Privacy Impact Assessment Update
for the

Application Authentication System (AppAuth)

DHS/ALL/PIA-060(a)

January 28, 2019

<u>Contact Point</u>
Stephen Pyfrom
AppAuth System Owner
Information Sharing Environment Office (IS2O)
Office of the Chief Information Officer
(202) 447-5647

<u>Reviewing Official</u>
Philip S. Kaplan
Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The Application Authentication System (AppAuth) is a Department of Homeland Security (DHS) enterprise system developed and operated by the DHS Headquarters Information Sharing and Services Office (IS2O). AppAuth is a DHS single sign-on enterprise authentication service, which provides a uniform authentication service based on Microsoft's Active Directory services. DHS is updating this Privacy Impact Assessment (PIA) because AppAuth will now share personally identifiable information (PII) outside of the Department and within a Government specific public-cloud instance (Azure).

Overview

The Application Authentication System (AppAuth) was developed by the DHS Headquarters Information Sharing and Services Office (IS2O) to support its mission to deliver the services required by the DHS enterprise for mission, business management, and information technology support. AppAuth provides the ability for DHS users across the Department to log on to enterprise applications using their normal component login credentials. The system provides basic authorization services via security groups that can be established within an organization and used as the basis for internal authorization logic to determine level of access for an individual user.

AppAuth provides cross-domain authentication[1] of DHS users for the purposes of using DHS enterprise applications via two-way trusts.[2] In a two-way forest[3] trust relationship, AppAuth will trust a component's Active Directory at the forest level[4] and a component's Active Directory will trust AppAuth. The forest allows separate active directory forests to exchange information with other environments while still allowing each component Active Directory forest to maintain complete control over its own forest. In this model, AppAuth is the trusted domain; AppAuth allows DHS Component end users to use their current component credentials to access DHS applications hosted within the AppAuth forest. In this role, AppAuth is the container for those enterprise applications that have subscribed to the Single Sign-On (SSO) service based on Windows Integrated Authentication (WIA), which is based on Kerberos.[5]

The two-way forest trust between AppAuth and DHS Components will ensure that components have a centrally controlled, robust authentication capability for accessing their

[1] Cross-domain authentication gives users the ability to log in to their enterprise applications from their component workstation.

[2] A two-way trust is an active directory authentication connection between two DHS components such as Headquarters and the Federal Emergency Management Agency (FEMA).

[3] A forest is a directory that houses all users' objects in their environment. These objects allow users to log on to their workstation.

[4] A forest level is the directory operating system level such as Windows 2008 level or Windows 2012 level.

[5] The Kerberos version 5 authentication protocol provides a mechanism for authentication - and mutual authentication - between a client and a server, or between one server and another server.

enterprise applications infrastructure and services. Component domains hold end user credentials but leverage AppAuth. This includes support for Data Center-provided as a service applications (*e.g.*, SharePoint as a Service, Work Place, and Customer Relationship Management as a service). These trusts are essential to the assurance that only authorized users are able to leverage AppAuth verification of credentials. These credentials are leveraged at a system level and are not directly accessed by end users. There is no direct input of PII or solicitation of PII from an end user. AppAuth itself, via approved trusts, ingests this information from already established identity stores from DHS components. The AppAuth Active Directory is populated via already gathered data from an existing DHS Active Directory. These credentials are input and controlled via the component's active directory by privileged users (system administrators). The PII that is collected is in the form of Human Resource Information Technology (HRIT), which contains basic attributes about the user account. These include name, user account, duty locations, phone numbers, work email addresses, and other non-sensitive identifiers. This is used primarily for the purposes of identifying users and organizing user communities. The PII is not extracted or used for any particular portable service, but is used for identification purposes. The PII is maintained in AppAuth Active Directory as long as the account is active.

AppAuth has established trusts with DHS component Active Directory domains such that users' home domain credentials can be accepted for access to shared information. Component Active Directory systems contain PII.

AppAuth has many benefits, especially those that minimize privacy risks. AppAuth provides the below benefits for all DHS components:

- Mitigates risk for access to 3rd-party sites (user passwords not stored or managed externally);
- Reduces password fatigue;[6]
- Reduces time spent re-entering passwords for the same identity; and
- Reduces IT costs due to lower number of IT help desk calls about passwords.

Reason for the PIA Update

With the rising need for integration of the DHS mission with external federal agencies, migration to the public cloud, and DHS users requiring access to internal and external information systems, AppAuth has received multiple requests to extend the federated identity servers beyond the DHS network in traditional datacenters. AppAuth itself does not own the identity attributes being shared, but is doing so on behalf of a DHS component that requires approved DHS federated

[6] Password fatigue is experienced when an individual is required to remember an excessive number of passwords as part of his or her daily routine.

identity services outside of the network. There is no change to the attributes being shared, but those attributes will now be leveraged to access information systems outside of DHS space. These attributes will still only apply to DHS users, but may simply provide access to other information systems.

Privacy Impact Analysis

In each of the below sections consider how the system has changed and what impact it has on the below fair information principles. In some cases there may be no changes and indicate as such.

Authorities and Other Requirements

The authorities carried forward from the previous update to this PIA, DHS/ALL/PIA-060 Application Authentication System (AppAuth) and those authorities listed in DHS/ALL-037 E-Authentication Records System of Records Notice (SORN),[7] to the extent that they are still applicable and current law, cover this sharing.

