submit, and other useful information about the certificate.

1. Medium Assurance	BUY	Step-by-Step Process
2. Medium Assurance Foreign Country	BUY	Step-by-Step Process
3. Medium Token Assurance	BUY	Step-by-Step Process
4. Medium Hardware Assurance	BUY	Step-by-Step Process
5. Medium Assurance SSL	BUY	Step-by-Step Process

SALES CONTACT

- 866.299.3335
- ECAsales@IdenTrust.com

CUSTOMER SUPPORT

- Helpdesk@IdenTrust.com
- 888.882.1104 (within the US)
- 801.924.8141 (outside the US)
- M-F, 6am-6pm MST

ECA CERTIFICATE PRICING

HOW TO BUY

- ECA Medium Assurance
- ECA Medium Assurance Foreign Country
- ECA Medium Token Assurance Foreign Country
- ECA Medium Token
- ECA Medium Hardware Assurance
- ECA Medium Assurance SSL
- ECA Foreign Countries Supported

Step by Step Process for Medium Token Assurance:

The screenshot shows the IdenTrust website's 'STEP-BY-STEP PROCESS TO PURCHASE A DoD PKI ECA MEDIUM TOKEN ASSURANCE DIGITAL CERTIFICATE' page. The navigation bar includes Home, Company, Solutions, Certificates, Partner, Library, and Support. Below the navigation, there are links for 'BEFORE YOU BUY', 'CERTIFICATE CENTER', 'AFTER YOU BUY', 'TRUSTID', 'ACES', and 'ECA'. The main content area is titled 'STEP-BY-STEP PROCESS TO PURCHASE A DoD PKI ECA MEDIUM TOKEN ASSURANCE DIGITAL CERTIFICATE' and includes a breadcrumb 'Certificates > ECA > Step-by-Step Registration Process'. A section titled 'STEP 1: APPLY ONLINE & PAY FOR YOUR ECA DIGITAL CERTIFICATE' explains that the user has selected an ECA Medium Token Assurance Digital Certificate and provides instructions on how to purchase. A section titled 'STEP 2: COMPLETE FORMS AND IN-PERSON IDENTITY AUTHENTICATION' is also visible. The right sidebar contains sections for 'SALES CONTACT', 'CUSTOMER SUPPORT', 'ECA CERTIFICATE PRICING', and 'HOW TO BUY'.

IdenTrust
WE PUT THE TRUST IN IDENTITY

Home | My Account | Contact Us

SEARCH

STEP-BY-STEP PROCESS TO PURCHASE A DoD PKI ECA MEDIUM TOKEN ASSURANCE DIGITAL CERTIFICATE

Certificates > ECA > Step-by-Step Registration Process

STEP 1: APPLY ONLINE & PAY FOR YOUR ECA DIGITAL CERTIFICATE

You have selected an ECA Medium Token Assurance Digital Certificate. If you are unsure of which certificate you need, check with the agency with which you will use your certificates.

Step 1

The IdenTrust online purchase process will ask you to provide personal and company information and pay for your digital certificate.

Below are the accepted Payment methods:

- Credit Card (Visa, MasterCard, and American Express)
- Voucher Number - A voucher number is obtained when your company submits a Purchase Order. Upon approval, IdenTrust issues the voucher number(s) which your company can distribute to its employees to be used as the form of payment. [Download ECA Voucher Purchase Order Form\[pdf\]](#)

STEP 2: COMPLETE FORMS AND IN-PERSON IDENTITY AUTHENTICATION

SALES CONTACT

- 866.299.3335
- ECAsales@IdenTrust.com

CUSTOMER SUPPORT

- Helpdesk@IdenTrust.com
- 888.882.1104 (within the US)
- 801.924.8141 (outside the US)
- M-F, 6am-6pm MST

ECA CERTIFICATE PRICING

HOW TO BUY

- ECA Medium Assurance
- ECA Medium Assurance Foreign Country
- ECA Medium Token Assurance Foreign Country
- ECA Medium Token

Look Here → **Order Your Certificate** ▶

Look Here → **Instructions**

Home

ORC has been approved to issue certificates to all Foreign Nationals except where prescribed by law.

All applicants (including US Citizens) are now required to show proof of citizenship.

