USACCESS Program

USAccess Program

READY! Guide

Version 1.6

May 27, 2008

CM # GSA-DI-00000164-1.6.0

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

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. FIPS establishes the requirements and business processes for the development of PIV contact and contactless credentials.

The USAccess Program powered by the EDS Assured Identity™ solution provides a turnkey service to produce compliant PIV credentials and to maintain associated identity accounts. The USAccess mission under the General Services Administration (GSA) HSPD-12 Shared Services Provider II contract 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 where to locate their HSPD-12 Credentialing Center(s) that will contain Enrollment and/or Activation Stations.

1.2 Scope

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

1.3 Plan Maintenance

This document has been reviewed against NIST Special Publications, Government security documents and other client specific security documents, and is commensurate with those requirements. This document is periodically reviewed by responsible parties within the program and updated as necessary.

1.4 Shared vs. Leased Credentialing Centers

The USAccess Program offers an Agency the choice of either hosting a Credentialing Center that is shared with other participating Agencies or leasing a Credentialing Center for the agency's sole use. Both Shared and Leased Credentialing Centers include an Enrollment Station and a separate, standalone Activation Station that can be used for unattended (Cardholder-performed) activations or attended (assisted) activations. Agencies may choose to purchase additional Activation Stations—either for use by sites with existing Credentialing Centers or sites with no other USAccess Program equipment.

Agencies that offer to host a Shared Credentialing Center for use by all participating organizations may request a GSA Managed Services Office (MSO)-provided Registrar to operate the Enrollment Station for one year. Agencies that choose to lease a Credentialing Center have the option to contract a Registrar but at an additional charge.

2.0 Roles & Responsibilities

The individuals listed in Table 1: Roles and Responsibilities play major roles regarding the site preparation of the Credentialing Center.

Table 1: Roles and Responsibilities

Role	Responsibility
MSO Deployment Manager	• Define the program deployment strategy • Guide the participating agencies in choosing sites • Provide policy guidance to the agency and to its partners • Approve sites for deployment • Participate in GO! Calls
Agency Representative	• Participate in the program Deployment Working Group meetings • Identify sites to receive Credentialing Centers • Identify the number of Enrollment/Activation Stations to be deployed to each site and whether a particular site will be a “Shared” or “Leased” (aka, “Dedicated” Center) • Provide complete Site POC information • Participate in the GO! Call
Site Point of Contact (POC)	• Participate in the program Deployment Working Group meetings, as necessary • Review the READY! Guide and ask questions to assure understanding • Provide the READY! Guide to anyone within their organization who might play a role in the successful deployment to their site • Provide accurate information, via the SET! Worksheet, to the EDS Deployment Team representative • Provide information on additional points of contact for appropriate site personnel, such as network engineers, facilities managers, and security personnel • Facilitate all site preparation activities for the site • Engage the other functional staff at the sites and confirm tasks are completed • Inform the EDS Deployment team of any changes to the schedule of site prep activities in a timely manner • Participate in the GO! Call
EDS Deployment Team	The EDS Deployment Team consists of the EDS Deployment Manager, Deployment Engineers, staging warehouse technicians, and field services personnel. These personnel:

Role	Responsibility
	• Participate in the program Deployment Working Group meetings. • Work with the Agency Representatives and Site POCs to prepare the identified sites to receive their USAccess Credentialing Center equipment • Create and maintain the various tools and documents used to facilitate the deployment process (encompasses site prep, building and shipping of workstations, site installations, and site certification) including, but not limited to: – USAccess Deployment Process and Procedures – The Right Now CMF Tool – Site ID Database – READY! Guide – SET! Worksheet – GO! Checklist – Site Certification Checklist – Deployment Schedule
Field Engineer	• Unpack, inventory, and install the equipment • Install patches and perform updates as necessary to prepare system for certification • Verify that the Credentialing Center meets READY! Guide requirements

2.1 Operating Roles & Responsibilities

2.1.1 Site POC

Each agency must identify a Site POC for each site. This person is responsible for the day-to-day operations of the Credentialing Center and acts as the ongoing Site POC to the USAccess Program Help Desk and the GSA MSO. The Help Desk maintains a list of contact information for Site POCs for use in notifying them of system updates and outages. Additionally, the Help Desk notifies the Site POC if his/her Credentialing Center is unexpectedly not open for business during normal operating hours (i.e., if an Applicant arrives for his/her appointment and the Credentialing Center is closed).

Each Site POC should also identify a backup POC for times when the primary POC is not available to perform this role.

