IBM Software Group
White Paper

IBM Tivoli Identity Management Version 5.1

Inhalt

Aufbau und Bestandteile der IBM Identity Management-Lösung

Für den Aufbau einer Identity Management-Infrastruktur gilt es folgende Bestandteile zu berücksichtigen:

- die Identity Management-Plattform und ihre Komponenten
- die einzubindenden Ressourcesysteme, Quell- und Zielsysteme der zu verwaltenden Benutzerkontendaten
- benötigte Zusatzfunktionen zur Erweiterung bzgl. des Compliance Monitoring und des Berichtswesens
- die Integration mit weiteren Produkten und Lösungen zur Erfüllung erhöhter Funktions- und Sicherheitsanforderungen, z. B. Web Single Sign-on (Web SSO), Desktop SSO (Enterprise SSO)

In Abbildung 1 sind sämtliche Komponenten der IBM Identity Management-Plattform (IdM) einschließlich beispielhafter Quell- und Zielressourcen für die zu verwaltenden Benutzeridentitätsdaten dargestellt.

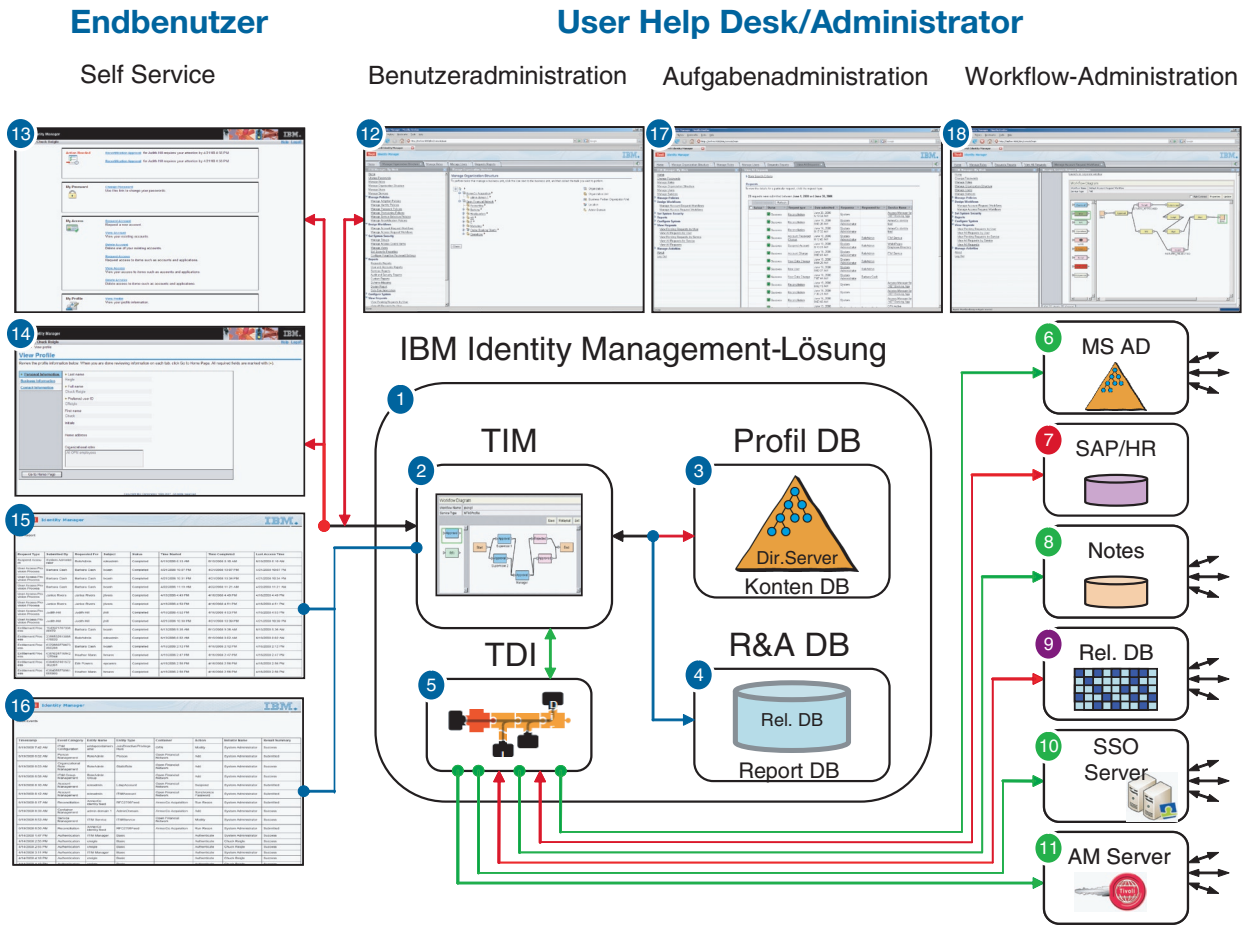


Abb. 1: IBM Tivoli Identity Management-Lösung

IdM – Lösung

1 Darstellung aller IdM-Systemkomponenten:

- Identity Management-Applikation – Tivoli Identity Manager (TIM)
- Repositories: LDAP und rel. DB – Tivoli Directory Server (TDS) und DB2
- J2EE™ Applikationsserver – WebSphere Application Server (WAS)
- Adapterplattform – Tivoli Directory Integrator (TDI)

2 Integrierte Kernkomponenten

TIM – Identity Manager-Applikationslogik (Workflow Engine, Policy Engine, ...)

Die Identity Management-Web-Applikation TIM (Tivoli Identity Manager) mit der zugehörigen Java-Laufzeitumgebung WebSphere Application Server. Es stehen Best Practices sowohl für verteilte als auch für Cluster-basierte Lösungen zur Verfügung.

3 Profil-DB – Benutzerkonten-Repository und Konfigurationsdatenbank

In der Directory-Server-basierten Profildatenbank werden die Informationen der Benutzerkonten persistiert, z. B. TIM-Accounts, Ressourcen-Accounts und deren zu verwaltende Attribute.

Durch den Ansatz der zentralen Datenhaltung hat das IdM-System jederzeit Zugriff auf den gesamten Datenbestand der Benutzerkonten und kann Operationen auf diesem Datenbestand auch dann durchführen, wenn die Zielsysteme, z. B. auf Grund von Systemfehlern, Netzwerkproblemen, etc. nicht online sind.

Weiterhin stellt dieser Datenbestand den Daten-Soll-Bestand dar, der bei einem ‚Reconcile' (Soll-Ist-Abgleich) gegen den Daten-Ist-Bestand der Ressourcen abgeglichen wird. Abschließend wird auf Basis von hinterlegten Regeln auf eventuell bestehende Diskrepanzen reagiert.

4 R&A-DB – Report- und Audit-Datenbank

In dieser relationalen Datenbank erfolgt u. a. die Speicherung der statischen Informationen, Logging-Daten, Audit-Daten für das Reporting, z. B. „Welcher Benutzer hat auf welchem System wann Berechtigungen durch wen erhalten?", getrennt von den Profilinformationen. Das Datenbankschema ist in dem Dokument „*Tivoli Identity Manager Database and Schema Reference*" detailliert beschrieben. Der Link hierzu ist im Abschnitt „Weitere Informationen" enthalten. Die Offenlegung des Schemas ermöglicht es kundeneigenen Applikationen, die Berichtsdaten zu nutzen.

5 Die Adapterplattform

Tivoli Directory Integrator (TDI) stellt eine generische Adapterplattform mit spezifischen Konnektoren für die Ziel-/Ressourcensysteme bereit.

Diese Plattform erlaubt eine „konfigurative Konnektivität" zu den Ziel- und Quellsystemen analog einer „Stecker-Buchse-Plattform". Sie bietet eine eigene Konfigurationsoberfläche und Entwicklungsumgebung und kann sowohl durch JavaScript (ECMA Script) als auch mit Hilfe von Java-Code funktional erweitert werden.

Zur Laufzeit werden einzelne Funktionsblöcke, die eine Funktionskette, Assembly Line, bilden, abgearbeitet. Damit können z. B. Konnektorlogik wie auch Applikationslogik, ebenso XML-Parsing und Validierung eines SPML-basierten Datentransports oder komplexe LDAP-Abfragen kombiniert mit relationalen Datenbankzugriffen abgearbeitet werden.

