



Workflow im Identity Management

Januar 2009

Georg Völl
Senior Consultant



Agenda

- **Was ist Workflow und braucht man das?**
- **Die Workflow Engine im Sun Identity Manager**
- **Sun Identity Management Portfolio Überblick**
- **Q & A**

Definition Workflow



- Ein Arbeitsablauf, englisch Workflow, ist eine **vordefinierte Abfolge von Aktivitäten** in einer Organisation.
- Der Arbeitsablauf betont dabei die **operativ-technische Sicht auf die Prozesse**, während der in der Definition nahe stehende **Geschäftsprozess** den Bezug zu betriebswirtschaftlichen Faktoren wie Kosten und Erlösen betrachtet, z. B. bei einem Handelsprozess.
- Dabei kann ein IT-System **den Ablauf unterstützen**, ihn mit notwendigen Daten versorgen und ihn gemäß einer im System hinterlegten Vorgabe oder eines dafür vorgesehenen Algorithmus abwickeln.
- Herstellerübergreifende, internationale Gremien wie **WfMC** **haben dazu Standards** wie BPML entwickelt.

Was steht zwischen den Zeilen?

- Arbeitsabläufe können automatisiert werden, sofern sie durch die IT unterstützt sind
 - > Weniger fehleranfällig
 - > Zeitersparnis (keine Medienbrüche)
- Ein Einbinden der spezifischen Arbeitsabläufe (z.B. im Identity Management) in übergreifende (Geschäfts-)Prozesse ist sinnvoll
- Anpassungsmöglichkeiten dringend notwendig
- Verwendung von Standards schafft Sicherheit und Investitionsschutz

Definition Identity Management



- Als Identitätsmanagement (IdM) wird der zielgerichtete und bewusste Umgang mit Identität, Anonymität und Pseudoanonymität bezeichnet. Der Personalausweis ist ein Beispiel für eine staatlich vorgegebene Form der Identifizierung.
- Identitätsmanagement befasst sich vornehmlich in der Welt der Datenverarbeitung mit der Verwaltung von Benutzerdaten, die einzelnen Personen zugeordnet sind. Eine Person kann dabei durchaus mehrere Identitäten besitzen, während eine Identität gewöhnlich nur einer Person zuzuordnen ist. Dabei ist die Identität eine Sammlung von personenbezogenen Attributen, die die Person, die sich dieser Identität bedient, individualisiert.

Umfang von IdM Lösungen

- Der Begriff Identity Management im Software-Umfeld umfasst keinen genau definierten Funktionsumfang.
- So fokussieren sich beispielsweise einfache Systeme ausschließlich auf die Synchronisation von personenbezogenen Daten z.B. ein Meta Directory.
- Umfassendere IdM-Architekturen bieten mehr Funktionalität z.B.: Self-Service, Reporting, GRC, Rollen, SSO, Federation, etc.

Unterschiedliche IdM Lösungen

Meta Directory

- Data Synchronisation
- Basic Provisioning
- Rules Engine

Provisioning

- Identity Synchronisation
- Passwordhandling
- Rules / Policies
- Audits / Reports
- Self-Service
- Delegated Administration / Single Interface
- Workflow

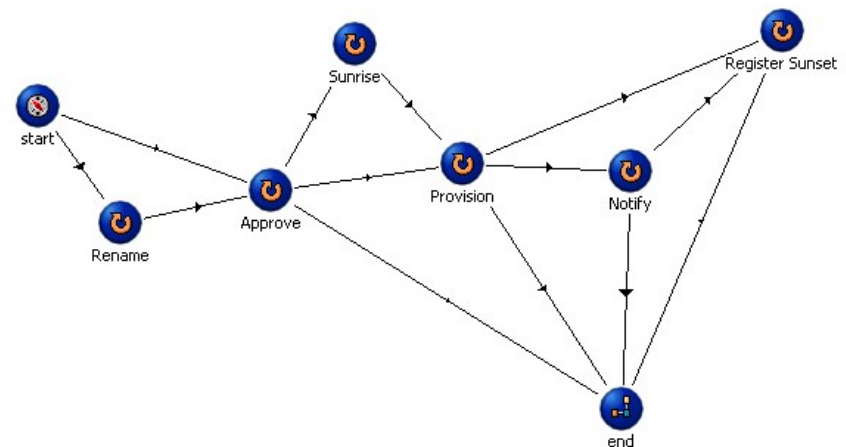
Definition Provisioning



- Als Versorgungsprozess bzw. provisioning process wird ein Prozess bezeichnet, der nötig ist, um einen Anwender eines IT-Systems mit den grundsätzlichen Voraussetzungen für seine Tätigkeit auszustatten.
- Es sind also primär EDV-getriebene Prozesse gemeint, die aber um Nicht-EDV-Prozesse ergänzt werden können. Diese Prozesse existieren meist schon als **Laufzettel**, werden aber im Rahmen einer Standardisierung und Computerisierung der **Prozesse elektronisch abgebildet**.
- Das Fachwort Versorgungsprozess bzw. provisioning wird vor allem in Zusammenhang mit Identitätsmanagement, bei **Meta-Verzeichnissen, die oft um Workflows erweitert werden**, um die Benutzerverwaltung schneller zu machen und zu **automatisieren**, aber auch in der Mobilfunk-Industrie angewendet.

