ORNL/TM-2019/1235

Using Pulse Connect Secure© to Implement Multi-Factor Authentication Solutions

B. Nance

August 12, 2019

OAK RIDGE NATIONAL LABORATORY
MANAGED BY UT-BATTELLE FOR THE US DEPARTMENT OF ENERGY

ORNL/TM-2019/1235

Data System Sciences and Engineering
Center for Infrastructure Security Analysis

Using Pulse Connect Secure© to Implement Multi-Factor Authentication Solutions

Brad Nance

August 12, 2019

Prepared by
OAK RIDGE NATIONAL LABORATORY
Oak Ridge, TN 37831-6283
managed by
UT-BATTELLE, LLC
for the
US DEPARTMENT OF ENERGY
under contract DE-AC05-00OR22725

CONTENTS

ACRONYMS

ADFS	Active Directory Federation Services
AWS	Amazon Web Services
CA	Certificate Authority
CFATS	Chemical Facility Anti-Terrorism Standards
CN	Common Name
DHS	U.S. Department of Homeland Security
HTML	Hypertext Markup Language
IAM	Identity and Access Management
IdP	Identity Provider
IIS	Microsoft Internet Information Services
IP	Internet Protocol
LDAP	Lightweight Directory Access Protocol
MFA	multi-factor authentication
ORNL	Oak Ridge National Laboratory
PCS	Pulse Connect Secure©
PIV	Personal Identity Verification
SAML	Security Assertion Markup Language
SP	Service Provider
SSL	Secure Socket Layer
SSO	Single Sign On
URL	Uniform Resource Locator
VPN	Virtual Private Network

ABSTRACT

Pulse Connect Secure© (PCS) is a trusted platform for government agencies to provide secure access to web portals. As more and more accounts are being hacked and web sites are being compromised, single-factor authentication with a username and password has become insufficient to adequately protect authenticated web portals. Multi-factor authentication (MFA), granting user access only when two or more independent pieces of information are presented, has become a necessary tool in the prevention of security breaches.

This paper provides an overview of three MFA solutions that utilize the features of PCS. Categories include Personal Identity Verification (PIV) card authentication, service provider initiated (SP–initiated) Security Assertion Markup Language based (SAML–based) authentication, and identity provider initiated (IdP–initiated) SAML–based authentication.

1. INTRODUCTION

For more than a decade, Pulse Connect Secure© (PCS) Secure Socket Layer (SSL) Virtual Private Network (VPN) (formerly Juniper SSL VPN) has been a trusted partner for government agencies in providing secure access to web portals. As more and more accounts are being hacked and web sites are being compromised, single-factor authentication with a username and password has become insufficient in adequately protecting authenticated web portals. Multi-factor authentication (MFA), granting user access *only* when two or more independent pieces of information are presented, now has become a necessary tool in the prevention of security breaches.

This white paper will present three MFA solutions that utilize the features of PCS. The first utilizes a certificate authentication server to implement authentication using a client-side certificate presented by a Personal Identity Verification (PIV) card. The second solution uses Security Assertion Markup Language based (SAML–based) authentication wherein PCS acts as a Service Provider (SP) that reaches out to an Identity Provider (IdP) to implement authentication. The third solution uses a SAML–based authentication wherein PCS acts as the IdP that forwards the user to the SP once the user has successfully authenticated using a PIV card.

2. PULSE CONNECT SECURE© ARCHITECTURE

The PCS SSL VPN appliance has several multi-level components that work together to provide a customizable user interface and an authentication framework for securely accessing protected resources. The high-level architecture of PCS, further explained in this section, is depicted in Figure 1.

The PCS architectural components are as follows:

- **Sign-in Policies –** The entry point, i.e., the Uniform Resource Locator (URL), used to access a PCS configuration.
- **Sign-in Pages –** The underlying customizable Hypertext Markup Language (HTML) used to render the user interface.
- **Authentication Realm –** A set of configured servers and policies that define the behavior of the secure portal.
- **Authentication Server –** The part of the interface that is responsible for the first challenge to the end user to validate their identity.
- **Authorization Server –** The part of the configuration that ultimately provides the identity of the authorized user to the underlying applications.
- **Authentication Policy –** The part of the configuration that limits access to a secure portal, based upon limiting parameters such as source Internet Protocol (IP) address or client-side certificate requirement.
- **Role Mapping –** The process of assigning user roles to an authorized user.

