



Corporate Metadirectorysystem im DLR

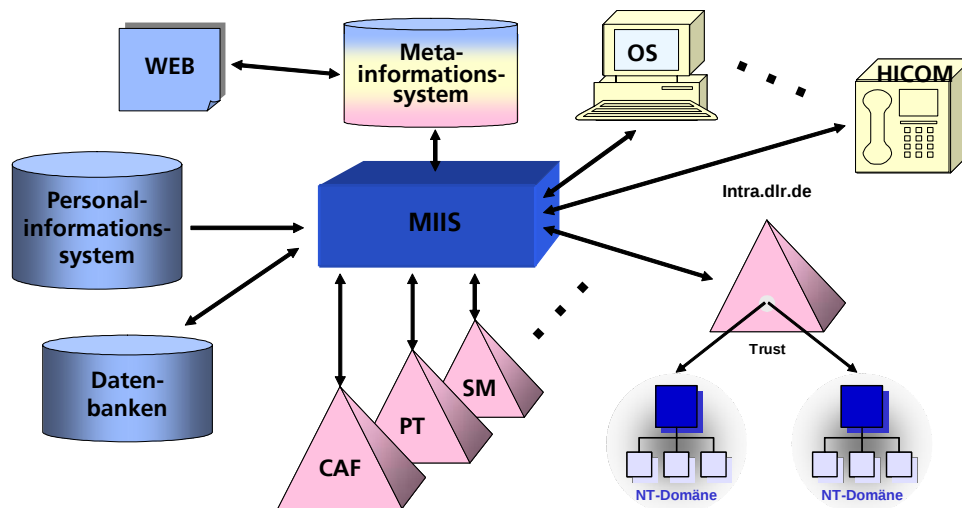


Im DLR werden sowohl die Menge der zu verwaltenden Daten als auch die Zahl der vorhandenen Datenquellen immer größer und unübersichtlicher. Zugriffs- und Berechtigungsinformationen werden redundant in unterschiedlichen Systemen verwaltet. Dadurch entsteht einerseits ein erhöhter administrativer Aufwand bei der Pflege dieser Informationen, andererseits wird die Suche nach Informationen erschwert, da man weder genau weiß, wo sich die Information befindet, noch von welcher Qualität und Aktualität die gefundenen Daten sind. Eine Synchronisierung zwischen einzelnen Datenquellen findet nicht statt, was zum erhöhten Auftreten von Redundanzen und Inkonsistenzen führt. Unvollständige und inkonsistente Benutzerinformationen lassen die Kosten für die Administration von Rechnersystemen stetig steigenden. Die Ansprüche der Benutzer an den Komfort und die Leistungsfähigkeit der Arbeitsumgebungen sowie gesteigerte IT-Sicherheitsanforderungen im DLR mit seinen heterogenen topologisch verteilten Einrichtungen erfordert zusätzliche Anstrengungen zum Erhalt der Integrität der Benutzerinformationen und der Garantie ihrer Konsistenz. Schließlich stellt die Unterstützung von Geschäftsprozessen, die sich in verschiedenen Ausprägungen der IT-Systeme bedienen, eine weitere Herausforderung dar. Diese Sachverhalte veranlassten das IT-Management des DLR zur Entwicklung eines kosteneffizienteren Verfahrens zur IT-Benutzerverwaltung. Die sich hieraus ergebenden Einzelaufgaben wurden im Projekt CoMet gebündelt.

Das Gesamtziel des Projekts CoMet ist die Entwicklung eines kostengünstigen und erweiterungsfähigen Infrastruktur-Informationssystems, das als zentrale Datenbasis IT-Verwaltungsinformation mit hoher Aktualität und Qualität bereitstellt. Es verwaltet, synchronisiert und vereinheitlicht alle relevanten IT-Benutzerinformationen und betrachtet die Organisationsstrukturen sowie weitere Informationen, die für die Sicherheit und den Betrieb der angeschlossenen Rechner- und Verzeichnissysteme benötigt werden. Mit seiner Erweiterbarkeit berücksichtigt CoMet insbesondere zukünftige E-Business-Anforderungen und stellt den beteiligten Einrichtungen gleichzeitig einen langfristig stabilen Datenbezugspunkt zur Verfügung.

