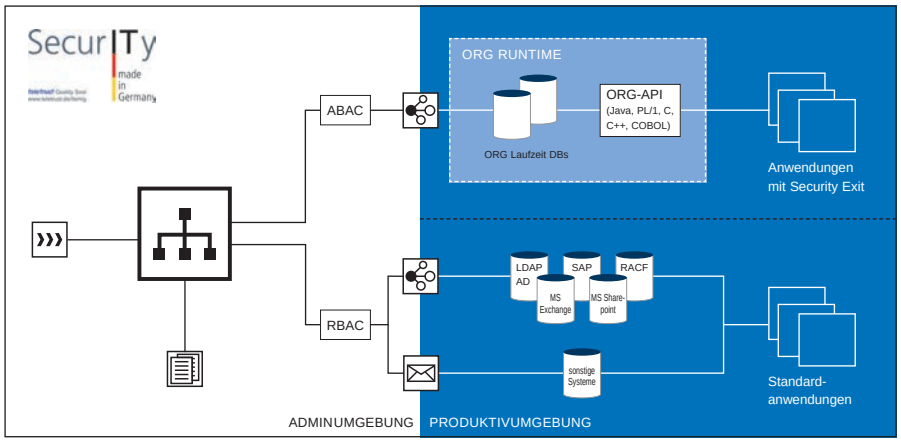
ORG
DAS BERECHTIGUNGSMANAGEMENT

FSP
SOFTWARE & CONSULTING
Wettbewerbsvorteile aus einer Hand.

Technische Informationen

ORG ist ausfallsicher, hoch perfomant und ermöglicht RBAC und ABAC. Genehmigungs-, Provisionierungs- und Rezertifizierungsprozesse sind konfigurierbar.



Die durchdachte Softwarearchitektur ist das Fundament von ORG.

Ausfallsicherheit

Das ORG-System unterteilt sich in die administrative und die produktive Umgebung (Grafik: linke und rechte Seite). Diese Trennung gewährleistet eine hohe Ausfallsicherheit.

Single Point of Administration & Control

Höchste Governance bietet ein zentralisiertes und standardisiertes Berechtigungsmanagement. Zugriffs- und Benutzerrechte werden automatisch an die einzelnen Business-Anwendungen provisioniert. Dies geschieht unabhängig davon, ob es sich um Mainframe-, C/S oder Webanwendungen handelt. In der zentralen Administrationsdatenbank von ORG sind aktuelle, zukünftige und abgelaufene Berechtigungen aller Anwendungen (Standardanwendungen und Anwendungen mit Security Exit) enthalten. Damit erfüllt ORG höchste Ansprüche an Revisionssicherheit und ermöglicht den Single Point of Administration and Control.

Datenmodell

Das Berechtigungsmodell von ORG unterstützt durch seine Mehrstufigkeit die Vergabe von Berechtigungen auf Basis fachlicher Objekte (Stellen). Diese lassen sich aus technischen Berechtigungsobjekten (Rollen) zusammensetzen. Darunter wiederum existieren als tiefste Ebene der Berechtigungen die feingranularen, attributbasierten Zugriffsrechte. Sie werden in ORG als Kompetenzen bezeichnet. Welche der Berechtigungsobjekte tatsächlich in einer ORG-Installation eingesetzt werden, kann kundenspezifisch und abhängig vom jeweiligen Umfeld entschieden werden.

Plattformübergreifend

Die zentrale Komponente der administrativen Umgebung ist der ORG Server mit der ORG Administrations-Datenbank. Der ORG Server läuft unter z/OS, Unix und Windows. In der ORG Admin-DB (DB/2 oder Oracle) wird das gesamte im Unternehmen implementierte Berechtigungsmodell abgebildet. Neben den aktuell gültigen Daten, sind auch die gesamte Historie und geplante Administrationen revisionssicher gespeichert.

Hochperfomante Abfragen

Zur Übertragung der jeweils aktuellen Berechtigungsinformationen an die produktive Umgebung stellt ORG zwei Wege zur Verfügung: Für Anwendungen mit Security Exit werden die feingranularen Berechtigungsinformationen über die ORG Laufzeitüberführung denormalisiert in Tabellen der ORG-Laufzeitdatenbanken der produktiven Umgebung übertragen. Diese ORG-spezifischen Tabellen können auch Bestandteil der Anwendungsdatenbanken sein. Der Zugriff auf die Berechtigungsinformationen erfolgt über APIs direkt aus den Anwendungsprogrammen. Die spezifischen ORG Konnektoren übertragen die Benutzer-Rollenzuordnungen in die Berechtigungsspeicher (z.B. LDAP, RACF, SAP, …) angebundener Standardsoftwaresysteme. Diese Architektur ermöglicht kurze Wege der Berechtigungsabfrage und garantiert eine hohe Performance.