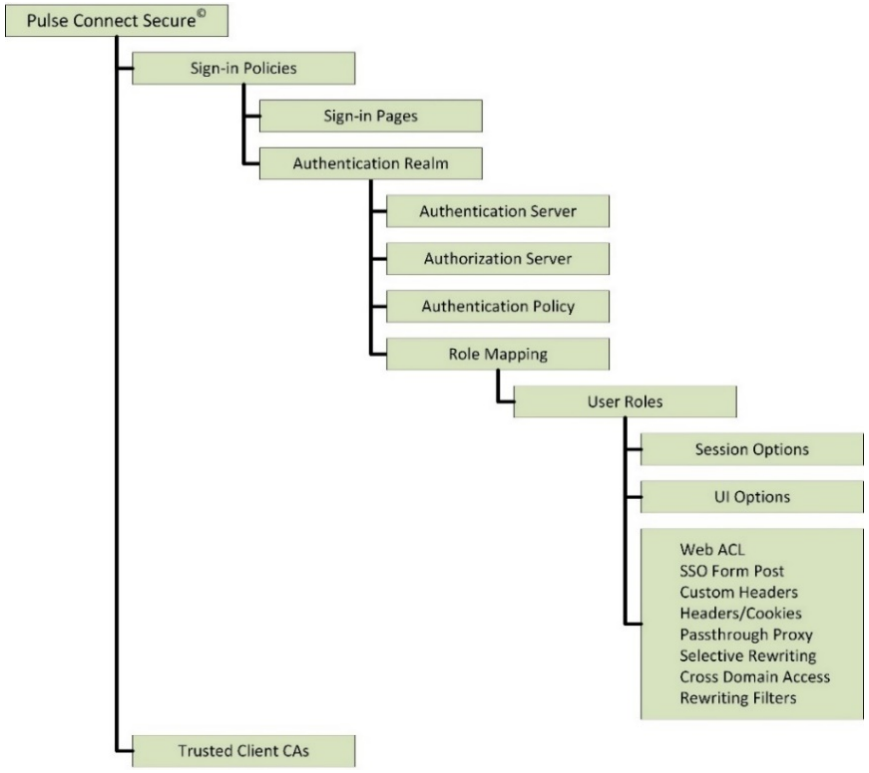

Figure 1. Pulse Connect Secure© architecture.

- **User Roles –** Categorizations of an authorized user that are based upon account attributes, including username and Lightweight Directory Access Protocol (LDAP) group membership, and are used to determine session options, user interface options, and other resource policies.
- **Trusted Client Certificate Authorities –** Intermediate and root certificate authorities (CAs) that *bgt5define client-side certificates that can be used to authenticate to a certificate-based authentication server.

3. SAML–BASED AUTHENTICATION

SAML is an open standard defining interaction between the user, the SP, and the IdP. The interaction between the SP and the IdP includes a one-time exchange of SAML metadata that is used to establish a trust relationship between the SP and the IdP. The exchange includes an entity ID that acts as a unique identifier for the metadata. The interaction between the user and SP/IdP occurs in the form of SAML requests and responses that take place throughout the authentication and authorization process. At the end of a successful authentication process, the SAML response includes an assertion that includes any user account attributes that need to be shared between entities.

PCS supports the SAML standard and can act as either an SP or an IdP, depending upon the configuration. When acting as the SP, PCS interacts with SAML–based IdPs that validate the identity of the end user. Examples of IdPs include Active Directory Federation Services (ADFS) and access management appliances/services. When acting as the IdP, PCS interacts with SAML–based SPs such as the Amazon Web Services (AWS) Management Console (MC). AWS MC can be configured as a SAML provider under their Identity and Access Management (IAM) category of services.

ADFS is a service provided by Microsoft wherein the user identity is validated using an enterprise Active Directory. Two examples of ADFS IdPs are AppAuth from the DHS at https://sso.dhs.gov and the Oak Ridge National Laboratory Single Sign On (ORNL SSO) at https://devintidp.ornl.gov/idp.

An example of an access management appliance is the SecureAuth IdP (https://www.secureauth.com) that at its core is a Microsoft Internet Information Server (IIS) website that provides cloud-based authentication services that support a myriad of MFA scenarios. For instance, SecureAuth IdP is used to support two-factor authentication for web portals that support the DHS CFATS program. The underlying web pages are highly customizable and provide seamless integration with PCS.

