USAccess Program

USAccess Program READY! Guide

Version 3.1

December 2018

GSA

Revision Chart

Version	Primary Author	Description of Version	Date Completed
1.0	Christian O'Keefe	Create document	05/29/2007
1.2	Christine Abruzzi	Revise with input from Deployment Working Group and Network Architect.	07/01/2007
1.3	Christian O'Keefe	Significant additions include the following: • Sample configuration diagrams • Power requirements • Activator role • Site Roles & Processes – Credentialing Center POC – Smartcard Receiving & Handling Process – Escort Process	07/15/2007
1.4	Christine Abruzzi	Updated with lessons learned	07/29/2007
1.5	Christian O'Keefe	Significant changes to IT Requirements include: • Removed 5505 reference • Added Cisco 3002 VPN Router • Added Linksys 2008 Switch • Added diagrams for network connection requirements	10/22/2007
1.6	Christian O'Keefe	Changes include: • Added high-level deployment timeline • Updated references to IPSec over UDP and IPSec over TCP • Removed high-level architecture diagram • Standardized terminology	05/27/2008
1.7	Terry Roper	Removed third IP address and changed EDS references to DXC. Updated all sections.	01/26/2011
2.0	Terry Roper	Updated for new environment as of 4/1/2012	04/12/2012
2.1	Terry Roper	Updated for Perspecta	11/2016
3.0	MSO	Significant changes to account for Credentialing Units and creation of a separate deployment process document	03/2018
3.1	MSO	Changed DXC references to Perspecta	12/2018

Table of Contents

List of Figures

1.0 Introduction

Homeland Security Presidential Directive 12 (HSPD-12), "Policy for a Common Identification Standard for Federal Employees and Contractors," established the requirement for a mandatory, Government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractor employees assigned to Government contracts in order to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy. As a result, the National Institute of Standards and Technology (NIST) released "Federal Information Processing Standard (FIPS) 201: Personal Identity Verification (PIV) of Federal Employees and Contractors" on February 25, 2005 (updated to FIPS 201-2 in August 2015). FIPS establishes the requirements and business processes for the development of PIV contact and contactless credentials.

The USAccess Program provides a turnkey service to produce compliant PIV credentials and to maintain associated identity accounts. The USAccess mission is to serve as the Executive Agent for Government-wide acquisition of information technology to implement HSPD-12. That mission includes the effort to provide Federal agencies with interoperable identity management and credentialing solutions that provide end-to-end services to enroll applicants, issue credentials, and manage the lifecycle of these credentials.

All HSPD-12 Credentialing Centers must meet the requirements set forth in this document.

1.1 Purpose

The USAccess Program READY! Guide is intended to provide Agency personnel with the requirements and information they need to make the decision about whether they are ready to host a Credentialing Unit (CU) at their site.

1.2 Scope

The scope of this document encompasses the requirements for site facility, power, security, Information Technology (IT), and telecom. This document also provides information on expected site processes and the USAccess system infrastructure.

2.0 Site Facility Requirements

The following sections describe the physical site requirements and additional recommendations for site setup. Also included are examples of Enrollment and Activation Station room footprints for ensuring privacy.

2.1 Physical Site

Potential locations for Credentialing Centers should be evaluated and selected based on the following set of specifications:

- The building is owned by the Federal Government or contains federally leased space.
- The building is accessible by public transportation, if available.
- The building meets Federal requirements for disabled individuals under the Americans with Disabilities Act requirements. This includes parking, ramps, automatic entryway, elevators, etc.
- The building maintains the applicable level of physical security.

Once a building has been identified as a potential Credentialing Center, appropriate space inside the building should be identified. The following Room Requirements and Recommendations provide guidelines for the location within the building and build-out of a room for the Credentialing Center.

2.2 Room Requirements and Recommendations

An identified space within the building selected as a potential Credentialing Center should be evaluated for the following requirements before finalizing its location:

- The Credentialing Center space is centrally located for easy access near a main entryway or elevator.
- The Credentialing Center space has adequate, accurate, and visible signage to help navigate from the main entrance(s).
- The recommended space is large enough that it can be configured to accommodate the Credentialing Unit(s), privacy counters and/or barriers, and a queuing/waiting area. Where possible, it is best to have the waiting area physically separated from the CU to allow for 1-to-1 privacy between a Registrar and an Applicant.
- The space is used for credentialing only. If that is not possible, all USAccess Credentialing Center equipment should be segregated from any other hardware used for other purposes.
- At a minimum, the space must be lockable from the outside.
- The space has functioning electrical outlets, a telephone with local contact number and voice mail, and a network connection.
- The space is well lit, clean, and secure.
- A copy of the USAccess PIV Privacy Notice must be posted in clear view, identifying what information is being collected, why it is being collected, who has access to it, and where it is stored. The USAccess Program has the PIV Privacy Notice available for printing in poster size and 8 ½” x 11”.