Anbindung vorgelagerter Systeme

Via einem SPML Interface können alle Objekte des ORG Berechtigungsmodells (z.B. Nutzer, Stelle, Rolle, Zuordnungen, etc. von einem externen System (z.B. SAP HR) angelegt, verändert, gelöscht oder ausgelesen werden. Jede Änderung wird von ORG kontrolliert und historisiert. So kann z.B. ein bereits vorhandenes IDM-System durch in ORG definierte komplexe fachliche Berechtigungsregeln aufgewertet werden. Der administrative Zugriff auf den ORG Server erfolgt über Web- oder Fat-Client.

ORG Admin

Berechtigungsadministration

ORG Workflow

Beantragung & Rezertifizierung

ORG Ticket

Teilautomatische Zuweisung

ORG Connect

Automatische Zuweisung

ORG Report

Regelmäßiges Auditieren

Unterstützung von Genehmigungs- und Rezertifizierungsprozessen

Über die Komponente ORG Workflow können Prozesse für die Beantragung, Genehmigung und Rezertifzierung von Berechtigungen abgebildet werden. Die dafür notwendigen Informationen sind über REST-Webservices abrufbar. Dadurch wird eine einfache Integration dieser Prozesse in ein schon vorhandenes Workflow-System wie z.B. MS Sharepoint, Camunda etc. ermöglicht. Ist diese Form der tiefen Integration nicht gewünscht, kann für die gleichen Zwecke auch die Web-Oberfläche von ORG Workflow genutzt werden.

ORG
DAS BERECHTIGUNGSMANAGEMENT

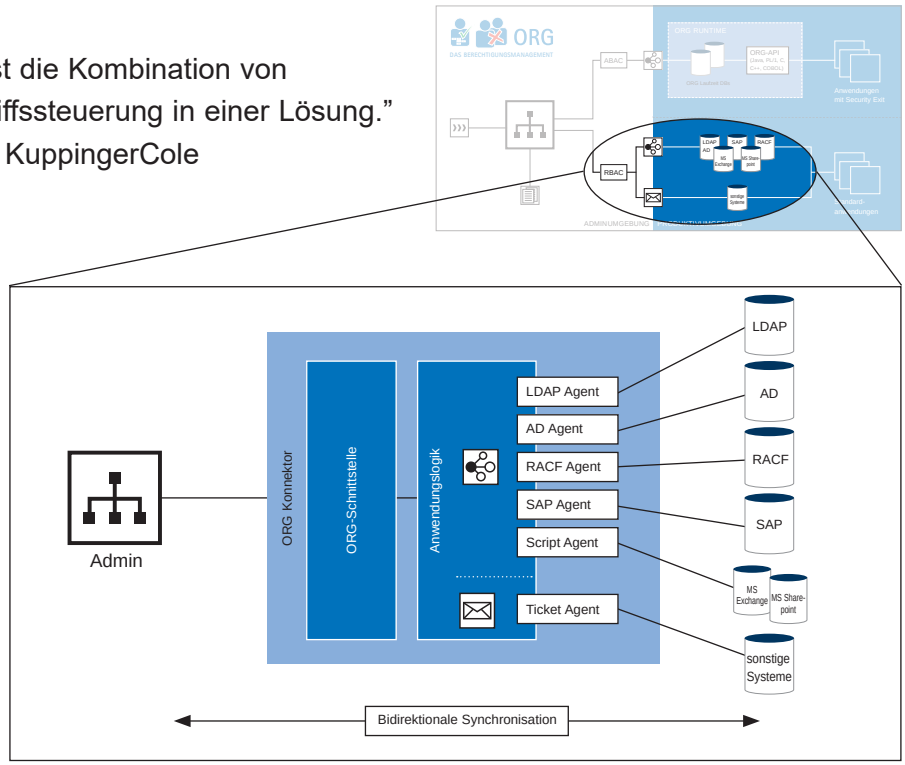
FSP
SOFTWARE & CONSULTING
Wettbewerbsvorteile aus einer Hand.

