Department of Homeland Security

Transportation Security Administration

Office of Information Technology

Operations and Engineering Division



Authentication at the Edge (AATE)

Application On-boarding Guide

**Version 2.1**

March 12, 2018

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid “need-to-know” without prior written approval of an authorized DHS Official.

Table of Contents

[Table of Contents 2](#_Toc508630563)

[List of Figures 4](#_Toc508630564)

[List of Tables 4](#_Toc508630565)

[Section 1 Change History 6](#_Toc508630566)

[Section 2 System Overview 7](#_Toc508630567)

[2.1 F5 Access Policy Manager (APM) as the Applications Authentication Gateway 7](#_Toc508630568)

[2.1.1 F5 Access Policy Manager (APM) 7](#_Toc508630569)

[2.1.2 Multi-Factor Authentication 7](#_Toc508630570)

[2.2 Platforms Supported 9](#_Toc508630571)

[2.3 User Populations Supported via Three Directories 9](#_Toc508630572)

[2.3.1 Network Active Directory (AD) 9](#_Toc508630573)

[2.3.2 Extra Active Directory (AD) 9](#_Toc508630574)

[2.3.3 Oracle Internet Directory (OID) 9](#_Toc508630575)

[Section 3 Platform by Platform and Methods 10](#_Toc508630576)

[3.1 Platforms 10](#_Toc508630577)

[3.2 Supported Methods 10](#_Toc508630578)

[3.2.1 Windows Integrated Authentication (WIA) 10](#_Toc508630579)

[3.2.2 Oracle Access Manager protected Applications 12](#_Toc508630580)

[3.2.3 Security Assertion Markup Language (SAML) 14](#_Toc508630581)

[Section 4 On-Boarding Work-To-Do 16](#_Toc508630582)

[4.1 Information Gathering 16](#_Toc508630583)

[4.2 Developer’s Information 16](#_Toc508630584)

[4.2.1 Process Steps Outline 16](#_Toc508630585)

[4.2.2 DFD Requirements 18](#_Toc508630586)

[4.2.3 ITE-DEV Environment 18](#_Toc508630587)

[4.2.4 PIV Test Cards and Linking 18](#_Toc508630588)

[4.2.5 Additional SAML Information 36](#_Toc508630589)

[4.3 User Preparation 40](#_Toc508630590)

[4.3.1 PIV to Directory Linking 40](#_Toc508630591)

[4.3.2 Duo Registration 41](#_Toc508630592)

[4.4 F5 APM Work-To-Do 41](#_Toc508630593)

[4.4.1 Application URL(s) 41](#_Toc508630594)

[4.4.2 Base AATE Flows may need to be adjusted for application eccentricities 41](#_Toc508630595)

[4.4.3 The F5 APM work has to follow the standard TSA SELC processes 41](#_Toc508630596)

[4.5 User Communications 42](#_Toc508630597)

[4.5.1 Communicate and ensure required User Preparation Steps and Completion 42](#_Toc508630598)

[4.5.2 Communicate login differences/login page changes 42](#_Toc508630599)

[4.5.3 Communicate cutover date and information 42](#_Toc508630600)

[4.5.4 Communication how to get support information 42](#_Toc508630601)

[4.6 Application Changes 42](#_Toc508630602)

[4.6.1 Application code changes should be minimal to none for supported methods 42](#_Toc508630603)

[4.6.2 Outlier Application types that may need more work 43](#_Toc508630604)

[Appendix A Glossary and Definitions 44](#_Toc508630605)

[Appendix B Initial Meeting Questionnaire for On-Premises Applications 46](#_Toc508630606)

[Appendix C Initial Meeting Questionnaire for SaaS Applications 49](#_Toc508630607)

List of Figures

[Figure 1 - "Dual" Login Screen 8](#_Toc508630608)

[Figure 2 - F5 Flow Diagram for Internal .Net Applications 11](#_Toc508630609)

[Figure 3 - F5 Flow Diagram for External Oracle OAM Protected Applications 13](#_Toc508630610)

[Figure 4 - F5 Flow Diagram for SAML Applications. Cloud or SaaS 15](#_Toc508630611)

[Figure 5 - F5 Flow Diagram for SAML Applications. Cloud or SaaS 17](#_Toc508630612)

[Figure 6 - AuthentX Certificate List 19](#_Toc508630613)

[Figure 7 - F5 APM - VLD8 Test Output 1 20](#_Toc508630614)

[Figure 8 - F5 APM - VLD8 Test Output 2 21](#_Toc508630615)

[Figure 9 - F5 APM - VLD8 Test Output 3 22](#_Toc508630616)

[Figure 10 - ActivClient User Console Application Location 24](#_Toc508630617)

[Figure 11 - ActivClient My Certificates Options 25](#_Toc508630618)

[Figure 12 - ActivClient My Certificates Output 25](#_Toc508630619)

[Figure 13 - Certificate Detail Box 25](#_Toc508630620)

[Figure 14 - Certificate Details 26](#_Toc508630621)

[Figure 15 - Subject Alternate Name Details 26](#_Toc508630622)

[Figure 16 - AD Container Screen 28](#_Toc508630623)

[Figure 17 - User Account Details 1 29](#_Toc508630624)

[Figure 18 - User Account Details 2 30](#_Toc508630625)

[Figure 19 - Group Membership Details 31](#_Toc508630626)

[Figure 20 - RDP Error Screen 32](#_Toc508630627)

[Figure 21 - E-mail Account Setup 1 32](#_Toc508630628)

[Figure 22 - E-mail Account Setup 2 33](#_Toc508630629)

[Figure 23 - E-Mail Account Setup 3 34](#_Toc508630630)

[Figure 24 - E-mail Account Setup 4 35](#_Toc508630631)

[Figure 25 - E-Mail Account Setup 5 35](#_Toc508630632)

[Figure 26 - SAML IdP Initiated User Flow 37](#_Toc508630633)

[Figure 27 - SAML SP initiated User Flow 1 38](#_Toc508630634)

[Figure 28 - SAML SP Initiated User Flow 2 39](#_Toc508630635)

List of Tables

[Table 1 - Glossary and Definitions 44](#_Toc508630695)

1. Change History

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Person** | **Description** |
| 0.1 | 3/22/2017 | Jay White, ITIP | Initial Draft |
| 1.0 | 4/22/2017 | Jay White, ITIP | Integrated comments about OAM, added status information where the AATE project that ended 4/28/2017 left off. |
| 2.0 | 2/21/2018 | Jay White, ITIP | Additional SAML Flow, General process information and updates to questionnaire as well as some additional developer information and other minor touchups. Replace Anakam with Duo. |
| 2.1 | 3/12/2018 | Jay White, ITIP | Changes and touchups from reviewers |

1. System Overview

Authentication at the Edge (AATE) is TSA’s moniker for a set of Authentication and Access Management technologies that provide PIV and multi-factor non-PIV Authentication services via F5 Access Policy Manager (APM). This provides authentication, access management, Federation and Single-Sign On (SSO) services to downstream applications and systems.

* 1. F5 Access Policy Manager (APM) as the Applications Authentication Gateway

Since almost all TSA Application (on-premises) traffic flows through the F5 for load balancing, TSA is using the F5 Access Policy Manager as an Application Authentication Gateway to do multi-factor authentication using PIV or UserID/Password plus Duo Soft Token. This is very convenient as most application traffic already goes through the F5 for load balancing.

