A Gradišćanska 24, HR-10000 Zagreb
T 00 385 1 5809 319
E international-office@algebra.university
www.algebra.university

CHAIR OF OPERATING SYSTEMS

Authentication systems and databases

Project Task

REV 2.0

Zagreb, 2023.

Introduction

The AAA process (Authentication, authorization, accounting) is part of our daily IT lives. For example, logging onto your computer starts your daily activities—you can run applications, log in to the business system at work, and log in to websites. The projects that follow are a logical extension of that mindset. Companies of all sizes use standard LDAP-based authentication systems to facilitate the administration of their business information systems.

Description of the environment – program direction

The company Authentication Services d.o.o. uses an environment based on standard operating systems and cloud solutions (Windows, Windows+Azure, or Linux) in its business. The SSO system must be implemented according to the required task.

Project for Software Engineering Students

This project involves the implementation of single sign-on (SSO) capabilities for web applications using Keycloak and FreeIPA, explicitly focusing on integrating OpenID and SAML authentication. Keycloak is an open-source identity and access management solution that allows users to be federated from various LDAP sources, including 389-Server, OpenLDAP, and MS Active Directory. It also allows clients to log in passwordless using Kerberos Ticket, adding convenience and security for users within the organization. The integration focuses on improving secure authentication in applications such as WordPress, enabling seamless login via OpenID/SAML without the need for passwords on Kerberos-enabled devices.

Requirements: The primary requirements to set up this integration include a basic installation of Red Hat Enterprise Linux (RHEL) 8 and the required subscriptions for Red Hat SSO and JBoss EAP. In addition, a configured FreeIPA or Red Hat IdM environment is recommended for identity management and integration with Keycloak, which allows for centralized user authentication. The project will also need a web application such as WordPress (or any OpenID/SAML platform with OpenID enabled) to test the authentication settings. Keycloak will serve as a central SSO solution, unifying users and offering flexible authentication mechanisms to support password-based and passwordless (Kerberos) logins.

Setup requires at least 4 GB of RAM and 50 GB of disk space, which is enough for the basic configuration. To successfully implement the project, you will need the following packages and repositories: JBoss Enterprise Application Platform, Red Hat CodeReady Linux Builder, and Single Sign-On packages for RHEL 8.

Subscriptions and tools required
Students need active RHEL 8 and JBoss EAP subscriptions to access Red Hat's supported software packages. To access subscriptions and licenses, log in to the RedHat page and request a free developer account (https://developers.redhat.com/), after which download the necessary image files from https://access.redhat.com/downloads/content/rhel. Also, this will

give you access to the required repositories to install the necessary packages (such as rh-sso, httpd, mod_ssl, and socat) and ACME shell scripts to handle Let's Encrypt certificates. Finally, students must configure Apache HTTP as a reverse proxy for secure communication, allowing Keycloak to manage SSL certificates efficiently.

Note: The template for creating a project can be found on InfoEduca.

Description of the environment – system engineering program

Authentication Services d.o.o. uses an environment based on standard operating systems and solutions (Windows or Linux) in its business. It is necessary to integrate Active Directory and OpenLDAP solutions so that a two-way trust is configured (you can choose whether to use an OpenLDAP or FreeIPA solution).

Project assignment for students of the Systems Engineering program

Prerequisite: You need to install one Windows Server 2012, 2016, 2019, or 2022, and one Linux server. Active Directory Domain Services must be installed on the Windows Server. On the Linux server, you need to install OpenLDAP, samba, SASL*, FreeIPA, or something similar, with the help of which you will complete the project task. The project task is to connect the two servers in question to achieve mutual trust. The way to check the *trust* is to try to make a user in AD, which must also be visible on the OpenLDAP/SAMBA/SASL*/FreeIPA server and vice versa.

Project Submission

The project should be submitted no later than 11.1.2025 at 23:59:59. Each delay means a loss of one point per outcome per week of delay. The template for the project is in the course folder on InfoEduca. In the project document, describe everything you have done – program code, screenshots, procedures – to achieve the project's goal. Also, write your data and direction on the project document's first page.

Submitting outside the defined deadline means repeating the course if you have not collected sufficient points. Consultations on work are possible by e-mail or in person during the exercise periods.

You submit the project to InfoEduka under the seminar paper in the ASBP subject – projects submitted by e-mail are not recognized.

Additional documentation – software engineering

http://woshub.com/configuring-kerberos-authentication-on-iis-website/

1. https://www.codemag.com/Article/1312041/Using-Active-Directory-in-.NET
2. https://auth0.com/blog/using-ldap-with-c-sharp/
3. https://www.freeipa.org/page/Web_App_Authentication
4. https://blog.delouw.ch/2019/06/01/openid-and-saml-authentication-with-keycloak-and-freeipa/
5. https://www.freeipa.org/page/Web_App_Authentication/Example_setup

Additional documentation – system engineering

1. https://www.geeksforgeeks.org/directory-services-in-distributed-system/
2. https://www.freeipa.org/page/Active_Directory_trust_setup
3. https://www.freeipa.org/page/Trusts
4. https://learn.microsoft.com/en-us/entra/identity/domain-services/concepts-forest-trust