For citizens of the United States, Great Britain, Canada, Australia and New Zealand, click the arrow to the right. **Get Certificate** →

For citizens of all other countries, click the arrow to the right. **Get Certificate** →

As a U.S. Government ECA, Operational Research Consultants (ORC) is authorized to provide digital certificates for:

- Identification/Digital Signature
- Encryption to secure email and digital files
- Server Authentication for identification of web sites and other devices
- Domain Controllers for securing your Windows domain and
- Signing of Code

Get Certificate Process

Order Your Certificate ▶

Ordering Process

Certificate Order Process

There are three main processes for obtaining your ORC ECA Certificates. They are [Online Application](#), [Identity Verification](#), and [Secure Online Certificate Delivery](#).

Online Application

- IMPORTANT:** Each Subscriber must perform the Online Application for themselves. You may NOT make an Online Application for another individual. This is grounds for immediate revocation of your certificate. (And any fees paid will not be returned.) *You must use the same work station you used for the online application process, when retrieving your certificate.*
- By the end of the online application process you will have: trusted the U.S. Government ECA Root and the ORC ECA Intermediate Certification Authority, generated a set of keys for your certificate(s) and assigned a password to protect the private key, and printed a customized, four page, certificate request form for each certificate that you need.
- You will need a work station with a FIPS 140-1/2 Level 1 cryptographic compliant web browser. This includes Internet Explorer 5.5 and above, Netscape 4.7 and above and Firefox 1.5 and above.
- ORC recommends, that a back-up copy of your Enrollment Private Key be made as soon as you submit your request - see the [Creating a Backup \(Export\) Copy of your Enrollment Private Key](#) instructions for the web application used during the request process. ORC recommends that you create a back-up copy of your key pair once issued - see the [Creating a Backup \(Export\) Copy of Your Certificate](#). This needs to be done in case of loss of certificates due to human error, network, operating system, or computer changes. If you need further assistance, please contact the help desk at 1-800-816-5548 or ecahelp@orc.com. Any operational copy of the private key must be protected in accordance with the ORC ECA CPS section on [Private Key Protection](#).
- Medium Hardware Assurance certificates (including Mobile Code Signing Certificates) must be applied for in the presence of a Registration Authority.

Products & Services | Partners | Support | My Account

US Home > Products & Services > Identity and Authentication Services > Authentication for Government > DOD Interoperability

Identity and Authentication Services

- Two-Factor Authentication
- Risk-Based Authentication
- Public Key Infrastructure (PKI) Services
- Authentication for Government
 - HSPD-12 Solution
 - Non-Federal Shared Service Provider PKI
 - VIP Authentication for Government
 - National PKI Solutions
- DOD Interoperability/ECA Certificates**
- Digital IDs for Secure Email
- Information Center
- Why VeriSign
- Authentication Partner Programs

DOD Interoperability

ECA Certificates

VeriSign is certified by the United States Department of Defense (DoD) as a provider of PKI digital certificates for external entities (government contractors, state and local governments and individuals). **External Certification Authority (ECA)** certificates enable secure on-line transactions with government agencies. Installed in a browser or email program, ECA certificates can be used for such activities as; authenticating identity for access to DoD Web sites and applications, digitally signing documents, and for encrypting e-mail communications.

VeriSign ECA certificates are sold as a set including both an ECA Identity certificate and an ECA Encryption certificate. A key escrow service protects and enables the recovery of a private encryption key in the event that a user loses the key and needs to access information previously encrypted with the key.

Who Can Purchase an ECA Certificate?

- Employees of organizations conducting business with U.S. government agencies.
- Employees of state and local governments conducting business with other U.S. government agencies.
- Employees of foreign governments or organizations conducting business with U.S. government agencies.
- Individuals who need to communicate securely with U.S. government agencies.

Scroll Down

Purchase ECA Certificates

Validity Period	Price
1 year	USD \$ 119
2 year	USD \$ 218
3 year	USD \$ 299

Contact Us

Technical Support:
Toll Free: 1-866-202-5570 option 2 or
Local: 650-426-3896

Sales Phone Support for 10 or More Certificates:
Local: 650-426-3614

Order status & Enrollment Questions:
Toll Free: 1-866-202-5570 option 1
eca-authentication@verisign.com

Installation Questions:
eca-support@verisign.com

Chat with Support
How can we help?

Who Can Purchase an ECA Certificate?