Erweiterte Anforderung

- Eine umfassende Identity-Management-Architektur sollte über ein Provisionierungsmodul verfügen, das es erlaubt, den Benutzern automatisch aufgrund ihrer jeweiligen Rolle (und auch Aufgaben) in der Organisation individuelle Berechtigungen zu erteilen.
- Dieser Provisionierungsprozess sollte anpassbar sein.
- Automatisierung



→ Provisioning Workflow

(oder z.B. Attestation, Remediation Workflow)

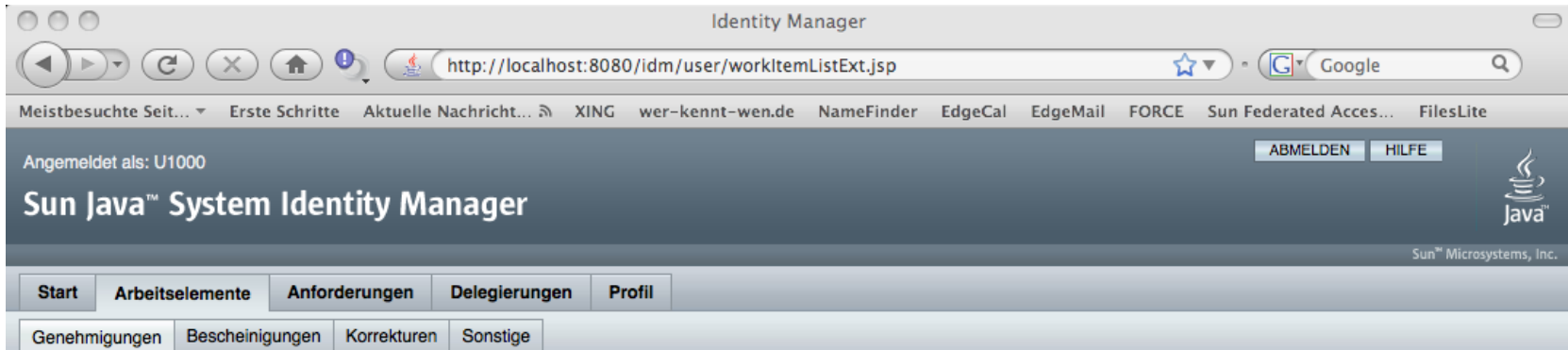
Erweiterte Anforderung (2)

- Eine umfassendere Architektur sollte auch Workflow-Prozesse einbeziehen, die ein hierarchisches Genehmigungs-Modell von Vorgesetzten beinhalten, um Datenänderungen umzusetzen.
- Approval (Zustimmung) durch “Vier-Augen-Prinzip”
- Interaktion mit mehreren Teilnehmern
- Keine Medienbrüche (Laufzettel)

→ Approval Workflow

Beispiel: Neuer Mitarbeiter in Organisation „Sun“ erfordert erst eine Genehmigung durch den Abteilungsleiter.

Approval durch Vorgesetzten



Identity Manager

http://localhost:8080/idm/user/workItemListExt.jsp

Meistbesuchte Seit... Erste Schritte Aktuelle Nachricht... XING wer-kennt-wen.de NameFinder EdgeCal EdgeMail FORCE Sun Federated Acces... FilesLite

Angemeldet als: U1000 ABMELDEN HILFE

Sun Java™ System Identity Manager

Sun Microsystems, Inc.

Start Arbeitselemente **Anforderungen** Delegierungen Profil

Genehmigungen Bescheinigungen Korrekturen Sonstige

Wartet auf Genehmigung

Markieren Sie ein Kästchen neben einer anstehenden Anforderung, um sie auszuwählen. Klicken Sie auf **Genehmigen**, um die Anforderung zu genehmigen, oder auf **Zurückweisen**, um sie abzulehnen. Um die Anforderungsliste zu sortieren, klicken Sie auf eine Spaltenüberschrift.

