Login.gov Authentication Training

External (Non-FTA) users

TAD-20

Federal Transit Administration

TBD

Please record this session

U.S. Department of Transportation
Federal Transit Administration

Agenda

- Why Are We Offering This Training?
- Why Login.gov?
- What is Multi-Factor Authentication?
- Login.gov Authentication options
- Live Demonstration

Why Are We Offering This Training?

- FTA is changing the way TrIAD external users sign into the TrIAD (Transit Integrated Appian Development) platform.
  - This platform includes the **TrAMS, NTD, JPC, SSOR, DGS, Transit COVID-19 Response Program, FACES,** and **Appian OTrak** applications.
- This change affects all **external users** (non-FTA users).
  - Examples: Recipients, Reporters, Contractors, etc.
- After September 10th, external users are required to register their email accounts in **Login.gov** and set up at least one Multi-Factor Authentication (MFA) solution to access the TrIAD platform. External users will be redirected to use Login.gov authentication instead of Appian username/password authentication.

Why Login.gov?

- A Presidential Executive Order requires all Federal agencies to implement multi-factor authentication.
- Login.gov provides users with one account to access multiple digital services and protects user accounts with strong multi-factor authentication options.
- Login.gov is a common federal multifactor authentication solution used by several other systems (e.g. USA Jobs, SAM.gov), and many users already have Login.gov accounts.

What is Multi-Factor Authentication?

- **Multi-factor Authentication** (**MFA**) is an authentication method that requires the user to provide two or more verification factors to gain access to a system or resource.
- In addition to a password, Login.gov requires users to set up at least one secondary authentication method to keep the account secure.

Authentication options provided by Login.gov

- Login.gov provides the following authentication options:
  - PIV (personal identity verification) cards or CACs (common access cards)
  - Security Key
  - Authentication Application (e.g., Google Authenticator, Authy, LastPass, 1Password)
  - Text Message/ Phone Call
  - Backup Codes

LIVE DEMO

Frequently Asked Questions

Question	Answer
How do I reset my Login.gov password?	If a user forgets their password, then the user can use the “Forgot password” link in Login.gov sign-in page. Please refer at slide 20.
How do I access my account if I don’t have access to any of the multi-factor authentication methods? For ex: I changed my mobile number (or) I have uninstalled Authenticator app	If a user no longer has access to their multi-factor authentication methods, they can delete their Login.gov account and re-register at Login.gov. Please refer to slide 21 for instructions.
What happens If a user enters an incorrect password multiple times?	• You will be unable to login for a few minutes if you have incorrectly entered your password 6 times. • You will be unable to login for 10 minutes if you have incorrectly entered your security code 3 times. • You will be unable to login for 10 minutes if you request more than 10 security codes in a 5 minute time period. • After several unsuccessful attempts, a user will be locked out for 24hours. https://www.login.gov/help/ for additional assistance logging in through Login.gov
What happens if a user attempts an incorrect MFA authentication password multiple times?	After 3 wrong password attempts, user will be locked out for 10 mins.

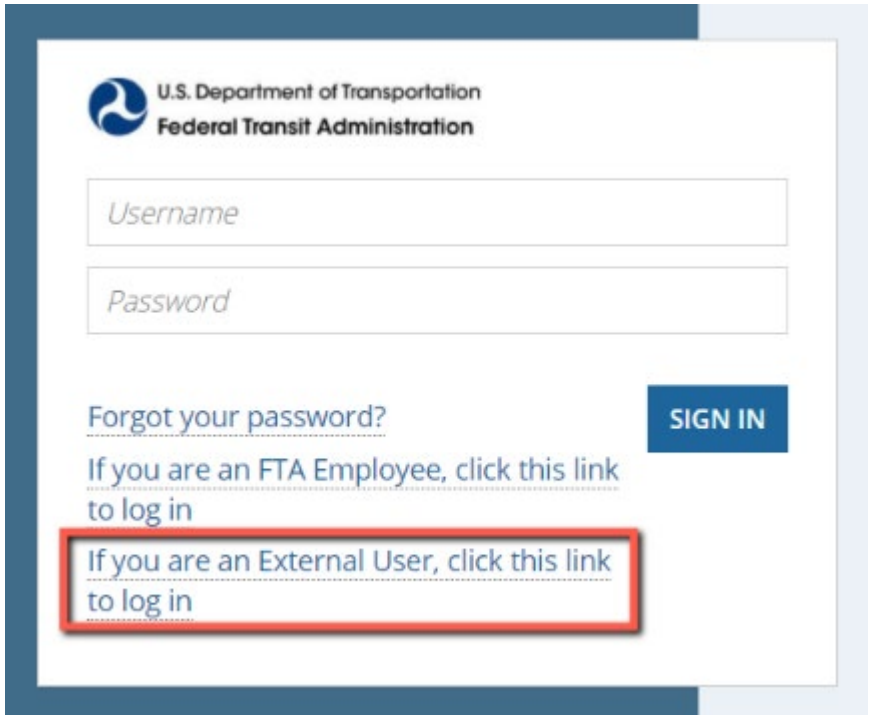
Frequently Asked Questions

Question	Answer
What is the email address I should use to register in Login.gov?	You must use the username that you use to access FTA applications. For ex: if you use, John.Smith@abcd.com to login then you must use that email address to register at Login.gov
I already have an account in Login.gov. Should I create another account?	If your Login.gov email address and the TrIAD (TrAMS, NTD etc) username is same, then you can use the same account to access the FTA applications.
What if a user has a Login.gov account with a different email address?	1.Go to https://secure.login.gov/ 2.In the Email preference section there is an + Add email button, click that button. You can also see that option on left-hand menu "Add email address" 3.If prompted, re-enter password and authentication code 4.Enter the additional email address you would like to associate with your Login.gov account 5.Verify that new email address in the email sent to that inbox 6.Repeat these steps for each additional email addresses you would like to associate to your login.gov account 7.Once the TrIAD email address is added to the Login.gov profile, user must use TrIAD email address when trying to access TrIAD platform
Can I recover my account if I lose my MFA authentication method/ password?	Login.gov is unable to grant you access to your account if you get locked out and/or lose your authentication method(s). You will have to reset the account by following the instructions on slide 21.
Where can I find training materials?	You can visit https://www.transit.dot.gov/fta-web-policies/web-policies/fta-logingov for additional training materials
Where can I find additional Login.gov help?	Go to https://www.login.gov/help/ for additional Login.gov assistance
Who should I contact incase of issues?	If you have any questions or issues, then please reach out to FTA IT Help Desk at FTAITHelpDesk@dot.gov