2.1.2 Registrars

Registrars operate the Enrollment Stations. Therefore, they must be trained and certified to perform this role. Agencies have the option of either providing their own Registrars or

requesting one through the USAccess Program. Classroom and Web-based training is available for agency personnel and contractors to train on the use of the USAccess Program enrollment system and performing the Registrar role.

All Registrars, whether agency or USAccess Program provided, must have a USAccess PIV Credential to login to and operate the Enrollment Station.

2.1.3 Activators

Activation Stations are configured to perform either unattended (Cardholder only) or attended activations (Cardholder and an Activator). Agencies should be prepared to have a trained, certified Activator available to perform attended activations and to assist Cardholders who are having difficulties with unattended activations. Registrars may be able to perform as Activators, but due to the large number of people that must be enrolled in a short period of time, Site POCs should not depend on Registrars to handle all activations.

3.0 Deployment Process Overview

This section gives a high-level overview of the deployment process.

3.1 Ordering

New agencies interested in participating in the USAccess Program must sign the GSA InterAgency Agreement form located at http://www.fedidcard.gov/participate.aspx, and submit the completed version to Spiro Papagjika at spiro.papagjika@gsa.gov.

Agencies interested in ordering new USAccess services must complete the USAccess GSA MSO Order Form located at http://www.fedidcard.gov/priceinfo.aspx and submit the completed form to Jim Schoening at jim.schoening@gsa.gov.

3.2 Data Configuration/Upload

After an agency has ordered USAccess services, the MSO and EDS Developers work with the agency's representatives to complete the GSA MSO Configuration Data Input Form located at http://www.fedidcard.gov/deployprocess.aspx, which determines the agency's card topography, agency-specific text, and various other data needed to prepare a site in the Identity Management System (IDMS). Sites also need to provide bulk upload personnel data to the EDS Developers prior to deployment.

3.3 Approval

Once GSA has received and processed an order for USAccess services, the MSO notifies the EDS Deployment Manager that the site has been approved for deployment, and is ready to be placed on the schedule. The following information is relayed to the EDS Deployment Manager:

- Name of agency
- Site POC (with phone number and e-mail address)
- Site type (Credentialing Center or Activation Center, and whether the site will be designated as Shared or Leased)
- Number of Enrollment and Activation Stations requested
- Number of MSO-provided Registrars requested

The EDS Deployment Manager works with the Operations Team to locate and hire a Registrar if one is requested.

3.4 Registrar Hiring Process

Aside from USAccess Installation Technicians, Registrars are the only personnel authorized to operate the USAccess workstations. Registrars can be either agency-appointed or MSO-provided. If an agency chooses to utilize an MSO-provided Registrar, the Operations Team

begins their process of locating a potential Registrar through one of the USAccess Program Partners. The Operations Team requires a 45-day lead-time from hiring to ready for work.

3.5 Scheduling

Approved USAccess locations are scheduled by the EDS Deployment Manager. Sites are scheduled for installation 45+ days following the completion and approval of the order by MSO. The EDS Deployment Manager takes into account the agency's readiness and previously scheduled installs to ensure proper coverage and resources from the USAccess Program Partners is available. An EDS Deployment Engineer is assigned to work with each site to provide a single point of contact for deployment-related activities.

3.6 Introduction E-mail

The EDS Deployment Manager sends a welcome e-mail to the Site POC no less than 45 days from the scheduled installation date. On this e-mail, the EDS Deployment Manager also copies the Agency Representative, GSA MSO representatives, Deployment Engineers, the EDS Operations Manager, and EDS Operations representatives.

3.7 Site Preparations

After the EDS Deployment Manager has sent out the introduction e-mail, a Deployment Engineer contacts the Site POC via phone or e-mail. The Deployment Engineer explains the Deployment process, and answers any questions. The current versions of the READY! Guide and SET! Worksheet are e-mailed to the Site POC at this time.

The READY! Guide provides agency personnel with the requirements that must be met to host a USAccess Credentialing Center. Subjects addressed include building, room, furniture, telecom, information technology, and security requirements.

The SET! Worksheet is a spreadsheet to accompany the READY! Guide. Site POCs are responsible for completing this worksheet and returning it to the Deployment Engineer. This worksheet captures critical information such as specific location, contact information for involved personnel, IT details, etc.

3.8 GO! Call

The purpose of the GO! Call is to coordinate the final requirements to be completed prior to installation, assign last minute action items, and confirm the arrival times for the Installation Technician and Registrar(s). **The GO! Call must be scheduled at least two and one-half weeks prior to scheduled installation.** The EDS Deployment Engineer schedules the GO! Call and provides a conference line.