RBAC & ABAC

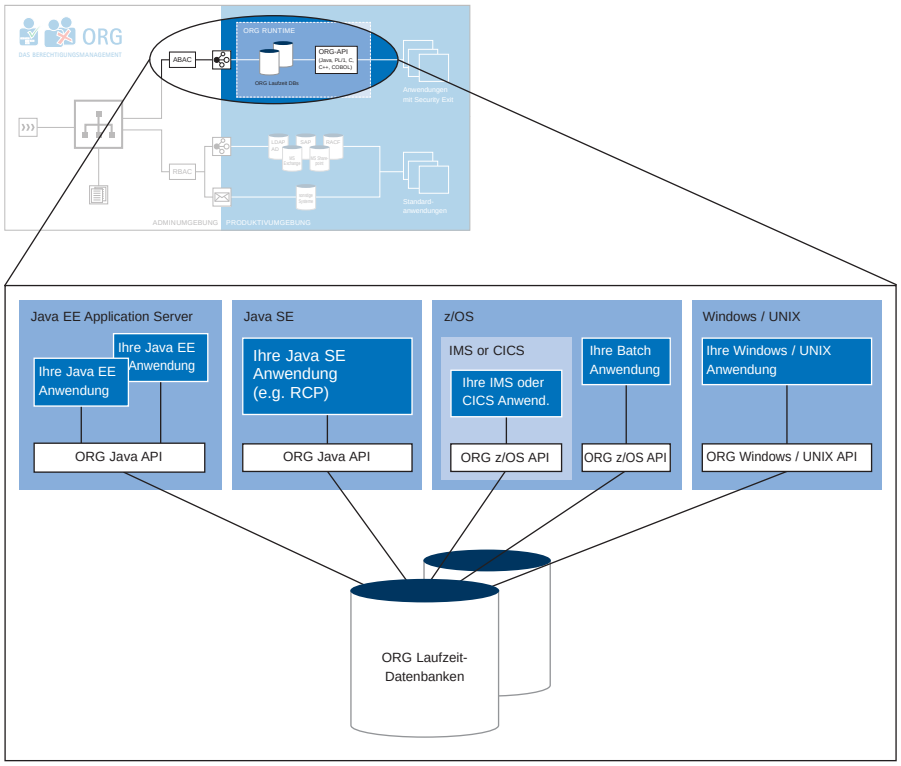
„Ein besonderer Vorteil von ORG ist die Kombination von rollen- und richtlinienbasierter Zugriffssteuerung in einer Lösung."
Martin Kuppinger, Principal Analyst KuppingerCole

RBAC

Die Konnektor-Architektur für den bidirektionalen Austausch von Berechtigungsinformationen mit Standardsoftware ist modular aufgebaut. Die Logik für den Austausch der Berechtigungsinformationen ist für alle angebunden Systeme gleich. Nur die schnittstellenspezifischen Anteile der angebundenen Anwendungssystem werden in Agenten implementiert. Diese Architektur ermöglicht es, weitere Anwendungssysteme mit geringem Aufwand anzubinden. ORG unterstützt Anwendungen, die ihre Berechtigungsinformationen rollenbasiert verwalten. Über den ORG Konnektor werden die in ORG administrierten Zuordnungen von Benutzern zu Rollen in das ausgewählte Zielsystem übertragen. Die rollenbasierte Berechtigungsprüfung erfolgt weiterhin in den angebundenen Systemen.



ORG-Konnektor-Architektur (RBAC)



ORG-Laufzeit-Überführung (ABAC)

ABAC

Für den Zugriff auf feingranulare Berechtigungsinformationen in den Laufzeitdatenbanken stellt ORG verschiedene APIs zur Verfügung: Das Java API kann in JavaEE und JavaSE Umgebungen eingesetzt werden. Das z/OS API steht für Cobol und PL/1 zur Verfügung und kann innerhalb von Transaktionsmonitoren (IMS oder CICS) oder in Batchanwendungen verwendet werden. Das Windows/Unix API ist für die C/C++ Entwicklung unter diesen Betriebssystemen vorgesehen. Die Zugriffe sind aufgrund der denormalisierten Tabellen der Laufzeitdatenbanken hoch performant.
Anwendungen, die feingranulare Berechtigungsinformationen benötigen, verwenden eines der ORG APIs. Die Berechtigungsentscheidung erfolgt aufgrund beliebiger Attribute, die die Anwendung bereitstellt. Die Anwendung selbst benötigt im Sinne des ‚Externalized Authorization Management' keinen eigenen Berechtigungsspeicher mehr.

Die FSP ist die
TeleTrusT Regionalstelle Köln

TeleTrusT
Pioneers in IT security.

Security made in Germany

Weitere Informationen:
FSP GmbH Software & Consulting
Albin-Köbis-Straße 8, 51147 Köln

+49 2203 37100 00, info@fsp-gmbh.com
www.fsp-org.com