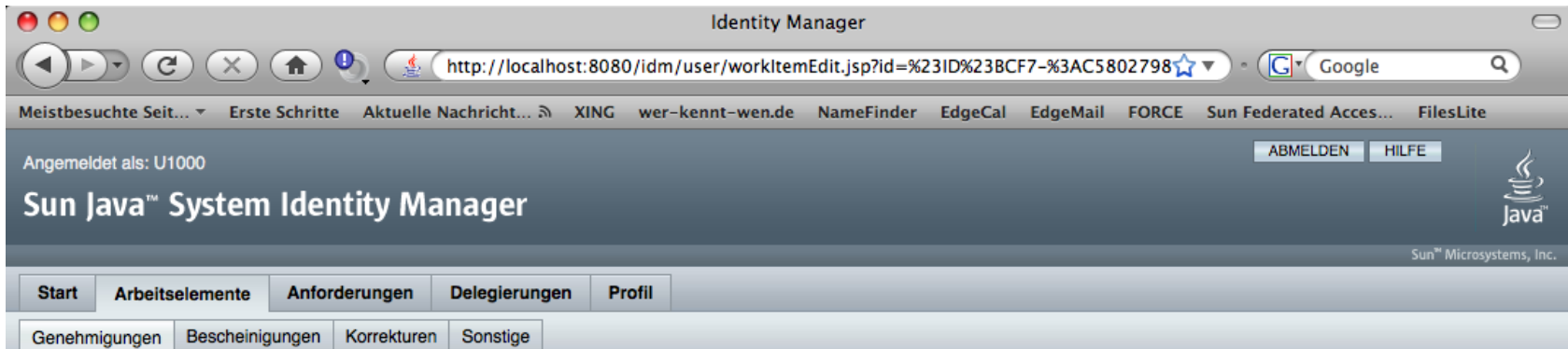
Genehmigungen auflisten für Eigenes Konto

<input type="checkbox"/>	▼ Genehmiger	Anforderung	Anfordernder	Datum der Anforderung	Beschreibung
<input type="checkbox"/>	U1000	Organisation Top:Sun genehmigen	Configurator	Mittwoch, 18. Februar 2009 13.56 Uhr CET	Konto U1004

Genehmigen Zurückweisen Aktualisieren Weiterleiten

Zurück zum Hauptmenü

Approval Details



The screenshot shows a web browser window titled 'Identity Manager'. The address bar displays the URL: `http://localhost:8080/idm/user/workItemEdit.jsp?id=%231D%23BCF7-%3AC5802798`. The browser's search bar contains 'Google'. The page header includes a navigation menu with links like 'Meistbesuchte Seit...', 'Erste Schritte', 'Aktuelle Nachricht...', 'XING', 'wer-kennt-wen.de', 'NameFinder', 'EdgeCal', 'EdgeMail', 'FORCE', 'Sun Federated Acces...', and 'FilesLite'. Below the header, it shows 'Angemeldet als: U1000' and buttons for 'ABMELDEN' and 'HILFE'. The main title is 'Sun Java™ System Identity Manager'. A sidebar on the left contains tabs for 'Start', 'Arbeitselemente', 'Anforderungen', 'Delegierungen', and 'Profil'. The 'Anforderungen' tab is selected, showing sub-tabs for 'Genehmigungen', 'Bescheinigungen', 'Korrekturen', and 'Sonstige'.

Anforderung bearbeiten

Zeigen Sie Anforderungsdetails an und bearbeiten Sie diese wahlweise. Klicken Sie auf **Genehmigen**, um Änderungen zu speichern und die Anforderung zu genehmigen, oder auf **Zurückweisen**, um Änderungen zu speichern und sie abzulehnen.

Anfordernder Administrator	Configurator
Anfordernde Anwendung	Administrator Interface
Konto-ID	U1004
Rolle	
Organisation	Top:Sun
E-Mail-Adresse	wilfried.stuettgen@sun.com
Individuelle Ressourcenzuweisung	
Kommentare	<input type="text"/>

Agenda

- Was ist Workflow und braucht man das?
- **Die Workflow Engine im Sun Identity Manager**
- Sun Identity Management Portfolio Überblick
- Q & A

Dynamic Workflow Engine

- Workflows sind parametrisierbar (dynamisch)
 - > Ein Workflow für verschiedene Anforderungen
- Basiert auf Standards:
 - > Workflow Management Coalition
 - > WFMC TC-1003 Workflow Reference Model
 - > Inestitionsschutz (da austauschbar / kombinierbar)