The Authority to Operate (ATO) for AppAuth was granted in November 2017, following the completion of the original PIA.

Characterization of the Information

AppAuth will continue to collect/transmit requested identifying attributes for DHS components. Those attributes are listed below:

Name;

Agency;

Title;

Country Code;

Department;

Telephone Number (DHS Listed #);

Company; and

Username.

The information above already is collected and maintained by the component/office and exists in Department/Component Active Directory instances. AppAuth leverages trusts between those Active Directory instances to query and validate identities for the purposes of authenticating users via Single Sign-On/Federated Services.

[7] DHS/ALL-037 E-Authentication Records System of Records, 79 FR 46857 (August 11, 2014).

The accuracy of the data in AppAuth continues to be the responsibility of the component administrators who provide the information through their own Active Directories or elsewhere, which is from where AppAuth pulls the information. Any changes made to the local component domain instances will propagate to AppAuth via Active Directory users and systems dashboards as well as supporting systems that leverage the AppAuth identity user/systems stores.

Uses of the Information

AppAuth continues to use the information to assist and establish the unique identification of DHS personnel.

Notice

AppAuth does not provide notice prior to collection of information because it does not collect information directly from individuals. Further, it is difficult to provide notice to individuals that their information will be used by AppAuth since there is no user interface.

However, AppAuth provides notice through this PIA Update that information may be shared externally in order to authenticate DHS personnel to external agency websites or platforms.

Privacy Risk: Individuals may not be aware that their information is being used by AppAuth and do not have an opportunity to consent prior to its use.

Mitigation: DHS provides employees with notice, and employees consent to general uses of their information, when they submit their biographic attributes to DHS upon the onboarding process. Privacy Act Statements are provided at the time of collection and have published SORNs to further provide notice. This PIA serves as additional notice that information collected during the onboarding process is used by AppAuth to provide individuals with the ability to log on to enterprise, as well as external, applications using their normal component login credentials.

Data Retention by the project

The AppAuth system leverages the credentials of component-maintained active directory identity stores. As a result, once components make changes or deletions from their active directory, the online record will be removed from within AppAuth. However, AppAuth maintains daily backups of activity directory databases that allows for the rollback of changes, recovery from disaster, or response to incidents. As a result, AppAuth subscribes to the DHS Data Retention Policy requiring the retention of data for no less than 7 years. This information is encrypted and stored at an offsite location.

Information Sharing

As a service provider, AppAuth enables authentication for Components that have applications that exist outside of the DHS network. In this instance, DHS Active Directory or other system attributes for the requesting agency/component may be shared outside of the DHS network for purposes of authenticating users. AppAuth leverages its federated services to pass those attributes to external DHS applications for the purposes of federated login with DHS credentials outside of the network.

AppAuth is not the data owner of the shared attributes and is not the origin of the passed identities. Components maintain the attributes and credentials in their component identity stores and they are passed via AppAuth upon request when a user requests access to their application. The internal assets for AppAuth are not shared outside of the DHS network.

AppAuth is not a primary source for the individual PII. The data originates with the DHS component that can re-disseminate information as stated in the original SORNs that cover the collection of the information during the onboarding process.

Redress

There are no changes to redress with this PIA Update. Individuals do not have direct access to AppAuth information, as authorization is a system-to-system transaction. Any update of information is performed at the component Active Directory authorization boundary or system level. Employees may update their Component Active Directory information by contacting the Component’s Help Desk.

Auditing and Accountability

AppAuth completes memoranda of understanding (MOU) between external DHS partners and the DHS stakeholder wishing to leverage federation outside of the DHS network as agreed upon within the AppAuth Enterprise System Security Agreement (ESSA). The MOUs will describe the endpoints leveraging the service as well as any security requirements that may result. All stakeholders in the information flow are expected to maintain privacy information indicating the endpoints associated with the data.

AppAuth services extend across multiple datacenters including DHS Datacenter 1, DHS Datacenter 2, and Microsoft Azure Government. The AppAuth Information System Security Officer ensures that all interconnections to the information system are done so via the approved AppAuth ESSA. Additionally, all external agencies must have an approved Interconnection Security Agreement (ISA) with approval to traverse approved DHS OneNet gateways.

AppAuth servers, gateways, and applications are continuously monitored via prescribed Information Security Continuous Monitoring (ISCM) processes and procedures tracking hardware and software assets, configuration management, vulnerability management, malware, and other supported hardware and operating system assets. Events are logged in real-time (near real time for Azure), and these logs allow for faster and more widespread incident response.

Responsible Official

Stephen Pyfrom
AppAuth System Owner
Information Sharing Environment Office (IS2O)
Office of the Chief Information Officer

Approval Signature

Original, signed copy on file at DHS Privacy.

____

Philip S. Kaplan
Chief Privacy Officer
Department of Homeland Security

Appendix A

At the time of this document, the below organizations currently leverage AppAuth outside the DHS boundary via DHS Single Sign (SSO). External systems do not interact with AppAuth domain services.

Component Application	URL
DOJ ICAM	https://dojsts1.idms.justice.gov
SAP Concur	https://usg.api.concursolutions.com