The space to house a Credentialing Center should meet all of the above requirements and recommendations.

2.3 Furniture Setup Requirements and Recommendations

Each Credentialing Center should be equipped with a furniture setup that meets the following specifications:

- For the CU, a large desk/table capable of handling a laptop with several peripherals. The desk/table may be modular (part of cubicle or wall structure) or standalone. The desk/table should be accessible

by seated users side by side so that both the role holder and the applicant can see the screen. The CU takes up approximately 48” x 33” of desk surface space and weighs approximately 50 pounds.

- The CU requires a minimum of two chairs—one for the Registrar and one for the Applicant.
- In order to optimize photo quality, standard office lighting is required in the area of the CU. However, overhead lighting that is too bright can adversely affect photo capture. In this case, supplemental, frontal lighting (such as a photo lamp) is recommended (but not provided by the USAccess Program).
- Additionally, a blue backdrop is provided with CUs. Allow space behind the Applicant’s chair for a blue backdrop and stand, if you have one.
- Excessive sunlight has a negative effect on photo quality. Plan to place the CU away from windows or shade the windows to block excessive sunlight.
- Whenever possible, a CU used for unattended activation should be located near or with easy access to an Activator to allow credential holders easy access to rained personnel, in case of questions during unattended activation.
- Barriers should be placed in a manner that shields screens from the view of waiting Applicants or from other Credentialing Units. This is only necessary if the room configuration does not allow for such privacy to occur naturally.
- A safe or a secured cabinet must be located within each of the Credentialing Centers. The safe (or cabinet) is used to store new credentials prior to issuing them to the credential holders and subsequent activation.

For a general idea of a possible station setup, see the example below.

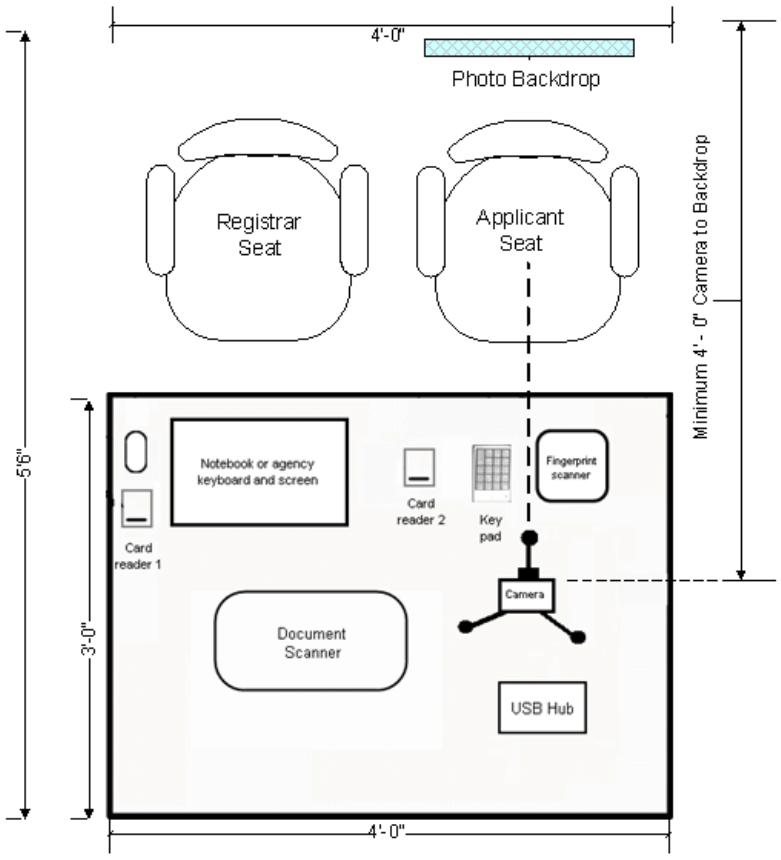

Figure 1: Minimum Footprint of CU

3.0 Power Requirements

Mobile and Fixed CUs, and the Virtual Private Network (VPN) communications equipment require standard 120 Volt AC power. The Mobile and Fixed CUs come with one surge protector each.

All of the equipment for a single CU requires a minimum of 3.3 amps of power.

Each VPN device requires a minimum of 1.8 amps of power.

Given that a standard 120 Volt AC 20 amp circuit should not be loaded to more than 80% (16 amps) of its capacity (20 amps), it is recommended that there be at least one dedicated 20 amp 120 Volt AC circuit for each group of no more than two CUs and one site VPN. See below for an example:

MCU or FCU	3.3 amps x 2=	6.6 amps
Site VPN Concentrator	1.8 amps x 1=	1.8 amps
		Total = 8.4 amps

This would also allow for additional CUs later if needed.