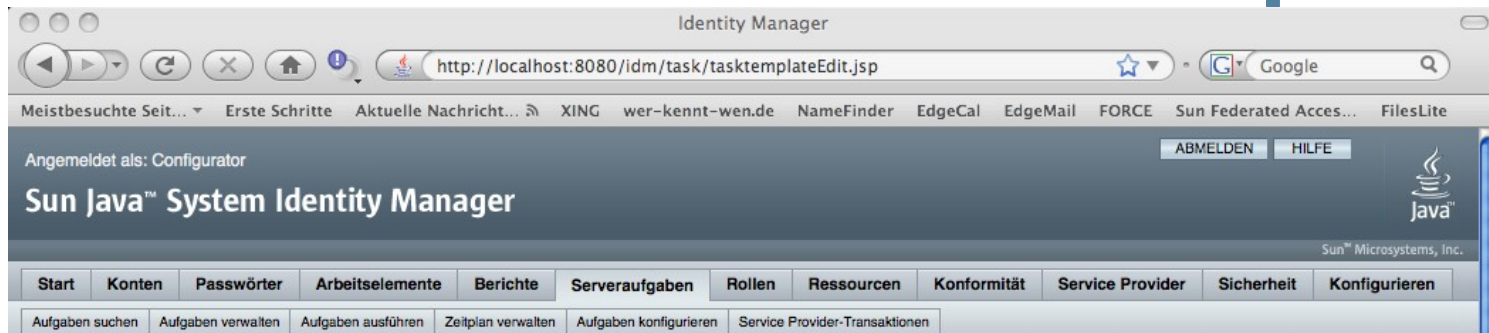
Workflow Management Coalition



<http://www.wfmc.org/>

- Workflows frei anpassbar (frei für Erweiterungen)
 - > Keine „Sackgassenlösung“

Parametrisierbar durch Templates



Aufgabenvorlage 'Create User Template' bearbeiten

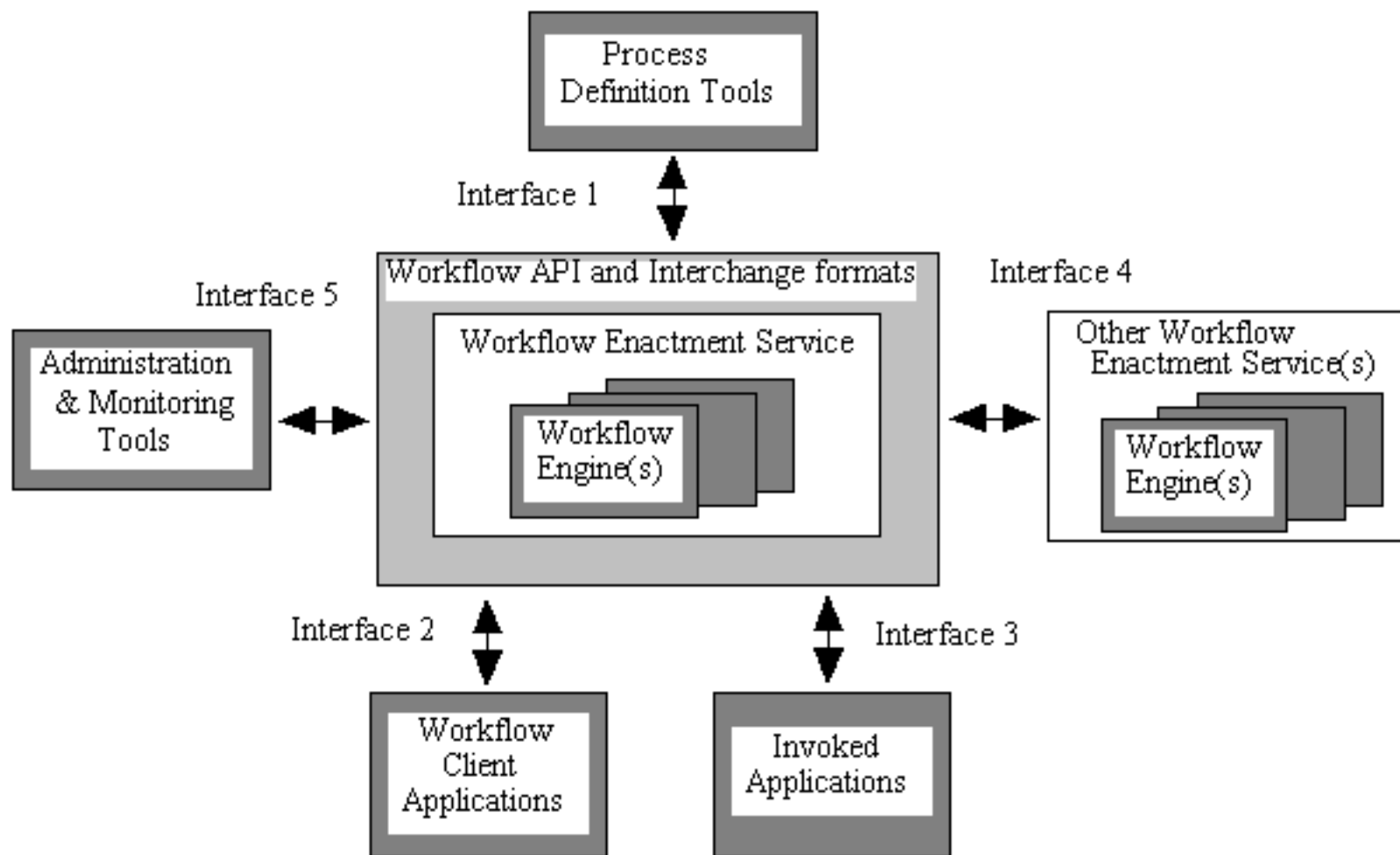
Bearbeiten Sie die Eigenschaften und klicken Sie auf "Speichern".