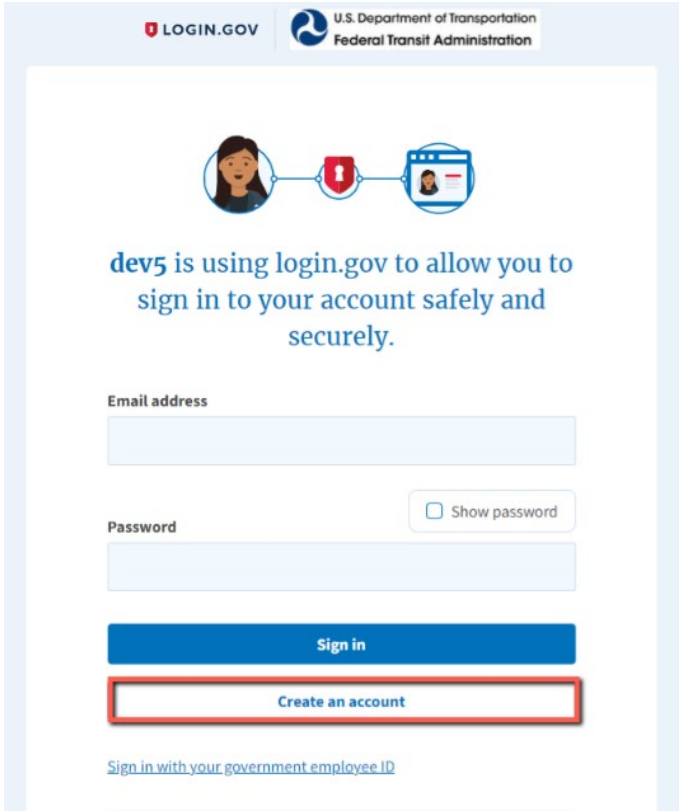
DEMO SLIDES

Login.gov Registration

1. Go to https://faces.fta.dot.gov/
2. Click on “If you are an External User, Click This Link to Login.

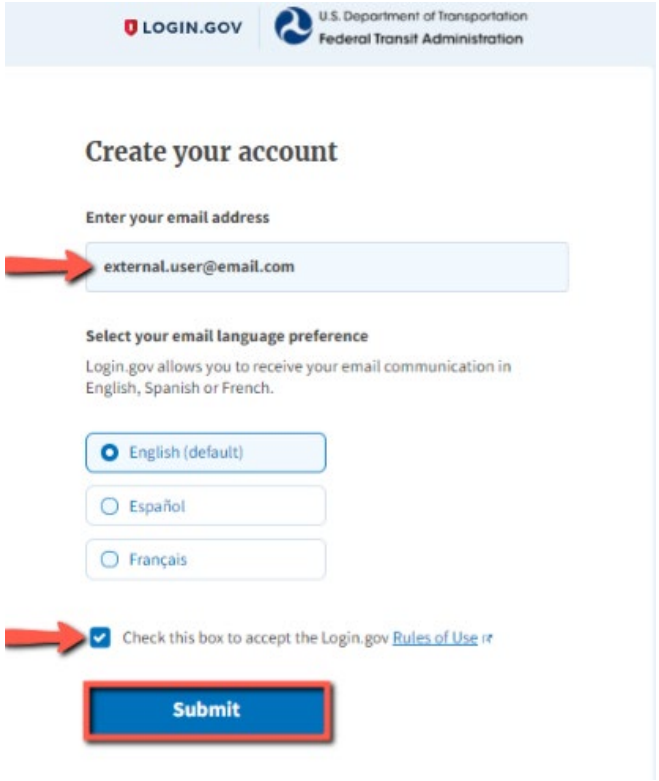


3. Click on Create an account.

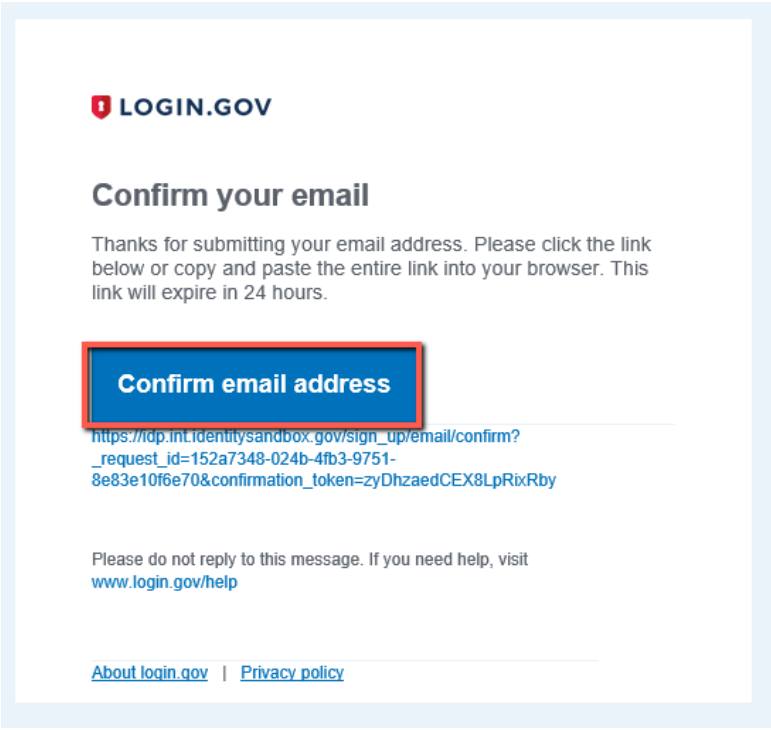


Creating Login.gov Account

4. Enter your email address and check the Rules of Use box.

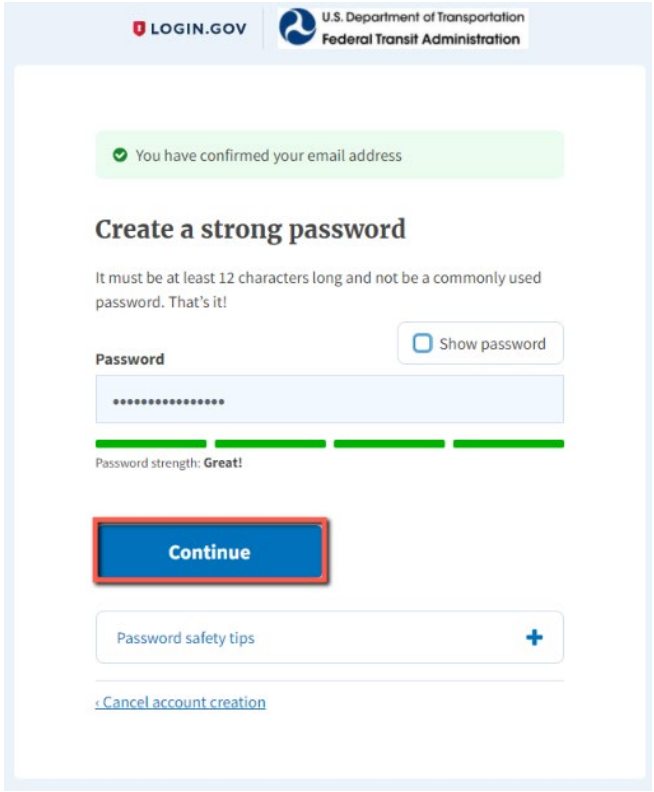


5. Look for “Confirm Your Email” email from Login.gov and click on Confirm email address.

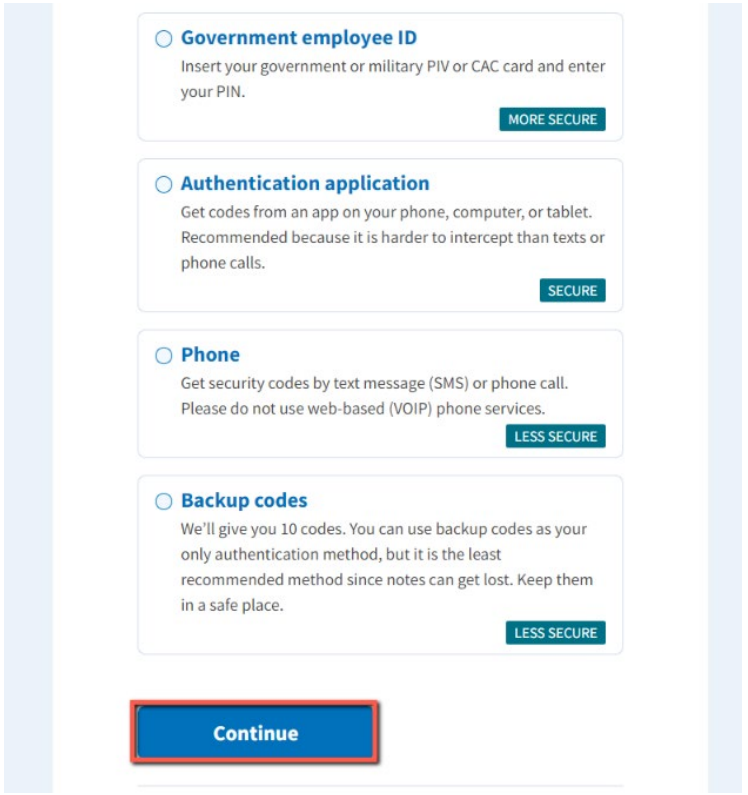


Setting up Login.gov Account

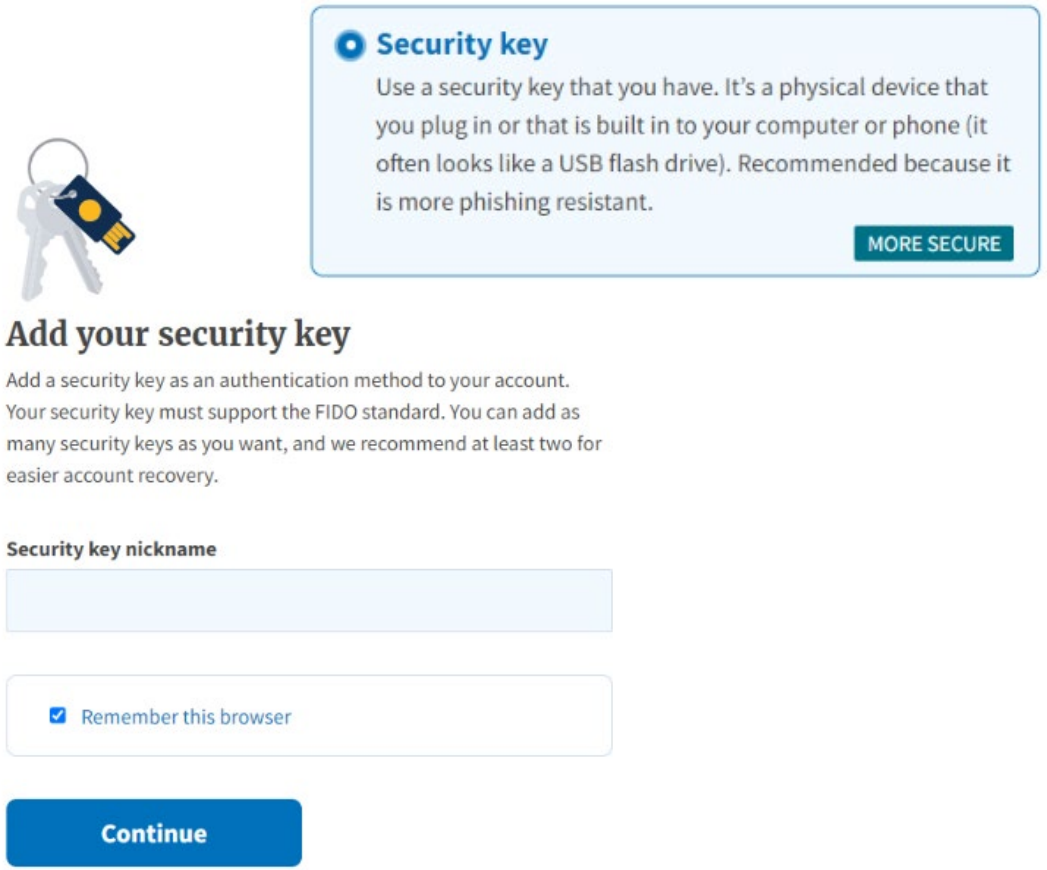
6. Create a strong password.



7. Select an Authentication method setup and follow setup instructions. Slides 15-19 provide additional information for each method.



Authentication Methods – Security Key

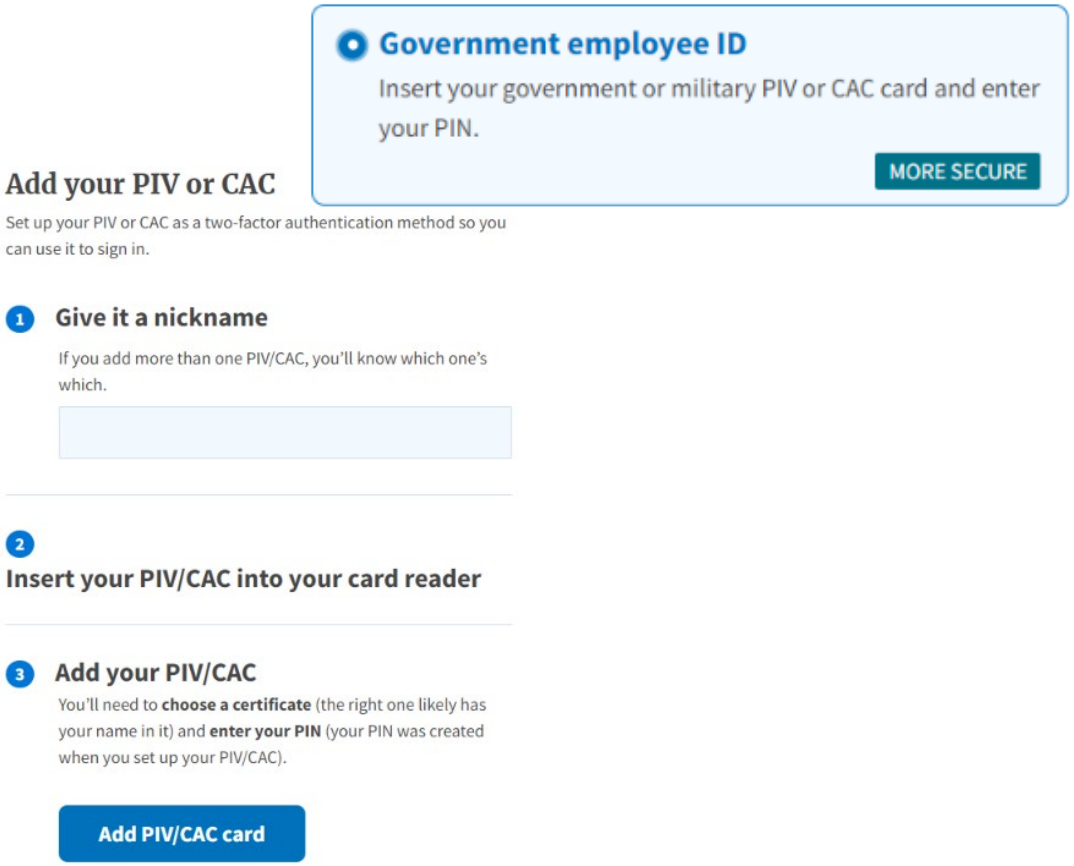


A security key is typically an external physical device, like a USB, that you plug into your computer. The key is linked to your accounts and will only grant access to those accounts once the key is plugged in and activated.

Login.gov requires security keys that meet the FIDO (Fast Identity Online) standards.

To use this secure option for login.gov authentication, plug the key into a USB port and assign the key a name to identify it with your login.gov account. The next step will ask you to activate your key. This is generally done by pressing a button on the key itself.