* + 1. F5 Access Policy Manager (APM)

When a user accesses an application URL protected by F5 Access Policy Manager (APM), the APM module within the F5 validates an “access policy” which can be thought of as a workflow within the F5. All access policies start with an incoming connection, and end with a “decision” for access. In between these two endpoints, authentication, authorization, and other logical items can occur. This is the basic premise of creating an access policy for an APM protected asset, deciding what attributes will be tested for the decision making.

On a typical flow, such as OWA (Outlook Web Access), a login page is rendered and prompts the user for a credential- either PIV, or Username and Password, once a user submits this information, the APM access policy flow will do Active Directory (AD) lookups, certificate validations, and other authentication metrics to form a decision on that user, against that page, at that time.

The reason why all of this is important, is that this can only be done with information provided via the web session (on initial page load, or on form submission). Any assumptions that the APM can check, validate, or cache information on a user based on a simple page load, can only be done passively via a client certificate challenge (i.e, PIV with no “button” to initiate it, similar to how Xceedium works) or Kerberos. There is no way to know anything about a user, from a simple page load, unless credentials, certificates, or Kerberos tickets are presented from that user to APM.

* + 1. Multi-Factor Authentication

Multi-Factor Authentication is required by FISMA for all Medium and High systems. The use of PIV is mandated and required for all Federal employees and most Federal contractors.

* Personal Identity Validation (PIV)

The PIV card is a strong vetted credential mandated to be used for all federal physical and logical access. It can only be obtained after a background investigation at the NAC-I level (or equivalent like DHS/TSA EOD) or higher. It has certificates, keys, biometric data and a PIN. PIV has an e-authentication Level of Assurance (LOA) of 4 (highest).

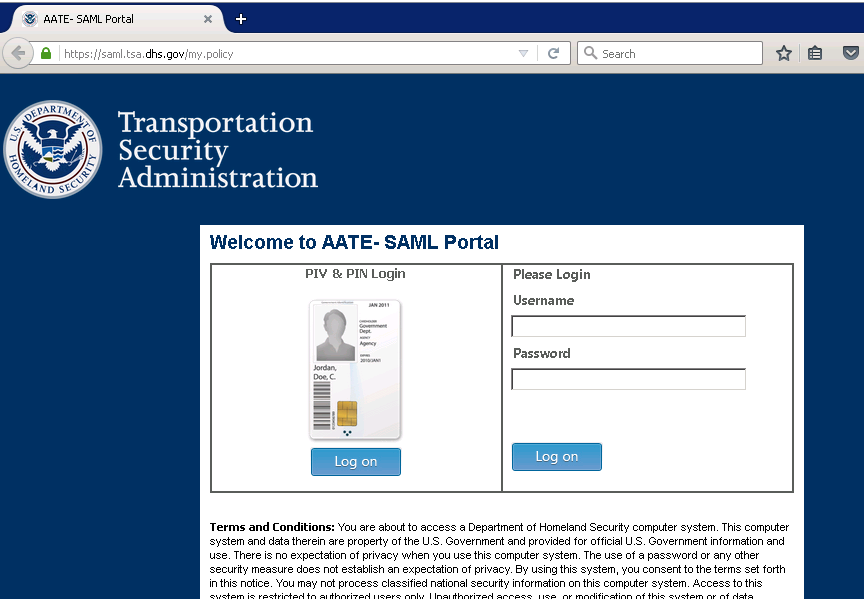
* UserID and Password plus Duo Two Factor Authentication (TFA)

DHS is still trying to decide on a PIV-I solution (PIV inter-operable) for non-federal users like partners. Until the DHS decision is made and a supportive technical solution implemented, TSA is using the Duo TFA (Two Factor Authentication) to add a second factor of authentication onto the existing UserID and Password to strengthen authentication and meet the multi-factor FISMA requirements. Duo is considered to have an e-authentication LOA of 3.

*AATE Status Note: Anakam TFA is being replaced by Duo. Duo is currently in procurement and not deployed yet.*

Below is a picture of an F5 APM “Dual” login screen – PIV and UserID/PW with Duo.

Figure 1 - "Dual" Login Screen



* 1. Platforms Supported

AATE supports the two main TSA platforms: Microsoft and Oracle. To further break this down: TOP Oracle, Oracle APEX and MOP V2 are supported. Additionally, Cloud and SAAS are also supported via the underlying technologies.

* 1. User Populations Supported via Three Directories

AATE supports various user populations that are tied to TSA’s main three identity stores. The three identity stores supported are: “Network” Active Directory, “Extra” Active Directory and Oracle Internet Directory. Applications with their own directory stores as well as the TIM platform are not supported by this solution.

* + 1. Network Active Directory (AD)

“Network” Active Directory is used on the Microsoft Platform and supports the user populations of TSA Employees and most TSA Contractors.

* + 1. Extra Active Directory (AD)

“Extra” Active Directory is used on the Microsoft Platform and supports the user populations of DHS, Other DHS Components, Other Government Agencies (OGA), Partners.

* + 1. Oracle Internet Directory (OID)

Oracle Directory is used on the Oracle Platform (TOP) and supports the user populations of TSA Employee and Contractors, DHS, Other DHS Components, Other Government Agencies (OGA) and Partners.

1. Platform by Platform and Methods
   1. Platforms

TSA has two main platforms with a number of frameworks that enable most of the TSA custom applications. Authentication at the Edge covers the following:

* MOP/.Net
* TOP Oracle
* Oracle APEX
* Cloud/SaaS/Other/AppAuth (DHS Auth as a Service)
  1. Supported Methods

There are several supported methods depending on the framework and particular application requirements. These Supported methods are:

* Windows Integrated Authentication (Kerberos)
* Oracle Access Manager
* Security Assertion Markup Language (SAML)
  + 1. Windows Integrated Authentication (WIA)

Windows Integrated Authentication (WIA or IWA) uses Kerberos to authenticate an application once the F5 PIV or Duo authentication has taken place to Active Directory. Below is a flow diagram of the F5 authentication flow. This is an Identity Provider (IdP) initiated flow.

*AATE Status Note: Testing revealed that F5 APM requires the password to do NTLM in the browser session. The users’ passwords will be randomized as TSA implements PIV User Based Enforcement (UBE) currently in process. Currently, it is believed that the applications will need to be changed authentication to use Kerberos or SAML. As TSA is preparing to move to the cloud, SAML is preferred. Engineers are continuing to explore ways to support NTLM apps with F5 APM without modification, but no method is known at this time.*

Figure 2 - F5 Flow Diagram for Internal .Net Applications



*AATE Status Note: By AATE Project closeout, .NetMOP/.Net F5 APM workflow not taken to production. NTLM does not work without the User Password which will be randomized with PIV UBE. See AATE Project Status Note in section 3.2.1 for more details. Kerberos is known working from the OWA workflow.*

* + 1. Oracle Access Manager protected Applications

Oracle Access Manager (OAM) currently manages authentication to TOP Oracle J2EE and EBS applications. Instead of presenting a login screen, OAM requests a SAML assertion from the F5. The F5 then runs through is authentication flow and send the SAML assertion to OAM. Below is a flow diagram of the F5 authentication flow. This is a service provider (SP) initiated flow.