- Employees of organizations conducting business with U.S. government agencies.
- Employees of state and local governments conducting business with other U.S. government agencies.
- Employees of foreign governments or organizations conducting business with U.S. government agencies.
- Individuals who need to communicate securely with U.S. government agencies.

Look Here

Purchase ECA Certificates

Validity Period	Price
1 year	USD \$ 119
2 year	USD \$ 218
3 year	USD \$ 299

To purchase certificates follow the process listed in the Enrollment Instructions.

Enrollment Instructions

Prices are in U.S. dollars.

Purchasing 10 or more Certificates?


To purchase or establish a Trusted Agent call (650) 426-3614 or email eca-sales@verisign.com.

If more than 10 employees in your company need a certificate VeriSign offers the following benefits to buying in bulk:

- Subscribers can use a single sales order to purchase certificates rather than paying by credit

Chat with Support
How can we help?

Enrollment Instructions:

Now from  **VeriSign Authentication Services**

United States [change] | [Contact Us](#)

Search

[Products & Services](#) | [Partners](#) | [Support](#) | [My Account](#)

Identity and Authentication Services

- Two-Factor Authentication
- Risk-Based Authentication
- Public Key Infrastructure (PKI) Services
- Authentication for Government
 - HSPD-12 Solution
 - Non-Federal Shared Service Provider PKI
 - VIP Authentication for Government
 - National PKI Solutions
 - DOD Interoperability/ECA Certificates**
- Digital IDs for Secure Email
- Information Center

US Home > Products & Services > Identity and Authentication Services > Authentication for Government > DOD Interoperability - ECA Certificates > Step-by-Step Overview

DOD Interoperability - ECA Certificates Step-by-Step Overview

Email | Share | Print

ECA certificates are specific to you and the computer you use. You need to complete the steps below using the browser on the computer where you will use ECA authentication and encryption services.

- Enrollment**

Initiate a request for an ECA digital certificate by completing the enrollment process. You will be asked to provide identity information online, print and complete enrollment forms, have them notarized, and mail them to VeriSign.

Symantec Corporation
Attn: VeriSign ECA Authentication Support
350 Ellis Street
Mountain View, California 94043

NOTE: New regulations require proof of citizenship prior to obtaining a certificate from the VeriSign ECA. At least one of the two forms of identification provided must be a government issued photo ID. To use auto-enrollment for renewals, users will need to have validated citizenship information in place.

If you are enrolling using **If you are enrolling using Trusted**


Contact Us

Technical Support:
Toll Free: 1-866-202-5570 option 2 or
Local: 650-426-3896

Sales Phone Support for 10 or More Certificates:
Local: 650-426-3614

Order status & Enrollment Questions:
Toll Free: 1-866-202-5570 option 1
eca-authentication@verisign.com

Installation Questions:
eca-support@verisign.com

 **Chat with a Customer Support Rep Now.**

How can we help?

Attachment E: Frequently Asked Questions (FAQs)

The following set of FAQs seeks to answer questions regarding upcoming changes to the Joint Personnel Adjudication System (JPAS) logon procedures as of 14 January 2011.

Section 1: General

1. *What should I use to log into JPAS and when will the logon methods change?*
 - a. Please continue to use your authorized username/password or Common Access Card (CAC).
 - b. In July 2011, users will have the ability to use a PIV card or ECA PKI certificate in addition to the username/password or CAC.
 - c. Users will need three items to access JPAS by January 2012. These three items are:
 1. An Active JPAS account (account management policies have not changed)
 2. An Approved Active PKI Certificate
 3. Hardware and Software needed to read the PKI Certificate (See Obtaining Future JPAS Logon Methods Attachment B – “Potential Hardware and Software”)
2. *Is there any written requirement to remove username/password?*
 - a. For DoD or Other Federal Agencies: Joint Task Force-Global Networking Operations (JTF-GNO) 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).
3. *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.
4. *What if I am using my boss, friend or co-worker's username/password 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’ at the bottom of this page,

you are agreeing to comply with all JPAS administration policies, to include the termination of JPAS access if usage terms are violated.

5. *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 web pages for alerts, notices, and user guide resources at <https://www.dmdc.osd.mil/psawebdocs>

6. *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.

7. *What is an active JPAS account?*

- a. Currently, a 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 in the past 60 days. Your JPAS account will be deleted if you do not log into over the course of 90 days per DoD Regulations (APP6240).