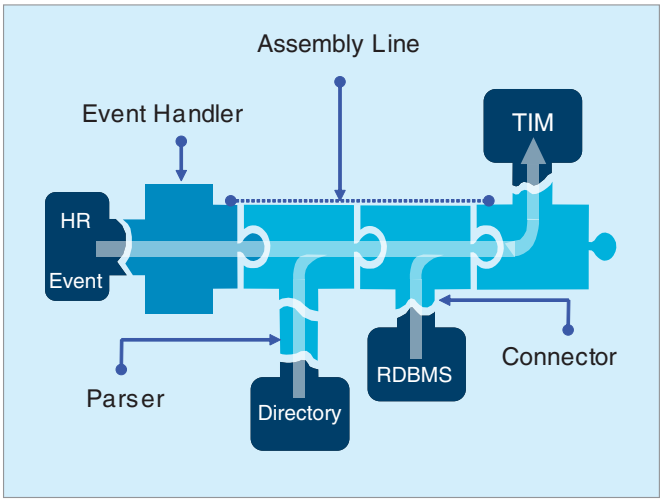


Abb. 2: Beispiel einer HR-System-Anbindung inkl. Anreicherung der Daten durch weitere Quellen

Dem IdM-Kernsystem werden erst nach Abarbeitung der Aggregations- und Datenoperationslogik die benötigten Identitätsinformationen zugeführt. Somit wird eine Separation von Adapterlogik und IdM-Kernsystem erreicht. Dies erlaubt u. a. lastintensive Verarbeitungsschritte, wie z. B. XML-Parsing, zu verteilen, die Separation von Konnektivität und IdM-Prozessplattform sauber voneinander zu differenzieren und durch entsprechende Architekturen den kundenspezifischen Anforderungen bzgl. Verfügbarkeit (HA – High Availability) und Lastverteilung (LB – Load Balancing) gerecht zu werden.

Durch die Trennung und Verteilung der Adapter-/Konnektorlogik vom IdM-Kernsystem ist somit eine Änderung/Erweiterung der Adapterlogik ohne Beeinflussung der IdM-Kernplattform möglich.

Konnektivität *groß* geschrieben

TIM kommuniziert, wie zuvor beschrieben, mit den Ziel- und Quellsystemen via der Adapter-Plattform TDI. Diese wiederum führt zielsystemspezifische Datenoperationen und -extraktionen durch und provisioniert die benötigten Attribute der Benutzerkonten.

Abbildung 3 zeigt die optionalen Schnittstellen der IdM-Plattform. TIM bietet ein offengelegtes und dokumentiertes Java-basiertes API-Set zur direkten Anbindung externer Applikationen (Applikationen I). Zur Nutzung des TIM API-Sets programmiersprachenunabhängig bzw. systemunabhängig via Web-Services verfügt TIM über eine Kapselung der Applikationsschnittstellen durch eine Web-Services-Schicht. Somit können beispielsweise Infrastruktur- oder Applikationskomponenten (Applikationen II), Portal-Dienste etc. existierende Identity Management-Dienste nutzen.

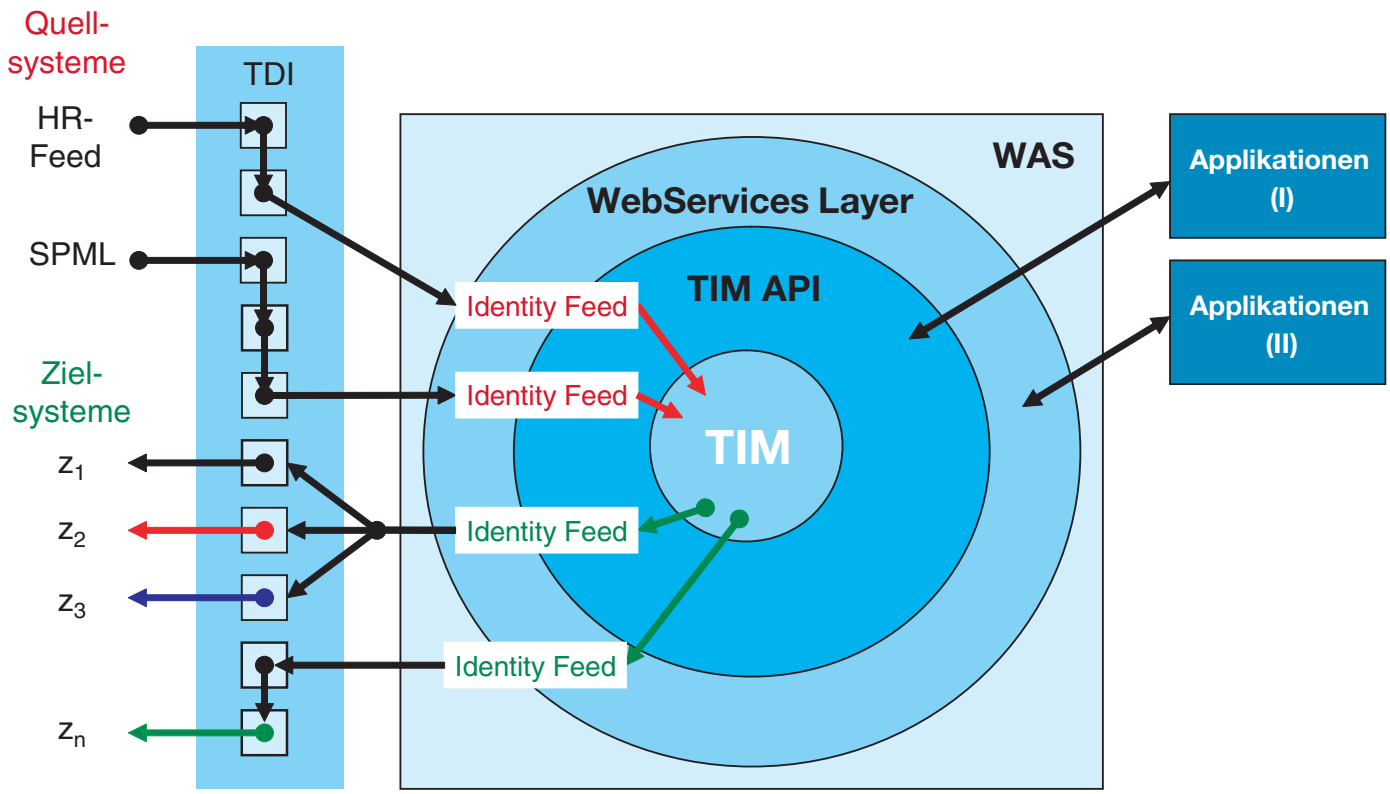


Abb. 3: TIM-Konnektivität durch Schnittstellenvielfalt

Zielsysteme – Beispiele

Die Zielsysteme werden vom IdM-System provisioniert, eine native Änderung der Benutzerkontendaten in den Systemen ist hier nicht beabsichtigt. Wird dies dennoch detektiert, so kann regelkonform reagiert werden. Konten werden markiert, korrigiert, oder nicht legitime Konten gesperrt bzw. gelöscht. Als Datenquellen für Identitätsdaten des internen Personals, wie Neuanlage oder Änderung der Personalstammdaten, werden in diesem Beispiel nur das SAP Personalsystem und der UHD (User Help Desk) zugelassen. Externe Mitarbeiter werden durch ein weiteres System gepflegt, welches die Daten in einer relationalen Datenbank führt.

Farblegende der Identitätsquell- und Zielsysteme

- Identitätsquelle
- Identitätssenke
- Identitätsquelle und -senke

Ressourcenbeispiele 1

Dies ist ein Beispiel eines häufig anzutreffenden Szenarios:

6 *Microsoft® Active Directory*

- Die Identitätsdaten werden über den TIM MS AD-Adapter provisioniert. AD dient als Benutzer-Repository der Windows®-Benutzer.

7 *Personalsystem SAP HR (interne Mitarbeiter)*

- Dies dient als Quellsystem für Personalstammdaten ausschließlich interner Mitarbeiter. Sämtliche Änderungen der Mitarbeiterdaten werden von diesem System autoritativ getriggert und anschließend durch das IdM-System verarbeitet und informations- und rollenabhängig die Zielsysteme provisioniert, Identitätsattribute aktualisiert, Benutzerkonten angelegt, gesperrt, gelöscht etc.

