

# Frequently Asked Questions (FAQ) for Strong Authentication with DOIAccess PIV Cards

Frequently Asked Questions for DOI workers provides short (3-5 sentences) direct answers to most commonly asked questions.

## Table of Contents

### Basics

[What is a PIV card?](#)

[What is the difference between a PIV card and a Smart Card?](#)

[What is “two factor authentication” \(TFA or 2FA\)?](#)

[Why are we starting to use PIV or smart cards?](#)

[What are the advantages of smart cards over usernames and passwords?](#)

[What else is PIV used for?](#)

### PIV Logon

[How does the DOIAccess card work for those with multiple network accounts?](#)

[A single card has enough certificates to authenticate more than one network account. Help desk and system administrators will be able to use a single card for multiple accounts.](#)

[How is this different from current DOI Virtual Private Network \(VPN\) Enterprise Remote Access?](#)

[How do I login to a computer with a PIV card?](#)

[Who will install the PIV card reader on my computer?](#)

[If I leave my computer unattended and the screen locks, will I need my PIV Card to unlock it?](#)

[Will the 15 minute screen lock activate if the DOIAccess card is in the reader?](#)

[Will I be able to login to more than one system at a time?](#)

[Whom do I contact for problems with logging in?](#)

[Will I be able to logon to all applications with the DOIAccess card?](#)

### Personal Identification Number (PIN) and Passwords

[What is a DOIAccess PIN?](#)

[How do I change my PIN if I don't remember it?](#)

[How often do I have to change my PIN?](#)

[How many times can I enter my PIN before I get locked out?](#)

[How do I reset the DOIAccess Card PIN if I get locked out?](#)

[Will I still have to remember passwords?](#)

[Will a locked PIN get released after a period of time \(e.g. 15 min\)?](#)

[If I know my DOIAccess PIN, can I change it without going to a GSA Credentialing Station?](#)

### Forgotten, Lost or Stolen Cards

[What happens if I forget my PIV card?](#)

[What happens if I can't find my card?](#)

[How do I find my bureau “Sponsor”?](#)

### Card Maintenance

[What happens if I have a name change?](#)

### Exemptions from using DOIAccess Cards

[What is the process and information needed for Strong Authentication exemption?](#)

### Certificate and Card Expiration

[What is a certificate?](#)

[What happens if my certificate expires?](#)

[What do I do if I see multiple certificates when I login?](#)

## Table of Contents (continued)

### [Active Directory and Authentication](#)

[How will the altSecurityIdentities LDAP attribute be populated?](#)

[How will the administrative accounts be mapped to my PIV Card for authentication?](#)

[What is the format of the altSecurityIdentities field to enable PIV Authentication?](#)

### [Applications](#)

[What applications will still require passwords?](#)

[What about bureaus who use Citrix for remote access instead of VPN?](#)

[When I login to Windows, will applications like SharePoint still use the 'Use Current Logon Credentials' feature that acts somewhat like single-sign-on?](#)

### [Mobile Devices, Remote Access and VPN](#)

[Can I use my personal equipment to remotely access the DOI network for work activities?](#)

[When logging into the DOI VPN the error: "Invalid username or password. Please re-enter your user information." comes up but I'm using a PIV Card. Why?](#)

[When logging into the DOI VPN the error: "You are not authorized to log in, please contact your system administrator" comes up. Why?](#)

[When using the Network Connect software seems unresponsive or does not work. Why?](#)

[What happens if I have a mobile device that doesn't have a card reader?](#)

## Basics ([back to Table of Contents](#))

### **What is a PIV card?**

A Personal Identity Verification (PIV) card is an official form of identification, and is a specific type of smart card. DOI provides smart cards with PIV, called DOIAccess cards, through the DOIAccess program to DOI workers.

### **What is the difference between a PIV card and a Smart Card?**

A smart card is a card with a computer chip embedded on it. A PIV card is a smart card with personal identity information on the face of the card and imbedded in the computer chip. The DOIAccess PIV card has your facial image, legal name, federal agency (DOI), type of worker (employee, contractor, etc.) and expiration date printed on the face of the card. The computer chip is the gold square at the bottom of the card and contains "certificates" with PIV information in them.

### **What is a certificate?**

Certificates are small encrypted text files with a combination of your personal identity information: fingerprints, your legal name, date of birth, PIN, agency, and/or bureau. The DOIAccess card can contain up to four certificates with combinations of your personal identity information: fingerprints, your legal name, date of birth, PIN, agency, and/or bureau. Each certificate is used for one or more network accounts, for digital signatures or for email encryption. The certificates are created at GSA's USAccess credentialing centers where each worker's photograph and fingerprints are taken, two forms of ID are verified and a signature is recorded onto the certificate(s).

### **Who is required to have a PIV Card?**

Effective since June 2009, the DOIAccess program requires all bureaus/office to complete the Personal Identity Verification (PIV) card for new workers. Most government employees and contractors will use a DOIAccess PIV card to gain physical access to buildings and logical (computer) access to government networks and applications. Only those meeting credential criteria will be issued DOIAccess cards. Credential criteria are:

- working 180 days in a five year period,
- requiring unescorted physical access
- requiring access to controlled logical systems data or networks.

A PIV enabled smart card is one way of using "strong authentication".

### **What is strong authentication?**

Strong authentication is the use of multiple elements to permit access. Elements can include knowledge, a physical object or a biological signature. Multiple elements of knowledge would be numerous questions with given answers, passwords or phrases or numbers. A physical element would be something a person has physical possession of (a card, a key generator, a cell phone). A biometric element is something the person is (a fingerprint, retinal scan, a typing pattern). Each of the elements must be independent of the others so that if one is obtained the other remains secure. Multi-factor authentication requires at least two different element types and is most commonly implemented as "two factor authentication". DOI Memorandum 09-06 (March 2009) established the DOI physical and logical access program, DOIAccess.

<http://www.myinterior.doi.net/ocio/directives.html>.

### **What is "two factor authentication" (TFA or 2FA)?**

A PIV enabled smart card is a form of two factor authentication, meaning it requires two factors (elements) to work. Typically, in civilian government, two-factor authentication is something you have and something you know. You have a PIV card and know a Personal Identification Number (PIN) uniquely keyed to your card. The card and the PIN are legal validation that only you, the card owner, have performed actions using your card and PIN. It is your responsibility to safeguard both the card and the PIN!

### **How is Two Factor Authentication (TFA) more secure?**

Two-factor authentication (TFA or 2FA) means two different types of items, e.g. something you have and something you know, have to be used together for logon. As long as you have your DOIAccess card in your possession, and maintain the secrecy of your PIN, nobody else can log on to the DOI network and access the information you are responsible for. It is critically important never, under any circumstances, to "loan" the DOIAccess card to any other person or give them your PIN, whether an assistant, supervisor or help desk. It is never appropriate for a help desk or supervisor to ask for another employee's PIV card or PIN, and never appropriate to offer your own PIV card or PIN to anyone.

### **Why are we starting to use PIV or smart cards?**

All federal agencies must move to the use of strong authentication (PIV, smart cards) for network access. President George W. Bush in August 2004, signed Homeland Security Directive (HSPD) -12 which was supplemented in 2011, by [Office of Management and Budget \(OMB\) Memorandum 11-11](#), mandating an interoperable federal identity infrastructure be used across all agencies. DOI Memorandum 09-06 (March 2009) established the DOI physical and logical access program, DOIAccess. DOIAccess is managed by the Identity [Credential and Access Management \(ICAM\)](#) office.

### **How long will it take to transition completely to strong authentication?**

The ultimate goal is to reduce the number of identity credentials that individuals must carry and/or remember for authentication and to have all federal workers use PIV cards to gain both physical access to federal buildings and logical access to computer systems.

Over the last five years, DOIAccess distributed 70,000 smart cards to DOI workers. In fiscal year 2012 DOI exceeded 90% use of DOIAccess cards for VPN which was the second phase of deploying strong authentication. The third (current) phase is to enforce use of DOIAccess cards for network (logical) access for 90% of those with credential criteria (see question above). The last phase is to PIV enable all applications so that once a person logs into the network appropriate access is granted to all applications they are authorized to use. Because of the time and cost involved in converting all applications to be PIV enabled, it will take 3-5 years to complete the transition.

### **What are the advantages of smart cards over usernames and passwords?**

Password management is a burden for each of us. How many passwords do you currently have? How long are they? How many times do you change the passwords each year? How do you keep track of all the passwords? Many write down passwords in unsecured places which can defeat their purpose which is to restrict access to only one authorized individual.

### **What else is PIV used for?**

- *Digital signatures* - you can currently digitally sign some PIV enabled documents. For example the DOI Telecommuting Approval form ([http://www.doi.gov/archive/nbc/formsmgt/forms/DI\\_3457.pdf](http://www.doi.gov/archive/nbc/formsmgt/forms/DI_3457.pdf)) accepts digital signatures. Use your PIV card to sign it and email it to your supervisor instead of hand carrying or faxing it up the chain.
- *Email encryption* - Individual's encryption certificates on the DOIAccess card permit encryption of e-mail and documents attached to e-mail.

This is another reason why your PIV card and PIN must be safeguarded. It is the legal equivalent of your signature and will validate that an email came only from you.

## PIV Logon ([back to Table of Contents](#))

### **How does the DOIAccess card work for those with multiple network accounts?**

A single card can authenticate more than one network account. Help desk and system administrators will be able to use a single card for multiple accounts.

### **How is this different from current DOI Virtual Private Network (VPN) Enterprise Remote Access?**

DOIAccess cards are required for remote access through the DOI VPN, when a person is off-site. The FY14 goal for DOIAccess is for those connecting to the DOI network, from DOI premises.

DOI has to measure and report quarterly to OMB on:

- the percentage of people who are required to log on to the on-premise network using DOIAccess card as the normal mode of authentication to the network with an **unprivileged** network account
- the percentage of people who are required to log on to the on-premise network using DOIAccess card as the normal mode of authentication with a **privileged** network account

### **How do I login to a computer with a PIV card?**

A PIV or smart card reader is a thin slot wide enough to insert your PIV card gold “chip” first. If you do not already have a reader installed on your desktop or laptop, your bureau technical staff or help desk will provide either a keyboard with a PIV reader or a smart card reader that will plug into a USB port on the computer. They will install the drivers for the card reader and configure your account to logon with PIV.

At a workstation slide your DOIAccess Card into a card reader and then enter your PIN. There are three types of smart card readers:

- **Most laptop** computers have a built in smart card reader on the left side of the laptop. There is a thin horizontal slot where the card can be inserted. Hold the card face up with the gold chip towards the computer. Slide the card into the slot. *Be careful to insert it in the slot and not between the slot and the laptop housing.*
- To use a **keyboard card reader**, hold the card with the gold chip facing you, chip on bottom. Slide the card into the slot on the keyboard. Once inserted, you should see a flashing green light to the left of the card (may depend on model of keyboard)
- To use an **external USB card reader**, hold the card gold chip up and insert the card into the reader chip first. Once inserted, you will see a green light flash on the card reader.

At the login button or screen for a program or application:

- Click the login button with the DOIAccess card inserted,
- Click OK at “Select a Certificate”<sup>\*\*\*</sup>
- Type in your PIN (Personal Identification Number).

There may be up to 4 certificates. Hover the mouse cursor over your name on each Certificate. A pop up “Government PIV Authentication Key” will identify the certificate to select.

### **Who will install the PIV card reader on my computer?**

Local bureau/office help desk or technical support will install a PIV reader on computers that do not have one.

Windows 7 is capable of using PIV authentication without additional software, however bureaus may opt to load ActivClient to aid in management of PIV certificates.

Windows XP is being replaced by Windows 7. [Windows XP SP3 and Office 2003 will go out of support on April 8, 2014.](#) Any computers still running the Windows XP operating system at that time and requiring TFA to the

network, will need ActivClient software (or an alternative) in order to use the PIV smart card for authentication to the network.

***If I leave my computer unattended and the screen locks, will I need my PIV Card to unlock it?***

Yes.

***Will the 15 minute screen lock activate if the DOIAccess card is in the reader?***

Yes. Use the DOIAccess card and PIN to unlock the screensaver.

***Will I be able to login to more than one system at a time?***

Depending on your bureau's policy, you may use your DOIAccess Card to login to one system, remove it and not have the system lock, then physically login to another.

If your Bureau/Office enforces machine lock when the smart-card is removed, remote logon to other systems may be a possibility.

***Are we required to leave the DOIAccess card in the computer to use the computer or can it be removed after logging in?***

Good practice dictates that one should lock the workstation, remove the card and keep the card with you whenever you step away from your workstation or laptop. However, it depends on bureau/office policy. Please check with your helpdesk or IT Security or the bureau PIV website.

- You may be permitted by machine policy to use the card to authenticate, then remove the card and replace it in its protective sleeve for physical building access.

or

- You may have to leave it in your machine for the duration of the session where taking it out could lock your machine. In this case you will have to remember to remove the card and keep it with you when you walk away from your machine. (BIA is currently an example).

***Whom do I contact for problems with logging in?***

Contact your local help desk or technical support person.

***Will I be able to logon to all applications with the DOIAccess card?***

It currently depends on the application. Some applications (programs) require separate authentication and will not yet be able to use the PIV Card. These systems will continue to use a username and password and a local (non domain/network) account to login. BisonConnect currently "passes PIV authentication through" if you are physically in a DOI facility or connected to the network via VPN and TFA. It is expected that programs such as Quicktime, FPPS, FBMS, Concur Government Edition (CGE), etc. and bureau major applications will become PIV enabled over the next 3-5 years.

## Personal Identification Number (PIN) and Passwords [\(back to Table of Contents\)](#)

### **What is a DOI Access PIN?**

A Personal Identity Verification (PIV) Personal Identification Number (PIN) is the number that you use with your card to validate you are who you claim to be. The card and the PIN are legally binding! The PIN can be any 6 to 8 numbers in length. PINs can ONLY be numbers. It is better to use a longer PIN if possible. Do not make the PIN a number associated with you **or** your family or one that can be easily guessed by finding out about you (e.g. date of birth, phone number, family dates of birth, etc.). If you use a birthdate or phone number make it one of your favorite deli, rock star, movie star, or author not directly traceable to you.

### **How do I change my PIN if I don't remember it?**

You have to go to a credentialing center. Changing a forgotten PIN is a time consuming chore. Make a conscious effort to remember your PIN. Do not write it down anywhere, especially not on your PIV card. Make sure the PIN is not accessible to anyone else. You are legally liable for any actions taken with your PIV and PIN, so never lend it to other people or tell them the PIN. Treat it at least as securely as you would your drivers license and debit/credit card and PIN.

The only way to change the PIV PIN if you have forgotten it **or are locked out**, is to go to one of the GSA or bureau hosted credentialing centers or light activation stations set up around the United States. Check with your bureau/office help desk for specific options. The website for making an appointment for a GSA Center is <https://app3.timetrade.com/tc/login.do?url=usaccess>.

### **How often do I have to change my PIN?**

Never, unless you suspect it has been revealed. A few of the advantages of using your PIV card and PIN are that you only have to use numbers for your PIN and you never have to change your PIN unless you think it has been compromised. If you suspect someone else knows your PIN report it immediately and change it. You are legally liable for all actions taken with your PIV and PIN.

### **How many times can I enter my PIN before I get locked out?**

You have 6 tries to enter your PIN. After the 6th consecutive, unsuccessful attempt the card is locked permanently, and you have to either:

- Make an appointment at a [GSA Credentialing Center](#) to reset the PIN.
- Visit a bureau/office light activation station (LAS)
- If your computer is Windows 7 and your bureau has purchased and installed ActivClient the PIN can be reset at your desktop.

That's why it is important to memorize the PIN and use your card regularly so that you don't forget it. In the future, think of a number that you can easily remember but that others will not be able to guess. For example, do not use your or your or family members' phone number, date of birth etc., as the PIN. Chose numbers related to a favorite movie star or personal hero.

### **How do I reset the DOI Access Card PIN if I get locked out?**

- Make an appointment at a [GSA Credentialing Center](#) to reset the PIN.
- Visit a bureau/office light activation station (LAS)
- If your computer is Windows 7 and your bureau has purchased and installed ActivClient the PIN can be reset at your desktop.

That's why it is important to memorize the PIN and use your card regularly so that you don't forget it. In the future, think of a number that you can easily remember but that others will not be able to guess. For example, do not use your or your or family members' phone number, date of birth etc., as the PIN. Chose numbers related to a favorite movie star or personal hero.

***Will I still have to remember passwords?***

For now, yes. If you remember to bring your PIV card to work, you will not have to use a login/password to login to the network. However, if you forget your PIV card you **will** need to remember your password, to login to the network without your PIV card. This password will still have to meet the Department's requirements for length, complexity, history and it will still have to be changed every 60 days. You will have to remember the passwords for non-PIV enabled applications like Quicktime, DOI Learn, FPPS, etc. and any bureau specific applications that require passwords. Because of the size of this project it is being done in phases. The first phase was distributing PIV for physical access, second phase was using PIV for VPN. Using PIV cards for network access is part of the third phase. The last phase (in the next 5 years) all federal applications will have to become PIV enabled. Eventually, PIV will be used to login to all applications required for work.

***Will a locked PIN get released after a period of time (e.g. 15 min)?***

No. A PIN you do not remember or have incorrectly entered six times locks the use of the card. However, locking the card/PIN does not lock your network account. Depending on your bureau's procedures, you can contact your help desk for assistance with temporarily using a username and password until you get the PIN reset. However, the card itself is disabled until the PIN is reset. To re-enable use of the DOIAccess card, you must:

- Make an appointment at a [GSA Credentialing Center](#) to reset the PIN.
- Visit a bureau/office light activation station (LAS)
- If your computer is Windows 7 and your bureau has purchased and installed ActivClient the PIN can be reset at your desktop.

Memorize the PIN so that you don't forget it. When resetting the PIN think of a number that you can easily remember but that others will not be able to guess. For example, do not use your or your or family members' phone number, date of birth, anniversary, other significant personal date, etc., as the PIN. Instead chose numbers related to a favorite movie star, personal hero, restaurant, etc.

***If I know my DOIAccess PIN, can I change it without going to a GSA Credentialing Station?***

Yes. If you suspect someone has discovered your pin you can change it at your desk. For Windows 7:

- a. Insert your DOIAccess card
- b. press CTRL+ALT+DEL
- c. Select Change a password
- d. Enter your old PIN
- e. Enter the New PIN (you cannot repeat the last 25 PINs)
- f. Click the arrow
- g. Click OK

If your bureau/office has ActivClient software installed please contact your helpdesk for instructions.

## Forgotten, Lost or Stolen Cards [\(back to Table of Contents\)](#)

### ***What happens if I forget my PIV card?***

For short term non-PIV access, and until all DOI applications become PIV enabled in a few years, there will be an option to login to the network with the same password (changed every 60 days) that you currently login with. If you forget your PIV card one day, call your bureau or office help desk for short term use of network login and password..

### ***What happens if my PIV card is lost or stolen?***

You are legally liable for any actions taken with your PIV and PIN. A lost or stolen card is a security breach. Immediately report the card lost or stolen according to your bureau/office incident procedure and initiate a replacement card. Your bureau help desk or local Information System Security Officer (ISSO) can provide assistance.

### ***What happens if I can't find my card?***

This falls into two situations; one if you think you can find it and a second one if you have looked everywhere and are sure it is permanently lost. If you have an idea of where you can find it then use alternative login procedures appropriate to your bureau. If you are sure it is lost, contact your help desk who will provide a list of the bureau sponsors.