The GO! Call is scheduled after:

- The SET! Worksheet has been completed in its entirety
- The SET! Worksheet has been approved by the Deployment Engineer

- The Deployment Engineer has verified all resources are available:
  - Installation Technician
  - Registrar (if applicable)
  - A USAccess PIV Credential is available to test the USAccess workstations

3.9 Installation

The installation date is confirmed during the GO! Call. The Deployment Team coordinates a date/time to send an Installation Technician to configure and install the USAccess equipment. At a minimum, the Site POC and a local IT representative need to be present on the day of the install from the agency side. Installation time varies depending on number of workstations and agency readiness.

3.10 Certification

After the USAccess equipment has been installed by the Installation Technician, the certification process will begin. The Installation Technician, Registrar, and Site POC follow the Site Certification Checklist to ensure all USAccess equipment has been properly installed, configured, and tested.

3.11 TimeTrade Setup

Following the Certification, the EDS Deployment Engineer confirms the TimeTrade setup information with the Site POC. This information includes the site's hours of operations, holiday schedule, points of contact, etc. Following deployment, if any additional changes need to be made to the TimeTrade information, sites need to contact the USAccess Help Desk at 1-866-493-8391.

4.0 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.

4.1 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 at least a minimal level of physical security.

Additionally, **shared** Credentialing Centers should also:

- Be centrally located among high concentrations of Federal Government employees and/or contractors, and
- Be able to accommodate the general public.

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.

4.2 Room Requirements & 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 Enrollment Station(s), Activation Station(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 Enrollment Stations to allow for 1-to-1 privacy between a Registrar and an Applicant. An example of an approved setup that meets privacy requirements is shown in Figure 1: Privacy Requirements Set-up.

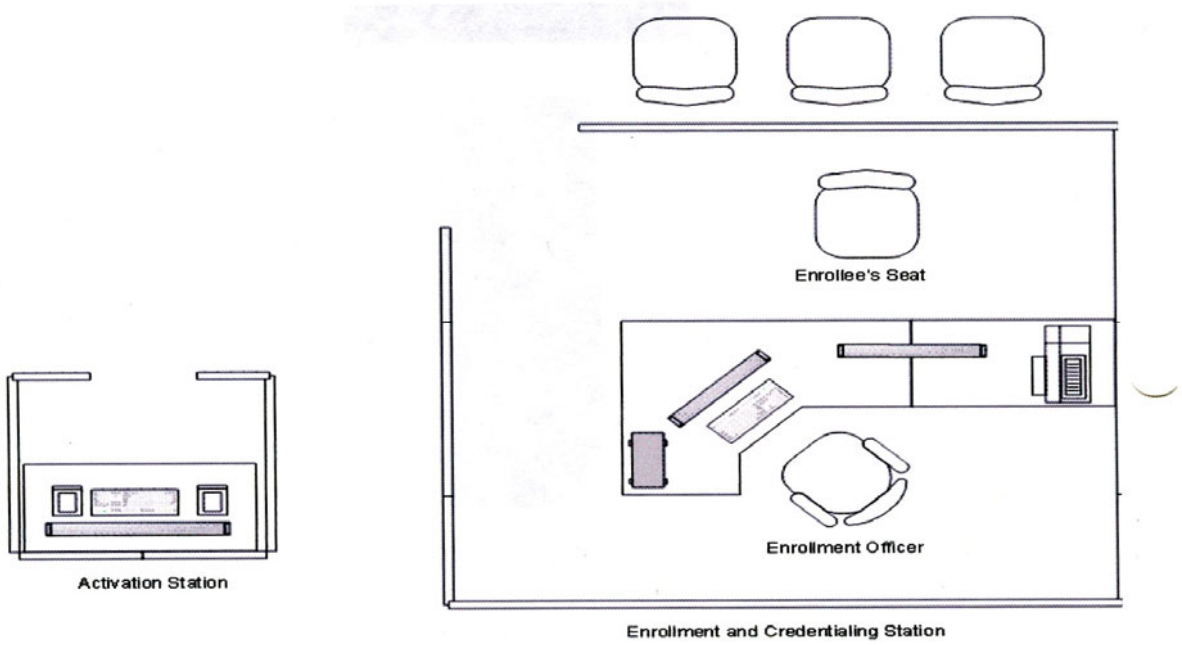

Figure 1: Privacy Requirements Set-up

- The space should be 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, 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.

4.3 Furniture Setup Requirements & Recommendations

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

- For the Enrollment Station, a large desk/table capable of handling a PC with 2 LCD displays, and 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 from both ends (where applicable). The Enrollment Station takes up approximately 48" x 33" of desk surface space and weighs approximately 50 pounds.