Allgemein	Benachrichtigung	Genehmigungen	Überwachung	Bereitstellung	Sunrise und Sunset	Datenumwandlungen																		
Genehmigung aktivieren																								
Organisationsgenehmigungen <input checked="" type="checkbox"/> Aktivieren																								
Ressourcengenehmigungen <input checked="" type="checkbox"/> Aktivieren																								
Rollengenehmigungen <input checked="" type="checkbox"/> Aktivieren																								
Zusätzliche Genehmiger																								
Festlegen zusätzlicher Genehmiger aus: <input type="text" value="Keine"/>																								
Konfiguration des Genehmigungsformulars																								
Genehmigungsformular: <input type="text" value="Approval Form"/>																								
<table border="1"> <thead> <tr> <th>Attributname</th> <th>Formular-Anzeigename</th> <th>Bearbeitbar</th> </tr> </thead> <tbody> <tr> <td>user.waveset.accountId</td> <td>Konto-ID</td> <td><input type="checkbox"/></td> </tr> <tr> <td>user.waveset.roles</td> <td>Rolle</td> <td><input type="checkbox"/></td> </tr> <tr> <td>user.waveset.organization</td> <td>Organisation</td> <td><input type="checkbox"/></td> </tr> <tr> <td>user.global.email</td> <td>E-Mail-Adresse</td> <td><input type="checkbox"/></td> </tr> <tr> <td>user.waveset.resources</td> <td>Individuelle Ressourcenzuweisung</td> <td><input type="checkbox"/></td> </tr> </tbody> </table>							Attributname	Formular-Anzeigename	Bearbeitbar	user.waveset.accountId	Konto-ID	<input type="checkbox"/>	user.waveset.roles	Rolle	<input type="checkbox"/>	user.waveset.organization	Organisation	<input type="checkbox"/>	user.global.email	E-Mail-Adresse	<input type="checkbox"/>	user.waveset.resources	Individuelle Ressourcenzuweisung	<input type="checkbox"/>
Attributname	Formular-Anzeigename	Bearbeitbar																						
user.waveset.accountId	Konto-ID	<input type="checkbox"/>																						
user.waveset.roles	Rolle	<input type="checkbox"/>																						
user.waveset.organization	Organisation	<input type="checkbox"/>																						
user.global.email	E-Mail-Adresse	<input type="checkbox"/>																						
user.waveset.resources	Individuelle Ressourcenzuweisung	<input type="checkbox"/>																						

