Technical information

The sophisticated architecture is the foundation of the unique features. The software is fail safe, provides high performance and supports RBAC and ABAC.
Numerous connectors make sure that ORG can be used across many different platforms.

Failsave

The ORG system is divided into the administrative and the productive environment (see illustration: left and right side).
This separation ensures a high reliability.

High Performance

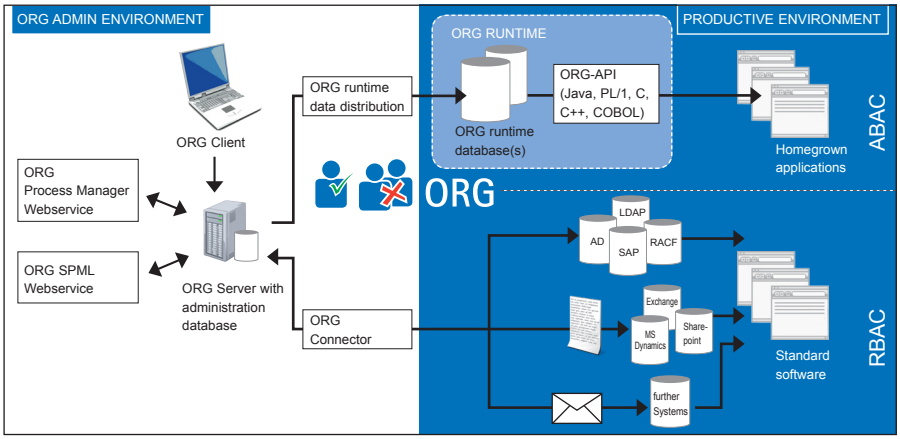
ORG supports two ways to transfer the current authorization settings to the productive environment.
To supply homegrown applications, the fine grained access rights are denormalized in tables using ORG runtime data distribution. Afterwards, they are transfered into the ORG runtime database in the productive environment. Optional, these ORG specific tables can be part of the application's database.
The access of the standard applications to the access rights occurs via API's. Specific ORG connectors transmit the settings of the relation between user and role into the permission storage (e.g. LDAP, RACF, SAP, …) of connected standard software systems.
The ORG architecture enables fast requests and ensures a high performance.

Single Point of Administration & Control

The ideal solution is a centralized and standardized user rights administration.
Access rights are automatically provisioned to the business applications. It makes no difference whether these are Mainframe, C/S or Web applications.
The central administration database of ORG contains all current, future and past permissions of all applications (standard applications and custom developments). Because of that, ORG meets the highest auditability and enables a Single Point of Administration and Control.

Cross Platform

The central component of the administration environment is the ORG server with the ORG administration database.
The ORG server runs on z/OS, Unix and Windows. Within the ORG Admin DB (DB/2 or Oracle), the entire company's implemented permission model is mapped.
In addition to the current valid data, the whole history and the planned administration are also stored tamper and audit proof.



ORG Connector (RBAC)

The ORG connector architecture for the bi-directional exchange of authorization information with standard software is of modular structure. The interface to the ORG Server and the logic for the exchange of access information is the same for all connected systems.
Just the interface specific parts of the connected systems are implemented into so-called agents.
This architecture enables the connection of further applications with little effort.
RBAC: ORG supports business applications that organize their user rights role based. The ORG connector pushes the user role information into the specific user rights data storage. The business applications still use their role based access control without any changes.

ORG API (ABAC)

ORG provides three APIS for the fine-grained access to privileged information on the runtime databases:
The Java API can be used in Java EE and Java SE environments. The z/OS API is available for Cobol and PL/1. It can be used within transaction monitors (IMS or CICS) or batch applications. The Windows/Unix API is designed for C/C++ development on these operating systems. Because of the de-normalized tables of the runtime databases the access is highly performant.
ABAC: Business applications that need fine grained access right information use one of the ORG APIs. An ORG access right decision is based on attributes that are supplied by the business application. The business application itself no longer needs a business application specific access rights storage.

Data Model

ORG's authorization model supports on the basis of its multi-stage the provisioning of permissions on the base of professional objects (position). These can be composed of technical authorization objects (roles).
The lowest level of authorizations consists of the fine grained and attribute based access rights. ORG calls them competences.
Which authorization objects are used, is an individual decision depending on the customer's requirements as well as the technical environment.

Links to upstream systems

The ORG SPML interface is a web service, which implements SPML 1.0 specification.
Via the ORG SPML interface ORG objects (e.g. user, position, role, mappings, etc.) can be created, changed, deleted or read by an external system (e.g. SAP HR). Every activity is checked and historicized by ORG.
An existing IDM system can be upgraded by ORG by defining complex technical authorization rules. The administrative access to the ORG Server is done via web or Fat-Client. Upstream systems (e.g. SAP HR) are able to send contracts for the automated administration to the ORG Server via SPML web service.

www.fsp-org.com

05/2016