Figure 3 - F5 Flow Diagram for External Oracle OAM Protected Applications



*AATE Status Note: Anakam TFA is being replaced by Duo. Duo is currently in procurement and not deployed yet.*

* + 1. Security Assertion Markup Language (SAML)

Many applications or systems can use SAML based authentication including cloud, SaaS, DHS AppAuth. Applications can also be written to use SAML directly, instead of through access managers. Once the F5 PIV or UserID/Password plus Duo authentication has taken place to Active Directory or other connected identity directories, a SAML assertion is produced and the user is forwarded to the application. The SAML Assertion to provide proof of authentication and needed attributes to downstream applications or systems. Below is a flow diagram of the F5 authentication flow. This is an IDP initiated flow.

Figure 4 - F5 Flow Diagram for SAML Applications. Cloud or SaaS



1. On-Boarding Work-To-Do

In order to on-board an application to the AATE, there are a number of steps that need to be accomplished.

* Information Gathering
* Developer Information
* User Preparation
* F5 APM Work-To-Do
* Application Changes Needed
  1. Information Gathering

Application On-boarding requires some information about the current context of your application. Please fill out the Questionnaire in **Appendix B for On-Premise Applications** or **Appendix C for SaaS application PRIOR to the INITIAL MEETING with the AATE team**.

* 1. Developer’s Information

Developers of internal TSA applications have to follow a process to integrate their application with the AATE. Below is a Process Diagram outlining the steps.

* + 1. Process Steps Outline

Figure 5 - F5 Flow Diagram for SAML Applications. Cloud or SaaS



* + 1. DFD Requirements

In order to use AATE and get into ITE, a DFD must be created showing the existing application infrastructure and the new linkage to AATE. AATE is shown as a black box as it has its own DFD. DFDs have to use a very specific template (on iShare DFD site) and are very detailed. Details needed include existing and new infrastructure, network links, Certificates, DNS names, urls, ip addresses, ports and protocols used and any external linkage. It then undergoes a formal review process. Once approved, it drives the needed infrastructure work to get into ITE.

* + 1. ITE-DEV Environment

TSA is heading toward getting rid of DTE as it moves to the Cloud. PIV validation infrastructure is not available in DTE. Development for PIV enabled application will need to be done in a carved out ITE-DEV environment. This is usually accomplished by separating off a part of the existing ITE application infrastructure. Best approach to setting up this ITE-Dev space will be discussed in the initial meeting.

* + 1. PIV Test Cards and Linking

PIV enabled applications in TSA ITE require the use of DHS Test PIV cards. Once the Test PIV card is obtained it needs to be linked to a test account in the appropriate directory store (Network AD, Extra AD or Oracle OID). The basic premise behind PIV is that the PIV card can be used to uniquely identify an account. As such:

* A PIV card can only be linked/associated with a single account within each directory.
* An AD or OID account can only have one PIV card linked/associated to it.

All Test PIV cards should be linked/associated with AD or OID Test accounts that match the PIV card itself and not linked to individual user accounts in ITE AD. For example:

* DUAL202.TESTCARD
* DUAL203.TESTCARD

These TEST accounts would then be used as user accounts within the application.

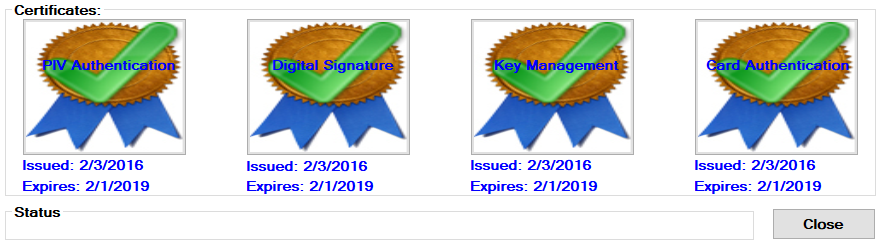
Additionally, two items need to be provisioned in ITE:

1. A Windows 10 Virtual Desktop (VD)
2. In order to access this VD, the NETWORK\ DUAL202.TESTCARD user account needs to be added to the **ADM-WKS-AllWorkstations-LclRdu** AD Group so that the account can be used to RDP into Windows 10 Virtual Desktop.

Once you get your VD:

1. Insert the TEST PIV card into your laptop
2. Launch RDP (i.e. mstsc) from your laptop and connect to one of the two ITE Windows jump boxes using your ITE AD Account credentials.
3. From the ITE Windows jumpbox, RDP to an ITE Windows 10 virtual desktop using your ITE AD Account credentials (requires #2 above)
4. Launch the “AuthentX Diagnostics Utility” from Windows to read the PIV card and validate the certificates on the card.

Figure 6 - AuthentX Certificate List



1. Once the PIV card has been validated to be good, the next step is to use the “validate PIV” tool/application to check the Test Account setup in ITE Active Directory (AD).  The URL is:  <https://vld8piv.tsa.dhs.gov>  The user interface for this utility is somewhat crude, but the it performs needed validation of the PIV card, access to the PIV card from the ITE Windows desktop, as well as the ITE PIV “infrastructure”.
2. The VLD8 test utility can help pinpoint any problems with the infrastructure or card linking. It runs three tests:
3. PIV card validation of the certificates against the DHS Test PKI
4. Tests that the PIV card unique identifier is associated with an account in Network AD and extracts the AD UPN value
5. Uses the UPN value and sees if the UPN is linked successfully to an Account in OID
   * 1. Note that not all cards will need to be linked in OID. If this is the case for your card, this test may show up as failed. This is OK for non-OID related applications.
6. F5 output screens below show successful VLD8 tests