Fertig

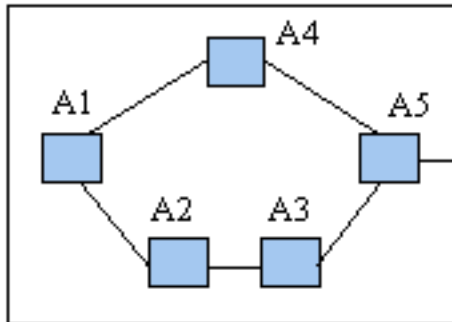
Workflow Reference Model

Components & Interfaces

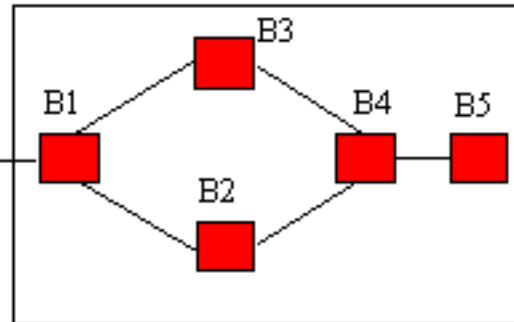


Workflow Interoperability

Process A

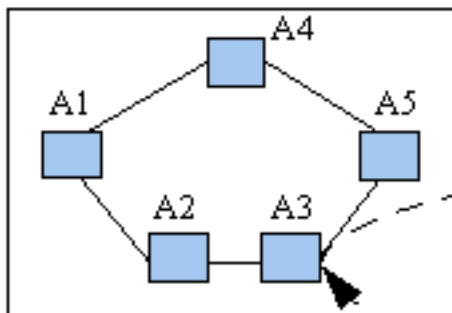


Process B

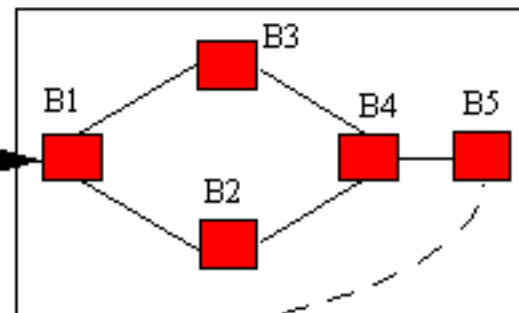


Chained Services Model

Process A



Process B

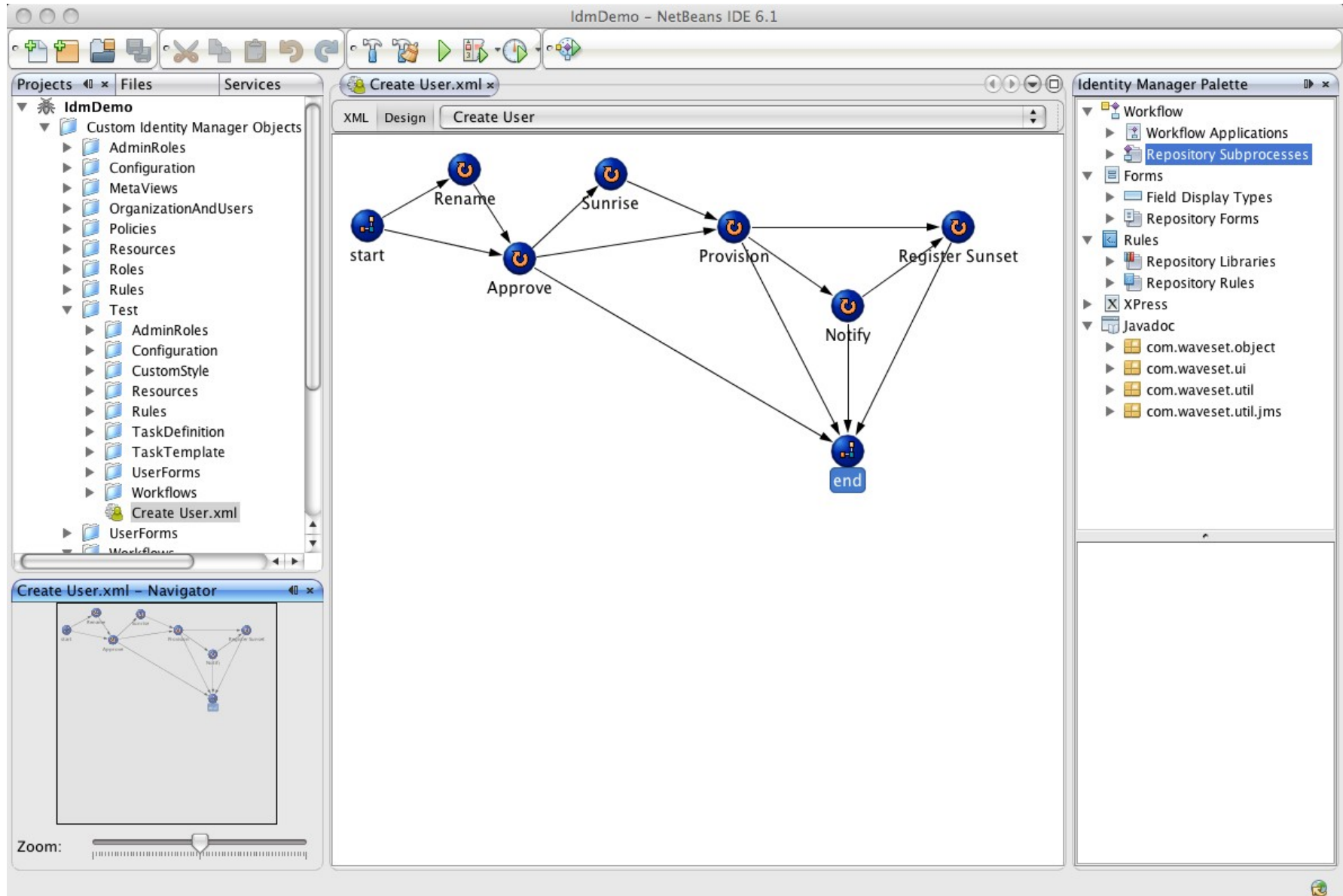


Domain of Workflow Service A

Domain of Workflow Service B

Hierarchical (Nested Subprocesses)