8 *IBM Lotus Notes*

- Benutzer-Mailkonten werden durch den Lotus Notes-Adapter angelegt, konfiguriert und freigeschaltet. Die umfangreiche Funktionalität des Adapters ist separat dokumentiert.

9 *Personalsystem (externe Mitarbeiter)*

- Das Personalsystem dient als Quellsystem für Personalstammdaten externer Mitarbeiter, ist häufig eine Eigenentwicklung basierend auf einer relationalen Datenbank.
- Über die administrative TIM-Benutzerschnittstelle können externe Mitarbeiter erfasst und dem Personalsystem zugeführt werden.

Ressourcenbeispiele 2

Weitere Komponenten einer Sicherheitsinfrastruktur werden durch das IDM-System provisioniert.

10 *Single Sign-On-Server*

- Die für das Desktop-SSO verantwortliche Komponente benötigt aktuelle Benutzerdaten.

11 *Access Management-Server*

- Das Web Access-Management, welches den Zugriff interner Mitarbeiter und externer Partner auf die internen Applikationen und Systeme regelt und daher eine zeitnahe Freischaltung oder Deaktivierung dieser Konten erfordert.
- Das firmeninterne Desktop Single Sign-On-System, welches den Benutzerkomfort bei gleichzeitiger Erhöhung der Sicherheitsstandards durch maximale Kennwortkomplexität, automatisierten Kennwortwechsel etc. verbessert.

12 Benutzerschnittstellen – Web Interfaces

- TIM-Administrationskonsole
- TIM-Endbenutzerkonsole (User Self Service)

TIM zeigt die vorselektierbare Funktionalität in Abhängigkeit vom Benutzertyp an. Zum Beispiel für Endbenutzer eine einfache Endbenutzersicht, Endbenutzersicht mit erweiterter Funktionalität (Vorgesetzte), Datensicht für den User Helpdesk (UHD), spezielle Datensichten für Auditoren, vollständige Datensichten für administrative oder konfigurative Benutzer.

Benutzerschnittstelle UHD – User Helpdesk

Die UHD-Benutzerschnittstelle wird vom IdM-System generiert, administrative Tätigkeiten werden vom UHD in der IdM-Benutzerschnittstelle erbracht. Der UHD hat Zugriff auf sämtliche im IdM-System hinterlegten Personenstammdaten und Benutzerkontendaten bzgl. der angeschlossenen Ressourcen bzw. der zu verwaltenden Kontenattribute.

Zu den Tätigkeiten können beispielsweise gehören:

- Anlegen neuer Benutzer, z. B. externe Mitarbeiter
- Ändern von Benutzerdaten existierender Benutzer, externer und interner Mitarbeiter
- Kennwortrücksetzung
- Löschen und Sperren von Benutzerkonten
- Manuelle Interaktionen bei Prozessabläufen, Workflow
- Einsehen der Aufgabenliste
- Bearbeiten der anstehenden Aufgaben aus der Aufgabenliste

Hier das Beispiel einer funktional eingeschränkten Benutzerschnittstelle:

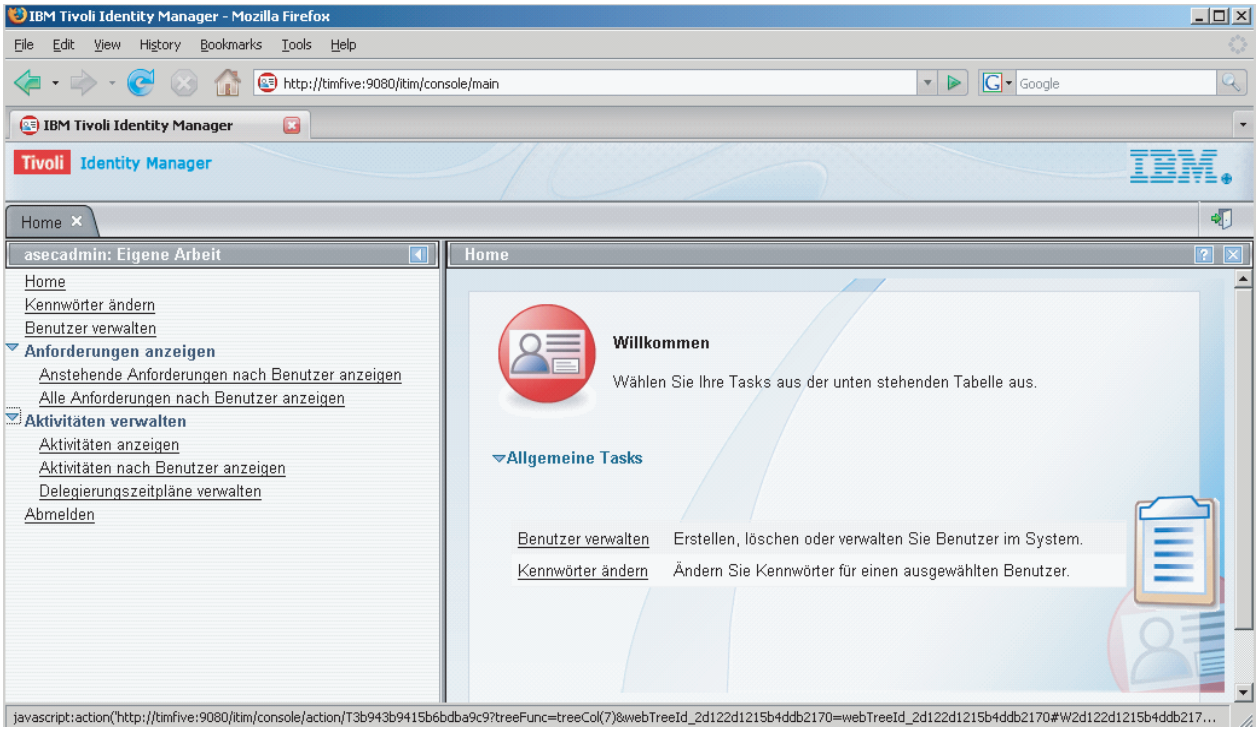


Abb. 4: TIM Web – Benutzerschnittstelle

13 14 Benutzerschnittstelle Endbenutzer

Abb. 5: TIM Web – Endbenutzerschnittstelle

Der Endbenutzer kann mit Hilfe der Self-Service-Web-Schnittstelle eigene Aufgaben wahrnehmen, die bisher dem UHD oder Vorgesetzten vorbehalten waren. Mögliche Tätigkeiten sind beispielsweise:

- Kennwörter zurücksetzten
- Konto/Zugriffe anfordern
- Kontendaten/Zugriffsdaten einsehen
- Profilinformationen einsehen/ändern
- Den Status der angeforderten Berechtigungen einsehen

Erweiterte Endbenutzerschnittstelle und administrative Benutzerschnittstelle

TIM bietet vorbereitete Gruppen (Manager, Auditor, Systemverantwortliche) an. Weitere können bei Bedarf angelegt und konfiguriert werden. Entsprechend der festgelegten Berechtigungen werden die ausgewählten Funktionalitäten angeboten.

Hier einige Beispiele:

Hierzu zählen auch die zahlreich angebotenen Vorlagen für das Ad-Hoc-Berichtswesen, die u. a. Berichte bezüglich Kontenoperationen, Genehmigungen und Ablehnungen, Benutzer und deren Konten, Rezertifizierungen, Datenabgleichsstatistiken, Diensten, Prüfungen und Sicherheitsinformationen, Zugriffsberichte, ruhende, gesperrte und nicht konforme Konten beinhalten.

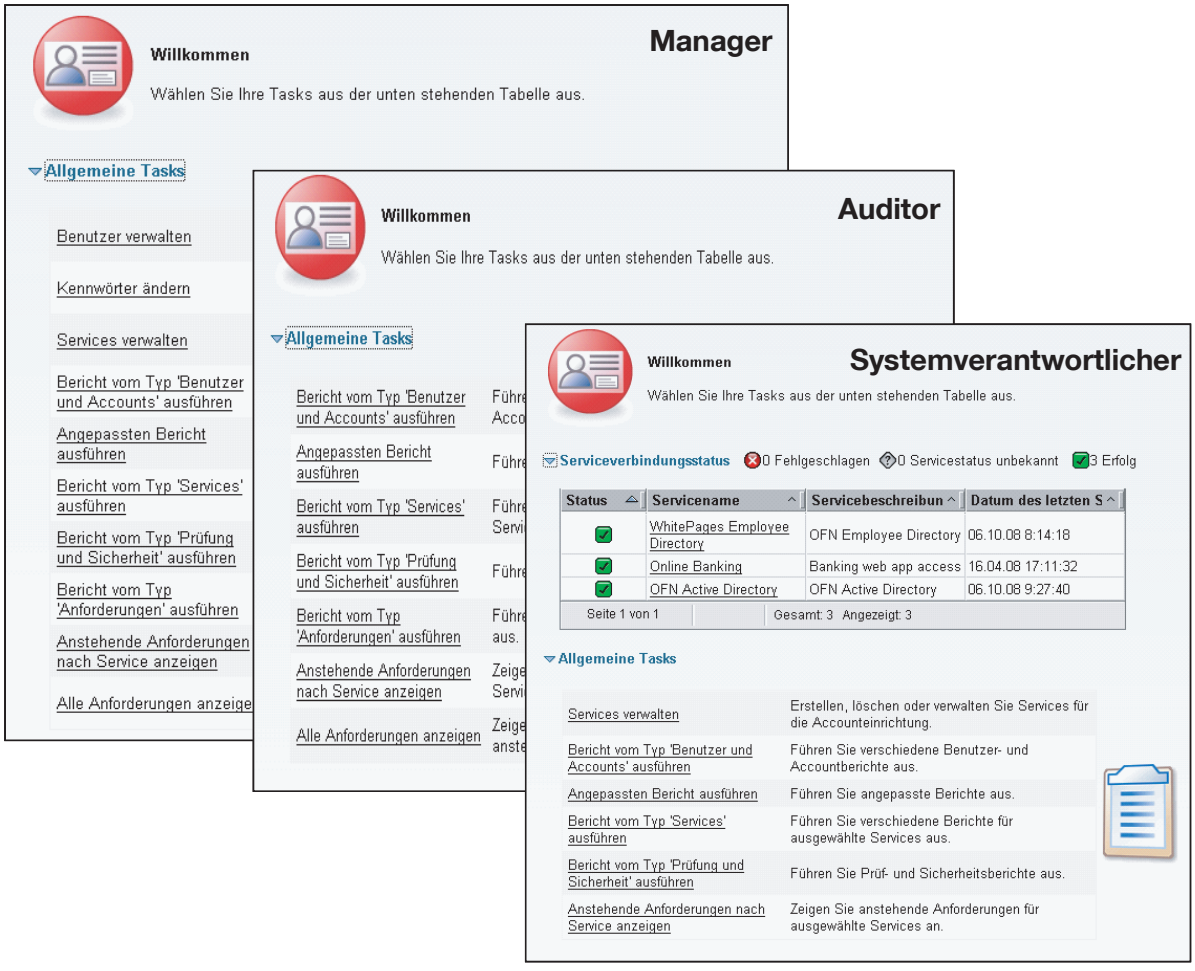


Abb. 6: TIM Web – erweiterte Endbenutzerschnittstelle und administrative Benutzerschnittstelle

18 Benutzerschnittstelle des konfigurativen Benutzers

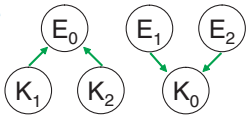
Die bereitgestellten Funktionen für diesen Benutzertyp ermöglichen die Verwaltung der Rollen, der Organisationsstruktur und der Benutzer. Die Ressource- und Zielsystemabhängigen Dienste und Richtlinien werden durch ihn konfiguriert. Weiterhin legt dieser IdM systemspezifische Konfigurationsinformationen fest, hat Zugriff auf entsprechende Richtlinieninformationen und Regeln, z. B. für die Kennwortgenerierung, die Sicherheitsgruppenfestlegung, Berichtskonfiguration etc. Eine weitere Konfigurationsoption ist die Prozessabbildung durch den Workflow-Editor.

Hierarchisches Rollenmodell

Mit TIM 5.1 wird das Konzept der hierarchischen Rollen eingeführt. Hierbei können Elternrollen (EX) ihre Eigenschaften an mehrere Kindrollen (KX) vererben, als auch eine Kindrolle von mehreren Elternrollen erben.

Das Modell implementiert folgende Funktionalitäten:

Abbildung der Rollen und Rechte



Veränderung der Rollenzuweisung bei Personen

Werden TIM-Personen neue Rollen direkt zugewiesen oder diese entfernt, so werden die Rechte automatisch auf Basis des neuen Rollensets, der aktualisierten Rollenmenge neu kalkuliert.

Verändern der Rollenhierarchie

TIM-Personen erhalten implizit Berechtigungen durch die Vererbungshierarchie. Wird diese durch Hinzufügen oder Löschen von Rollen verändert, so werden alle betroffenen TIM-Personen ermittelt, die Vererbungshierarchie neu berechnet und der *Modify_Person* Workflow für jede Entität gestartet.

Dies bedeutet, eine Berechtigungsänderung ist sowohl durch eine direkte Zuweisungsänderung der Rolle als auch über die Hierarchieabbildung möglich. Die neuen Berechtigungen gilt es nun auf den Zielsystemen mittels des *Modify_Person* Workflow durchzusetzen.

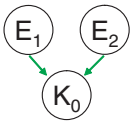
Policy Enforcement und hierarchische Rollen

Um die autorisierten Rechte einer Person zu erhalten, müssen sämtliche Rollen, explizite und implizite Rollen, also statische, dynamische, ererbte Rollen, ausgewertet werden.

Kindrollen erben alle Privilegien der Elternrollen.

Hierzu wertet die „Role Engine“ den gerichten Graphen aus und übergibt das Ergebnis der Separation-of-Dutiy-Prüfung. Liegt keine SoD-Verletzung vor, so werden sämtliche betroffenen Benutzer ermittelt und das Workflow-Partitioning gestartet. Dieses übergibt die Daten an die Provisioning Engine, welche die Account-Operationen (Erstellung/Änderung/Löschung) als Subprozesse der Message Queue übergibt. Die Workflow Engine entnimmt der Message Queue die Einzelaufträge und verarbeitet diese. Sind sämtliche Subprozesse verarbeitet, so wird der übergeordenete Prozess abgeschlossen.

Workflow-Teilnehmer und hierarchische Rollen



In einer Workflow-Deklaration können Aktivitätsteilnehmer, z. B. für die Benachrichtigung via E-Mail zur Bestätigung einer Zuweisung, angegeben werden. Wird in einem Workflow als Teilnehmer einer solchen Aktivität eine Rolle festgelegt, z. B. bei einer Bestätigungsaktivität die Rolle „Manager Zahlungsverkehr“, so werden alle TIM-Personen, die diese Rolle besitzen, benachrichtigt.

Mit dem hierarchischen Rollenkonzept erweitert sich dieser Ansatz. In diesem Beispiel ist die Rolle K0 als Teilnehmer in einer Workflow-Aktivität angegeben und durch eine nachträgliche Änderung/Erweiterung der Hierarchie erbt K0 von E1 und E2, so werden auch alle Besitzer der Rollen E1 und E2 als Teilnehmer der Aktivität eingebunden, also benachrichtigt.

Rolle als Rolleneigentümer

Eine Rolle kann einem Rolleneigentümer bzw. einem Rollenverantwortlichen zugeordnet werden. Dies erlaubt es, dass für die Zuweisung dieser Rolle die Zustimmung des jeweiligen Eigentümers bzw. Verantwortlichen erforderlich ist. So könnte beispielsweise ein Sicherheitsadministrator prinzipiell sein Einverständnis bestätigen müssen, sobald die Zuweisung einer sicherheitsrelevanten Rolle, die den Zugriff auf sensitive Daten erlaubt, erfolgen soll. In einem weiteren Beispiel bedarf der Zugriff auf eine HR-Applikation der Zustimmung eines HR-Verantwortlichen, da der Zugriff durch die Zuweisung der entsprechenden Rolle geregelt ist. In Abhängigkeit der Zustimmung oder Ablehnung werden rollenabhängige Privilegien vergeben.