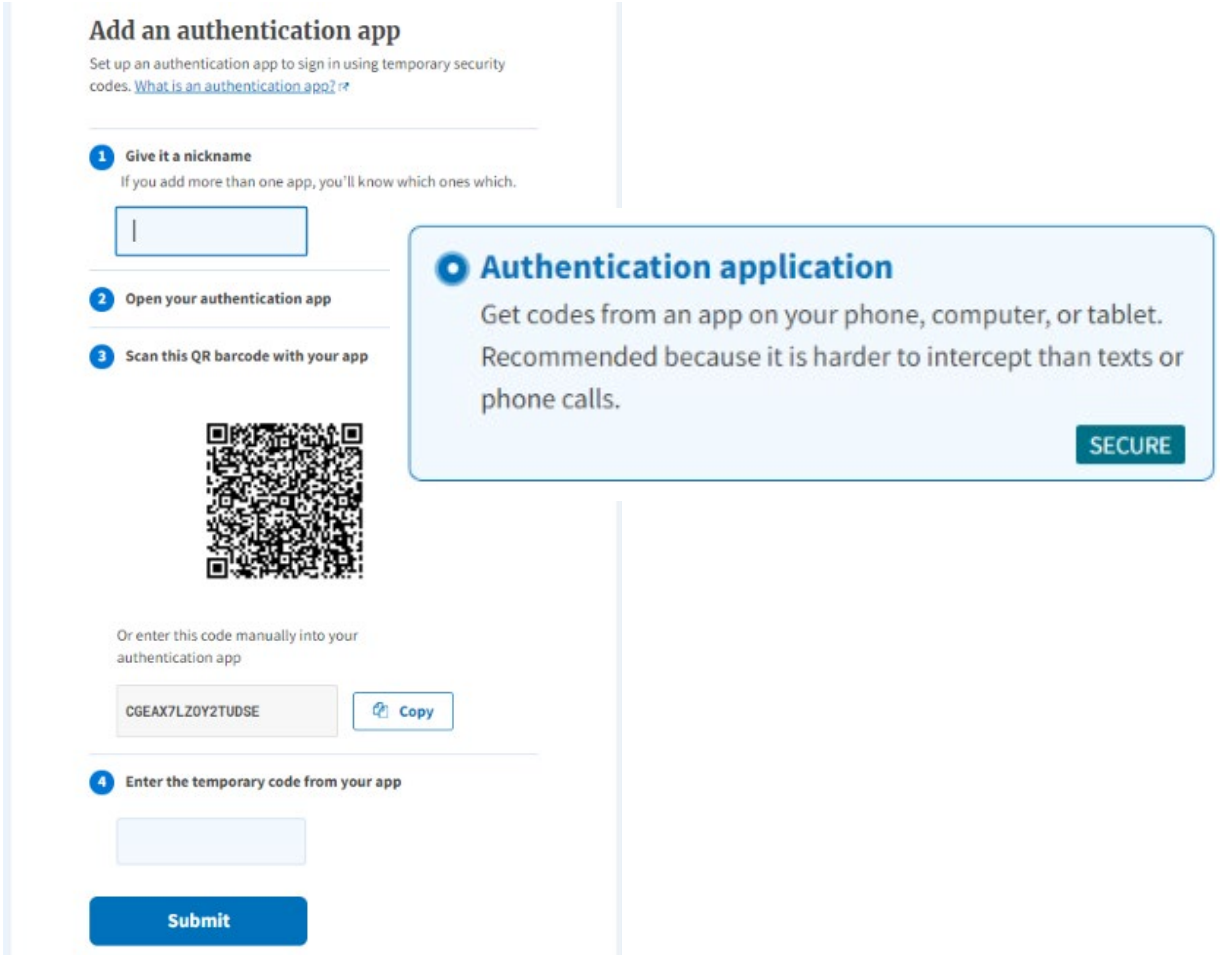
Authentication Methods – Gov’t Employee ID



Physical PIV (personal identity verification) cards or CACs (common access cards) are secure options for federal government employees and military personnel. These cards, with encrypted chip technology, are resistant to phishing and difficult to hack if stolen.

15

Authentication Methods – Authentication App



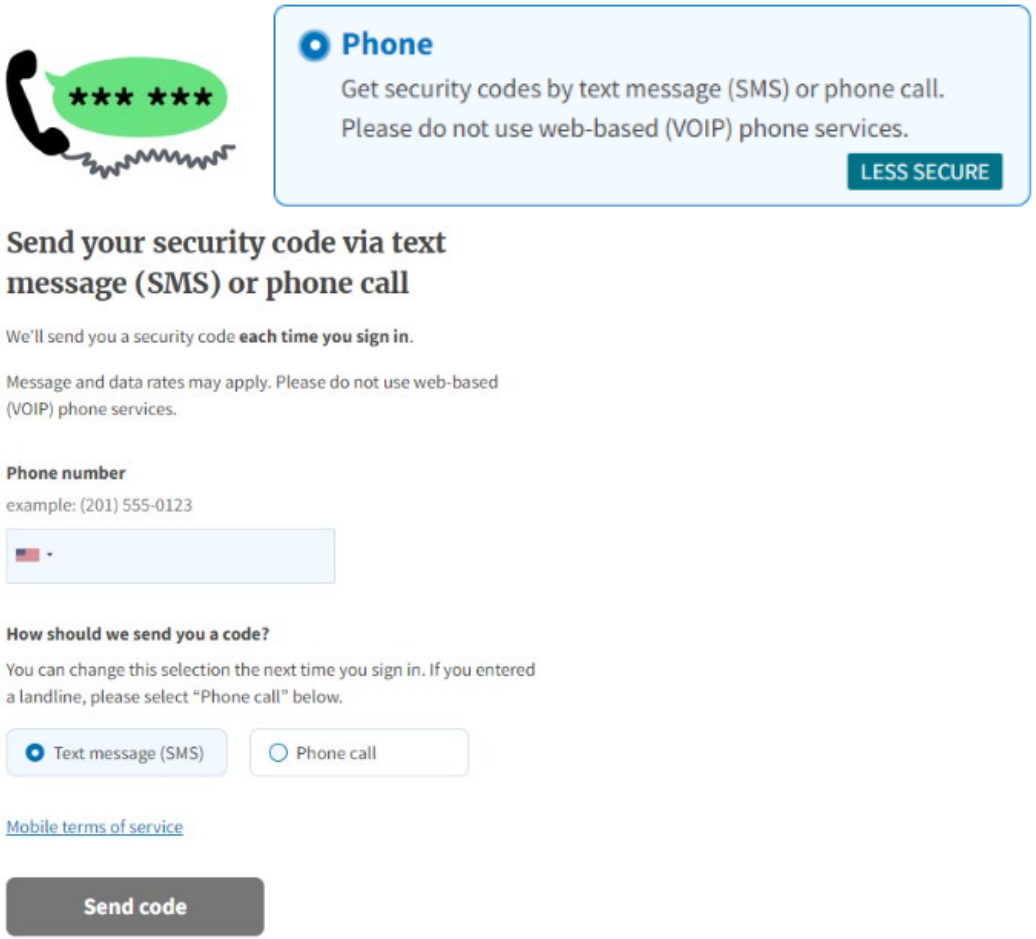
Authentication applications are downloaded to your device and generate secure, six-digit codes you use to sign into your accounts.

