Available online www.ejaet.com

European Journal of Advances in Engineering and Technology, 2020,7(10):92-94

Research Article ISSN: 2394-658X

Unified Authentication and Authorization Framework for Pega: A Plug-and-Play Solution for Enterprise Access Management

Aindrila Ghorai

Senior System Architect
Email ID – aindrila.ghorai@gmail.com

ABSTRACT

In today's diverse IT landscape, organizations are increasingly relying on both cloud-based and on-premise solutions to manage their business operations. Ensuring secure and efficient user access management across these environments is crucial. This paper delves into the need for the development of an enterprise-level, re-usable, plug-and-play framework for managing authentication and authorization for Pega Applications. This framework can integrate seamlessly with any standard Identity Access Management (IAM) systems, such as Azure Active Directory, Active Directory Federation Services, and AWS Managed Microsoft Active Directory. The proposed solution can also address the need for a generic, scalable, and platform-independent authentication and authorization framework.

Key words: PEGA, Authentication, Authorization, Access Management, Plug and Play, Business Process Management, Customer Relationship Management

1. INTRODUCTION

Pega is a robust platform for developing business process management (BPM) and customer relationship management (CRM) applications. As organizations expand their IT infrastructure across various environments, the need for a unified authentication and authorization solution becomes evident. Existing systems often involve disparate authentication mechanisms, leading to inefficiencies and security vulnerabilities. A standardized framework that can integrate with various IAM systems and work across different deployment models (cloud-based and on-premise) is essential for maintaining robust security and operational efficiency.

A. Background: Authentication and Authorization

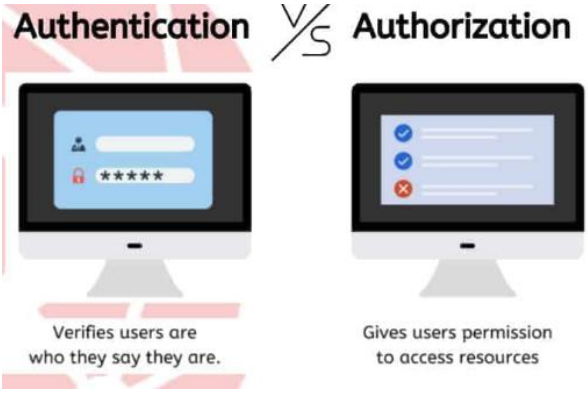

Figure 1 Authentication Vs Authorization

Authentication is the process of verifying a user's identity to determine who can access an application, while authorization is the process of determining what users can do once they are logged in. [1]

[1]. Authentication – Authentication in the Pega Platform ensures that only verified users and systems can access applications, web pages, APIs, and data. This involves verifying user credentials, handling Pega Platform requests to external services, and managing external service requests to Pega. Typically, users must provide an Operator ID (usually their email address) and a unique password. Depending on security needs, applications can implement advanced authentication methods like SAML 2.0, OpenID Connect, or token credentials for single sign-on (SSO), reducing the need for repeated credential requests. Configuring authentication services to enforce policies like multi-factor authentication further enhances security.

[2]. Authorization – Authorization in Pega Platform defines what users can do after accessing an application, controlling their access to specific features, data, and actions. Pega employs three main authorization models: Role-Based Access Control (RBAC), which assigns permissions based on user roles; Attribute-Based Access Control (ABAC), which grants access based on user and object attributes; and Client-Based Access Control (CBAC), which manages access to personal customer data in compliance with regulations like GDPR. [2]

B. Research Objective/Scope

The objective of this research is to look into the possibility of developing a unified, scalable, and re-usable authentication and authorization framework specifically for Pega applications, capable of integrating with various standard Identity Access Management (IAM) systems. The scope encompasses the design and implementation of a plug-and-play solution that ensures seamless integration with IAM systems such as Azure Active Directory, Active Directory Federation Services, and AWS Managed Microsoft Active Directory. This framework aims to simplify and automate user access management, enhance security through real-time synchronization of user attributes, and support various deployment models, including cloud-based, on-premise, and hybrid environments. The research also explores the benefits of such a framework in reducing onboarding time, automating user provisioning and de-provisioning, and maintaining compliance with organizational security policies.

2. PROBLEM STATEMENT

The objective is to develop a single, generic solution from Pega that integrates with any standard IAM system, such as Azure Active Directory (AD), Active Directory Federation Services (ADFS), and AWS Managed AD Service, regardless of whether the IT landscape is on-premise or in the cloud. This solution must be platform-independent and capable of managing authentication and authorization seamlessly.

3. SOLUTION APPROACH

A. Pega Application Framework

The proposed solution involves creating a Pega Application Framework (Application Rule) that houses the complete codebase along with applicable data instances and configurable settings. This framework will serve as a built-on application, ensuring it can be easily plugged into any Pega Application stack. Key components of the framework include:

[1]. Authentication Module to manage user authentication using various IAM systems.
[2]. Authorization Module to control user access levels based on predefined roles and permissions.
[3]. Synchronization Module to ensure real-time syncing of user attributes and parameters between the centralized Active Directory and Pega Applications/Platform.