- The Enrollment Station 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 Enrollment Station. 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 and stand is provided with Enrollment Stations. Allow added space behind the Applicant's chair for a blue backdrop and stand.
- Excessive sunlight has a negative effect on photo quality. Plan to place the Enrollment Station away from windows or shade the windows to block excessive sunlight.
- Whenever possible, an Activation Station should be located near the Enrollment Station to allow Cardholders easy access to Registrars, or other trained 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 Stations. 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 Cardholders and subsequent activation.

For a general idea of possible station setups, see the examples below for Enrollment Stations and Activation Stations, including the minimum footprint of each.

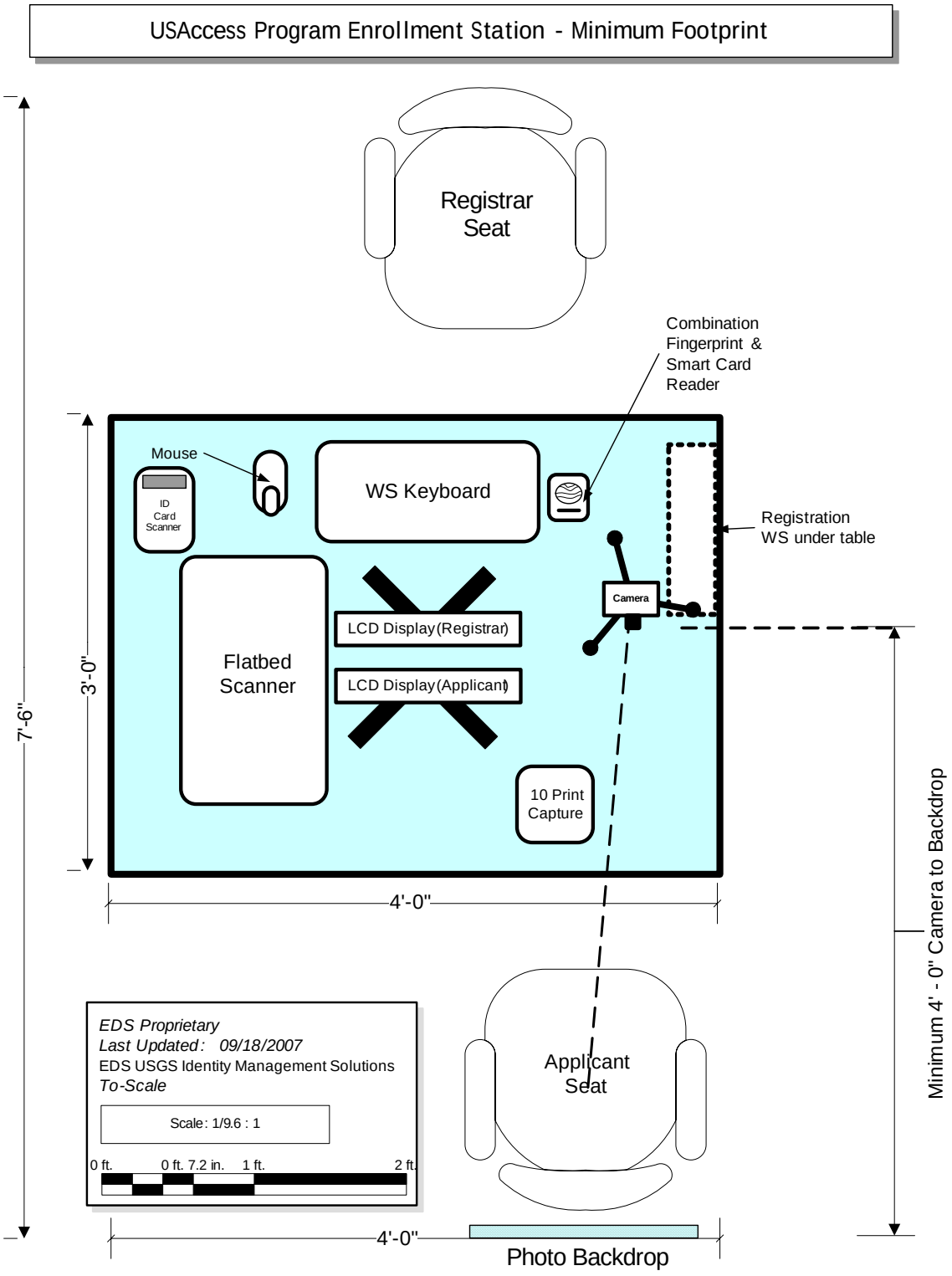

Figure 2: Minimum Footprint of Enrollment Station

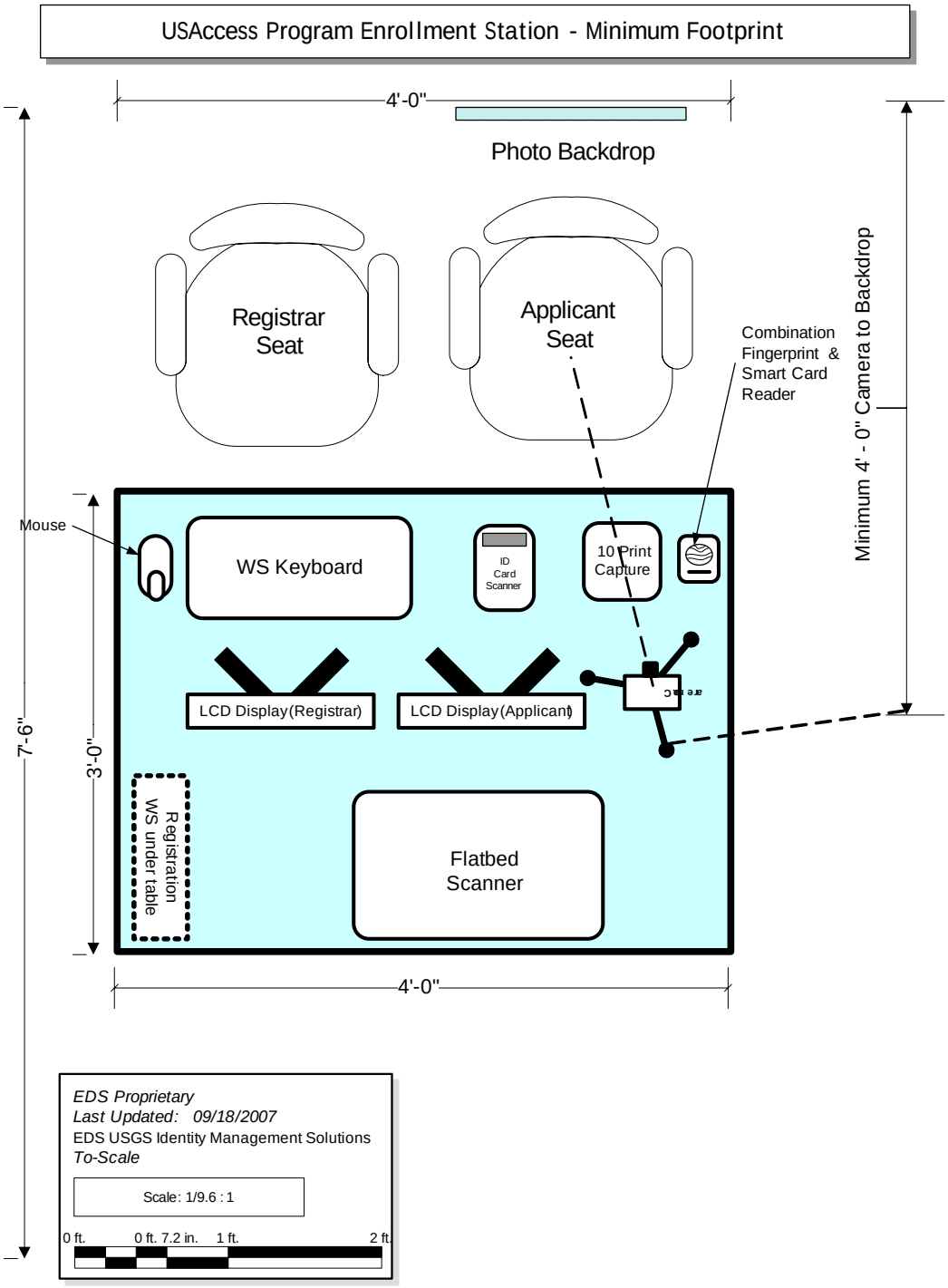

Figure 3: Alternative Footprint of Enrollment Station Registrar and Applicant Sit Side-by-Side

USAccess Program Activation Station
(Allows for Attended and Unattended activation)