Figure 7 - F5 APM - VLD8 Test Output 1

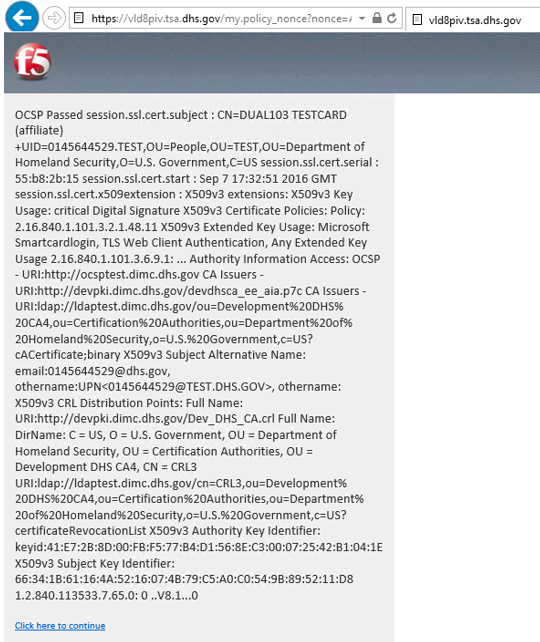


Figure 8 - F5 APM - VLD8 Test Output 2

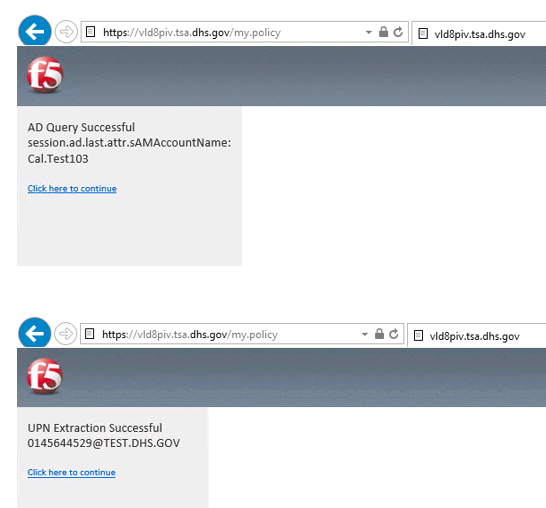
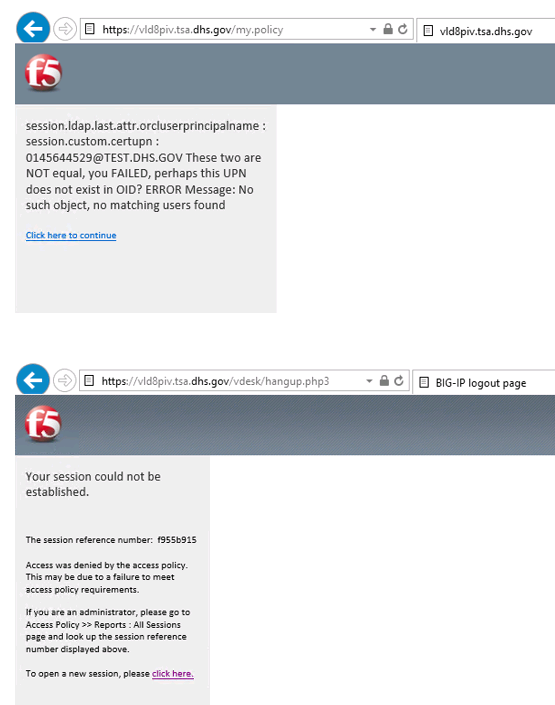


Figure 9 - F5 APM - VLD8 Test Output 3



1. Once all of the above are successful, your test card is properly working in the test AATE infrastructure.

Here are the high level steps to check the validity of a Test PIV card and to validate the account setup for the Test PIV account.

Use a Windows 10 machine that is joined to the ITE domain to validate the PIV card.

1. Launch the “AuthentX Diagnostics Utility” to read the PIV card and validate the certificates on the card.
2. Once the PIV card has been validated to be good, the next step is to use the “validate PIV” application to check the Test Account setup in ITE Active Directory (AD).  The URL is:  <https://vld8piv.tsa.dhs.gov>

Note that an ITE Windows 10 Virtual desktop can be used if a physical device is not available.  Here are the specifics steps to accomplish this:

1. Insert the TEST PIV card into your laptop
2. Launch RDP (i.e. mstsc) from your laptop and connect to one of the two ITE Windows jump boxes using your ITE AD Account credentials.
3. From the ITE Windows jumpbox, RDP to an ITE Windows 10 virtual desktop using your ITE AD Account credentials
4. Proceed with Step 1 above.

Sample Test Card Info

Issued To: DUAL109 TEST CARD (affiliate)

First Name: DUAL109

Last Name: TEST CARD

MSN: 00886748

Serial Number: 987C023A18

EDIPI: 0821048288  
Email: 0821048288@dhs.gov

Friendly Name: DUAL109 TEST CARD (affiliate)'s U.S. Government PIV Authentication

RFC822 Name= 0821048288@dhs.gov

Other Name:

Principal Name=0821048288@TEST.DHS.GOV

SSN: 100000109

DOB: 1/1/1985

CN=DUAL109 TEST CARD (affiliate)

OU=People

OU=TEST

OU=Department of Homeland Security

O=U.S. Government

C=US

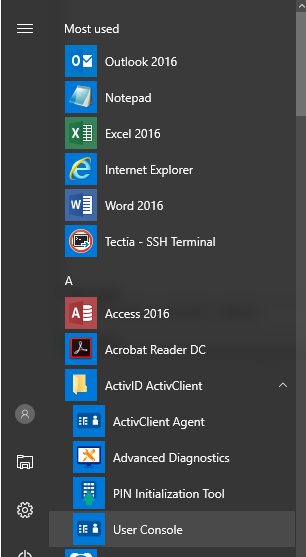
AD PW = Pa$$word123456

PIN Card code = 123456

Retrieving Test Card Information

1. On your Windows 10 desktop, insert your Test PIV card and then launch the **User Console** application under the ActivIntitiy ActivClient application group:

Figure 10 - ActivClient User Console Application Location



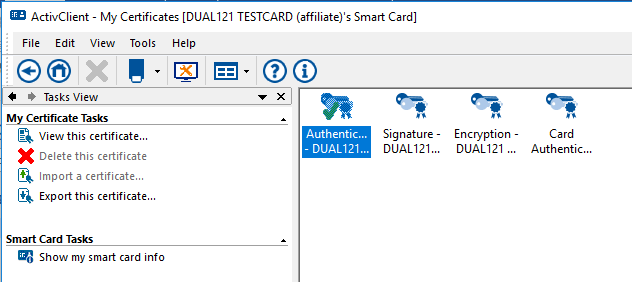
1. Double-click on ‘My Certificates’:

Figure 11 - ActivClient My Certificates Options



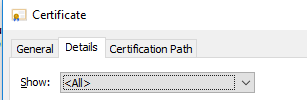
1. Double-click on the ‘Authentication’ certificate:

Figure 12 - ActivClient My Certificates Output



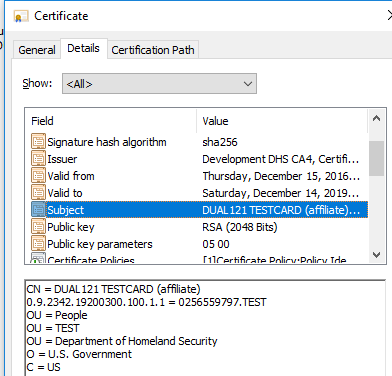
1. In the dialog box that now appears, click on the ‘Details’ tab:

Figure 13 - Certificate Detail Box



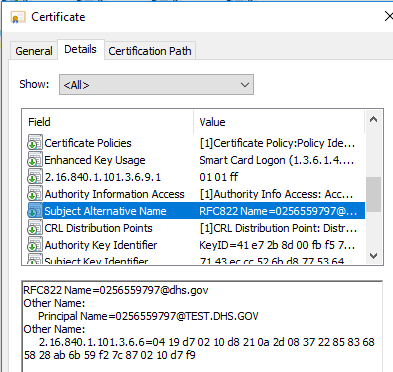
1. Scroll down to the ‘Subject’ attribute and click on it. Capture a screen shot for sharing the card info. Recommend using the Windows Snipping Tool to just ‘snip’ the needed portion (as below).

Figure 14 - Certificate Details



1. Scroll down to the ‘Subject Alternative Name’ attribute and click on it. Capture a screen shot for sharing the card info. Recommend using the Windows Snipping Tool to just ‘snip’ the needed portion (as below).

