OAuth2 toolkit for OpenEdge

OAuth2 is the industry standard protocol for authorization and authentication. The Consultingwerk OAuth2 toolkit is designed to simplify and extend integration of OAuth2 in OpenEdge client and backend applications.

OAuth2 toolkit for the OpenEdge AppServer

The OpenEdge AppServer component of the OAuth2 toolkit enables organizations to use existing ABL authentication and authorization logic as the central security authority. The OAuth2 toolkit enables PASOE or the classic AppServer to serve as the authorization server following the OAuth2 standards.

Enabling the OpenEdge AppServer as identity server

Simply speaking an OpenEdge AppServer will be enabled to issue an open-standards based JWT token that can be used to grant access to resources provided by various applications (OpenEdge or not). The toolkit allows the inclusion of the JWT token details from custom ABL code that is executed by the toolkit. Token details will contain JWT claims for user information, token validity, session ID, authorization claims, etc – in addition, applications are able to provide further custom details to be included in the access token as well (application-specific security realms such as branch offices, item categories, customer groups, ...). Token details will be returned as a JSON object. The API provided by the toolkit simplifies issuing a meaningful JWT token in response to the authentication and authorization request issued to an ABL AppServer routine. Authentication and authorization may be implemented based on database users and optionally tenants, application, or framework users. The toolkit includes a signing component that is responsible for digitally signing the JWT token and managing the public and private key pairs in appropriate key stores. An endpoint to provide the JSON Web Key set (JWK) is provided out of the box.

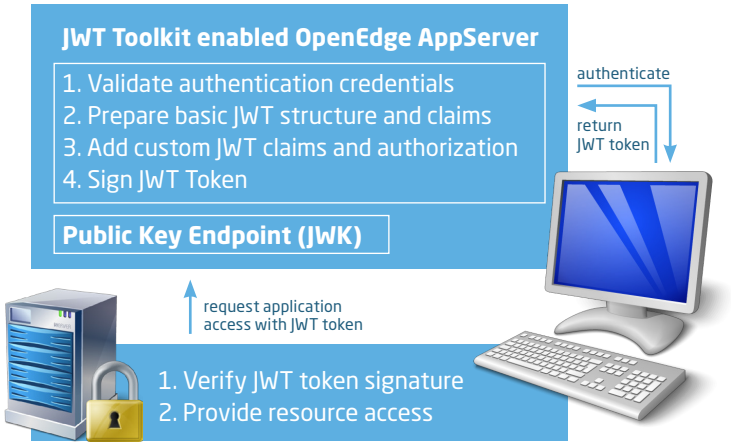
When implementing authentication and authorization using the OAuth2 toolkit, a developer will only focus on the user authentication itself and the details to be included in the JWT token. All surrounding infrastructure is provided by the toolkit.

Enabling SSO over various applications in the organization

An application that provides resources will be configured to trust the JWT token issued by the OAuth2 toolkit. An OpenEdge AppServer backend (PASOE or classic AppServer) can also be configured to accept the JWT token issued by the OAuth2 toolkit for request authorization. This provides a lean and standards-based method to separate user authentication from the AppServer that provides backend application logic and data.

The usage of the JWT tokens will also simplify load-balancing and fail-over implementation as the JWT token is managed by the client application and does not need to be stored in the session memory of a single PASOE or Tomcat server.

A client application (e.g. an Angular, Vue.JS, or React based web application) that has retrieved an JWT token from the OAuth2 toolkit server can use the same JWT token for multiple backend applications (resource servers).



OAuth2 toolkit for OpenEdge GUI applications

The OpenEdge GUI client component of the OAuth2 toolkit enables developers to integrate the OIDC authentication flow into an OpenEdge GUI application. Based on OIDC, GUI applications can be enabled for single-sign-on and multi-factor authentication.

Integrating OIDC into OpenEdge GUI applications

The Consultingwerk OAuth2 toolkit allows you to replace a classic login screen in a GUI application, with typical login flows known from web applications, integrating authentication providers such as Office 365/Azure AD. To host the authentication-flow, a specialized web browser component is provided that will be integrated into the OpenEdge GUI or GUI for .NET application. Typical OIDC providers support single-sign-on over multiple applications and multi-factor authentication including authenticator apps, one-time-passwords retrieved via email, or text-messages, or hardware tokens.

The authentication will be integrated seamlessly in the application bootstrap in place of the alternative standard login dialog. Standard and custom OID providers can be integrated.

The toolkit provides APIs that simplify the authenticity validation of the retrieved JWT token and access to standard and custom claims in that token. The toolkit supports issuing a client-principal based on the JWT token based on ABL functionality or access to a specialized PASOE web application that serves as a token-exchange service.

Single-sign-on based on OAuth2

The OpenEdge GUI application has full access to the retrieved JWT token. The JWT token can be passed to (web) services accessed by the GUI application so that those are accessed with the same user identity and authorization as the OpenEdge GUI application – regardless of whether the requests are made from the client or an accessed AppServer component. This makes it unnecessary to store user passwords in the session context to be able to log on to other applications and services.

The toolkit especially allows you to share the user authentication between the OpenEdge GUI application, and an embedded web application based on popular web frameworks such as Angular, Vue.JS, or React. In the context of application modernization, our embedded web browser allows us to host modernized, browser-based screens within the legacy GUI application while resolving the need to login both in the legacy application and the modernized web application.

To learn more about the components of the OAuth2 toolkit for OpenEdge GUI applications, watch this Webinar: ***https://bit.ly/openedge-oidc***

Progress Partner
AUTHORISED SERVICE DELIVERY
#ProgressProud

Consultingwerk was awarded the 2017 Community Service Award by Progress Software, is a founding member of the Common Component Specification initiative and is a Progress Software Service Delivery and Technology Alliance Partner.

Consultingwerk Software Services Ltd

Schanzenstraße 31
51063 Köln / Germany

Tel.: +49 221 / 6 77 88 55 0
Fax: +49 221 / 6 77 88 55 5

info@consultingwerk.com
www.consultingwerk.com