OREIN

Powered by plain concepts

OREIN is a corporate identity server with the objective of integrating and centralizing authentication logic and flows for any type of application in your company.

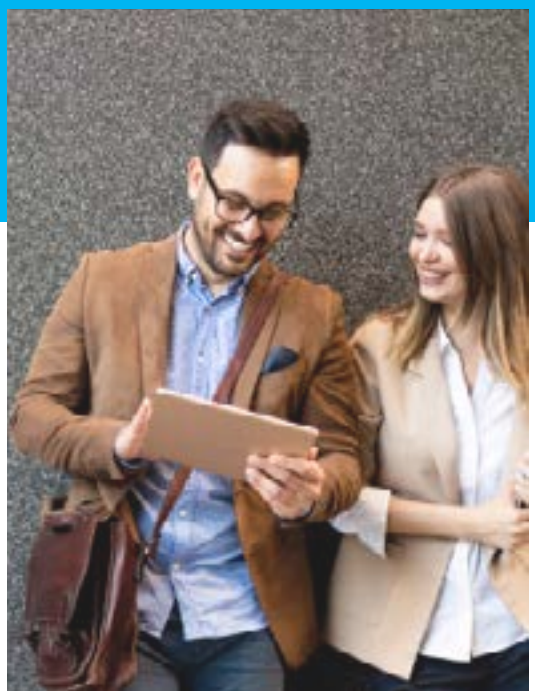
Why OREIN for your company?

- **Security** based on standard protocols such as:
  - » OpenID Connect
  - » OAuth2.0
- **Centralizes** authentication for any type of company application (web, native, mobile, services, etc.)
- Provides a common form of applications to all applications.
- **Identity management** through a simple and intuitive interface.
- I**ntegration of different identity providers** (IdPs) in an easy and transparent way for the rest of the corporate applications.

- **Customization of authentication logic** based on complex logic or integrating other systems.
- **Increase the information** available to applications globally.
- **Simplify** identity management tasks through a simple and intuitive interface.
- Increase the information available to applications globally.

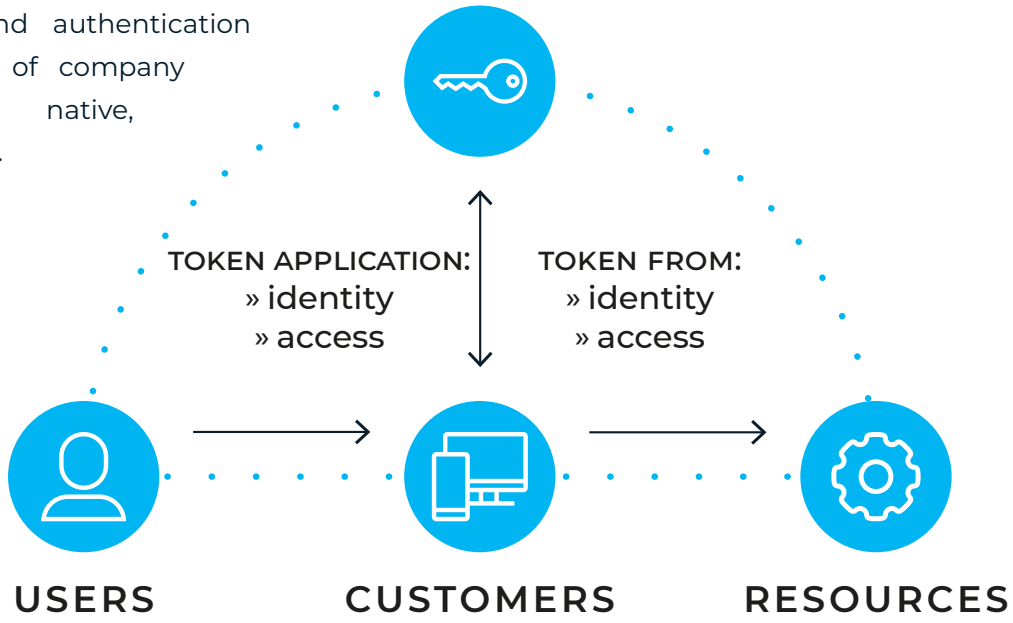
OREIN is able to deploy quickly and easily in different environments such as:

- → Cloud
- → On-premises
- → Azure App Service
- → Kubernetes



OREIN benefits

- Multi-factor authentication.
- Wide parameterization model avoiding the highest number of errors.
- Extensive user management capabilities.
- Issue identity and client access tokens – token validation.
- Reduction in the management of passwords in the database.
- Centralizes logic and authentication flows for any type of company application (web, native, mobile, services, etc.).



OREIN adapts to the needs of each organization and all its applications.

Benefits of OREIN

Customizable and extendable

Many aspects of OREIN are customizable to the needs of the client, allowing to write code to adapt to the system in a way that makes sense for each scenario.

User Interface

It has an administration user interface from which the different elements of the identity server can be configured. Accessible through an API protected and documented with Open Api.

Management portal

The configuration of Identity Server, users and customized configurations for each of the applications will be done from the management portal.

Configuration Lock

Possibility of locking finished settings to prevent unwanted changes.

Based on IdentityServer

Open-source authentication server that implements the OpenID Connect (OIDC) and OAuth 2.0 standards.

OpenID Connect Certification

Identity layer over protocol. The benefits of this certification are:

» *Single sign-on/sign-out*

Single sign-on (SSO) and single sign-off for multiple applications and application types.

» *Access control for API*

Provides access tokens for API for various clients, also allowing the configuration of restricted access to them.

» *Federation Gateway*

Centralizes the configuration of external identity providers, avoiding that corporate applications have to deal with them, supporting the federation of different identity providers.

» *Autenticación multi-Factor -TOPT and FIDO2*

Simplifies the configuration of double-factor authentication for local users

Do you want to know more?

contact us at
info@plainconcepts.com

www.plainconcepts.com

plain concepts

Spain · United States · UEA · United Kingdom · Germany · Netherlands