Your bureau sponsor will ask if you have lost your card and have no chance of finding it, or if you believe you may find it (for example perhaps it is under your car seat).

- If you have no chance of finding it, a card reprint (at a cost of \$30 to your bureau) will be requested and your lost card will be terminated.
- If you believe that you may find the card later, your card will be suspended;
- If you find the card, contact your bureau Sponsor, inform them that you found your card and it will be re-enabled.

### ***How do I find my bureau "Sponsor"?***

The location of information on bureau sponsors is changing as this is being written. Contact your local help desk for the most current instructions. When you locate the bureau sponsor that person will ask:

- if you have lost your card and have no chance of finding it, or if you believe you may find it (for example perhaps it is under your car seat).
- If you have no chance of finding it, a card reprint (at a cost of \$30) will be requested and your lost card will be terminated.
- If you believe that you may find the card later, your card will be suspended;
- If you find the card, contact your Sponsor, inform them that you found your card and it will be re-enabled.

## Card Maintenance [\(back to Table of Contents\)](#)

### ***What happens if I have a name change?***

The name change process for:

- **Federal employees** is through Human Resources department. The employee completes an SF-50 and submits it to the local HR office.
- **Contract employees** contact the contract supervisor and their government Contract Officer Representative (COR) who will contact the bureau USAccess Sponsor

### ***What happens if my card stops working?***

- Verify that the card is not working, or not, by testing it at <https://wiki.doi.net/cardcheck/> (To test, you need to be on the network or VPN'ed in)
- Record, print or take a snapshot of the answer
- Contact your help desk for further instructions.

## Exemptions from using DOIAccess Cards [\(back to Table of Contents\)](#)

### ***What is the process and information needed for Strong Authentication exemption?***

An exemption is authorization not to use the DOIAccess card for logical access. As bureaus/offices comply with the 2013-06-26 DOI Memoranda “Achieving the Administration’s Cross-Agency Priority: Cybersecurity Goal”, fewer exemptions will be granted. Currently (FY14) there is an exemption for those not meeting credential criteria (appointments less than 180 days, students, interns, volunteers, special populations, etc.). Those groups will log in with the current username and password authentication. Beginning in FY15 and beyond, when there is mandatory enforcement of DOIAccess card use for all accounts, alternative processes will be developed for special cases.

Follow individual bureau procedures for exemptions. Current exemption requests for strong authentication require the following information:

- Your Full Name
- Bureau
- Designation as Employees or Contractor
- Your Duty Location
- Your Phone
- Your Email
- Reason for Needing an Exception
- Period of Authorization

## Certificate and Card Expiration [\(back to Table of Contents\)](#)

### ***What is a certificate?***

A certificate is an encrypted text file, stored in the gold chip on each DOIAccess card. All PIV cards have more than one certificate on them and all certificates must be updated every three years. However, you may only see one certificate come up for selection when you use the card to authenticate to your system.

### ***How do I reauthorize my certificate(s) before they expire?***

If your email address is correct on the PIV card you will receive an email from [HSPD12Admin@usaccess.gsa.gov](mailto:HSPD12Admin@usaccess.gsa.gov) notifying you that your certificates require re-authorization before they expire. Emails are sent at intervals 90, 60, 30, 15, 10, 5, 3, 2, and 1 day(s) prior to the expiration of the certificates. It is your responsibility to reauthorize your certificates before they expire. Check with your bureau help desk for options. Make the appointment the first time you receive the notice. DO NOT leave this to the last minute as it may be difficult to get an appointment on short notice.

### ***What happens if my certificate expires?***

- Make an appointment at a [GSA Credentialing Center](#) to reset the PIN.
- Visit a bureau/office light activation station (LAS)
- If your computer is Windows 7 and your bureau has purchased and installed ActivClient the PIN can be reset at your desktop.

### ***What do I do if I see multiple certificates when I login?***

The DOIAccess card can contain up to four certificates. Each certificate is used for one or more network accounts, for digital signatures or for email encryption. There may be up to 4 certificates. Hover the mouse cursor over your name on each Certificate. A pop up: "Government PIV Authentication Key" will identify the certificate to select.

### ***When does my DOIAccess card expire?***

The expiration date of the card is written on the front of the card. The DOIAccess cards (separate from the certificates on them) expire every 5 years and must be completely replaced. A new photograph will be taken, fingerprints, and two forms of ID will be required. Do not leave either PIV certificate or PIV card renewal to the last minute.

- Make an appointment at a [GSA Credentialing Center](#) to get a new card..
- Visit a bureau/office light activation station (LAS) to get a new card

## Active Directory and Authentication [\(back to Table of Contents\)](#)

### ***How will the altSecurityIdentities LDAP attribute be populated?***

Currently the altSecurityIdentities field must be manually populated. In the future, DOIAccess will automatically populate this field.

### ***How will the administrative accounts be mapped to my PIV Card for authentication?***

These will be manually configured similar to the standard accounts.

### ***What is the format of the altSecurityIdentities field to enable PIV Authentication?***

0.9.2342.19200300.100.1.1 = 14001000906502

CN = ALBERT EINSTEIN

OU = National Park Service

OU = Department of the Interior

O = U.S. Government

C = US

## Applications [\(back to Table of Contents\)](#)

### ***What applications will still require passwords?***

Until they are PIV enabled, many applications still require use of login ID and password, including but not limited to

- BisonConnect outside DOI facilities,
- Quicktime,
- DOI Learn,
- FPPS,
- Citrix
- Bureau specific applications that require passwords

PIV Enabled:

- Concur-Government Edition (CGE)
- MAX portal
- FBMS
- others

### ***Can Citrix or similar Virtual Desktop Environment (VDI) be used with PIV for remote access?***

Citrix is one of the applications that will be PIV enabled in the future. Citrix is a remote access application that views screenshots of data and applications on servers inside DOI data centers. Some federal agencies have PIV enabled Citrix. Each bureau with Citrix farms will need to configure Citrix for PIV access as part of the 3-5 year plan to move all applications to PIV authentication.

### ***When I login to Windows, will applications like SharePoint still use the 'Use Current Logon Credentials' feature that acts somewhat like single-sign-on?***

Yes. Whether you use your PIV card or your username and password, the "pass through authentication" in SharePoint and similar applications and websites will not change as long as you are logged in from inside DOI facilities. From within DOI facilities DOI Access credentials will continue to be passed to those sites/applications.

## Mobile Devices, Remote Access and VPN [\(back to Table of Contents\)](#)

### ***Can I use my personal equipment to remotely access the DOI network for work activities?***

DOI's Security policy and Control Family documentation requires explicit approval for external access (including the use of non-GFE (non-Govt. Furnished Equipment or Personally Owned Equipment)) to any DOI systems. There are a number of security issues with permitting non-GFE to access BisonConnect so at this time the risk has not been accepted and no explicit permission has been granted for BisonConnect.

### ***DOI VPN error: "Invalid username or password. Please re-enter your user information."***

The wrong username is being passed to the VPN when using your PIV Card. This typically indicates that either you are trying to use the wrong certificate or the PIV Card is not properly configured and may need to be updated in USAccess. Try another certificate and if that doesn't work call your help desk.

### ***When logging into the DOI VPN the error: "You are not authorized to log in, please contact your system administrator" comes up. Why?***

Your Active Directory administrator has not added you to the correct group, to allow you to use the VPN. Please contact your helpdesk for resolution support.

### ***When using the Network Connect software seems unresponsive or does not work. Why?***

The Juniper VPN is designed to operate in the background with minimal configuration on the client. ESN recommends that users connect to the VPN using their web browser and allowing the VPN to launch Network Connect. DOI Access Card authentication is complex and using advanced security development built into web browsers works much better than using the Network Connect software to authenticate.

### ***What happens if I have a mobile device that doesn't have a card reader?***

There are card readers available for most types of government furnished mobile devices. Each bureau help desk has information on the mobile devices used within the bureau.