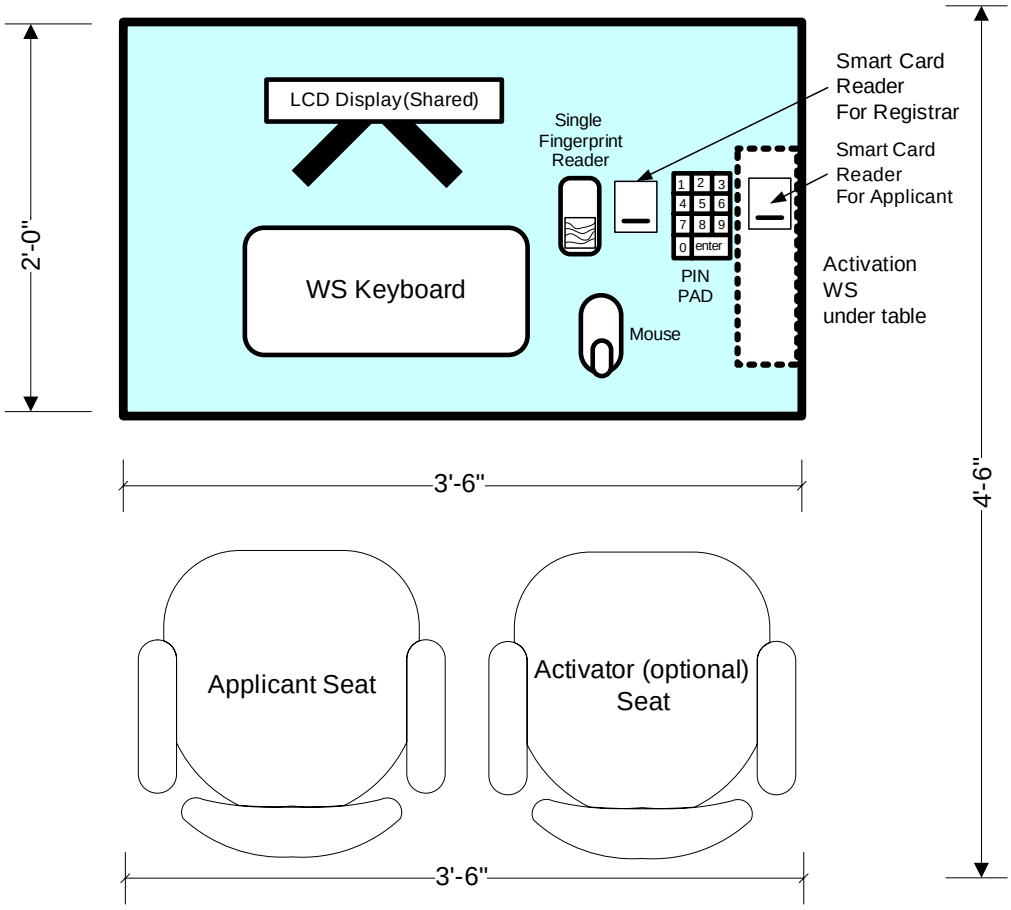

Figure 4: Activation Station

5.0 Power Requirements

Enrollment Stations, Activation Stations, and the Virtual Private Network (VPN) communications equipment require standard 120 Volt AC power.

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

All of the equipment for a single Activation Station requires a minimum of 2.1 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 Enrollment Stations with two Activation Stations and one site VPN. See below for an example:

Enrollment Station	3.3 amps x 2=	6.6 amps
Activation Station	2.1 amps x 2=	4.2 amps
Site VPN Concentrator	1.8 amps x 1=	1.8 amps
	Total =	12.6 amps

This would also allow for one additional Enrollment or Activation Station later if needed.

6.0 Security Requirements

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

- A safe or a secured 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, added to, or changed in any way.
- Enrollment Stations, Activation Stations, and Credentialing Center VPN devices may not be moved. Requests to move, add, or change Credentialing Center equipment must be made through the USAccess Help Desk.
- Only trained Registrars should have access to the Credentialing Center equipment. This does not include the Activation Stations which may be accessed by Cardholders (for unattended activation), or Activators and Cardholders (for attended activation).

7.0 IT and Telecom Requirements

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

7.1 IT Requirements

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

- A VPN device that is FIPS 140-2 validated.
- A Switch to provide 802.1x security if the VPN device does not already provide this
- Enrollment Station
- Activation Station

The network requirements for standing up a USAccess 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. This 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 three IP addresses on port 443:
  - 65.205.50.66
  - 192.112.145.4
  - 12.41.67.242
- For IPSec over UDP, traffic must be allowed both inbound and outbound to the following three IP addresses:
  - 65.205.50.66
  - 192.112.145.4
  - 12.41.67.242
- The 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 Enrollment or Activation Stations. Software is installed on all the stations 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. All support requests are handled by the USAccess Help Desk.
- Optionally, a separate circuit (i.e. DSL, T-1, etc.) may be used. Recommended bandwidth for this option is 1.5mbps up and down. Although a line provisioned less than 1.5mbps will work, it increases processing time for enrollments. The minimum bandwidth required is 768Kbps per pair of workstations (one Enrollment Station and one Activation Station). The USAccess Program does not provide a dedicated circuit.
- Upload speed is important, as the Registrars send 3-5MB of data for each enrollment processed.