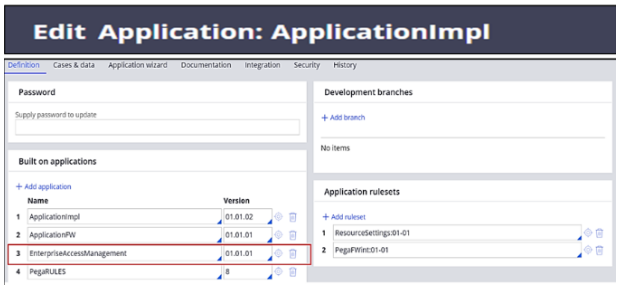

Figure 1: Access Management Framework Application

B. Plug-and-Play Integration

The framework will be designed to support plug-and-play integration, allowing it to be seamlessly incorporated into any Pega Application stack. This requires ensuring proper application pre-requisites and built-on hierarchies are correctly referenced. Key features include:

[1]. Configurable Settings which allow administrators to easily configure the framework to integrate with different IAM systems.
[2]. Scalability which ensures the framework can scale with the growing needs of the organization.
[3]. Flexibility which supports for various deployment models, including cloud-based, on-premise, or hybrid environments.

C. Integration with IAM Systems

The framework will integrate with various IAM systems through standard protocols such as SAML, OAuth, and LDAP. Typical examples of IAM systems include: [3]

[1]. Azure Active Directory (AD) in MS Azure Cloud
[2]. Active Directory Federation Services (ADFS)
[3]. AWS Managed Microsoft Active Directory in AWS Cloud

Each of these integrations will follow a standardized approach to ensure compatibility and security

4. STEPS TO BUILD AN ENTERPRISE ACCESS FRAMEWORK IN PEGA

A. Obtain and Import IDP Metadata: Acquire the IDP metadata file, including the X.509 digital certificate, from a standard IAM provider. Import it to populate necessary parameters.
B. Import and Position Framework: Use Pega's Import Wizard to import the Enterprise Access Management Framework, ensuring it is positioned correctly within the Pega Application/Framework stack.
C. Configure System Settings: Adjust and configure the Rule Admin System Settings based on the environment. Execute the Data Page "D_SAMLEnvSettings."
D. Customize Authorization Logic: Modify the Decision Table rule to align with specific authorization requirements of the Pega application/platform.
E. Platform-Specific Configuration: Configure the web.xml file to map the new authentication protocol and ensure correct mapping in the Data-Admin-AuthService instance.
F. Set Up AuthService Instance: Create a Data-Admin-AuthService instance with necessary servlet mappings for the framework.
G. Manage Security Settings: Utilize digital certificates like X.509 for centralized TLS/SSL management, avoiding local truststore maintenance.
H. Operator Identification Setup: Configure 'Operator Identification' for creating new Operator/Login IDs in Pega, typically using the user's email address.
I. Map Attributes: Use a Data Transform Rule to map authentication response attributes to Operator ID profile properties.
J. Environment-Specific Settings: Configure environment-specific values in the Application Settings Rule, referenced by 'D_SAMLEnvSettings.'
K. Post-Processing Activity: Design the Post-Processing Activity to handle user authorization after authentication, including clearing and mapping Access Group properties.
L. Requestor Instance Configuration: Ensure "Browser" Requestor details point to the Unauthenticated Access Group created in the framework for proper rule invocation.
M. Configure Access Groups: Set up Access Group instances for unauthenticated users during login and for system administrators to manage and debug the framework.

5. BENEFITS

A. Automation of User Access Management

The proposed framework automates the user access management (authentication and authorization) processes in any Pega-based application or platform. This reduces the effort and time required for onboarding new applications and users within the Pega environment.

B. Automated Provisioning and De-provisioning

The framework enables automated provisioning of new users in any production and non-production Pega environments without any development effort. It also ensures the de-provisioning or removal of users in sync with the organizational IAM system, maintaining security and compliance.

C. Real-time Synchronization

Leveraging this framework, almost real-time synchronization of user attributes and parameters between the centralized Active Directory and Pega applications/platform can be achieved. This ensures that any changes in the IAM system are reflected promptly across all Pega applications.

6. CONCLUSION

The proposed enterprise-level, re-usable, plug-and-play framework for managing authentication and authorization in Pega applications addresses the critical need for a standardized, scalable, and platform-independent solution. By integrating seamlessly with various IAM systems, this framework ensures robust security, operational efficiency, and real-time synchronization of user data. This solution not only simplifies user access management but also enhances the overall security posture of organizations utilizing the Pega platform.

REFERENCES

[1]. PEGA Systems, "Role-based access control (RBAC)," [Online]. Available: https://academy.pega.com/topic/role-based-access-control-rbac/v4/in/38221/38296. [Accessed September 2020].
[2]. PEGA Systems, "Authentication and authorization," [Online]. Available: https://academy.pega.com/topic/authentication-and authorization/v1#: ~:text=Authentication%20addresses%20who%20can%20access, of%20a%20Pega%20Platform%20application. [Accessed September 2020].
[3]. Cisco, [Online]. Available: https://www.cisco.com/c/en/us/products/security/identity-services-engine/what-is-identity-access-management.html. [Accessed September 2020].