Mit TIM 5.1 ist es zusätzlich möglich, Rollen wiederum als Eigentümer/Verantwortlicher für Rollen zu definieren und somit komplexere Szenarien abzubilden.

Klassifizierung der Rolle

TIM 5.1 erlaubt die eindeutige Klassifizierung einer Rolle. Aktuell sind die Standardwerte Applikationsrolle und Geschäftsrolle vordefiniert. Diese Werteliste kann erweitert werden, z. B. zur Einordnung der Rollen in Bezug auf eine sicherheitskritische Einstufung: „Level 1 Security Clearance“, „Level 2 ..“, „Level x ..“.

Die Abbildung 7 stellt die Verknüpfung der einzelnen Funktionseinheiten, Role Manager, Policy Engine, SoD Engine, Data Service dar. Die Role Engine übernimmt in Zusammenarbeit mit dem Role Manager die Aufgabe der Verifizierung der Rollenhierarchie. So werden beispielsweise Hierarchie-Zyklen, hier im Beispiel (R4 + R5 + Rx) und auch Vererbungsredundanzen, hier im Beispiel für R3, unterbunden.

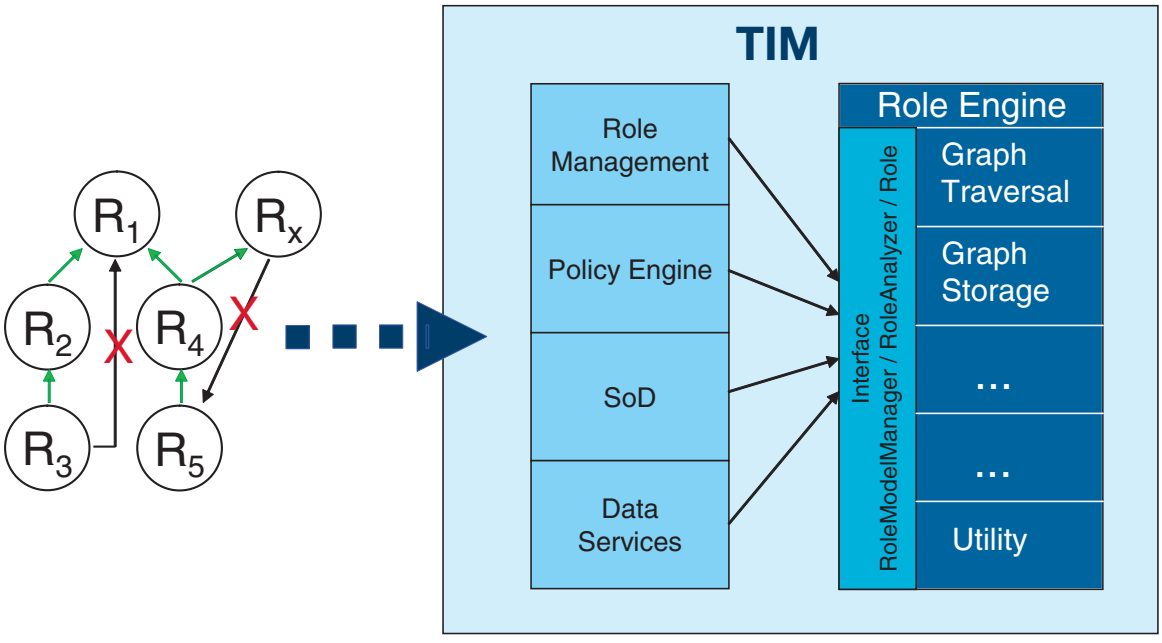


Abb. 7: TIM Role Engine

Der Role-Manager verarbeitet die Rechteset-Vererbung, also auch die Berechnung der sich ergebenden Berechtigungen durch Einfach- und Mehrfachvererbung.

Die SoD Engine (Separation of Duty) ermittelt auf Basis der hinterlegten Richtlinien und Regeln, ob eine Richtlinienverletzung auf Basis der Rollen vorliegt. Ist dies der Fall, so wird der Verantwortliche ermittelt und benachrichtigt, eine Ausnahme kann genehmigt oder abgelehnt werden. Im Positivfall werden nun die Provisionierungsaufträge an die Workflow-Engine übergeben.

Separation of Duties – SoD

Mit TIM 5.1 wird die Funktionalität der Trennung der Aufgaben auf Basis der Geschäftsrollen und funktionalen Rollen eingeführt. Somit kann eine strikte Trennung der Verantwortlichkeiten auf der Ebene der organisatorischen Geschäftseinheiten durchgesetzt werden, d. h. unterschiedliche SoD-Richtlinien für eigenständige Organisationseinheiten oder übergeordnete SoD-Richtlinien für untergeordnete Organisationseinheiten, z. B. Abteilungshierarchien.

SoD-Richtlinien (Policies) bestehen aus SoD-Regeln, welche die sich gegenseitig ausschließenden Rollen beinhalten.

Hierbei gilt folgende Abbildungsregel:

SoD-Richtlinie $_{1\,..\,n}$ SoD-Regel $_{1\,..\,m}$ Rollen mit (m-1) erlaubten Rollenkombinationen

In diesem (einfachen) Beispiel besteht die SoD-Richtlinie aus den SoD-Regeln Regel1 und Regel2. Die Regel1 erlaubt eine Kombination von zwei aus drei der angegeben Rollen, die Regel2 jedoch schließt die gemeinsame Zuweisung der Rollen Rolle1 und Rolle3 aus. Somit sind mit diesem Beispiel für die existierenden Rollen Rolle$_{1..3}$ gemäß Regel1 folgende Permutationen der Rollenkombinationen möglich:

Rolle1 + Rolle2 , Rolle1 + Rolle3 und Rolle2 + Rolle3, Regel2 schließt die in Regel1 erlaubte Kombination aus Rolle1 und Rolle3 wieder aus.

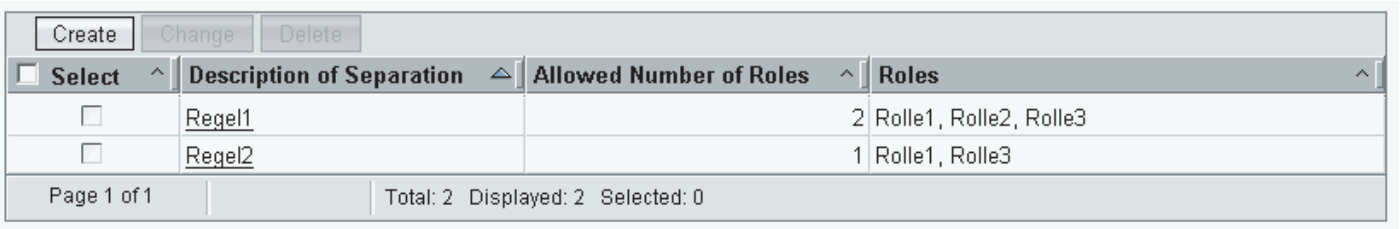


Abb. 8: Regelliste der SoD Policy

SoD-Ausnahme Lebenszyklus

SoD-Richtlinienverletzungen werden ausgelöst durch eine Rollenzuweisung oder Veränderung einer bestehenden Zuweisung. Diese initiiert durch eine manuelle, administrative Aktion, wie Personendatenänderung und Personendatenanlage oder einer automatisierten, autoritativen Datenquelle, z. B. durch ein führendes Personalsystem (HR-Feed), führt zu einer Ausnahme, die von einer verantwortlichen Person bearbeitet werden muss.

Abbildung 9 zeigt die unterschiedlichen Startpunkte zur Interaktion mit den SoD-Richtlinien (RL).