4.0 Security Requirements

The following minimum security requirements apply to all Credentialing Centers, whether Shared or Dedicated:

- A safe or a locked cabinet must be utilized to secure the USAccess PIV Credentials until activated.
- The Credentialing Center must be locked when not occupied.
- Security measures must be in place that safeguard against the disclosure of sensitive information, and prevent unauthorized access to USAccess Credentialing Center equipment.
- USAccess Credentialing Center equipment may not be tampered with.
- USAccess Credentialing Center Fixed equipment may not be added to, or changed in any way.
- Network cables and USB cords must not be moved to different ports without permission from the USAccess Help Desk.
- Credentialing Center VPN devices may not be moved without MSO authorization. Requests to move, add, or change Credentialing Center equipment must be made through the GSA MSO.
- Only trained Registrars should have access to the Credentialing Center equipment. This does not include the Fixed CUs being used for activation, which may be accessed by credential holders (for unattended activation), or Activators and credential holders (for attended activation).

5.0 Information Technology and Telecommunications Requirements

This section defines the IT requirements, the recommended site network configuration, and telecommunications requirements.

A Fixed Credentialing Center consists of at least one of each of the following components:

- A VPN device that is FIPS 140-2 validated (Fixed Sites only).
- Credentialing Unit
- Surge Protector

5.1 IT Requirements

The network requirements for standing up a USAccess Fixed Credentialing Center are as follows:

- An Internet Protocol (IP) address must be established for each VPN device.
- The IP address must be communicated to the USAccess Deployment Engineer, via the SET! Worksheet, prior to the deployment of the Credentialing Center.
- The IP address for the VPN device must have either a publicly routable IP address or a static translation to a publicly routable IP address

Two VPN tunnel solutions are supported. Internet Protocol Security (IPSec) over Transmission Control Protocol (TCP) and IPSec over User Datagram Protocol (UDP).

- For IPSec over TCP, traffic must be allowed outbound to connect to the following IP addresses on port 443:
  - 206.164.88.135
- 204.105.88.64For IPSec over UDP, traffic must be allowed both inbound and outbound to the following IP addresses:
  - 206.164.88.135
- 204.105.88.64The following ports and protocols are used for IPSec over UDP:
  - UDP 500
  - UDP 4500
  - IP Protocol 50 (ESP)
  - IP Protocol 51 (AH)
- No third-party software or hardware may be added to the Fixed CUs. Software is installed on all the Fixed CUs that prevents the installation of any additional software or drivers.
- Outside of local network connectivity and performance, no support is expected from local network administrators for the Fixed CUs. All support requests for Fixed CUs are handled by the USAccess Help Desk. For Mobile CUs, local IT or other agency personnel are responsible for all network, proxy, configuration settings and anti-virus. The USAccess Help Desk is available to troubleshoot enrollment, activation or other USAccess software issues.
- Optionally, a separate circuit (i.e. DSL, T-1, etc.) may be used.
- Recommended bandwidth is a minimum of 5-10 mbps up and down. Although a line provisioned less than 5 mbps may work, it increases processing time for enrollments. Since enrollments are web-based and information is being sent throughout the enrollment and activation process rather than just at the end of the enrollment/activation activity, a consistent network connection and adequate speed are necessary for a good user experience. The USAccess Program does not provide a dedicated circuit. Note: if adding more stations to that line more throughput could be needed.
- Upload speed is important, as the Registrars send 3-5MB of data for each enrollment processed.

5.2 Recommended Installation Configuration

The ideal configuration for Fixed CUs is that all deployed terminals are directly connected to the VPN device. A CAT6 cable should be plugged into the back of the router and the other end into your network jack. The VPN router should be connected to a surge protector. For Mobile CUs, all deployed terminals should be directed connected to the surge protector. All of these components should exist within the same physical boundary (i.e. within the same room, behind locked doors).

5.3 Possible Network Configuration Options

The Agency's choice in network configuration must be indicated on the SET! Worksheet before deployment.

Configuration	Characteristics/Requirements
Installed on Agency Wide Area Network (WAN) utilizing IPSec over UDP	• Site must provide an IP address, which is configured into the VPN device prior to deployment. • Protocols 50 and 51 and ports 500 and 4500 must be opened to outbound communications. • Proxies and Internet monitoring tools (such as Web Sense and Web Inspector) may interfere with workstation authentication and must be changed to permit IPSec traffic flow.
Installed on Agency WAN Utilizing IPSec over TCP	• Site must provide an IP address, which is configured into the VPN device prior to deployment. • Port 443 must be opened to outbound communications. • Proxies and Internet monitoring tools (such as Web Sense and Web Inspector) may interfere with workstation authentication and must be changed to permit IPSec traffic flow.
Dedicated Circuit (DSL, T1, etc.)	• Site must obtain a static IP address from network provider, which is configured into the VPN device prior to deployment. • Recommend symmetrical networks whenever possible to provide best performance.