- Google Authenticator
- Authy
- LastPass
- 1Password
- OTP Manager
- Authenticator

This method offers more security than phone calls or text messaging against phishing, hacking, or interception.

A one-time passcode generated by the application each time you sign in to login.gov.

Authentication Methods – Phone



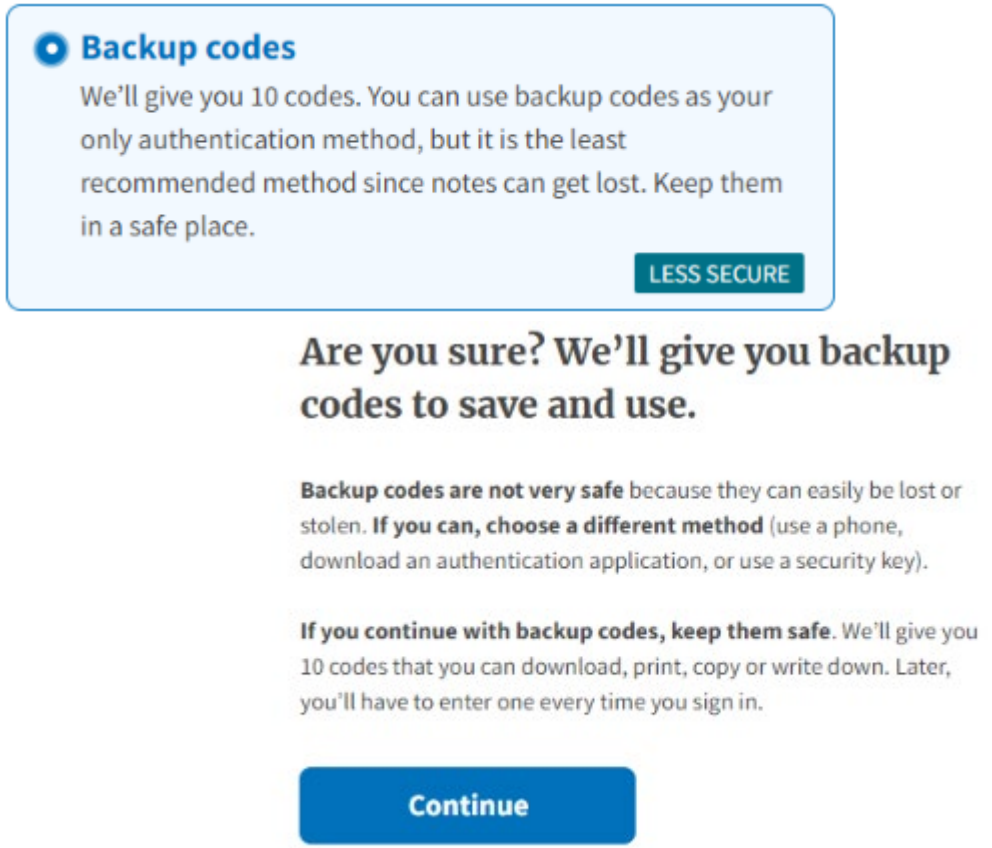
If you choose to use this less secure option, enter a phone number at which you can receive phone calls or text messages. If you only have a landline, you must receive your security code by phone call. *Login.gov cannot send security codes to extensions or voicemails.*

A unique security code is sent to that phone number each time you sign in to your login.gov account. Each security code expires after ten minutes and can only be used once.

After you receive the code, type it into the "one-time security code" field.

You will receive a new security code each time you sign in to your login.gov account.