7.2 Recommended Installation Configuration

The ideal configuration, as defined by the Certification and Accreditation (C&A) documentation is that all deployed terminals are directly connected to the supplied Switch, and the Switch is directly connected to the VPN device. All of these components should exist within the same physical boundary (i.e. within the same room, behind locked doors). Figure 5: C&A Configuration for Credentialing Center illustrates the C&A configuration for installing Credentialing Center equipment on an existing agency's network.

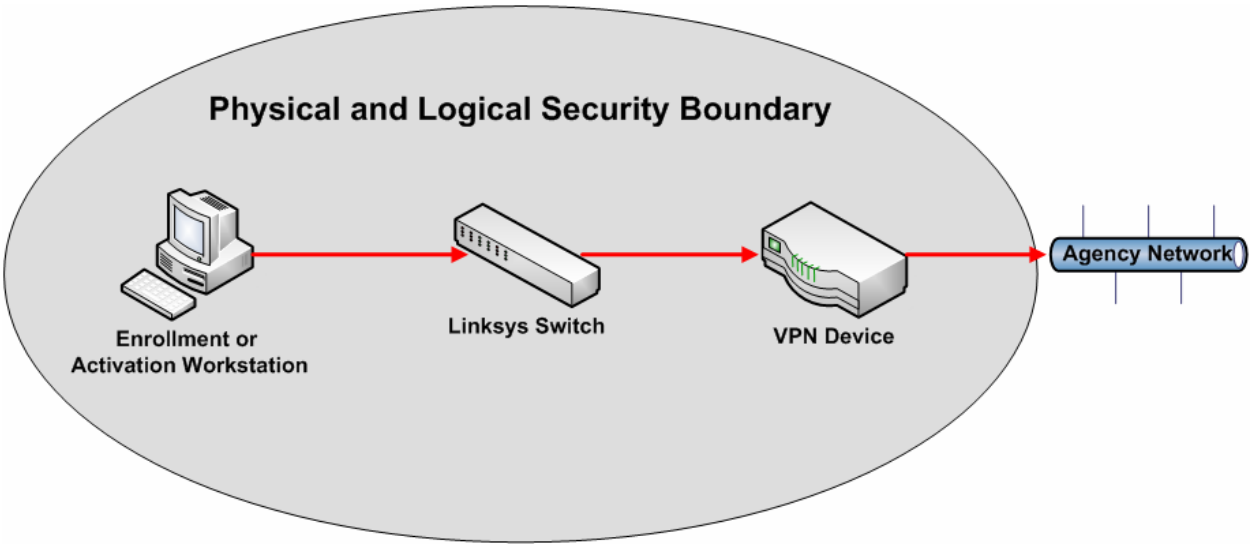

Figure 5: C&A Configuration for Credentialing Center

7.3 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 IP address from network provider and provide it to Deployment Team prior to deployment. • If the IP address is Dynamic Host Configuration Protocol (DHCP), the range of IP addresses must be listed in the SET! Worksheet. One IP address will be selected by the USAccess Deployment Team to configure into the VPN device. • Recommend symmetrical networks whenever possible to provide best performance.

7.4 Telecom Requirements

At least a single telephone line must be installed in each room, and needs to be in close proximity to the Enrollment Station. If the site is an activation-only site, the telephone line must be in close proximity to the Activation Station. Each line must have a local contact number and voicemail setup for the Registrars. This number must be provided to the Deployment Engineer for reference.

8.0 Site Processes

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

8.1 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 card 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 provide a Primary Card Receiving POC, a Secondary Card Receiving POC, and contact information for both. This information is provided to the USAccess PIV Credential production 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 POC). Once received, the cards must be placed in a safe or secure cabinet.

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 Credentials (i.e., from loading dock personnel to Primary Card Receiving POC).

8.2 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 register or activate 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.

Read-Only access to TimeTrade, the online appointment scheduling application, can be made available to personnel needing to browse the appointments schedule. Contact the USAccess Help Desk for more information.

9.0 USAccess Infrastructure

The backend of the USAccess Program system infrastructure is designed into zones and layers. This approach, in coordination with firewalls, limits interaction between system components to 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 audited periodically. All systems employ Intrusion Prevention System (IPS), Intrusion Detection System (IDS), antivirus, and firewalls to assist in ensuring they remain secured at all times. Additionally, system components utilize Odyssey software to implement further security of the components.

