

Session #56

Two-Factor Authentication

Steven Burke & James McMahon
U.S. Department of Education



START HERE
GO FURTHER
FEDERAL STUDENT AID®

Project Overview

To comply with the White House through the United States Office of Management and Budget (OMB) mandate, Memorandum M07-16 attachment 1, and as part of our ongoing efforts to ensure the security of Federal Student Aid data systems, the U.S. Department of Education is required to implement a security protocol through which all authorized users will enter two forms of “authentication” to access Federal Student Aid systems via the Internet.

This process is referred to as Two-Factor Authentication (TFA).

Post-Secondary School Federal Financial Aid Eco-System

- 6,400 unique institutions of higher education
- Over 3,000 financial partners
- Over 90K privileged accounts
- Over 70-million unique identities
- Over 320-million loans
- Over 96-million grants
- Supporting students in 35 countries
- \$1T loan book
- Over 13M students
- Over 30M aid awards
- Over \$120B injected into the eco-system each year

FSA

- Staff: ~1,300
- Contractors: ~ 10,000
- Services
 - Aid Apps
 - Grants
 - Loan Origination
 - Loan Servicing
 - Debt Collection
 - Compliance

Cost of a Breach



Theft of Credit
Card
Information



E-mail Account



Full Identity
(name, SSN,
address, etc.)



Bank Account
Information



Individual Loss



Keyloggers, Malicious Threats

- Keyloggers
 - What is it?
 - What can be captured?
 - How does it exploit?



Two-Factor Authentication Scope

- Provide safe and secure access to FSA network services
- Encompasses all FSA, Dept. of Education, and partners
 - Postsecondary Schools and Sub-Contractors
 - Guaranty Agencies
 - Servicers/PCA's/NFPs
 - Call Centers
 - Developers/Contractors and Sub-Contractors
- TFA project is focused on privileged users
 - A privileged user is anyone who can see more than just their own personal data

What is Two-Factor Authentication?

Something that you know is the First Factor:

User ID and Password

Something that you have is the Second Factor:

Token with a One Time Password

- The One Time Password (OTP) will be generated by a small electronic device, known as the TFA Token, that is in the physical possession of the user
- To generate the OTP, a user will press the “power” button on the front of the token
- A different OTP will be generated each time the button is pressed
- *Alternative Methods of obtaining OTP without TFA Token:*
 - A) Answer 5 Challenge Questions online
 - B) Have the OTP sent to your Smart Phone



How do I Register my Token?

- Once you receive your token you must register it for each system for which you have access to and utilize
- Each FSA System website will be slightly different when logging in and registering your token

Next Steps:

Click on the following link:

<https://fafsa.ed.gov/FOTWWebApp/faa/faa.jsp>

Then click on the [Register/Maintain token](#) URL on the top right hand side of the screen.

Login - FAA Access to CPS Online

[Edit Account](#) [Change Password](#) [Register/Maintain Token](#)

* User ID:

* Password:

The virtual keyboard can be used in conjunction with your keyboard. The value of the key will be entered by clicking on the key on the keyboard.

This is a U.S. Federal Government owned computer system, for the use by authorized users only. Unauthorized access violates Title 18, U.S. Code Section 1030 and other applicable statutes. Violations are punishable by civil and criminal penalties. Use of this system implies consent to have all activities on this system monitored and recorded, which can be provided as evidence to law enforcement officials.

TFA Profile Information

- **Step One** – Enter general identifying profile information
 - If you ever forget your assigned password or misplace your token, you may choose to complete the cell phone information to receive this information via “text” message

The screenshot shows a web form titled "New Token Registration" with a "Help" link and a red asterisk indicating required fields. Below the title is a text box with instructions: "To register your credential, please fill out the following required information and click on the 'Submit' button." The form is divided into "Step One: Enter Profile Information" and contains the following fields:

- * First Name: ?
- * Last Name: ?
- * Office Desk Number: ?
- Cell Phone Number: ?
- Confirm Cell Phone Number: ?
- * Email: ?