Netbeans IDE



Vorteile IDE

- Spezifischer Teil als PlugIn
- Allgemein bekannt (OpenSource)
- Syntax Highlighting und Code Completion
- Ein Tool für die Entwicklung (Java und Workflow)
- Build in Sandbox und verschiedenen Umgebungen
- Source Level Debugger
- Profiler integriert
- CVS (oder Subversion) integriert

IDE PlugIn

- Versionen für Eclipse und Netbeans



- Dokumentation und Download
 - > <https://identitymanageride.dev.java.net/servlets/ProjectDocumentList>

NetBeans

Developer.com: Product of the year 2009

<http://www.developer.com/java/other/article.php/3795991>

- **Development Tool:** NetBeans Platform
- **Development Utilities:** NetBeans Profiler
- **Wireless/Mobile:** NetBeans Mobility Pack for Connected Device Configuration (CDC) 5.5
- **Java Tool:** NetBeans IDE
- **Open Source:** NetBeans

“It is worth noting that in the past Sun has been able to dominate many categories, but it took multiple products to achieve that distinction. This year one product, NetBeans, dominated the categories by winning five out of twelve.”

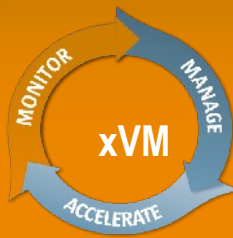


Agenda

- Was ist Workflow und braucht man das?
- Die Workflow Engine im Sun Identity Manager
- **Sun Identity Management Portfolio Überblick**
- Q & A