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.

9.1 System Security

The Enrollment Stations and Activation Stations are configured to establish a tunnel using 256-bit symmetric keys and the Advanced Encryption Standard (AES) encryption algorithm.

9.2 Network Address Translation

The Enrollment Stations and Activation Stations do not use Network Address Translation (NAT). The Credentialing Center operates in its own, segregated VPN zone. The VPN provides DHCP services that issue IP addresses that are viable network destinations accessible from the system Demilitarized Zone (DMZ) or “inside” network zones.

9.3 Firewall

The backend system utilizes a Cisco ASA5540 Firewall, which is certified at Evaluation Assurance Level (EAL) 4. Firewalls are configured to only allow specific traffic between identified network nodes that are required to communicate—and deny all other attempts from unspecified network nodes to communicate with other network nodes that are not approved. Furthermore, the nodes are limited to communicating on ports with protocols that are implicitly specified. All other ports and protocols are denied.

9.4 XML Gateway/Firewall

All Web services transactions are filtered through the Extensible Markup Language (XML) gateway. The XML gateway is configured to analyze the XML packages for malicious code and Web service attacks (Simple Object Access Protocol [SOAP] and attack vectors). Only values within the XML package that are deemed appropriate and benign are allowed for

further processing. Additionally, the software generating the XML package filters fields for acceptable values prior to processing the package.

9.5 Web Application Scanning

Web applications and services are scanned on a monthly basis. The Managed Service Provider networking team utilizes scanning tools such as nmap and similar detection tools. Once made aware of a vulnerability, efforts to mitigate the vulnerability are initiated through Change Management and the system is updated accordingly.

9.6 Component Critical Files

Each system component operates the Odyssey Software. This product monitors the component's resources and sensitive files. In the event that a critical file or security breach occurs (or a file is illegitimately modified), a security alert is sent out notifying administrators, and the component is locked down to prevent further system tampering.

9.7 Workstation VPN

Enrollment Stations and Activation Stations run a VPN client and attach to a VPN Device through a provided Switch. This Enrollment and Activation Station client communicates by establishing a tunnel using 256-bit symmetric keys and the AES encryption algorithm. The VPN device connects to a backend VPN concentrator. The workstations are assigned intra-system routable IP addresses for centralized management (patch and configuration updates) to communicate with the endpoint security controller.

9.8 Highly Secure Device Level Authentication

Each system component has a Juniper endpoint security agent running on it. These agents interact with a centrally managed endpoint security Juniper Infranet Controller device that authenticates and authorizes specific actions within the system. The authentication is X.509 certificate based and the certificates issued from a system trusted Certificate Authority. The authentication methodology is 802.1x compatible.

9.9 Security Policy

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

- Accessing the Internet (unrestricted)
- Loading unapproved software
- 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. 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.

9.10 Intrusion Prevention System

All system components are locked down by the Juniper Odyssey clients. This product provides host-based checking in real-time whenever the host connects to the network. It also prevents well-known intrusion methods employed by would-be hackers to exploit the vulnerabilities of the system in order to gain access to it.

9.11 AntiVirus

All system components run the Symantec AntiVirus agents. These agents are centrally managed by a server configured to manage the agents. The server checks the subscription service for updates to virus definitions. Once definitions are updated, the server automatically deploys the updates to all the agents associated with the server.

9.12 Centrally Managed Security

All security policies, patches, updates, DAT files, and configurations are pushed to components and are administered through a secure central service.

9.13 Endpoint Security Controller

The system uses a Juniper Infranet Controller (a hardened, purpose-built network appliance) to manage all system components outfitted with endpoint security agents. The Juniper implements 802.1x security methodology (device authentication) in addition to managing privilege and access of device components on the network. The Juniper Infranet Controller can manage up to 3,000 security agent connections.

9.14 Data Management

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
ACL	Access Control List
AES	Advanced Encryption Standard
DAT File	Data File
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
EAL	Evaluation Assurance Level
EDS	Electronic Data Systems Corporation
FIPS	Federal Information Processing Standard
GSA	General Services Administration
HSPD-12	Homeland Security Presidential Directive 12
IDMS	Identity Management System
IDS	Intrusion Detection System
IP	Internet Protocol
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security
ISSO	Information System Security Officer
IT	Information Technology
MSO	Managed Services Office
NAT	Network Address Translation
NIST	National Institute for Standards and Technology
NOC	Network Operations Center
PC	Personal Computer
PIV	Personal Identity Verification
POC	Point of Contact
SOAP	Simple Object Access Protocol
VPN	Virtual Private Network
XML	Extensible Markup Language