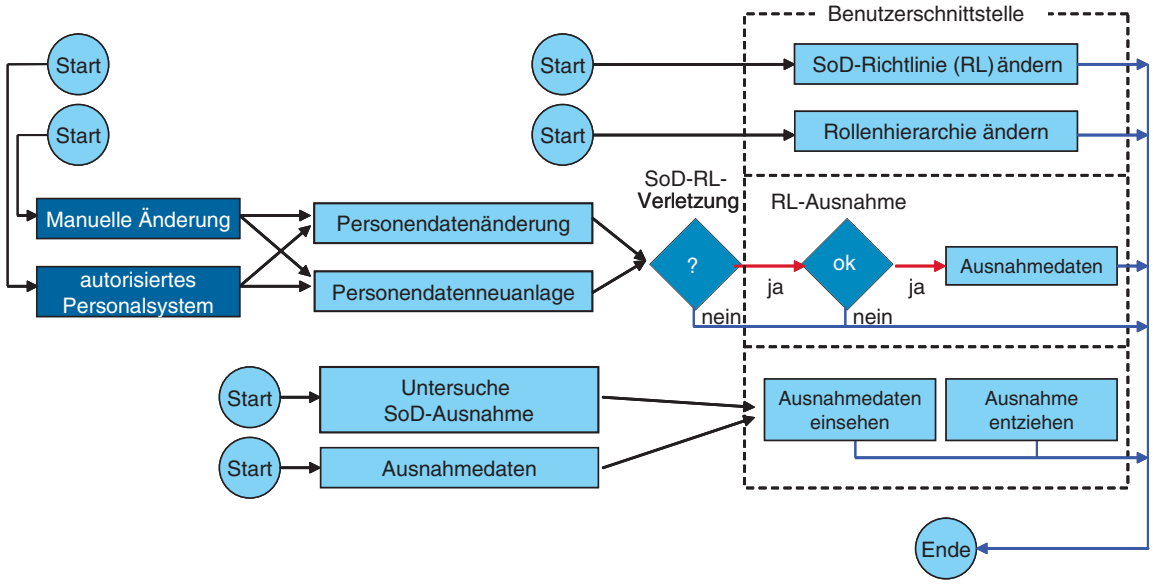


Abb. 9: SoD-Lebenszyklus

Beispielhafter Ablauf – involvierte Mitarbeiter/ Personen (P1..P5)

1. P1 – Ein Rollenverantwortlicher erstellt die notwendigen SoD-Regeln. Dies beinhaltet die Rollen und die Rollenseparation gemäß den Sicherheitsrichtlinien.
2. P2 – Ein SoD-Administrator erstellt die SoD-Richtlinien (Policies) in TIM.
3. P3 – Ein Sicherheitsverantwortlicher, verantwortlich für die Überwachung und die Ausnahmebestätigung (violation monitoring, exemption handling), erhält die Benachrichtigung per E-Mail oder prüft selbstständig, ob Verletzungen vorliegen.
4. P4 + P5 – Beantragender Mitarbeiter und sein Vorgesetzter.

Beispielhafter Ablauf – Sequenz

1. Alle SoD-Richtlininen wurden definiert und im System deklariert (P1 + P2).
2. Ein Mitarbeiter beantragt via Browser-Benutzerschnittstelle Zugriff auf eine weitere Ressource bzw. ein weiteres Benutzerkonto (P4).
3. Der Zugriff auf sicherheitssensitive Informationen verlangt auf Grund des hinterlegten Workflows eine Bestätigung des aktuellen Vorgesetzten (P5). Dieser wird per E-Mail benachrichtigt und bestätigt die Notwendigkeit des Zugriffs. Diese Informationen werden dem Berichtswesen zugeführt.

Der Zugriff auf die kritischen Daten wird durch eine separate Rolle abgebildet. Es kommt zu einer Ausnahme, da die Zuweisung der Rolle den Vorgaben des Rollen- bzw. Richtlinienverantwortlichen (P1) widerspricht. Dies könnte z. B. die Berechtigung zur Rechnungserfassung und der gleichzeitigen Berechtigung zur Zahlungsfreigabe sein.

4. Der SoD-Richtlinienverstoß bewirkt automatisch eine Ausnahme im SoD-Modul. Diese wird dem Verantwortlichen (P3), festgelegt durch eine Rollenzuweisung oder eine personenbezogene Festlegung (z. B. „Manager Zahlungsverkehr“), per E-Mail mitgeteilt.
5. Der Verantwortliche (P3) kann nun die gewünschte Rollenzuweisung ablehnen oder die Ausnahme akzeptieren und zusätzlich eine textuelle Begründung hinterlegen.
6. Der beantragende Mitarbeiter (P4) erhält im Positivfall den Zugriff.

Sowohl die Ausnahme als auch die Begründung werden gespeichert und im Berichtswesen angezeigt. So könnte beispielsweise ein Personalmangel zu einer solchen begründeten Ausnahmesituation führen und ist hierdurch im Falle eines Sicherheitsaudits auch berichtbar – inklusive Begründung.

Der Sicherheitsverantwortliche kann sowohl einzelne als auch sämtliche vorhandenen Ausnahmen einsehen und diese den SoD-Richtlinien widersprechenden Berechtigungen wieder entziehen, um so einen richtlinienkonformen Zustand herbeizuführen. In diesem Beispiel wurde der Personalmangel behoben, die erteilte Ausnahme muss widerrufen werden, der Administrator entzieht dem Benutzer die jetzt unrechtmäßigen Rollenzuweisungen.

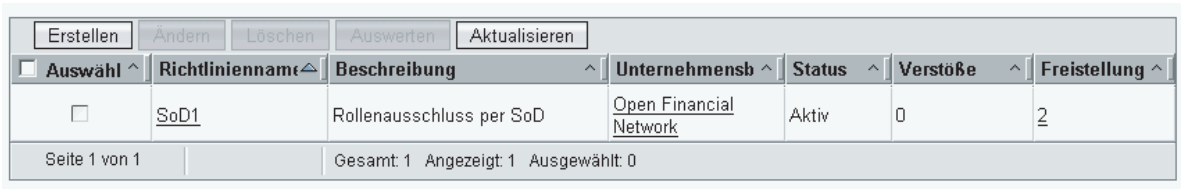


Abb. 10: Übersicht der Verstöße und Freistellungen

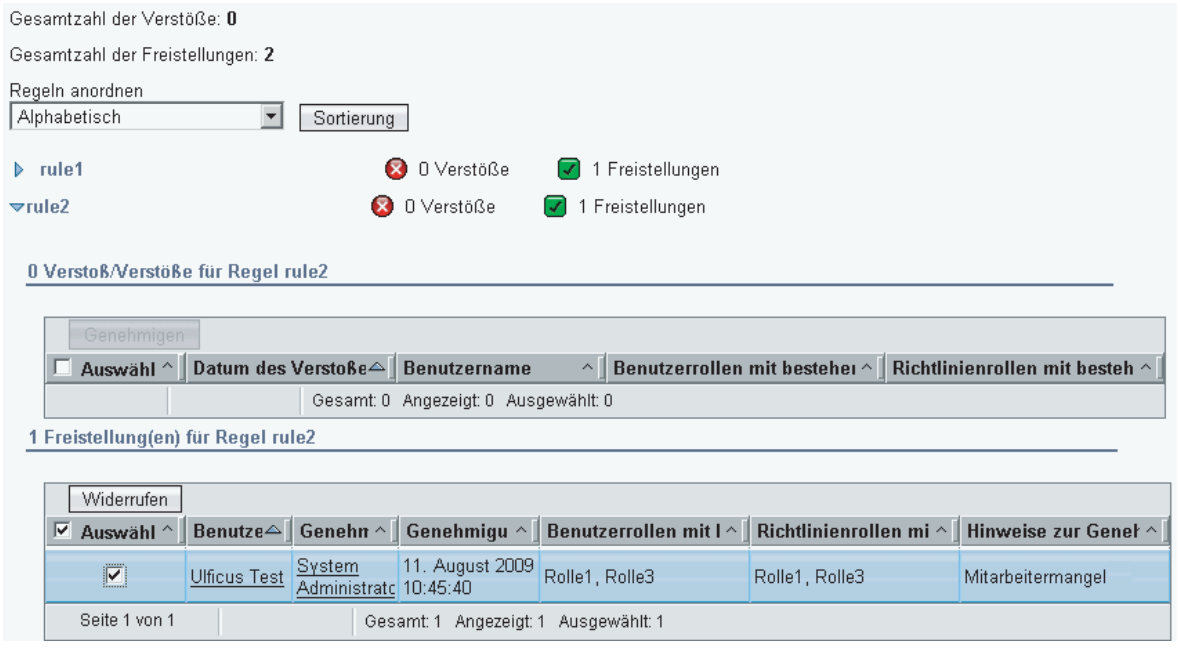


Abb. 11: Widerruf der Freigabe zur Wiederherstellung der Richtlinienkonformität

Die SoD-Richtlinienverletzung und die Aufforderung zur SoD-Ausnahmebestätigung oder -ablehnung werden dem/den Verantwortlichen sowohl in der Administrationskonsole als auch in der Self-Service-Benutzerschnittstelle angezeigt. Sowohl die SoD-Richtlinienmanipulationen als auch die Ausnahmebehandlung (Annahme/Ablehnung) werden dem Berichtswesen zugeführt.