4. MFA SOLUTIONS

This section describes three MFA solutions utilizing the features of PCS. A required component of each solution is a method to map the authenticated user (i.e., the user whose identity is verified by the authentication process) to the authorized user (i.e., the user who is granted access to the underlying applications). In most cases, the authenticated user exists in a different domain from the authorized user; therefore, mapping is accomplished by passing an attribute from the authenticated user that uniquely identifies the authorized user. Unique identifiers include information such as username, email address, or badge number. The attribute in the authorized user's domain can be an existing one that already uniquely identifies the account or one that is added for the sole purpose of an MFA integration. The method of establishing this "link" between the two accounts will be covered with each solution presented in this section.

4.1 SOLUTION 1: PIV CARD AUTHENTICATION

This solution demonstrates a configuration that is integrated within PCS. In this case, integration means that neither an IdP nor an SP is used for the implementation and that the solution utilizes the core features of PCS. With this solution, the end user authenticates using a client-side certificate presented from a PIV card. Figure 2 shows the PIV card authentication process.

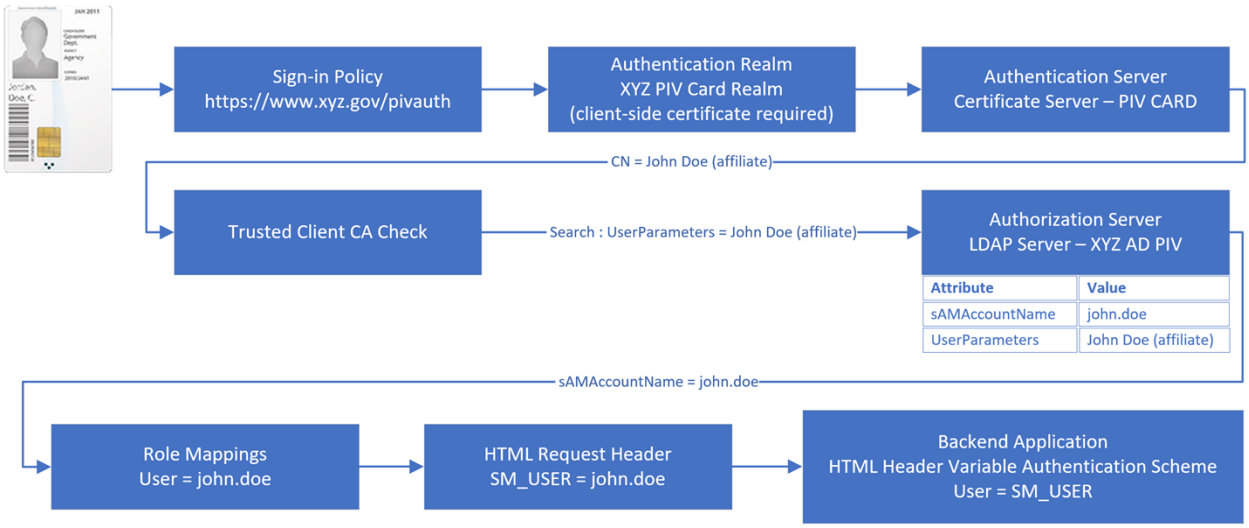

Figure 2. PIV card authentication flow.

The steps depicted in Figure 2 are defined as follows:

- The Sign-in Policy https://www.xyz.com/pivauth provides the URL for accessing the website.
- The Sign-in Policy is configured to access the Authentication Realm named XYZ PIV Card Realm, which has an Authentication Policy that requires a client-side certificate.
- The Authentication Realm is configured to use the Authentication Server of type Certificate Server named PIV CARD. PIV CARD passes the Common Name (CN) attribute from the client-side certificate to the Authorization Server.
- The list of Trusted Client CAs is checked for the Intermediate and root CAs for the client-side certificate that is presented.
- The Authentication Realm is configured to use an Authorization Server of type LDAP Server named XYZ AD PIV. This authorization server, XYZ AD PIV, is configured to search for the user with UserParameters attribute matching the CN attribute from the client-side certificate.
- The Authentication Realm is configured to assign User Roles based upon the Role Mapping rules for the authorized user.
- Policies for Custom Headers and Headers/Cookies allow the authorized username to be passed to the backend applications via an HTML request header.