Die zentralen Elemente des CoMet sind ein Metainformationssystem (MIS) zur Verwaltung von Benutzerinformationen mit webbasierten Benutzerschnittstellen und der Microsoft Identity Integration Server (MIIS) mit den Management Agenten zur Synchronisation der angeschlossenen Datenquellen und -senken. Das MIS ist ein relationales Datenbanksystem in dem die Daten erfasst und konsolidiert werden. Mit dessen Hilfe werden die Daten der Quellen evaluiert und für die Verarbeitungs- und Synchronisationsprozesse des MIIS bereitgestellt.

Dass MIIS ist die neueste Generation eines im Umfeld des Active Directory Konzepts von Microsoft bereitgestellten Systems zur Synchronisation von Verzeichnissen und Rechnersystemen auch über Verzeichnissgrenzen hinweg.



Neben der Erfassung und Verteilung dieser Informationen im Gesamtsystem sowie der Gewährleistung der Konsistenz und Integrität der Daten, realisiert CoMet das wichtige Konzept der Rollen, Rechte und Services.

Das Rollen- und Rechtekonzept basiert auf grundlegenden Überlegungen zum Entwurf eines strukturierten rollenbasierten Rechtemodells (**R**ole **B**ased **A**ccess **C**ontrol), bei dem die verschiedenen Rechte nicht an eine Person, sondern an eine Rolle gebunden werden. Mit diesem Ansatz wird die Unabhängigkeit von Personen und eine hohe Flexibilität hinsichtlich einer variablen Gestaltung von Portalen und Zugriffsmechanismen angestrebt, wie sie sowohl in den Sicherheitsbemühungen des DLR als auch im Informationsmanagement gefordert werden.

Ein weiteres grundlegendes Prinzip des rollenbasierten Rechtemodells ist die Anforderung, dass ein Benutzer nicht mehr Rechte haben darf, als seine Aufgabe es erfordert.

Das Rollenmanagement von CoMet ermöglicht

- das Erstellen und Pflegen eines Rollenkatalogs,
- das Einordnen von Rollen hinsichtlich der Organisationsstruktur und
- berücksichtigt fachliche und technische Funktionen als Jobtitel.

Es stellt Verfahren bereit, die die gegenseitigen Abhängigkeiten, der Delegation von Teilberechtigungen und der organisationsabhängigen Ausprägung von Rollen unterstützen.

Die Rollen werden aus den Organisationsstrukturen des DLR abgeleitet und spiegeln die Führungs- und Verantwortungsstruktur des DLR wieder. Unter anderem werden jedem Mitarbeiter des DLR mindestens die Rolle „Mitarbeiter“ zugeordnet. Er erhält damit die Berechtigung festgelegte Services des DLR in Anspruch zu nehmen. Jeder Mitarbeiter mit Führungsverantwortung erhält entsprechend seiner Einordnung in die Führungshierarchie des DLR eine zur Rolle „Mitarbeiter“ spezialisierte Rolle. Inhaber spezialisierter Rollen können den ihnen disziplinarisch zugeordneten Mitarbeitern Jobtitel vergeben. Diese sind aus den Aufgabenbeschreibungen der Mitarbeiter abzuleiten und beschreiben das Können und die Fertigkeiten zur qualifizierten Durchführung IT-bezogener Aufgaben. Letztendlich erhalten die auf Rollen/Jobtitel abstrahierten Mitarbeiter Zugriff auf die hierfür festgelegten Services.

Mit der Assoziation zwischen Rollen (Jobtiteln) und festgelegten Services greift CoMet ein wichtiges Konzept der serviceorientierten Architekturen (SOA) auf. Serviceleistungsanbieter stellen wohldefinierte Serviceleistungen bereit, die an zentraler Stelle (CoMet) informell verwaltet werden. Die Serviceleistungen können technisch zentral oder dezentral bereitgestellt werden. Die technische Ausprägung und Beschreibung als Serviceleistung obliegt dem Serviceleistungsanbieter. Grundsätzlich werden die Serviceleistungen mit Berechtigungsgruppen assoziiert. Die Berechtigungsgruppen erhalten einen semantisch sinnvollen sprechenden Namen, die so genannte Rolle oder den Jobtitel.

Für Vorgesetzte und Serviceleistungsanbieter ergeben sich somit Zuordnungsaufgaben. Einerseits die Zuordnung einer Rolle (Jobtitel) zu einem Mitarbeiter als organisatorisch fachliche Aufgabe, andererseits die Zuordnung der Rollen (Jobtitel) zu den Berechtigungsgruppen. Dieses Konzept erfüllt das Prinzip der Pflichtentrennung, der organisatorischen (dynamischen) und technischen (statischen) Trennung von Pflichten, und ermöglicht die eindeutige Zugriffsregelungen und strikte Trennung von Zuständigkeiten und Verantwortlichkeiten.