Figure 15 - Subject Alternate Name Details



Issued To: DUAL109 TEST CARD (affiliate)

First Name: DUAL109

Last Name: TEST CARD

MSN: 00886748

Serial Number: 987C023A18

EDIPI: 0821048288  
Email: 0821048288@dhs.gov

Friendly Name: DUAL109 TEST CARD (affiliate)'s U.S. Government PIV Authentication

RFC822 Name= 0821048288@dhs.gov

Other Name:

Principal Name=0821048288@TEST.DHS.GOV

SSN: 100000109

DOB: 1/1/1985

Create The Test Card User in Active Directory

Create the Test Card User in the following container (Network AD Example, Extra AD Similar):

Domain: **.network.ad.tsa.gov**

OU: **TSA**

OU: **EUS**

OU: **Users**

OU: **General**

**Note: Adding a user to AD is a privileged action and may require a Support ticket to be created for the Test environment support staff to create the AD account.**

Figure 16 - AD Container Screen

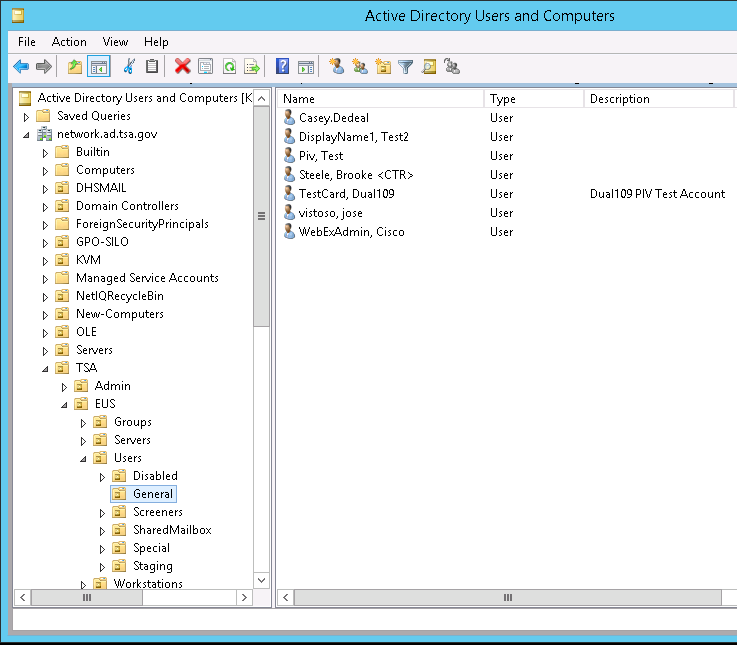
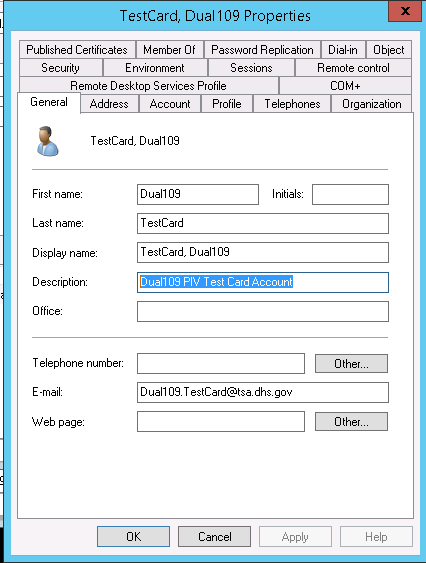
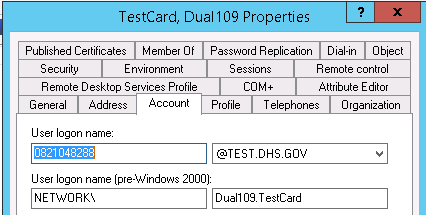


Figure 17 - User Account Details 1



Make sure the EDIPI number for the card is specified in the AD User Logon Name (the domain must be @TEST.DHS.GOV)

Figure 18 - User Account Details 2

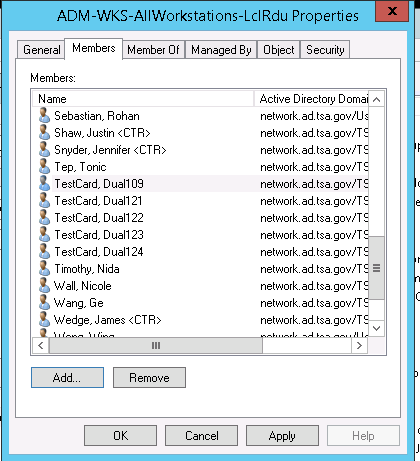


Note: Oracle OID is similar. The attribute in OID is orclUserPrincipalName.

Enable RDP to Windows 10 Virtual Desktops

Add the Test Card User to the **ADM-WKS-AllWorkstations-LclRdu** AD Group so the user can RDP into Windows 10 Virtual Desktops.

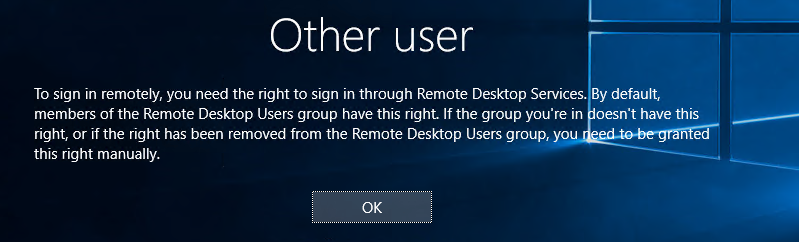
Figure 19 - Group Membership Details



This is important. If the account is not a member of the **ADM-WKS-AllWorkstations-LclRdu**

Group, you will get the following error screen.

Figure 20 - RDP Error Screen

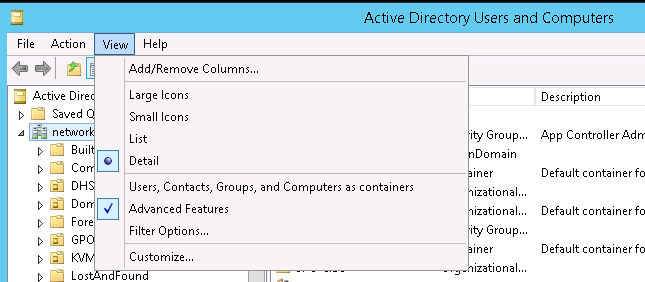


**Optional if test user needs e-mail or OWA access**

To manually set the iShare Contact Information so that the Test User account can test OWA

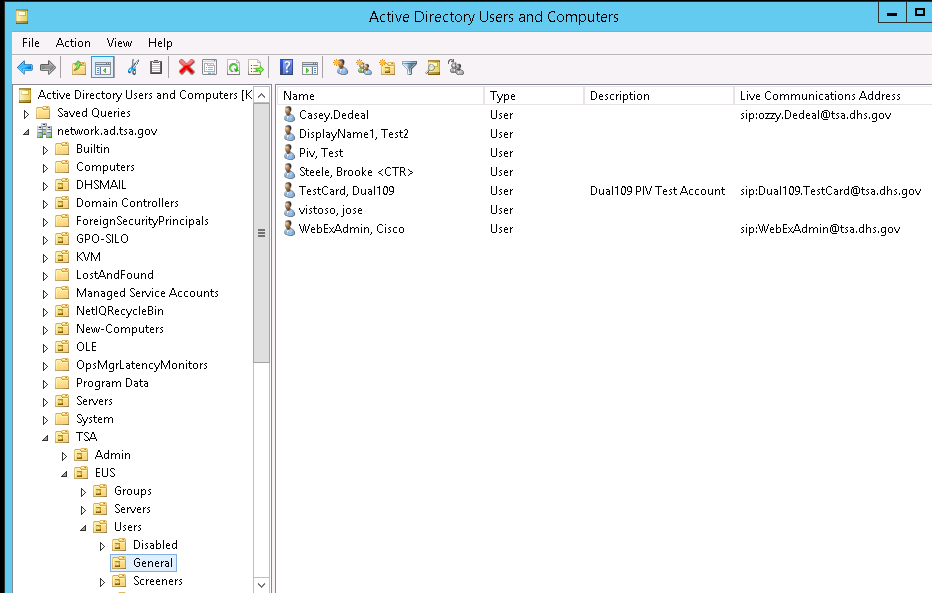
1. Request that a mailbox be created for the Account
2. As an Admin:

Figure 21 - E-mail Account Setup 1



1. Navigate the Test User

Figure 22 - E-mail Account Setup 2



1. Do properties

Figure 23 - E-Mail Account Setup 3

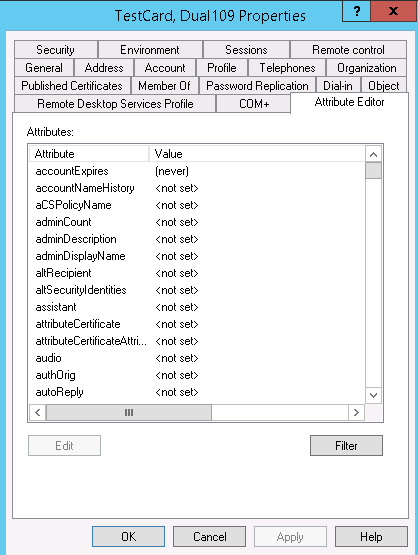


Figure 24 - E-mail Account Setup 4

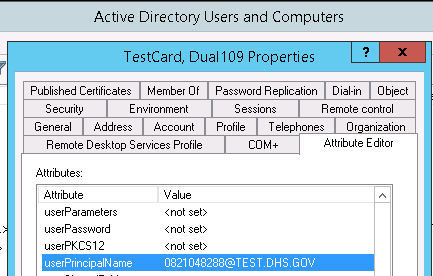
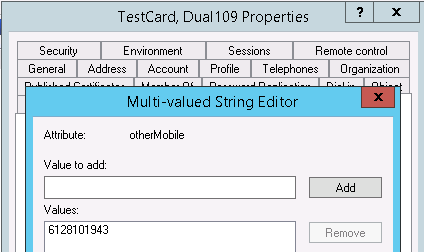


Figure 25 - E-Mail Account Setup 5



Note that this equates to the same user field under ‘Telephone’ and ‘Other…’

* + 1. Additional SAML Information

F5 APM is acting as TSA’s SAML Identity Provider (IdP) and can provide SAML Assertion after authenticating to TSA’s main three Identity Stores (Network AD, Extra AD or Oracle OID). F5 APM is flexible and can accommodate IdP initiated SAML of SP (RP) initiated SAML. IdP initiated is preferred except in certain complex cases.

**SAML Flows – User Perspective (Source Oracle Blog** <https://blogs.oracle.com/dcarru/sp-vs-idp-initiated-sso>**)**

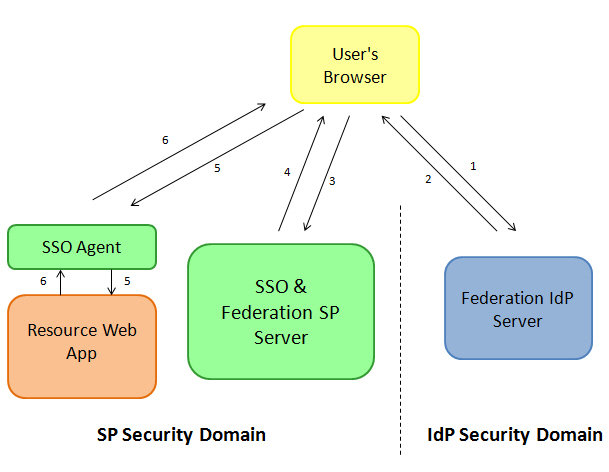
**IdP Initiated SAML User Flow**

This use case is that the User starts by going to an F5 protected URL.

The IdP initiated SAML flow would involve the following steps:

1. The user's browser accesses the IdP to start a Federation SSO flow by specifying
   1. The SP to be used
   2. Optionally the URL where the user's browser should be redirected after the Federation SSO is complete
2. After having identified the user, the IdP creates an SSO Response with a SAML 2.0 Assertion containing user information as well as authentication data, and redirects the user's browser to the SP with the message and the RelayState parameter
3. The user's browser presents the SSO response to the SP server
4. The SP validates the SAML 2.0 Assertion and creates an SSO session for the user. The SSO server will then redirect the user's browser back to the resource originally requested
5. The user's browser requests access to the resource. This time the SSO Web Agent grants access to the resource
6. The Web Application returns a response to the user's browser

Figure 26 - SAML IdP Initiated User Flow



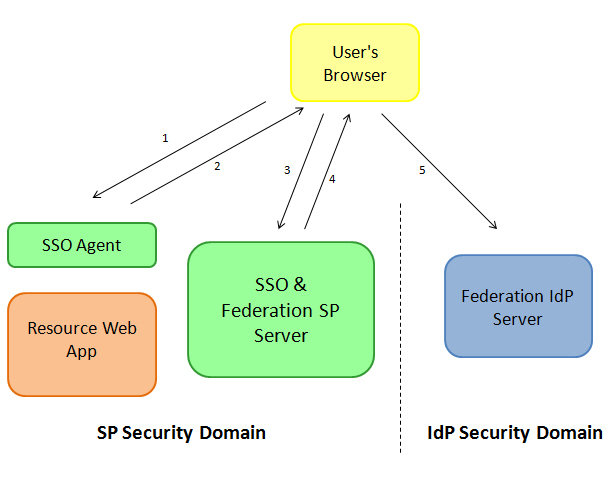
**SP Initiated SAML User Flow**

This use case is that the User starts by going to the SaaS or SP protected URL.

The IdP initiated SAML flow would involve the following steps:

1. User's browser request access to a protected resource
2. The SSO Web Agent intercepts the call, determines that the user needs to be authenticated and issues a redirect back to the user's browser
3. The user's browser accesses the SSO server, being redirected by the SSO Web Agent
4. The SSO Server determines that the user should be authenticated via Federation SSO, selects an IdP, creates a SAML 2.0 AuthnRequest message, saves the operational state in the SSO server store and redirects the user's browser to the IdP with the SAML message and a string referencing the operational state at the SP
5. The user's browser accesses the IdP SAML 2.0 service with the AuthnRequest message.

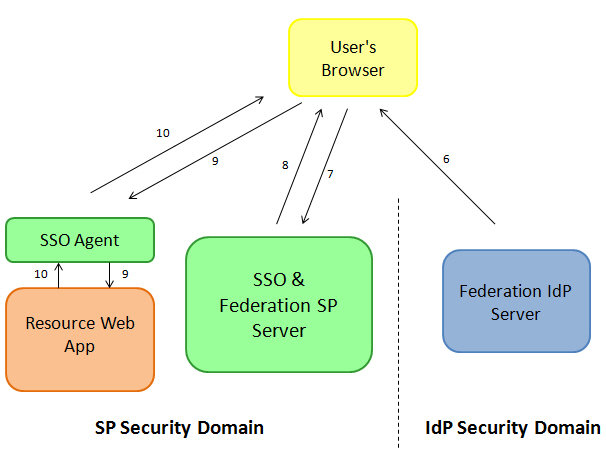
Figure 27 - SAML SP initiated User Flow 1



Once the IdP receives the SAML 2.0 AuthnRequest message, the server will determine if the user needs to be challenged (not authenticated yet, session timed out...). After the possible identification of the user, the Federation SSO flow will resume:

1. The IdP creates an SSO Response with a SAML 2.0 Assertion containing user information as well as authentication data, and redirects the user's browser to the SP with the message and the RelayState parameter
2. The user's browser presents the SSO response to the SP server
3. The SP validates the SAML 2.0 Assertion and creates an SSO session for the user. The SSO server will then redirect the user's browser back to the resource originally requested
4. The user's browser requests access to the resource. This time the SSO Web Agent grants access to the resource
5. The Web Application returns a response to the user's browser

Figure 28 - SAML SP Initiated User Flow 2



**SAML Metadata**

TSA’s current SAML metadata provides three main attributes from Network AD. These are:

* ADUPN – EDIPI rom the PIV card linked to the AD user Account (0123456789@tsa.dhs.gov)
* ADMail – TSA e-mail Address
* CN – Common Name

Note that other directory (AD or OID) attributes can be added to the SAML assertion metadata. Application developers will need provide their requirements.