5.4 Telecommunications Requirements

At least a single telephone line must be available in each room, and needs to be in close proximity to the CU. Each line must have a local contact number, and voicemail setup is recommended for the Registrars. This number is provided on the SET! Worksheet.

6.0 Site Processes

This section describes standard processes each site must adopt, and security rules to follow in developing the processes.

6.1 USAccess PIV Credential Receiving and Handling Process

Even though the USAccess PIV Credentials do not contain any electronically stored personal information at the time they are shipped from the manufacturer, they are still considered controlled media. As such, a "chain of trust" must be maintained from the time the credential is received on site until the time it is turned over to the Applicant for activation.

Each site must define and document a secure process for receiving and handling the USAccess PIV Credentials after they are received from the manufacturer. This process should take into consideration any site-specific receiving processes.

During the Site Preparation Process, the Site POC is asked to indicate a Primary Ship To POC in Site Manager, . This information is provided to the USAccess card printing facility for use as the Ship To name and phone number for USAccess PIV Credentials being shipped to the site. **Under no circumstances should a card shipment be signed for by anyone other than the designated POCs** (Registrars may be a designated Ship To POC).

At no time prior to the activation of the USAccess PIV Credentials should the USAccess PIV Credentials be left unsecured or unattended. A hand-receipt and/or logging process should be implemented to track any internal transfers of the USAccess PIV Credential packages (i.e., from loading dock personnel to Primary Ship To POC). The PIV Credentials are then "Checked-In' to the USAccess Credential Inventory Tool before being locked in a secure cabinet or safe.

6.2 Escort Process

Depending on site-specific visitor policies, a Credentialing Center POC may also have to devise a process to provide access to non-Agency personnel using the Credentialing Center to enroll for, activate, or update their USAccess PIV Credentials. For instance, the POC may choose to print out a list of all Applicants with appointments for that day and provide the list to the front desk to allow scheduled Applicants access to the Credentialing Center.

View-Only access to the GSA Online Scheduling System can be made available to personnel needing to browse the appointments schedule. Contact the USAccess Help Desk for more information.

7.0 USAccess Infrastructure

The backend of the USAccess Program system infrastructure is designed in zones and layers. This approach, in coordination with firewalls, limits interaction between system components to only required interactions.

All accounts on any backend systems are provisioned only with necessary privileges. All accounts and associated privileges follow security standard operation procedures and are required to be periodically audited. All USAccess systems employ Intrusion Prevention System (IPS), Intrusion Detection System (IDS), antivirus, and firewalls to assist in ensuring they remain secured at all times..

FIPS 140-2 level 1, 2, and 3 certified cryptographic modules are used to store all cryptographic keys. All cryptographic operations are executed using FIPS compliant algorithms and key sizes. The system uses an nCipher nShield for NetHSM, which is FIPS 140-2 level 3 compliant.

7.1 Security Policy

All security elements combined in coordination with the overall security policy prevent system components from:

- Accessing the Internet unrestricted (Fixed CUs Only)
- Loading unapproved software (Fixed CU's Only)
- Using the enrollment component for other than its intended purpose.

Personnel security training includes the acknowledgement and acceptance of their trusted role, and undesired actions such as these are expressly disallowed (subsequently logged and audited periodically). Further, system components are technologically prevented from performing such actions. On Fixed CUs, administrative access is exclusive to the remote administrators at the USAccess Program Network Operations Center (NOC). The remote administrators also run regular audit and production reports.

7.2 Centrally Managed Security (Fixed CUs Only)

All security policies, patches, updates, DAT files, and configurations are pushed to the Fixed CUs and are administered through a secure central service. In order to maintain up-to-date configurations on the network, the sites must leave the networking equipment and workstations on at all times. This is applicable only to Fixed CU equipment.

7.3 Data Management

USAccess data is never stored on the USAccess workstations. No partial enrollments are permitted—if an enrollment cannot be completed for any reason, no data is stored.

Appendix A: Acronym List

Acronym	Description
AC	Alternating Current
DAT File	Data File
DHCP	Dynamic Host Configuration Protocol
FDE	Full Disk Encryption
FIPS	Federal Information Processing Standard
GSA	General Services Administration
HSPD-12	Homeland Security Presidential Directive 12
IDMS	Identity Management System
IP	Internet Protocol
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security
ISSO	Information System Security Officer
MSO	Managed Service Office
NAT	Network Address Translation
NOC	Network Operations Center
PC	Personal Computer
POC	Point of Contact
SOAP	Simple Object Access Protocol
UDP	User Datagram Protocol
UPS	Universal Power Supply
VPN	Virtual Private Network
XML	Extensible Markup Language