Register Token Serial Number

- **Step Two** – Enter the Token Serial Number located on the back of the token
 - The credential will begin with three letters and nine numbers (i.e. AVT8000000000)



**VIP Security Token
(Model HAI08)**
The credential ID is on the back of the token.

Step Two: Enter Token Serial Number

Note: The Token Serial Number is the letter and numbers that are followed by S/N located on the back of the token.

* Serial Number (S/N):



* Confirm Serial Number:



TFA Challenge Questions

- > **Step Three** – Complete five separate questions and responses
 - You may not repeat questions nor may any question have the same response

Step Three: Choose Challenge Questions and Enter Responses

Note: You must choose 5 different questions and your answers cannot be duplicated.

* Question 1:	<input type="text" value="Select from the list below."/>	
* Answer 1:	<input type="text"/>	
* Question 2:	<input type="text" value="Select from the list below."/>	
* Answer 2:	<input type="text"/>	
* Question 3:	<input type="text" value="Select from the list below."/>	
* Answer 3:	<input type="text"/>	
* Question 4:	<input type="text" value="Select from the list below."/>	
* Answer 4:	<input type="text"/>	
* Question 5:	<input type="text" value="Select from the list below."/>	
* Answer 5:	<input type="text"/>	



TFA Terms of Service

Step Three continued – You must read the Terms of Service before checking the acknowledgment statement and proceeding

Step Three: Read and Agree to the Terms of Service

1. Read the entire Terms of Service and arrive at the bottom of the scrollable area below.
2. Read the paragraph under the Terms of Service and select the associated checkbox if you understand, agree, and accept the statement.
3. Click an action button at the bottom of the page to accept or reject the Terms of Service.

- You are accessing a U.S. Government information system, which includes (1) this computer, (2) this computer network, (3) all computers connected to this network, and (4) all devices and storage media attached to this network or to a computer on this network. This information system is provided for U.S. Government-authorized use only.
- Unauthorized or improper use of this system may result in disciplinary action, as well as civil and criminal penalties.

- I acknowledge receipt of, understand my responsibilities, and will comply with the 'Terms of Service' for the Department of Education Systems I access. I understand that failure to abide by the above rules and responsibilities may lead to disciplinary action up to and including dismissal. I further understand that violation of these rules and responsibilities may be prosecutable under local, State, and/or Federal law.

SUBMIT



START HERE
GO FURTHER
FEDERAL STUDENT AID

TFA – Security Code

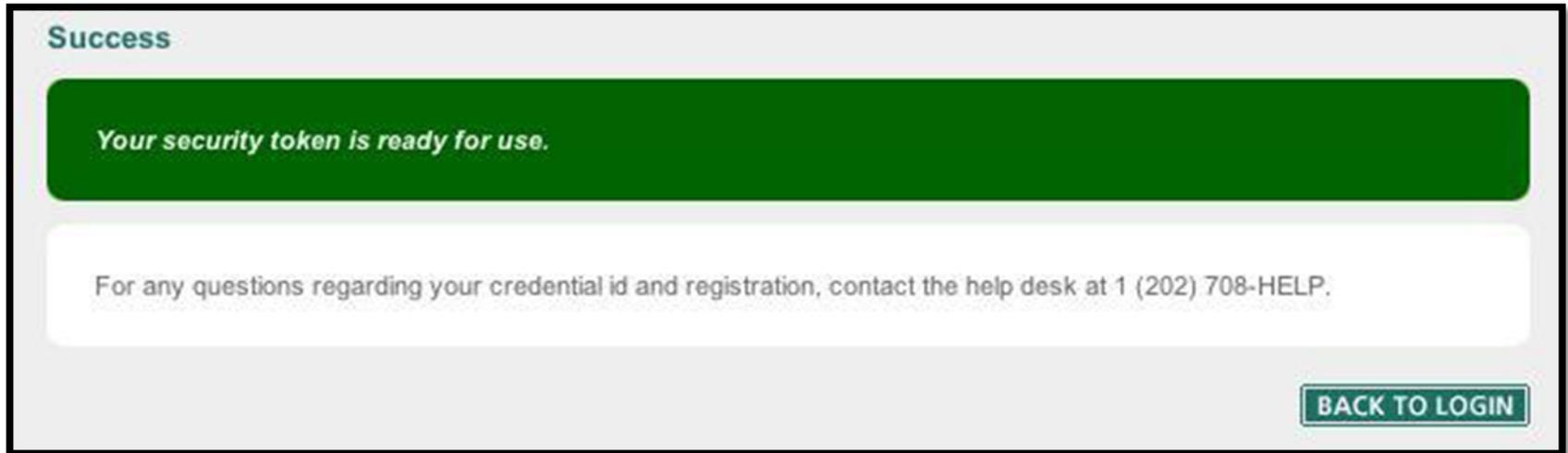
- You will then be directed to the security code entry screen