Die Entscheidungen über den Zugriff auf Serviceleistungen werden von Rolleninhabern „Führungskraft“ getroffen. Ein Mitarbeiter ohne „Führungsrolle“ kann keine Berechtigungen auf andere Mitarbeiter übertragen sondern, zur Wahrung einer eindeutigen Verantwortlichkeit, nur an den jeweiligen Führungsrolleninhaber zurückgeben.

Sind einmal die Rollen/Jobtitel mit ihren zugehörigen, das heißt erlaubten, Serviceleistungen definiert, besteht die Hauptaufgabe darin, neue Mitarbeiter in Rollen aufzunehmen oder ausgeschiedene Mitarbeiter zu löschen.

Nutzen durch das Projekt CoMet

Offensichtlich ist, dass mit der Pflege der verschiedenen IT-Systeme ein erheblicher administrativer Aufwand verbunden ist. Es ergeben sich durch die verschiedensten Fehlerquellen bei der Verwaltung der administrativen Daten Inkonsistenzen, die im ungünstigsten Fall dazu führen, dass Informationen den Adressat nicht erreichen und dem DLR Schaden entsteht. Neben den datentechnischen Aspekten lassen sich durch den Einsatz eines einheitlichen Metadirectorys nachhaltig die Betriebskosten senken. Der Gewinn durch das Projekt "Corporate Metadirectorysystem im DLR" CoMet kann wie folgend benannt werden:

- Verschiedene Datenausprägungen desselben Objekts werden miteinander in Beziehung gestellt und synchronisiert.
- Ähnliche Daten auf verschiedenen IT-Systemen, können einheitlich prozessiert werden. Inkonsistenzen, die durch die unterschiedliche Verwendung der Daten in den Systemen entstehen, können erkannt und durch geeignete Abbildungsvorschriften (Synchronisationsregeln) verhindert werden. Damit wird eine deutliche Verbesserung der Datenqualität erreicht.
- Kurze Reaktionszeiten bei veränderten Geschäftsprozessen sind aufgrund zentraler Änderungen im Metainformationssystem realisierbar.
- Die einheitliche Sicht auf vorhandenen Daten und ihre gemeinsame Nutzung in hoher Qualität und Aktualität sowie der geringere Administrationsaufwand lassen erwarten, dass ein ROI (Return of Investment) frühzeitig erreicht werden kann.

- Durch das Prinzip der Minimierung der notwendigen Berechtigungen und deren Bindung an wohldefinierte Serviceleistungen werden nur die Berechtigungen zur Erledigung einer Rollen-Aufgaben-Kombination erteilt.
- Das Rollen- und Rechte-Modell von CoMet ermöglicht eine vereinfachte Administration durch die dezentrale Vergabe / Entzug von Jobtiteln. Führungsrollen werden zentral durch das Human-Ressources-System des DLR bereitgestellt.
- Durch die zentrale informelle Verwaltung der Serviceleistungen und ihre Bindung an Rollen/Jobtitel, kann durch Definition weiterer Rollen-Serviceleistungs-Kombinationen leicht eine neue spezifische Aufgabe eingeführt werden und zur Menge der bestehenden Rollen-Serviceleistungs-Kombinationen hinzugefügt werden.
- Durch das Granulat „Serviceleistung“ bietet CoMet durch die Beschränkung der Berechtigung auf wohldefinierte Serviceleistungen und die Dreidimensionalität (Mitarbeiter, Rolle, Serviceleistung) eine praxisgerechte Detaillierung und Strukturierung an.
- Der jederzeit aktuelle Kenntnisstand der Berechtigungen reduziert das Sicherheitsrisiko im DLR. Mit den eindeutigen Verantwortlichkeiten ist eine grundlegende Sicherheitsanforderung des IT-Sicherheitskonzepts des DLR erfüllt.

Weitere Informationen zum Projekt CoMet:



Auftraggeber:

Heinz Gesche, IT-Management
Heinz.Gesche@dlr.de

Projektleiter:

Dr. Gerhard E. Töpfer, Institut für Strukturmechanik
Gerhard.Toepfer@dlr.de