8. *Will JPAS accounts be handled different (e.g. System Access Request (SAR), 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 procedures for that JPAS account. A JPAS user will still need to qualify, submit a SAR, and receive a JPAS account. A JPAS user will need three things to logon to JPAS. Users will need three items to access JPAS by January 2012. These three items are:
 - i. An active JPAS account;
 - ii. An approved active PKI Certificate; and,
 - iii. Hardware and Software needed to read the PKI certificate (See Attachment B – “Potential Hardware and Software”).
- 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.

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

9. *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.

10. 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 (Directive Type Memorandum (DTM) 08-003). 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. To find out more information:
 1. On the CAC, you can visit <http://www.cac.mil/>
 2. On the DTM 08-003, you can visit
 3. <http://www.dtic.mil/whs/directives/corres/pdf/DTM-08-003.pdf>
 4. For a non-official DoD source but has good information you can also visit http://en.wikipedia.org/wiki/Common_Access_Card

11. How do I login to JPAS with my CAC?

- 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, or other approved DoD PKI on a smartcard).
 2. Obtain a smartcard reader, smartcard reader driver, and (if necessary) smartcard middleware
 - a. Installation of smartcard readers and smartcard middleware is the responsibility of the Department/Agency/company that controls the workstation configuration.
 - b. Plug in the smartcard reader to the Personal Computer (PC).
 - c. Install the smartcard reader driver on the PC.
 - i. 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.
 - ii. If necessary, install smartcard middleware on the PC.
 3. Simply insert the smartcard into the smartcard reader and logon to JPAS by selecting “CAC Log in”. In July 2011 this button will read “CAC/PKI Log in”.
 4. JPAS will prompt first time users to register their cards within JPAS.

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

- a. Attempt to login using your username/Password to confirm that your JPAS connection is working and your account is active.

1. If you cannot login with your username/password, please contact your Department/Agency/Company's Account Manager. The JPAS Account Manager can unlock your JPAS account.
2. If you are a JPAS Account Manager and your account is locked, please call the Call Center
- b. If you can login with your username/password, contact your internal IT Help Desk to determine if there is an issue with your CAC, hardware or software.
- c. 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 timed out is still active in your Internet browsing history.
 2. If you receive a 'cannot find DEERS Identifier', please use your username and password to log into JPAS. You will receive this error if you have received a new CAC or are part of Industry. It takes anywhere from 30-60 days for the DEERS Identifier to populate JPAS for those with new CACs. Please try back at a later time to see if you are still receiving this error.

13. 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.

14. What are 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.
- b. PIV Cards: Personal Identity Verification (PIV) Card required to be issued to all US Federal employees and contractors under HSPD-12. Each Federal Agency is responsible for issuing PIV cards to qualifying employees and contractors.¹ Please use your internal procedures such as contacting your Security, IT or Human Resource office to get additional information on determining qualification for a PIV from your Federal Agency and explain the process for obtaining it as it varies from Agency to Agency. Please see Obtaining Future JPAS Logon Methods Attachment C – "Agencies Who Distribute PIVs To Their Employees" for a listing of agencies who current issue PIV cards. Obtaining Future JPAS Logon Methods Attachment C – "Agencies Who Distribute PIVs To Their Employees" also contains a list of those Agencies who do not distribute PIV cards.
- c. ECA PKI Cards: 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 "smart card" qualifies. Please refer to <http://iase.disa.mil/pki/eca/> for more information. These need to at a Medium Token Assurance or Medium Hardware Assurance certificate level.
- d. Other DoD PKI cards: PKI certificates that have completed Joint Interoperability Test Command testing and received DoD approval for use on DoD systems are also authorized for JPAS access. A complete list of companies that may provide their employees these PKIs is located at http://jitic.fhu.disa.mil/pki/pke_lab/partner_pki_testing/partner_pki_status.html

15. Can I access JPAS if I have other types of DoD approved PKI certificates?

- a. Yes. DMDC authorized the use of DoD approved PKI certificates other than CACs for JPAS. Please see Obtaining Future JPAS Logon Methods Attachment E - "FAQ's" Section 2:

Common Access Card (CAC) and Public Key (PK) Enabling Question #5 for more details (the previous question).