A screenshot of a web application interface titled "Security Code Entry". The page has a light gray background. At the top right, there is a "Help" link. The main content area is white and contains the following text: "To check and verify your VIP Credential, generate and enter two consecutive security codes in the input fields below. To enter the second security code, wait for the display to clear then press and release the button. Click the 'Submit' button to synchronize the current token or the 'Back to Main' button to return to the main menu." Below this text are two input fields, "Security Code #1:" and "Security Code #2:", each followed by a yellow bar representing the input field. To the right of each input field is a small question mark icon. At the bottom right of the form, there are two buttons: "BACK TO LOGIN" and "SUBMIT". Two red arrows point from the security tokens on the left to the input fields in the screenshot.

- You must enter two consecutive security codes successfully
- A new code is generated once every 30 seconds and will require you to click the "On Button" in between attempts

TFA Registration Complete

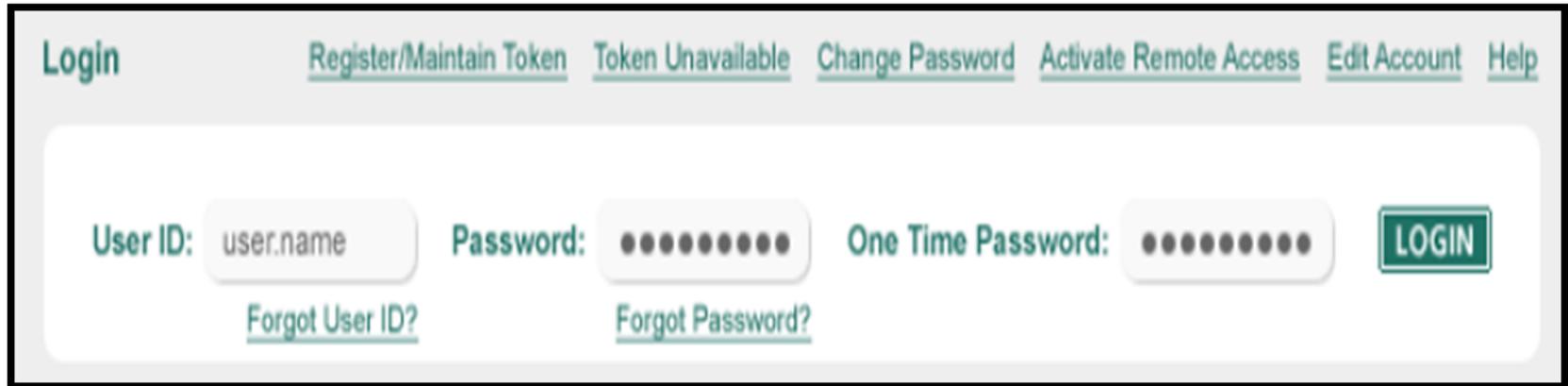
- Registration Completion – When successful you will receive confirmation and your security token will now be ready for use



The screenshot shows a success message in a light gray box. At the top left, the word "Success" is written in a teal font. Below it is a large green rounded rectangle containing the text "Your security token is ready for use." in white. Underneath the green box is a white rounded rectangle containing the text "For any questions regarding your credential id and registration, contact the help desk at 1 (202) 708-HELP." in gray. In the bottom right corner of the gray box is a teal button with the text "BACK TO LOGIN" in white.



TFA Login Process



The screenshot shows a login interface with the following elements:

- Navigation Links:** [Login](#), [Register/Maintain Token](#), [Token Unavailable](#), [Change Password](#), [Activate Remote Access](#), [Edit Account](#), [Help](#)
- Input Fields:**
 - User ID:** A text input field containing "user.name" with a [Forgot User ID?](#) link below it.
 - Password:** A password input field with 10 dots, with a [Forgot Password?](#) link below it.
 - One Time Password:** A text input field with 10 dots.
- Action:** A green **LOGIN** button.

- Once your token is registered you must log in using both factors of authentication:
 - Factor One – Assigned User ID and Password
 - Factor Two – One-Time generated Password (OTP)



Primary Systems Impacted Across the Enterprise

- CPS FAA Web Access 04/20/2011
- COD 10/23/2011
- NSLDS move Behind AIMS 12/18/2011
- FSA Financial Management System (FMS) 02/12/2012
- SAIG/EDconnect 02/12/2012
- Ombudsman 02/12/2012

TFA – Token Deployment Status

- ❑ Phase 1 FSA – Citrix users 1,300 completed 5/1/2011
- ❑ Phase 2 Dept. of ED Staff 5,200 completed 7/1/2011
 - ❑ FSA Contractors completed 10/28/2011
- ❑ Phase 3 International users at Foreign Schools
 - ❑ Group 0 – Foreign Schools
 - ❑ 650 confirmed users 11/28/2011
 - ❑ Group 0 – DeVry University
 - ❑ 820 confirmed users 11/28/2011
 - ❑ Group 1 – DC, DE, MD, VA, WV
 - ❑ 2,622 estimated users
 - ❑ Complete attestation and ship tokens by 12/31/2011
 - ❑ Groups 2-9 11/16/2012



Token Deployment Schedule 2011-12

Group	Implementation	Scope
Group 1	Q4 2011	DC, DE, MD, VA, WV
Group 2	Q1 2012	NC, NJ, NY, SC
Group 3	Q2 2012	KY, MI, NE, NH, OH, PA, RI, VT
Group 4	Q2 2012	CA, FL
Group 5	Q3 2012	AK, ID, MN, ND, OK, OR, SD
Group 6	Q3 2012	AR, CO, GA, KS, MO, MS
Group 7	Q3 2012	AZ, CT, IA, IL, IN, LA, TX
Group 8	Q4 2012	AL, AS, FC, FM, GU, HI, MA, ME, MH, TN
Group 9	Q4 2012	MT, NM, NV, PR, PW, UT, WA, WI, WY

Two-Factor Authentication Next Steps

Action Items and Next Steps (Internal)

- Contractor/Vendor attestation of Developers, Testers, and Call Center Representatives (CSRs)
- FSA Project Team to provide information on confirmation processes, TFA training, and tokens
- Contractor/Vendor are to register tokens
- FSA to TFA Enable Systems

Action Items and Next Steps (External)

- Primary Destination Point Administrator (PDPA) and COD Security Administrators (CSA) attestation of FAA, Servicers and Guaranty Agencies, etc., associated with their account and who are working on behalf of their institution
- FSA Project Team to provide information on confirmation processes, TFA training, and tokens
- Institutions are to register tokens

Contact Information

We appreciate your feedback & comments.

Steven Burke

- Phone: 202-377-4683
- E-mail: TFA_Communications@ed.gov