Das Berichtswesen des Tivoli Identity Manager (Tivoli Common Reporting) wurde um die zwei Standardberichte „Separation of Duty – Richtliniendefinition“ und „Separation of Duty – Richtlinienverletzung“ erweitert.

Arbeitsabläufe – Workflows

Prozessabbildung durch automatisierte Workflow-Aktivitäten

Die TIM-eigene Workflow Engine bietet die Möglichkeit, sowohl standardisierte Identity Management-Prozesse als auch beliebig erweiterbare Abläufe mittels einer geführten Erstellung zu konfigurieren oder unter Nutzung des grafischen Editors anzufertigen.

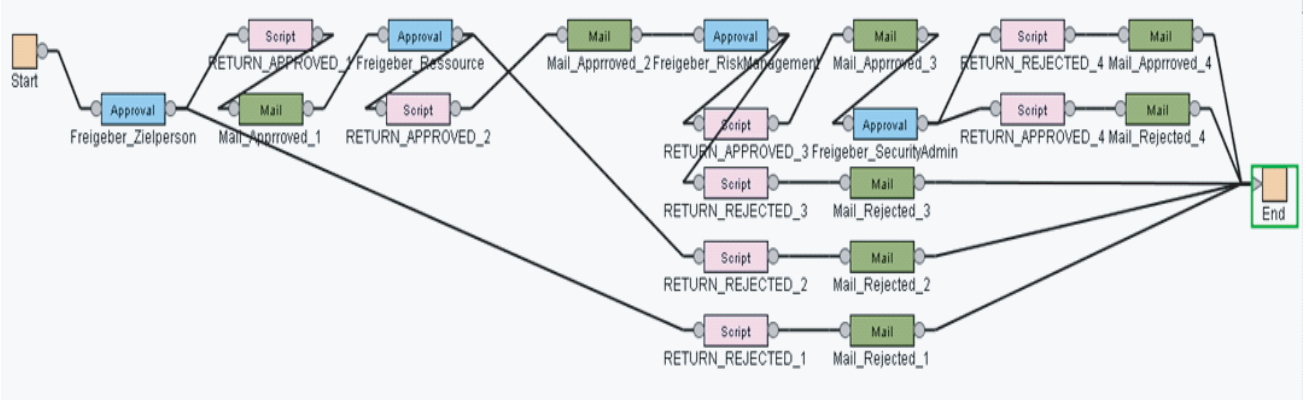


Abb. 12: TIM Workflow Editor – Aktivitätenabbildung

Hier ist die Abbildung eines komplexeren Ablaufs unter Einbeziehung des Vorgesetzten, des Systemverantwortlichen, des Risikomanagements und der Sicherheitsadministratoren zur Freigabe einer sicherheitsrelevanten Ressource dokumentiert.

Hierzu stehen vorbereitete Komponenten zur Verfügung, die komplexe Aktionen und Aktivitäten abbilden. Diese werden via GUI konfiguriert, beispielsweise wenn eine Beantragung eine Freigabe benötigt, wie in obiger Prozessabbildung (Abb. 12).

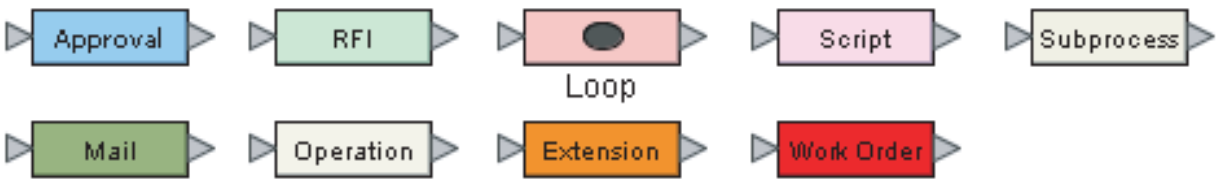


Abb. 13: TIM Workflow-Komponenten

Rezertifizierung einfach und leicht gemacht:
Unterliegen Zugriffe oder Benutzerkonten einer sich wiederholenden, erneuten Zertifizierung, die auch entsprechend im Reporting nachgewiesen werden muss, so bietet TIM „out-of-the-box“ eine Rezertifizierungsrichtlinie an.

Diese wird zeitlich gesteuert vom IDM-System angestoßen, z. B. täglich, wöchentlich, monatlich oder vierteljährlich und verlangt vom Benutzer, Manager oder Rolleneigentümer nach einer Aufforderung via E-Mail die Bestätigung, dass er den Zugriff bzw. Account noch benötigt.

Werden zeitliche Grenzwerte nicht eingehalten, so können Zugriffe automatisiert entzogen oder (mahnende) Mitteilungen versandt werden.

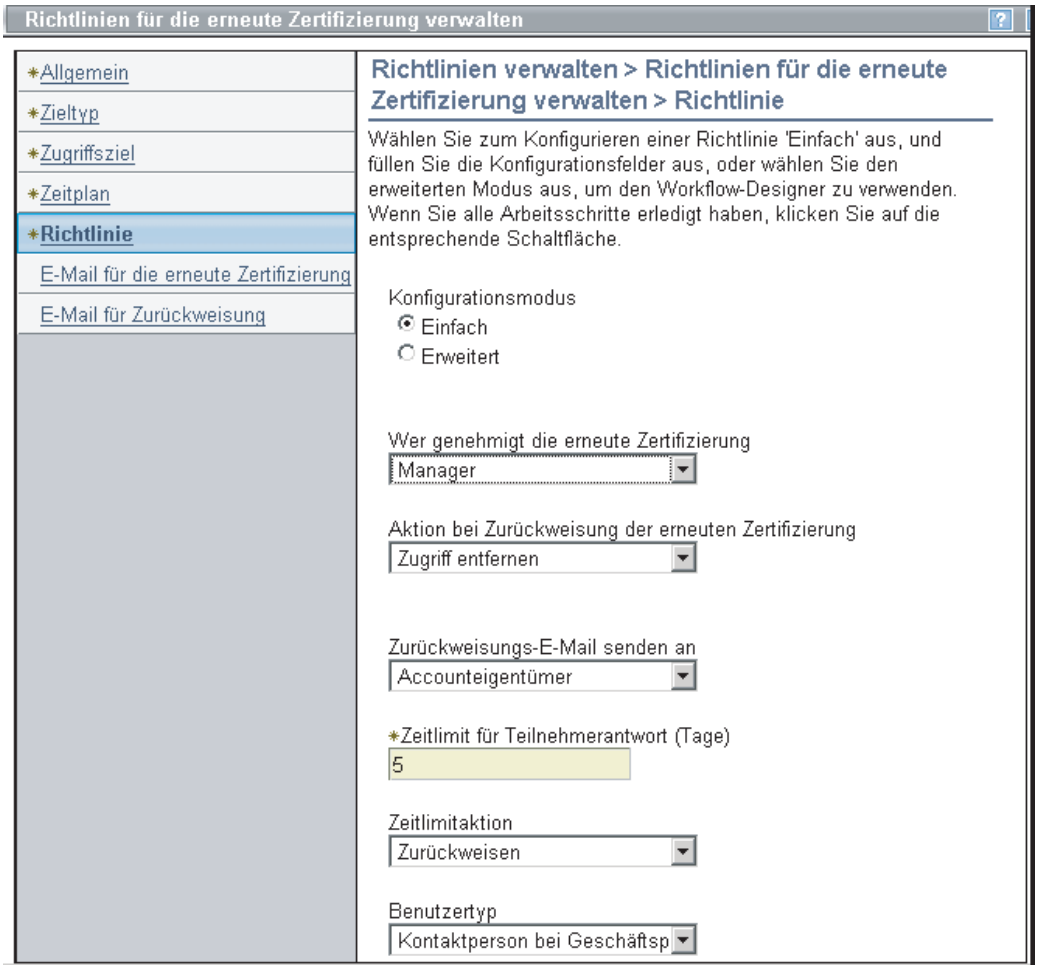


Abb. 14: Zugriffs- und Konten-Rezertifizierungsrichtlinie, Konfigurator

Sollte der benutzerfreundliche Konfigurationsassistent, siehe Abbildung 14, nicht ausreichen, so kann die Richtlinie auch im grafischen Editor bearbeitet werden. Dies betrifft sowohl die einzelnen Ablaufschritte und Aktionen als auch die zu versendenden Benachrichtigungen bzgl. Format und Inhalt der Nachricht.