Sun Software: ein breites Portfolio

- Multi-Plattform und Open Source



solaris
opensolaris

Rechenzentrum



Datenbank



Identity Manager Desktop

Software Infrastructure



Java / Client / Mobility



Sun
Developer
Network



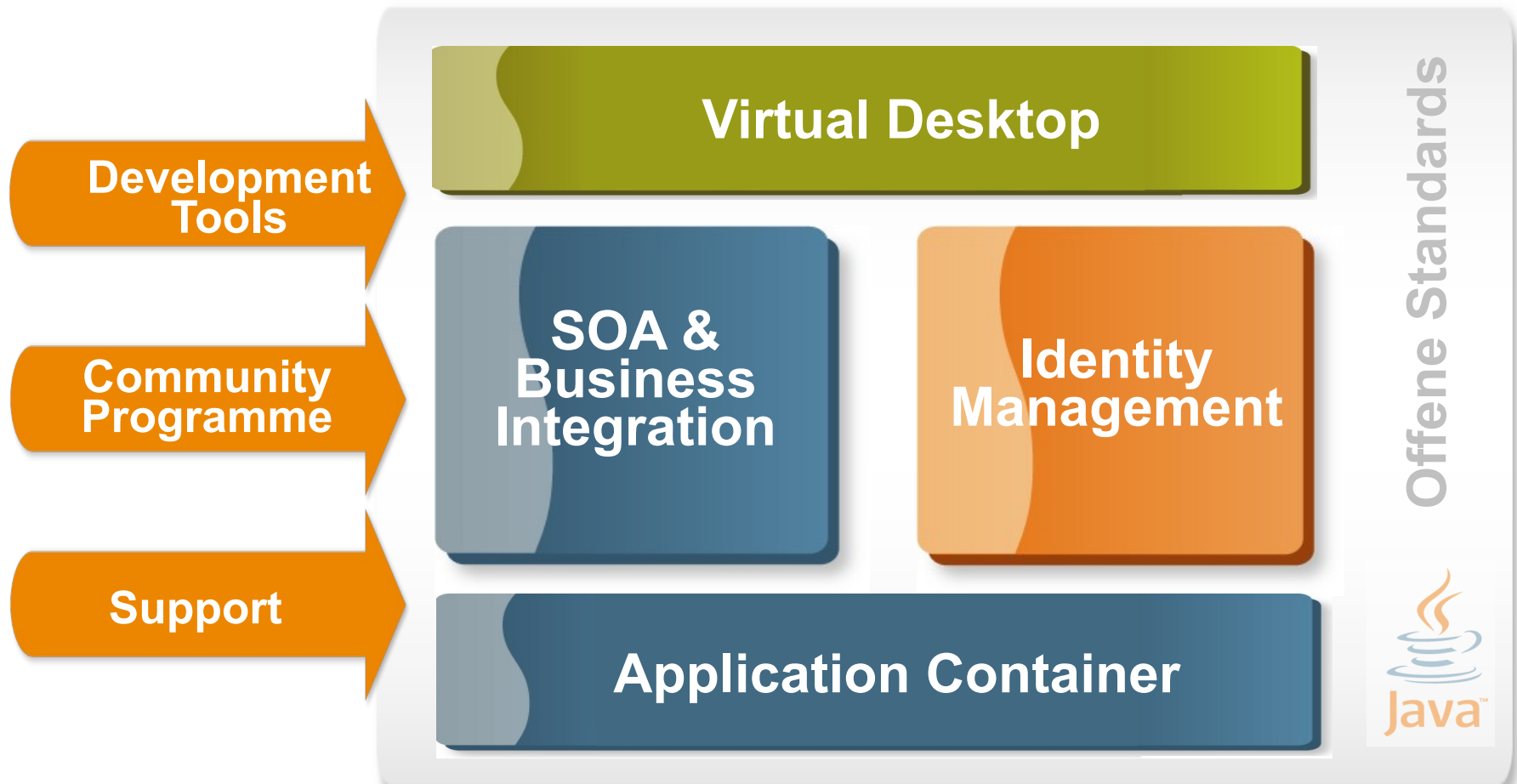
Sun
Studio

Developer



Cloud Computing

Sun Software Portfolio - Software Infrastructure



Identity Management Portfolio



OpenSSO Enterprise

- Web single sign-on
- Account linking
- Global log-out
- Federation Services



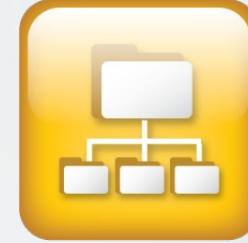
DesktopSSO

- Partner Solution



Identity Manager

- User Provisioning
- Password Management
- Identity Synchronization
- Identity Auditing



OpenDS Enterprise

- Directory services
- Virtual directory services
- Security/failover services
- AD synch services



Compliance Manager

- Compliance Check
- Access Certification
- Enterprise SoD Enforcement
- Identity Compliance



Role Manager

- Role Engineering
- Role Maintenance
- Role Certification

3+ Milliarden Identitäten Verwaltet

Sun Identity Solution

Enterprise Role Management Role Life-cycle Management

- Role and Rule Discovery
- Data Rich Identity Warehouse

Identity Compliance Compliance Checks

- Periodic Access Review
- Audit Policy
- Compliance Reporting



User Provisioning Identity Life-cycle Management

- Password Management
- Identity Synchronization
- Delegated Administration
- SoD Enforcement

Single Sign On Access Management & Federation

User Management, Identity Compliance, and Role Management

Analysteneinschätzung

Gartner

FORRESTER®

Butler Group*

- Leader in User Provisioning, Gartner 2008
- Leader in Back-End Application Integration, Gartner 2007
- Leader in Horizontal Portal Product, Gartner 2007
- Leader in Web Access Management, Gartner 2007
- Fastest Application Platform Server, SPECjAppServer, 2007
- Strong Positive in Identity, Gartner Vendor Rating 2008
- Strong Performer in Identity Management, Forrester 2008
- Strong Performer in Application Server Platforms, Forrester 2007
- Visionary in Application Infrastructure, Gartner 2007
- Visionary in Composite Applications, Gartner 2007
- Visionary in New Service-Oriented Business Applications, Gartner '07
- Visionary in Application Enterprise Servers, Gartner 2008
- Visionary in Data Integration Tools, Gartner 2008

Produkteinschätzungen der Analysten bestätigen die Strategie

Kundenliste (Auszug)


Weltweit mehr als 2000 Kunden, u.a.



Gap
Banana Republic
Old Navy



Warum Identity Management mit Sun?

- 
- Starke, erfolgreiche Kundenbasis mit den meisten Installationen
 - Erfahrene System Integratoren
 - Marktführende Produktsuite
 - Verpflichtung zu Heterogenität und Offenheit
 - Sun bietet die Komplettlösung: Software, Server, Storage und Dienstleistung

> Battle Tested by Fortune 100



Fragen?

georg.voell@sun.com





Dieses Dokument wurde mit StarOffice erzeugt -- ein Softwareprodukt von Sun Microsystems.

Lesen Sie mehr unter:
<http://www.sun.de/staroffice/>