4.2 SOLUTION 2: SERVICE PROVIDER INITIATED SAML–BASED AUTHENTICATION

This solution is described as SP–initiated SAML–based authentication because the end user initiates the authentication process by first accessing the PCS which is acting as the SP. Figure 3 shows the authentication flow for this solution.

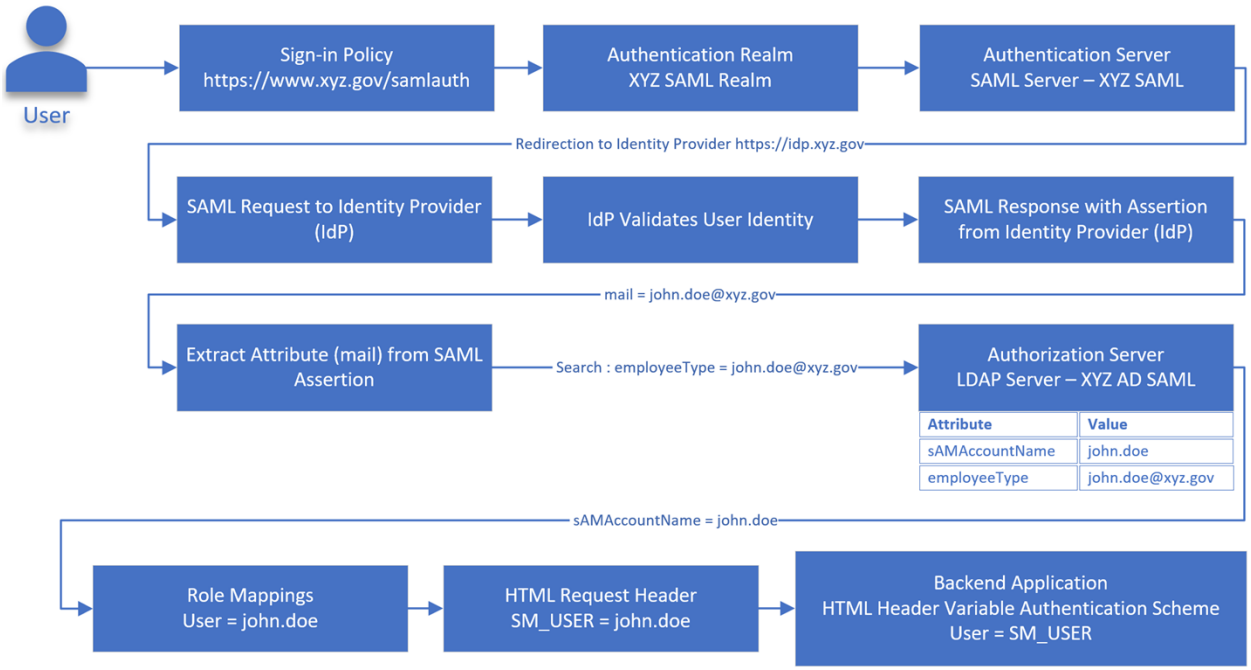

Figure 3. SAML–based authentication.

The SP–initiated SAML–based authentication process elements shown in Figure 3 are defined as follows:

- The Sign-in Policy https://www .xyz.com/samlauth provides the URL for accessing the website.
- The Sign-in Policy is configured to access the Authentication Realm named XYZ SAML Realm.
- The Authentication Realm is configured to use the Authentication Server of type SAML Server named XYZ SAML, which redirects the user by sending a SAML request from the SP to the IdP at https://idp.xyz.gov.
- The IdP validates the identity of the user and returns the SAML response to the SP. The SAML response includes the SAML assertion containing the attribute as configured by the SAML metadata. In this case, the attribute is the e-mail address from the account used by the IdP for validation.
- The Authentication Realm is configured to use an Authorization Server of type LDAP Server named XYZ AD SAML. This authorization server is configured to search for the user with an employeeType attribute value matching the e-mail address contained in the SAML assertion.
- The Authentication Realm is configured to assign User Roles based upon the Role Mapping rules for the authorized user.
- Policies for Custom Headers and Headers/Cookies allow the authorized username to be passed to the backend applications via an HTML request header.

