



OpenIDM: die Übersicht Für alle, die eine sichere und effiziente Benutzerkontenverwaltung brauchen!

OpenIDM

Seit die meisten Firmen ihre Geschäftsabläufe über Computer abwickeln, sehen sich diese vermehrt mit den Schwierigkeiten einer effizienten und sicheren Benutzerverwaltung konfrontiert. Dabei geht es um Themen wie Lebenszyklen der virtuellen Identitäten wie z.B. simples Erzeugen von Benutzereinträgen und deren späterer Löschung aber auch um komplexe Vorgänge wie das automatische Reagieren auf eine Veränderungen der Situation eines Benutzers.

OpenIDM hilft den Unternehmen die Lebenszyklen der virtuellen Identitäten automatisch und in Echtzeit zu pflegen. Dabei werden auch Themen wie Benutzerberechtigungen in logischen wie auch physikalischen Anwendungen (z.B. Zugang zu Gebäuden) behandelt.

OpenIDM ist eine voll ausgebaute Lösung für Identitätsmanagement und Compliance, die die nötigen Möglichkeiten für die Umsetzung der verschiedensten Szenarien bereitstellt. Ein Beispiel hierfür ist das Überwachen von Änderungen an Benutzerkonten für die Wirtschaftsprüfung.

Der Einsatz von OpenIDM wird sowohl die Produktivität und Sicherheit Ihrer Benutzerverwaltung erhöhen als auch die verbundenen Kosten senken. Um diese Ziele zu erreichen unterstützt OpenIDM die Verwaltung der Benutzerkonten, Benutzerinformationen und Zugangsberechtigungen zu den schützenswerten Einrichtungen Ihrer Firma.

Der Lebenszyklus einer Identität beinhaltet die Etablierung und Veränderung von Benutzerkonten aber auch deren Terminierung.

Prozesse die im englischen gerne als on-boarding/off-boarding und identity life-cycle bezeichnet werden.

Wenn ein neues Konto angelegt werden soll, sollen dabei nach Möglichkeit sofort die entsprechenden Zugangsberechtigungen, die der künftige Mitarbeiter für die Erledigung seiner Aufgaben laut Positionsbeschreibung braucht, mit angelegt werden. Die Pflege des Kontos beinhaltet das Aktualisieren von Benutzerdaten und die Nachjustierung der Berechtigungen je nach Bedarf und unter Betrachtung eventueller Berechtigungskonflikte. Die Terminierung des Kontos beinhaltet die Löschung oder das Deaktivieren, in jedem Fall aber die Löschung der vorhandenen Berechtigungen in Übereinstimmung mit den vorgegebenen Bestimmungen.

OpenIDM ist 100 % quelloffene Software. Die Entwicklung erfolgt durch ForgeRock und weiterer Quellen, der so genannten Community. OpenIDM basiert auf einer modernen OSGi Architektur und einer RESTful API die sich leicht sowohl mit hoch modernen als auch mit traditionellen Technologien verbinden lässt. Die modulare Architektur bietet den Kunden ein Höchstmaß an Flexibilität um das Produkt an die verschiedensten Anforderungen und Geschäftsprozesse anpassen zu können. Dies reicht von relativ einfach anzupassenden Arbeitsabläufen (Stichwort Business Workflow) bis zur Anpassung auf Ebene von JavaScript und Java, falls nötig. Ein wichtiges Ziel von OpenIDM ist es einerseits entwicklerfreundlich, einfach zu installieren und modular zu sein, andererseits aber auch alle Anforderungen moderner Geschäftsprozesse zu befriedigen.

Funktionalität

Datenbank und flexibles Datenmodell

OpenIDM verfügt über ein flexibles, objektbasiertes Datenmodell, verwirklicht durch ein integriertes DBMS-Speichersystem, das gleichzeitig auf Skalierung, Sicherheit, Einfachheit und Transaktion optimiert ist. Es gibt weder strikt vordefinierte Objekte noch Relationen. Daher kann das Modell nahezu grenzenlos um Objekttypen, Attribute und Relationen erweitert werden. Eine externe Datenbank ist nicht nötig.

Eingebettet Architektur

Diese Struktur hilft die Implementierungs- und Testphase zu verkürzen, was sich positiv auf die Stabilität der angepassten Lösungen auswirkt.

Passwordmanagement

OpenIDM bietet die Möglichkeit für einer unternehmensweite Passwortverwaltung inklusive einer unternehmensweit einheitlichen Passwortrichtlinie. Weitere Möglichkeiten sind Passwortsynchronisation von ForgeRock OpenDJ und Microsoft Active Directory, Passwortreset und sichere Passwortübermittlung.

Selbstständiges Erkennen externer Änderungen

Hier bietet OpenDJ eine gut skalierende Methode um neue, gelöschte oder geänderte Benutzerkonten auf externen Systemen zu finden und automatisch abzugleichen. In diesem Fall liegt es in der Verantwortlichkeit von OpenIDM die Änderungen zu erkennen.

Logbasiertes Erkennen externer Änderungen

Falls das externe System Unterstützung für das Erkennen von Änderungen liefert (Stichwort Changelog, Timestamp oder Change Sequence Number) kann OpenIDM diese Information nutzen um die Änderungen effektiver zu prozessieren. Hier kann das System Änderungsmaßnahmen in nahezu Echtzeit vornehmen. Z.B. kann das

Einrichten eines neuen Benutzerkontos im HR-System dazu führen, dass wenige Minuten später ein entsprechendes Konto in OpenIDM und allen weiteren benötigten Systemen inklusive individuell benötigter Berechtigungen eingerichtet wird.