Authentication Methods – Backup Codes



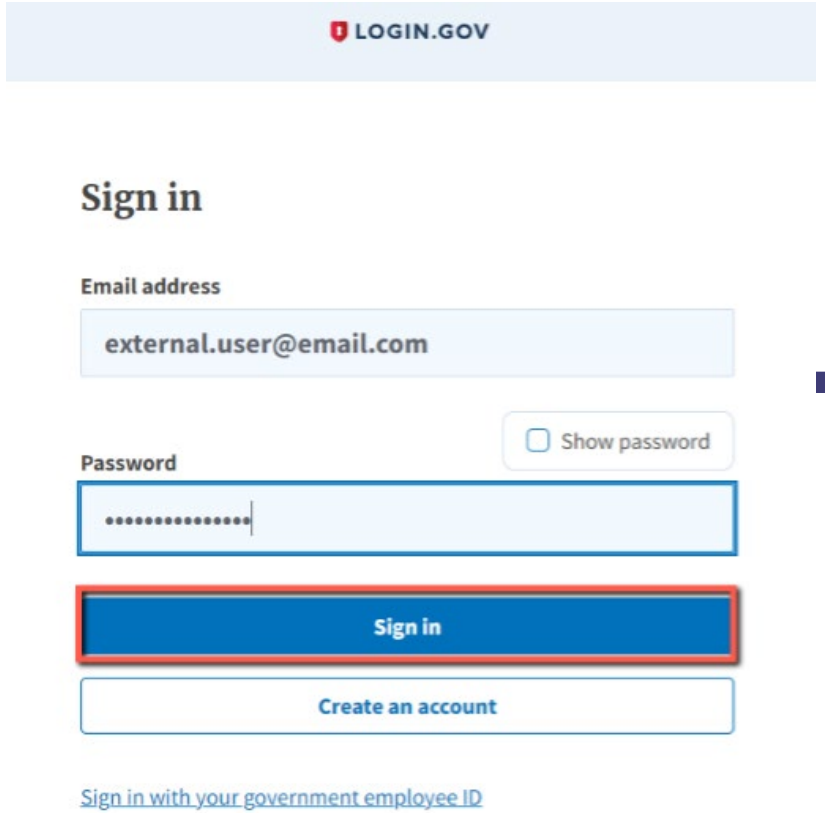
Backup codes are an accessible option for users who do not have access to a phone that can either be direct-dialed or receive text messages. However, backup codes are the least secure option for two-factor authentication.

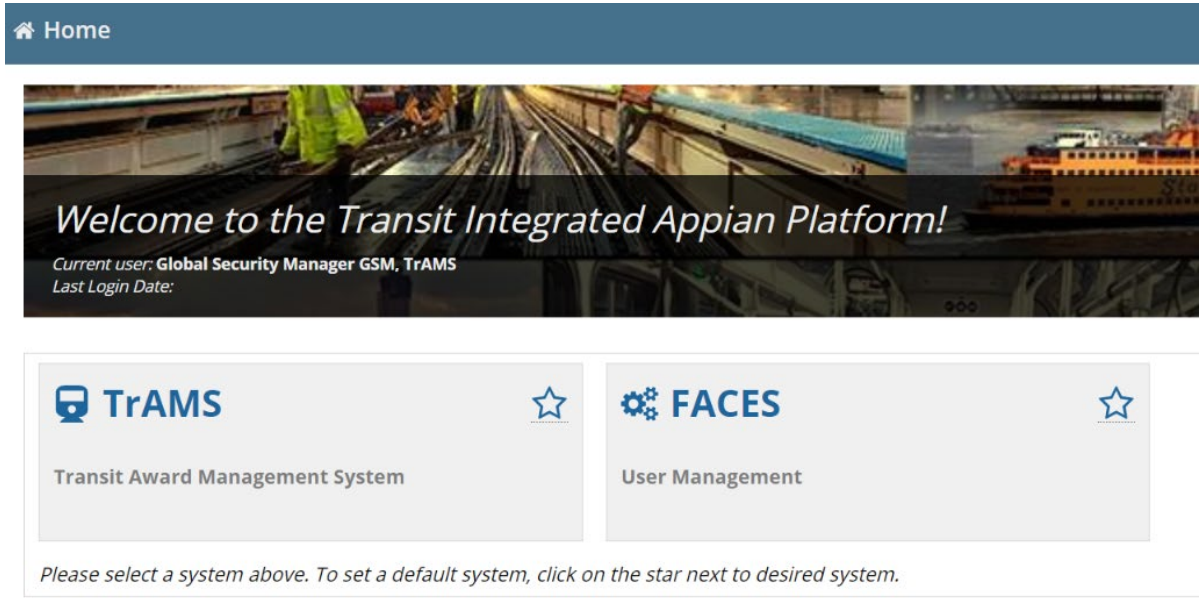
login.gov will generate a set of ten codes. Backup codes must be printed or written down which makes them more vulnerable to theft and phishing.

After you sign in with your username and password, you will be prompted for a code. Each code may be used only once. When the tenth code has been used you will be prompted to download a new list.