4.3 SOLUTION 3: IDP–INITIATED SAML–BASED AUTHENTICATION (WITH PIV CARD AUTHENTICATION TO IDP)

This solution is described as IdP–initiated SAML–based authentication because the user initiates the authentication process by first accessing the PCS, which is acting as the IdP, then is directed to the SP once a successful authentication process is completed. A practical application of this solution would be PIV authentication to the AWS MC. Once the user successfully authenticates with PIV card, they are redirected to the AWS MC that is acting as the SP. Figure 4 shows the authentication flow for this solution.

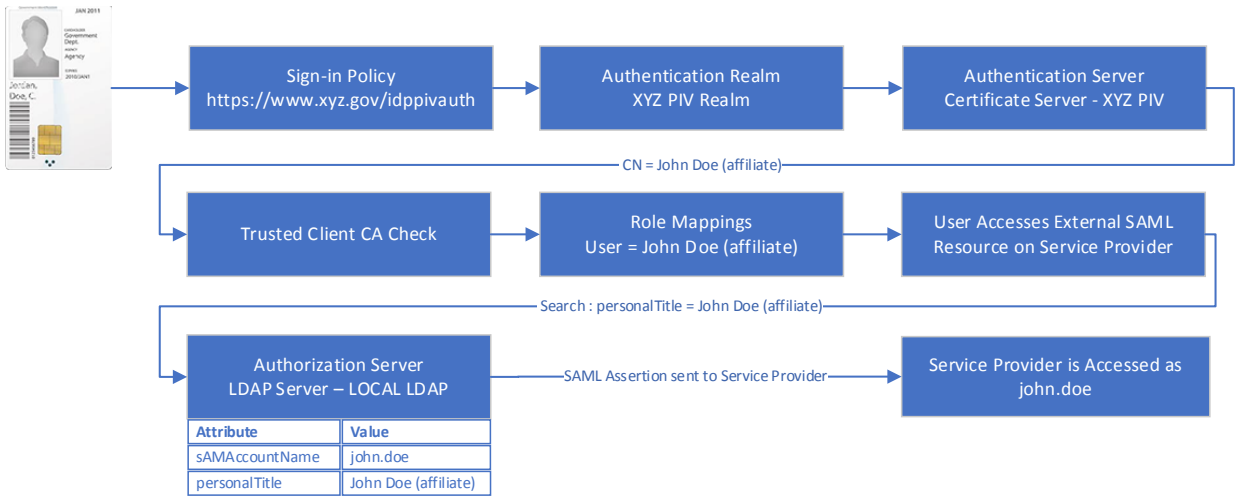

Figure 4. IdP–initiated SAML–based authentication

The IdP–initiated SAML–based authentication process elements shown in Figure 4 are defined as follows:

- The Sign-in Policy https://www.xyz.com/idppivauth provides the URL for accessing the website.
- The Sign-in Policy is configured to access the Authentication Realm named XYZ PIV Realm, which has an Authentication Policy that requires a client-side certificate.
- The Authentication Realm is configured to use the Authentication Server of type Certificate Server named XYZ PIV which passes the CN attribute from the client-side certificate to the Authorization Server.
- The list of Trusted Client CAs is checked for the Intermediate and root CAs for the client-side certificate that is presented.
- The Authentication Realm is configured to use an Authorization Server of type LDAP Server named LOCAL LDAP. This authorization server, LOCAL LDAP, is configured to search for the user with personalTitle attribute matching the CN attribute from the client-side certificate.
- The Authentication Realm is configured to assign User Roles based upon the Role Mapping rules for the authorized user.
- The IdP sends the SAML response to the SP. The SAML response includes the SAML assertion containing the attribute as configured by the SAML metadata. In this case, the attribute is the username of the authorized user.
- The SP is accessed as the authorized user.

5. CONCLUSION

PCS provides multiple configuration options for supplying MFA to secure web portals. PCS can act as both an SP and an IdP in a SAML–based configuration. It also can be configured to accept client-side certificates (including certificates presented on PIV cards) from a trusted client CA. With the capability to provide solutions for client-side authentication and SAML–based authentication, the PCS SSL VPN appliance should continue as a primary player when building authentication solutions in government environments.

BIBLIOGRAPHY

"Security Assertion Markup Language." Wikipedia: https://en.wikipedia.org/wiki/Security_Assertion_Markup_Language.

Hughes, J. et al. "Profiles for the OASIS Security Assertion markup language (SAML) V2.0." OASIS Open 2005. OASIS: http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf.