



USACCESS Program

# Blue Top Newsletter

## Upcoming Meetings and Training

Meeting/Training	Date & Time (EST)	Location	Dial-In Info
Registrar Classroom Training	Wed and Thu Mar 18-19 Apr 8-9	HP Chantilly, VA	Contact Jim Schoening for information or to Register
CAB	Thu, Apr 2 9:30 to 12:00	Grant Thornton 333 John Carlyle Dr., Alexandria, VA 4th Fl. Conf. Rm	No Telecon Provided
User Group	Tue, Apr 21 9:00-12:00	GSA Central Office 1800F St. NW Conference Rm. 3046	888-455-1864 Passcode: USER GROUP

Special Points of Note:

Now found on  
[www.fedidcard.gov](http://www.fedidcard.gov):

- > Service Order Requests and Test Card Orders
- > Role Holder Web Based Training Registration
- > Deployment Activities and USAccess Center Status Alert
- > Contact Steve Sill ([Stephen.sill@gsa.gov](mailto:Stephen.sill@gsa.gov)) to be added to User Group (UG) distribution list.
- > Contact Jim Schoening ([jim.schoening@gsa.gov](mailto:jim.schoening@gsa.gov)) for Registrar Classroom Training sign up

## Tri-Interface Cards to be Removed from Approved Products List (APL) December 2015

This is a reminder that the tri-interface cards (Cards with the 125 MHz coil) issued by the USAccess PIV program will be removed from the FICAM APL in December 2015.

Removal of these tri-interface cards from the APL means the USAccess Program can no longer print new tri-interface credentials for a USAccess customer starting in January 2016. Tri-interface cards that were printed (but not activated) before January 2016 can still be activated, and any existing active tri-interface cards in the field will not be terminated and will remain active until the card expiration date printed on the front of the card.

The GSA MSO realizes that several Agency customers use tri-interface cards with their existing PACS/LACs systems, and discontinuing this type of PIV credential has impact on Agency IT infrastructures.

The MSO has reached out to impacted Agencies, and can provide a list of Agency credential holders who were issued a tri-interface credential.

If you have any questions on this, please contact Matt Arnold at [matthew.arnold@gsa.gov](mailto:matthew.arnold@gsa.gov).

### Inside this issue:

Training Calendar	1
Spotlight Articles	1-3
Service Enhancements	4
Security Tip	5

### *NIST Workshop Recap*

The NIST Workshop on Special Publications (SPs) Supporting FIPS 201-2 was held on March 3-4 in Gaithersburg, MD. Presentations were given on recent changes to SPs, future changes to existing SPs, and the status of forthcoming SPs. Focus was mainly on Physical Access Control Systems (PACS), authentication mechanisms, ways to improve authentication, and derived credentials. Steve Sill gave a presentation on Chain-of-Trust in the shared service environment as it relates to the forthcoming draft SP 800-156 (Representation of PIV Chain-of-Trust for Import and Export).

NIST will be posting the slides used during the presentation to IDManagement.gov in the coming weeks.

### *Derived Credentials Working Group and Industry Day updates*

The MSO hosted the inaugural meeting of the new USAccess Derived Credentials Working Group on February 23. The session included presentations by customers about their current derived credential implementations. The next Working Group session is scheduled for March 25 at the GSA Central Office. The USAccess Derived PIV Credential Industry Day is scheduled for April 27. Stay tuned for more information regarding Industry Day in the coming weeks.

### *USAccess Order Process Reminder*

Please be reminded that if requested system enhancements are specific to a single agency, the order must be funded by the requesting agency. All work that the MSO/HP needs to perform on agency SIP interfaces requires an order before the work can be started.

## *Fixed Infrastructure Windows 7 Workstation Replacement Update*

The schedule for fixed workstation replacement will be sent to Agency leads for final review and comment by the end of this week. We ask that Agencies respond with requests for any changes immediately, as the first wave of workstation replacement activities begin this week.

Agency sites slotted for wave 1 will receive an email this week to attend a Prep Call. Emails will be sent to the email addresses listed in the fixed workstation replacement schedule. Call attendees should include the Site POC, Site IT POC or Installer and the Registrar/Activator. It will also include an HP and/or MSO Deployment Manager. Each attendee plays a crucial role in ensuring the new equipment is unpacked and set up, the site is certified and the non-Windows 7 equipment is packed and returned to HP. Site personnel attending the call should be the same people who will be on hand during the site's Install call, which will be scheduled once the Prep Call occurs.

Prep calls are 1 hour (presentation followed by Q&A) and will review the process, roles and responsibilities and the timeline for replacement. Attendance is mandatory. If a site does not attend a prep call, equipment will not be shipped to the site and the replacement process will not move forward until the site attends a prep call. **If the install date passes and the site is not certified, the site cannot operate within the USAccess infrastructure.**

Once the prep call occurs, equipment will ship and the site has 2 weeks from the time of its arrival to schedule an install call with HP using a special GSA Online Scheduling link that is provided during the prep call. Install calls are led by an HP Deployment manager and walks the site's local IT and Registrar through the process of setting up the new Windows 7 system and certifying the site with a test enrollment/activation, and then packing up and returning the Windows XP system.

**All sites must be upgraded by mid-June in preparation for the MSO ATO. If a site is not upgraded, the site cannot operate in the USAccess infrastructure.**

Weekly reports will be made available to Agency leads showing the schedule for their sites, as well as their progress in meeting all their milestones.

## Service Enhancements

### System Changes Since Last Blue Top

- Maintenance was completed as scheduled on Saturday, February 28, 2015. Fixed enrollment machines updated with required certificate.

This release updated the fixed enrollment workstations with the new certificate that is required by March 12 as the current certificate is set to expire on March 13. All but a handful of fixed workstations received this updated certificate and the help desk is following up with the site directly. Please ask your offices to respond to the help desk immediately if they receive a phone call. Any fixed or enrollment or LCS machine that does not get the updated certificate by March 12 will experience issues completing enrollments when it expires on March 13.

This same certificate must be applied to LCS machines in the field by March 12, and is available with the LCS Installer v3.4 that is available on the SFTP server. This update was discussed in the January and February User Groups, the Thursday customer calls and in past Blue Tops. If more information is needed, please reference the February User Group presentation and the Light Installers v3.4 release notice posted on the Agency Lead Portal.

The updated SIP certificates that are required to be updated within Agency SIP infrastructures by March 12 were made available to Agencies and emails were sent to Agency contacts.

### Planned Changes

- USAccess Software Release 9.6.3 is scheduled for Saturday, March 28.

This release includes monthly maintenance as well as support for Internet Explorer 11. Following this release, USAccess customers can access USAccess portals using this version of Internet Explorer. A release notice will be posted by end of the week on the Agency Lead portal.

## *Security Tip*

### *Re-capture Everything During Re-enrollments*

Remember that you must always re-capture fingerprints, photo, and re-scan ID documents during a re-enrollment. Since Registrars do not have the ability to determine why a re-enrollment was requested, you must always re-do the entire enrollment process. Failure to do so causes problems during the Activation process and compromises the mission and security of the PIV Credential program.

In most cases, in order to re-capture fingerprints, you must first clear the original fingerprints. You may do so by clicking the "Clear All" button in the Capture Window of the 10-print screen.

**FINALLY, Never, ever use someone else's PIV for any reason, or let anyone use yours. This applies to individual cardholders as well as roleholders.**