* 1. User Preparation

All users need a one-time preparation step, if not already done. This step can be done via self-service for most users and is very easy.

* + 1. PIV to Directory Linking
* PIV Card Provisioning and Enabling System (PCPES) for Network AD, Extra AD or OID

The user’s PIV card (unique identifier) must be linked to the identity store account that the application uses.

*“Network” Active Directory (AD)*

“Network” Active Directory (AD) linking is done when the PIV card is created in the badging offices. Users of any applications using Network AD as their identity store will not need to do any additional linking for those applications. PCPES for Network AD is also available at: <https://pcpes.tsa.dhs.gov>.

*Oracle Internet Directory (OID)*

Most TSA employees and contractors have had their OID accounts pre-linked to their PIV cards via a project in 2016 that matched their Network AD accounts with their OID accounts. There were some users that could not be automatically matched and any new users since that project will not be pre-linked. They will need to run the PCPES for OID linking self-service at: <https://pcpes.tsa.dhs.gov/oid>. This linking needs to be done on TSA Net either internally or on VPN via their GFE equipment.

*“Extra” Active Directory (AD)*

This will all users in DHS, other DHS components and other government agencies (OGA) to link their PIV cards to their accounts in “Extra” Active Directory. This is really a future capability, as the DHS system to do PIV validation for other Government agencies (OGA) is not finished yet.

They will need to run the PCPES for EXTRA linking self-service at: <https://pcpes.tsa.dhs.gov/extra>. This is currently available on TSANet.

*AATE Project Status Note: At AATE project closeout, PCPES for Extra AD and OID are tested and in production. They are currently turned down pending first need.*

* + 1. Duo Registration

Duo is a soft token system that sends a one-time code via an “out-of-band” method. These methods are: SMS message, e-mail message to private e-mail and Voice (IVR). There is a one-time registration process where the end user needs to register the contact information needed so the tokens can be send.

*AATE Status Note: Duo is replacing Anakam TFA and this section will need to be revised once Duo is deployed. It is currently in the procurement process.*

* 1. F5 APM Work-To-Do

The Authentication at the Edge project developed several F5 APM workflows to cover basic PIV and Duo based authentication. There is some F5 work-to-do for each application to be enabled.

* + 1. Application URL(s)

The existing application URL (or a new one if desired) needs to be tied to the F5 APM AATE workflow. If your application uses shared URLs, this may be a good time to make a separate URL for each application to ease the transition to the cloud. The current cloud strategy is to have each application “self-contained”.

* + 1. Base AATE Flows may need to be adjusted for application eccentricities

The AATE team talked to many application groups and tried to come up with a good set of common interfaces. Some applications will probably have some “eccentricities” that may require some work to these basic F5 workflows.

To keep this custom work to a minimum, applications should follow one of these authentication patterns:

* Windows Applications – Windows Integrated Authentication or SAML using “Network” or “Extra” AD
* Oracle or J2EE applications – Oracle Access Manager protected or SAML using OID
  + 1. The F5 APM work has to follow the standard TSA SELC processes
* ITE Testing, RFCs, Production Cutover
  + DFD or SDD creation or update
  + Ensure that the test teams have valid DHS ITE Test PIV cards
  + Create Test accounts in Application to match ITE Test PIV cards
  + Register ITE test user in Duo, Link the ITE User in PCPES
  + SAML linkage (metadata exchange and certificate exchange)
* RFCs/Release Management
  + As Required – Standard processes
* Production Cutover
  + Once successfully tested in ITE, the application changes should be moved to the production environment in consultation with OED. The timing of the application changes need to be coordinated with the F5 team to ensure that the work flow is moved to production. This will require an RFC and use the normal TSA SELC process.
* This work can be accomplished as part of an existing application project or a separate onboarding project. The duration of the on-boarding effort will require a project, it is not covered by OIT O&M.
  1. User Communications

While application changes have been minimized, the user preparation, login screen differences, cutover dates and support information will need to be communicated to affected users well in advance by the application development team following the standard user communication process. For large user population it is recommended to roll this out in a phased approach – pilot and then logical groups of users.

* + 1. Communicate and ensure required User Preparation Steps and Completion

Users possibly need to do a one-time PIV linking or Duo registration in order to authenticate to the application. This needs to be communicated to the affected users. See section 3.2 for information on this.

* + 1. Communicate login differences/login page changes

The login page will be different from the one they currently use. The F5 will present a “dual” login page (PIV and Duo) in most cases. This will need to be communicated to the users.

* + 1. Communicate cutover date and information

Users will need to be informed of the cutover date and any new access information.

* + 1. Communication how to get support information

If there is any new support information (how to get help) is needed, this should be communicated.

* 1. Application Changes
     1. Application code changes should be minimal to none for supported methods
* Windows Applications – Windows Integrated Authentication or SAML using “Network” or “Extra” AD
* Oracle or J2EE applications – Oracle Access Manager protected or SAML using OID. Logout functionality changes might need to revisited while onboarding the applications.
  + 1. Outlier Application types that may need more work
* Applications that have their own identity store
  + Applications should target or migrate to one of the three main identity store that TSA supports.
  + If this is impossible, there will need to be unique identifier in common between the application identity store and one of the three main TSA identity stores for unique matching. Currently TSA has e-mail address and PIV EDIPI number as unique identifiers. E-mail address while unique, is not completely consistent as the format has changed several times in the past. Using e-mail address may incur large number of mismatches in applications not using the current e-mail format consistently.
* Applications that use direct LDAP authentication calls to Active Directory or NTLM
  + Applications that use direct LDAP authentication calls to Active Directory or NTLM will not work once TSA moves to PIV User Based Enforcement (UBE) by end of FY2017. When PIV UBE is enabled, the user will no longer know their AD password (it will be randomized to a 128-bit value) so LDAP UserID/Password authentication or NTLM authentication via F5 APM browser session will not be possible.
  + These applications should move Windows Integrated Authentication methods of SAML or Kerberos. SAML is preferred as TSA is moving to the Cloud.
* “Standalone” Oracle and J2EE applications
  + These applications should become Oracle Access Manager (OAM) protected and enabled
* Mobile Applications
  + Mobile PIV is still a problem area. There is resistance to buying PIV sleds for mobile devices and the DHS PIV derived credential solution is not completed.