Flexibles Regelwerk mit JavaScript

Für die Umsetzung individueller Regelwerke steht die weit verbreitete Sprache JavaScript in OpenIDM zur Verfügung. Z.B. können Datensätze aus externen Systemen nahezu beliebig transformiert und bearbeitet werde bevor sie in weitere Systeme geschrieben werden.

Audit und Report

Alle wichtigen Aktionen, manuelle oder automatische, werden von OpenIDM erfasst und zur späteren Verwendung, z.B im Rahmen einer Wirtschaftsprüfung aufbewahrt. Auf diese Daten kann über vorgefertigte oder individuell erstellte Reports zugegriffen werden. Für die Weiterverarbeitung in externen Systemen können die Ereignisse auch direkt an eine externe Datenbank weitergeleitet werden.

Workflow

Jede Aktion in OpenIDM löst einen Prozess aus, der entweder über einen so genannten Workflow oder durch den direkten Aufruf von eigenen Java oder JavaScriptmethoden individualisiert werden kann.

Anbindung externer Ressourcen

Zur Anbindung externer Ressourcen verwendet OpenIDM Konnektoren des ebenfalls quelloffenen Identity Connector Frameworks, OpenICF. Bereits jetzt existiert eine breite Menge individueller Konnektoren zu den gängigen Datenbanksystemen, Betriebssystemen und Verzeichnisdiensten. OpenICF kann einfach durch die Erstellung weiterer Konnektoren an nahezu beliebige externe Systeme angebunden werden.

Wichtigste Eigenschaften

Eigenschaft	Beschreibung
Kontenadministration	Erstellen, Lesen, Ändern und Pflegen von Benutzerkonten
Kontenerkennung	Erkennen von neuen oder gelöschten Konten auf externen Systemen
Synchronisation	Synchronisierung von Benutzerdaten über Systemgrenzen
Passwordmanagement	Unterstützung von Passwortregeln in der gesamten IT-Infrastruktur
Workflow	Die Möglichkeit OpenIDM Prozesse individuell zu gestalten
Log, Audit und Report	Alle relevanten Aktionen in OpenIDM werden zur späteren Verwendung in einem Report mitgeschrieben.

Resourcekonnektoren

Konnektor	Beschreibung	
Active Directory	Auf ADSI basierender Konnektor zu Microsoft AD	OpenIDM Werdegang OpenIDM ist zu 100 % quelloffene Software. Das Projekt wurde von ForgeRock gestartet und unterstützt und von einer breiten Entwicklergemeinde weiterentwickelt. Die Architektur basiert auf OSGi und der RESTful API und lässt sich gut mit modernen oder traditionellen Technologien verbinden. Die modulare Architektur bietet den Kunden ein Höchstmaß an Flexibilität um das Produkt an die verschiedensten Anforderungen und Geschäftsprozesse anpassen zu können. Dies reicht von relativ einfach anzupassenden Arbeitsabläufen (Stichwort Business Workflow) bis zur Anpassung auf Ebene von JavaScript und Java. Ein wichtiges Ziel von OpenIDM ist einerseits eine hohe Entwicklerfreundlichkeit, einfach Installation und Modularität, andererseits aber auch die Möglichkeit alle Anforderungen individueller Geschäftsprozesse zu befriedigen.
CA Unidesk	Zur Pflege von Benutzerkonten im CA Unidesk HelpDesk System.	
Database Table	Konnektor zu Datenbank Tabellen mit fester Funktionalität	
DB2	Zur Pflege von IBM DB2 Systemusern	
Exchange	Management von Mailkonten in Microsoft Exchange	
Flat File Active Sync	Erkennung von Änderungen durch CVS Dateien	
Google Apps	Verwaltung von Google Apps Konten	
LDAP	Zur Verwaltung von Benutzern und Gruppen auf LDAPv3 kompatiblen Verzeichnisdiensten	
MS SQL User	Zur Pflege von MS SQL Systemusern	
MySQLUser	Zur Pflege von MySQL Systemusern	
Oracle	Zur Pflege von Oracle Systemusern	
RACF	Zur Pflege von Konten in IBM RACF	
Scripted SQL	SQL basierter Konnektor zu Datenbank Servern	
Solaris	Account- und Gruppenadministration in Solaris	
SPMLv2	Zur Pflege von Konten in SPML v2 kompatiblen Systemen	
Tivoli Access Manager	Zur Pflege in IBM Tivoli Access Manager	
VMS	Account Administration in HP OpenVMS.	ForgeRock ForgeRock ist eine global operierende Firma mit festen Standpunkten in UK, USA und Norwegen. ForgeRock hat sich der kontinuierlichen und innovativen Weiterentwicklung von Software im Bereich Interaktion, Identitätsverwaltung und Integration, I3 Plattform genannt, verpflichtet. In diesem Rahmen bietet ForgeRock seinen Kunden und Partner professionell bediente Supportverträgen, Training und Zugang zu einer aktiven Entwicklergemeinschaft.
Web TimeSheet	Zur Pflege in Web TimeSheet	Weitere Informationen unter: http://www.forgerock.com .
XML File	Integration und Pflege von Konten mit XML-Dateien	Kontakt ✓ Matthias Tristl : ForgeRock AS ✓ t: +47 47707662 ✓ e: matthias.tristl@forgerock.com ✓ w: forgerock.com

This document is provided for information purposes only and the contents hereof are subject to change without notice. This document is provided "as-is" and not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. ForgeRock, OpenAM, OpenDJ and OpenIDM are trademarks of ForgeRock AS. All other product or service names are trademarks of their respective companies.