Sign In to Login.gov

8. Sign in using credential you just created

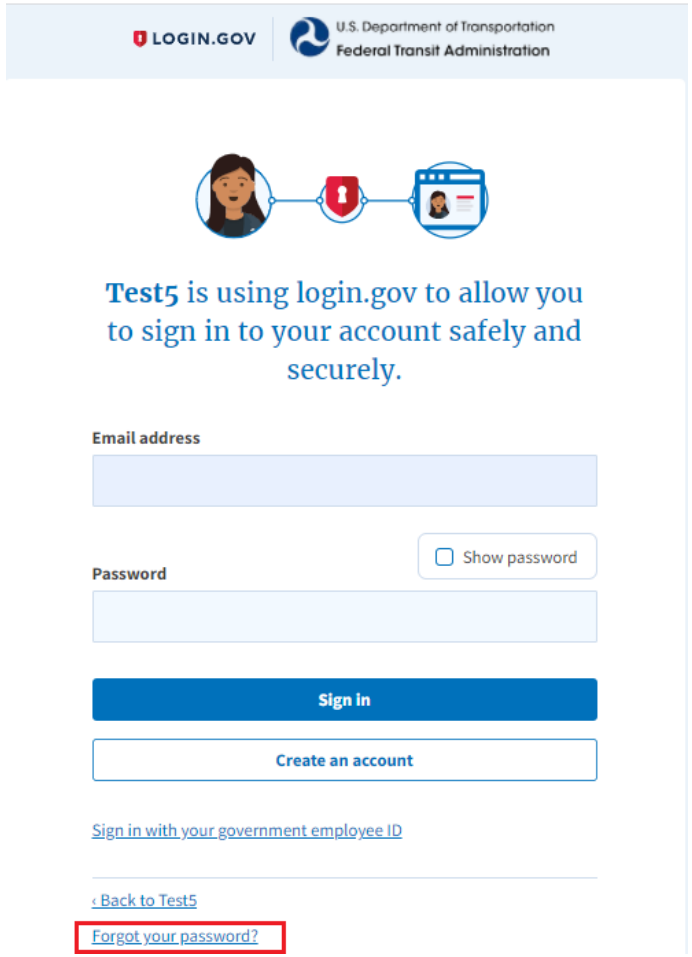


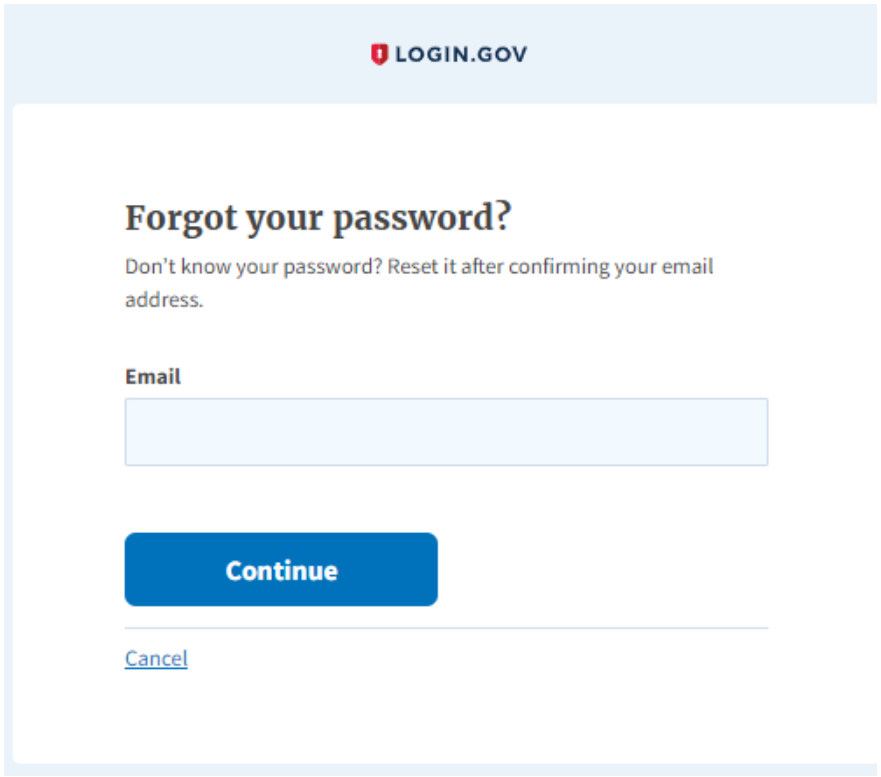


19

Forgot password

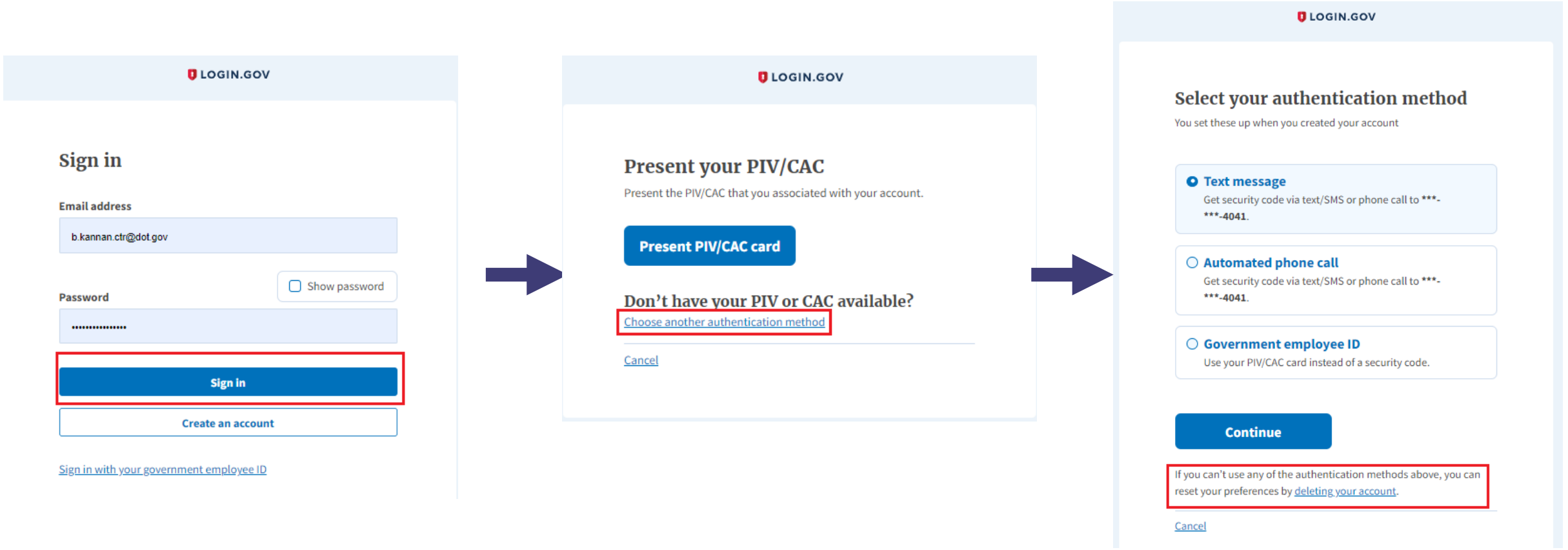
https://www.login.gov/help/trouble-signing-in/forgot-your-password/





How to reset my account

https://www.login.gov/help/manage-your-account/delete-your-account/



Questions

TRANSIT.DOT.GOV