1. Glossary and Definitions

Table 1 - Glossary and Definitions

|  |  |  |
| --- | --- | --- |
| AD | Active Directory | Microsoft Active Directory Service – Used as an Identity Store for Microsoft Platform and some applications |
| AATE | Authentication at the Edge | Authentication at the Edge (AATE) is TSA’s moniker for a set of Authentication and Access Management technologies that provide PIV and multi-factor non-PIV Authentication services via F5 Access Policy Manager (APM). This provides authentication, access management, Federation and Single-Sign On (SSO) services to downstream applications and systems. |
| ADFS | Active Directory Federation Service |  |
| APM | F5 Access Policy Manager |  |
| DTE | Development Test Environment | TSA Environment for Application Development |
| DUO | Duo Trusted Access | Two Factor Authentication system employing Soft Tokens |
| EDIPI | Electronic Data Interchange Primary Identifier | A ten-digit number, usually associated with a suffix identifying Agency and component. Example: 1234567890@tsa.dhs.gov. EDIPI plus suffix guaranteed unique across DHS. Used as a unique identifier and UPN login to Active Directory |
| GFE | Government Furnished Equipment |  |
| IDP | Identity Provider | In a federated identity management system, there are two main parts. The Identity Provider (used to assert the user is who they say they are) and the Service Provider (Application relying on the proof the IDP sends) |
| ITE | Integrated Test Environment | TSA Environment for Application Testing within the whole TSA ecosystem |
| LDAP | Lightweight Directory Access Protocol | A digital signature is an encryption based method using PKI certificates and public/private keys to verify the authenticity and integrity of software, email, or a digital document |
| OAM | Oracle Access Manager | An Access control and Single Sign-on product used to protect Oracle and J2EE Application on the TSA Operating Platform (TOP) |
| OGA | Other Government Agencies | Used to describe other government agencies outside DHS and other DHS Components |
| OID | Oracle Internet Directory | Oracle Directory Service – Used as an Identity Store for Oracle Platform and some applications |
| PCPES | PIV Card Provisioning and Enabling System | A badging station and self-service utility application used to copy the EDIPI off the PIV and put it into a directory where it can be used for login or user matching between directories |
| PIV | Personal Identity Verification | A United States Federal smart card that contains the necessary data for the cardholder to be granted to Federal facilities and information systems and assure appropriate levels of security for all applicable Federal applications. |
| RP | Relying Party | See Service Provider (SP) |
| SAML | Security Assertion Markup Language | The private part of a key pair. Private keys are generated on the client whenever a certificate request is made. Private keys must be securely stored to prevent unauthorized access and accidental deletion. In general, information encrypted with a private key can only be decrypted with the corresponding public key. A digital signature involves encrypting messages with a private key and allows anyone with a corresponding public key to decrypt the message to be certain of who sent the message and that it has not been tampered with. |
| SP | Service Provider | In a federated identity management system, there are two main parts. The Identity Provider (used to assert the user is who they say they are) and the Service Provider (Application relying on the proof the IDP sends). The SP is also known as the Relying Party. |
| TFA | Two Factor Authentication | Soft Token Two Factor Authentication used to add a second factor of authentication to strengthen UserID and Password based applications. Used where PIV cannot be done. Duo is being procured to meet this requirement as an Anakam replacement. |
| WIA | Windows Integrated Authentication | A Microsoft term to group some Microsoft Authentication Methods like NTLM and Kerberos. |

1. Initial Meeting Questionnaire for On-Premises Applications

Please fill out the questionnaire completely and provide a copy of the current DFD (Data Flow Diagram) or SDD (System Design Document). Please send this information to the AATE team PRIOR to the first meeting with the AATE team.

Which On-Premises Platform

What platform does the application current reside on: Top Oracle, Oracle APEX, MOP, Other (specify)? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Which Framework

What framework does your application use  
\_\_\_\_ .Net

\_\_\_\_ J2EE

\_\_\_\_ Oracle EBS

\_\_\_\_ SharePoint

\_\_\_\_ TIBCO

\_\_\_\_ Other (Specify) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

User Populations and Quantities

Please specify the user population type and approximate quantities of users

Quantities

\_\_\_\_ TSA Employees and Contractors

\_\_\_\_ DHS and other DHS Components

\_\_\_\_ Other Federal Government Agencies (non-TSA and non-DHS)

\_\_\_\_ Partners, other Government and non-Government

Coming from Inside, Outside, Both or AppAuth

Please specify where your users are coming in from:

\_\_\_\_ Inside TSA (TSANet)

\_\_\_\_ Outside (Internet Facing)

\_\_\_\_ AppAuth (DHSNet)

Client Hardware to support

\_\_\_\_ GFE \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_ non-GFE \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Describe how the application currently authenticates

Description: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Current SSO solution

\_\_\_\_ Windows Integrated Authentication

\_\_\_\_ Oracle Access Manager

\_\_\_\_ Other (Specify) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Multi-Factored Type Required

\_\_\_ PIV

\_\_\_\_ UserID/Password plus Duo

Duo provides Soft Token additional authentication factor. This is only used where PIV is not required, but multi-factor authentication is required (Medium and High CIA systems).

Where are the user accounts stored currently?

\_\_\_\_ Network Active Directory (AD)

\_\_\_\_ Extra Active Directory (AD)

\_\_\_\_\_ Oracle Internet Directory (OID)

\_\_\_\_\_ Other (Specify) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Current Application URL (s) – ITE and PROD

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Copy of Current System Design Document (SDD) or Data Flow Diagram (DFD)

Please provide copy of current SDD or DFD

Required SAML Authentication Flow – IDP or SP initiated

In order to ease future transition to Cloud providers, TSA prefers to use F5 APM for SAML authentication and Single Sign-On. Note: Oracle OAM protected applications are always SP initiated.

\_\_\_\_ IDP Initiated (Preferred):

Authentication happens at the F5 then the user and SAML assertion is passed to the application. F5 provides URL protection, Load balancing and authentication services.

\_\_\_\_ SP Initiated:

Application requests a SAML assertion from F5 APM and then accepts the assertion for authentication.

1. Initial Meeting Questionnaire for SaaS Applications

Please fill out the questionnaire completely and provide a copy of the current TSA DFD (Data Flow Diagram) or separate diagram showing TSA interfaces. This information is required PRIOR to the first meeting with the TSA OIT team. This guide and questionnaire is for SaaS Application On-boarding to be used by Third Parties.

Short Background Information on the Application

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Vendor Contacts

Business/Project Contact Information: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Technical SAML Contact Information: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

TSA Project Contact Information: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

User Populations and Quantities

Please specify the user population type and approximate quantities of users

Quantities

\_\_\_\_ TSA Employees and Contractors

\_\_\_\_ DHS and other DHS Components

\_\_\_\_ Other Federal Government Agencies (non-TSA and non-DHS)

\_\_\_\_ Partners, other Government and non-Government

Client Hardware to support

\_\_\_\_ GFE - Types: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_ non-GFE - Types: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Describe how the application currently authenticates

Description: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Does your application or access management infrastructure support SAML? If so, does it use an access manager? Which one?**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Current User Identity Store, Unique User Identifier and other attributes required

Current User Identity Store: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Current User Unique Identifier: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Other Required Attributes to be sent in SAML Assertion: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Current Application URL(s) – Test and Production

Test: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Prod:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Need Copy of TSA Approved Dataflow Diagram (DFD) or diagram showing SAML Service Provider Infrastructure. Must include URLs, IP ranges, host names, Ports needed open (needed for firewall and whitelisting for access from TSA).

Please provide copy of current SDD or DFD

Required SAML Authentication Flow – IDP or SP initiated

In order to ease future transition to Cloud providers, TSA prefers to use F5 APM for SAML authentication and Single Sign-On.

\_\_\_\_ IDP Initiated (Preferred):

Authentication happens at the F5 (APM) then the user and SAML assertion is passed to the application. F5 provides URL protection and authentication services.

\_\_\_\_ SP Initiated:

Application requests a SAML assertion from F5 APM and then accepts the assertion for authentication. This is not the preferred approach, please provide justification why IdP initiated SAML cannot be used. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_