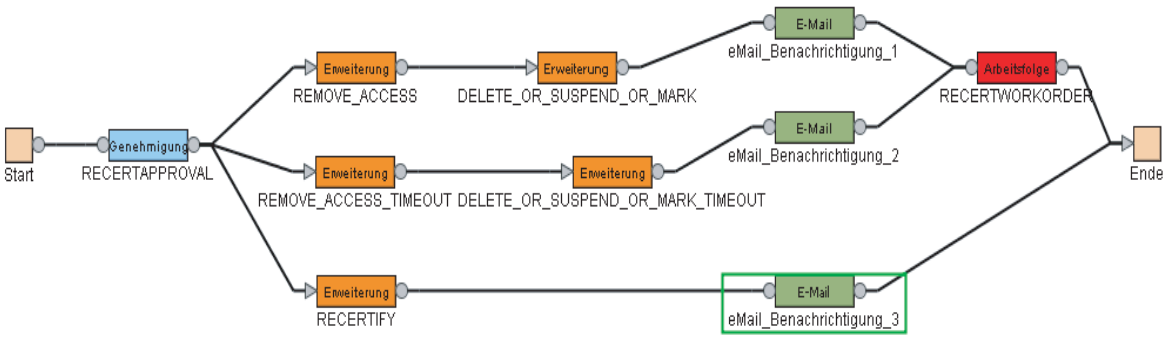


Abb. 15: Zugriffs- und Konten-Rezertifizierungsrichtlinie, Workflow-Editor

Übersicht

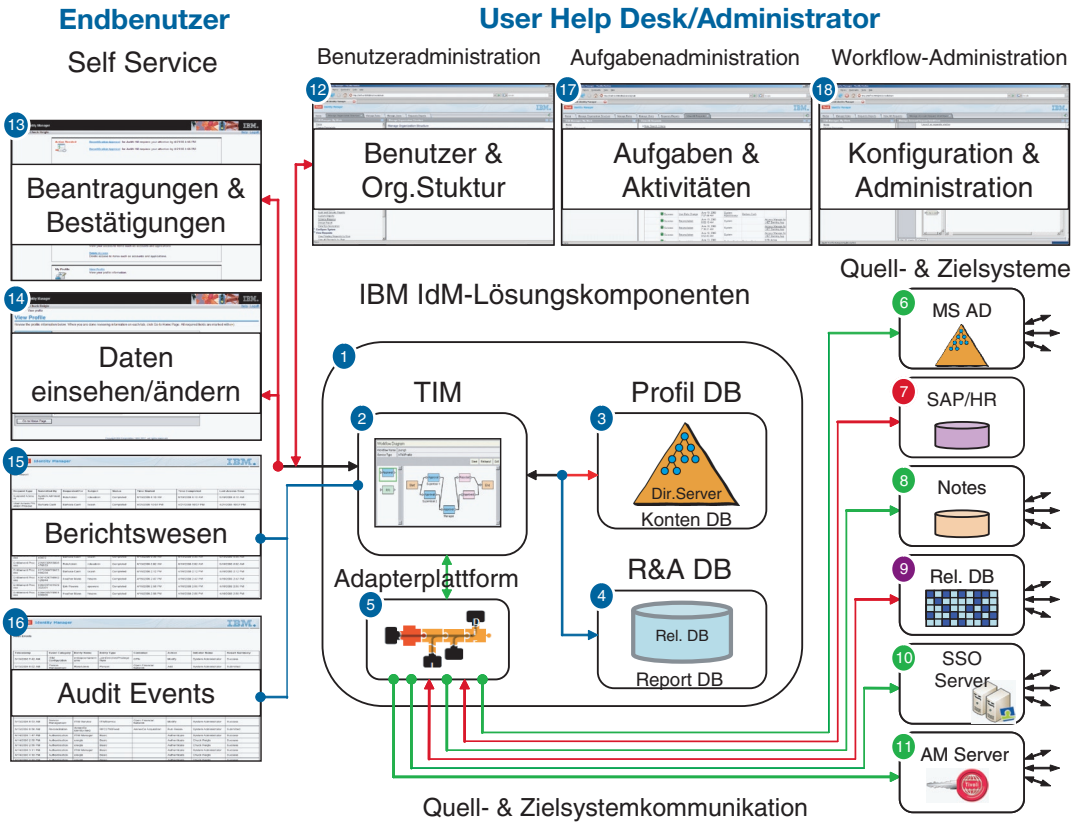


Abb. 16: Übersicht der IBM Tivoli Identity Management-Lösungskomponenten

Weitere Informationen

Werkzeuge/Tools

- GCE – Graphical Configuration Editor
  www-01.ibm.com/software/brandcatalog/portal/opal/details?catalog.label=1TW10IM0G
- ADT – Adapter Development Tool
  www-01.ibm.com/software/brandcatalog/portal/opal/details?catalog.label=1TW10IM0H

Community

- www.tivoli-ug.org/
- www-306.ibm.com/software/tivoli/community/
- ibm.com/developerworks/forums/tivoli_forums.jspa
- http://www-128.ibm.com/developerworks/forums/dw_forum.jsp?forum=259&cat=15
- ibm.com/developerworks/wikis/display/tivoli/Home

Sicherheitsarchitekturen

Security-Architekturen, Compliance-Werkzeuge und Berichtswesen – sprechen Sie uns an.

Wir beraten Sie gerne, sowohl bei technischen Fragen, Fragen zu Identity Management- Prozessen als auch im Hinblick auf IdM- bzw. Sicherheitsprojekte durch Unterstützung unserer projektbezogenen *Best Practices*, Architekturen und unserer Projektmethodiken.

Kostenlose Redbooks (Auszug)

- Identity Management Design Guide with IBM Tivoli Identity Manager
- www.redbooks.ibm.com/abstracts/SG246996.html?Open
- Deployment Guide Series: IBM Tivoli Identity Manager 5.x
- www.redbooks.ibm.com/abstracts/sg246477.html?Open
- Suche über den Index
  www.redbooks.ibm.com/cgi-bin/searchsite.cgi?query=identity+and+management

Weitere Produktinformationen, multilingual in Abhängigkeit der Spracheinstellung Ihres Browsers, siehe

Alle Produkte alphabetisch sortiert:

http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm.tivoli.az.doc/welcome.htm

Identity Manager:

http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?toc=/com.ibm.itim.doc/toc.xml

Weitere Service-Informationen unter:

www-01.ibm.com/software/tivoli/services/consulting/

Weitere IBM Security-Produkte und Informationen unter:

www-01.ibm.com/software/de/tivoli/ts_mgmt.html
www-05.ibm.com/de/security/
www-01.ibm.com/software/de/itsolutions/compliance/

Ihre Ansprechpartner

Wenn Sie weitere Informationen benötigen, wenden Sie sich an Ihre IBM Ansprechpartner:

Ulf Feger
E-Mail: ulf.feger@de.ibm.com

Matthias Lehmann
E-Mail: mlehmann@de.ibm.com

IBM Deutschland GmbH
IBM-Allee
71139 Ehningen
ibm.com/de

IBM Österreich
Obere Donaustrasse 95
1020 Wien
ibm.com/at

IBM Schweiz
Vulkanstrasse 106
8010 Zürich
ibm.com/ch

Die IBM Homepage finden Sie unter:
ibm.com

Recyclingfähig, bitte der Wiederverwertung zuführen

TIW14053-DEDE-00