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

- a. Phase 1 – CAC-Enabled JPAS deployed on January 15, 2011.
- b. Phase 2 – PK-Enabled JPAS will be deployed in July 2011.
- c. Phase 3 –Username and Password will be removed in January 2012.

17. *What is a Smart card?*

- a. A smart card, 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 . Smart cards may also provide strong security authentication for single sign-on (SSO) within large organizations.
- b. For a non-official DoD source but has good information you can also visit <http://en.wikipedia.org/wiki/Smartcard>

18. *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. For a non-official DoD source but has good information you can also visit http://en.wikipedia.org/wiki/Card_reader

19. *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. For a non-official DoD source but has good information you can also visit http://en.wikipedia.org/wiki/FIPS_201

20. *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. For a non-official DoD source but has good information you can also visit <http://en.wikipedia.org/wiki/Middleware>

21. 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. Their primary responsibilities are:
 1. Identifies and resolves 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. Identifies significant threats to the GIG. Develop, disseminate and implement countermeasures to these threats in a timely manner via Information Assurance Vulnerability Messages (IAVM)
 3. Assesses 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. Coordinates the response actions taken by the CC/S/A CND service providers (CNDSP)
 5. Identifies emerging technologies and their associated threats in order to integrate migrations and response actions into current CND posture
- c. For a non-official DoD source but has good information you can also visit http://en.wikipedia.org/wiki/Joint_Task_Force-Global_Network_Operations

22. 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.[1] 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. For a non-official DoD source but has good information you can also visit http://en.wikipedia.org/wiki/Public_key_infrastructure
- c. Another source on What is PKI? A PKI (public key infrastructure) 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:
 - 6. A certificate authority (CA) that issues and verifies digital certificate. A certificate includes the public key or information about the public key
 - 7. A registration authority (RA) that acts as the verifier for the certificate authority before a digital certificate is issued to a requestor
 - 8. One or more directories where the certificates (with their public keys) are held
 - 9. A certificate management system

23. How Public and Private Key Cryptography Works?

- 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

24. 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. For a non-official DoD source but has good information you can also visit http://en.wikipedia.org/wiki/Certificate_authority.

25. *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. For a non-official DoD source but has good information you can also visit http://en.wikipedia.org/wiki/Public_key_infrastructure

26. *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. For a non-official DoD source but has good information you can also visit http://www.dhs.gov/xabout/laws/gc_1217616624097.shtm#0

27. *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 cyphertexts, 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. For a non-official DoD source but has good information you can also visit <http://en.wikipedia.org/wiki/Cryptography>

28. *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 ECA PKI providers have Call Centers that are able to assist various users to include those with no technical background. The ECA PKI provider's Call Centers are able to answer all questions and walk their customers through their processes.

29. *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 prior to submitting a SAR to obtain a JPAS account. By January 2012, a potential JPAS user will need both an active JPAS account in addition to an active PKI certificate to logon to the application.

30. *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 within JPAS the first time they logon. This will link the certificate on the smartcard to their active JPAS account.

31. *If an active duty/reservist/DOD civilian is issued a CAC, can they use their CAC if they are in JPAS in a different role (e.g. contractor)? E.g. John Smith is a security consultant for ABC Company part-time. John uses his government issued CAC to access JPAS for the work he's performing for ABC Company. Is this an authorized use of the CAC as many users will fall under this category?*

- a. The use of a Military/Civilian CAC in the performance of an Industry role is against DoD Policy and will be considered misuse of Government property. Please see the Federal Code of Regulations § 2635.704-Use of Government property.

(a) Standard. An employee has a duty to protect and conserve Government property and shall not use such property, or allow its use, for other than authorized purposes.

(b) Definitions. For purposes of this section: (1) Government property includes any form of real or personal property in which the Government has an ownership, leasehold, or other property interest as well as any right or other intangible interest that is purchased with Government funds, including the services of contractor personnel. The term includes office supplies, telephone and other telecommunications equipment and services, the Government mails, automated data processing capabilities, printing and reproduction facilities, Government records, and Government vehicles. (2) Authorized purposes are those purposes for which Government property is made available to members of the public or those purposes authorized in accordance with law or regulation.

The web site is at the following: <http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?c=ecfr&sid=e62a2086dab40719f9b70b63a58695eb&rgn=div5&view=text&node=5:3.0.10.10.9&idno=5#5:3.0.10.10.9.7.50.1>