

Whitepaper

IAM Migrationsstrategie



Technologien Lösungen Trends Erfahrung

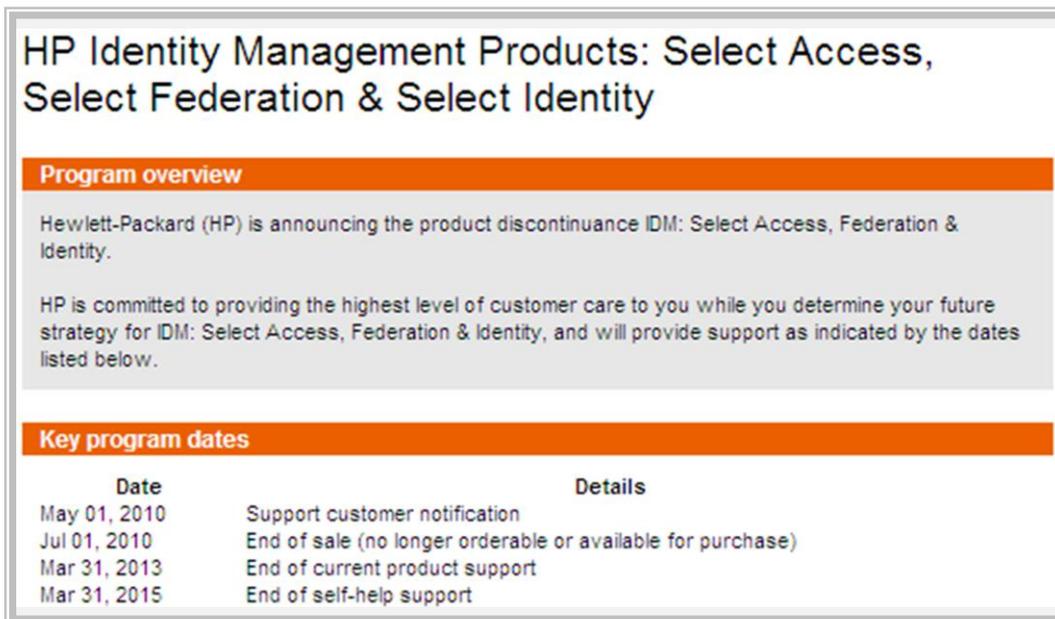
Lebt Ihr Identity Management noch oder stirbt es schon?

Marktturbulenzen sorgen für unfreiwilliges Ende von Identity & Access Management¹ Lösungen.

Anwender von Identity & Access Management (IAM) Lösungen leiden in letzter Zeit verstärkt unter den oft fatalen Folgen eines sich rasch verändernden IAM-Anbieter-Marktes, oft verbunden mit einer unfreiwilligen Verkürzung der Lebensdauer ihrer Identity & Access Management Lösungen. Anwenderunternehmen, die sich oft erst vor kurzem aus Sicherheitsgründen für die Softwarelösung eines Global Players entschieden hatten, stehen heute bereits vor der Frage: **Wie geht es weiter?**

CIO's zahlreicher Unternehmen mussten jüngst gleich mehrfach schmerzlich erfahren, dass der große Name eines IT-Unternehmens nicht automatisch die Garantie für eine möglichst lange Lebensdauer des Software-Produktes ist, das sie gekauft haben.

- Ob beispielsweise **Hewlett Packard** aus Gründen der Rentabilität, Produkt- oder Unternehmens-Philosophie das IAM aus seinem Portfolio streicht und den Support dafür einstellt:



HP Identity Management Products: Select Access, Select Federation & Select Identity

Program overview

Hewlett-Packard (HP) is announcing the product discontinuance IDM: Select Access, Federation & Identity.

HP is committed to providing the highest level of customer care to you while you determine your future strategy for IDM: Select Access, Federation & Identity, and will provide support as indicated by the dates listed below.

Key program dates

Date	Details
May 01, 2010	Support customer notification
Jul 01, 2010	End of sale (no longer orderable or available for purchase)
Mar 31, 2013	End of current product support
Mar 31, 2015	End of self-help support

Abb. 1: Information über die Einstellung des Supports für die „IDM“ Lösung auf der HP Webseite [Quelle: http://support.openview.hp.com/encore/identity_mgmt.jsp]

¹ Die Begriffe „Identity & Access Management (IAM)“ „Identity Management (IdM)“ werden hier synonym gebraucht

- ... oder der US-amerikanische Computer-Hardware-Gigant **DELL Inc.** im September 2012 die **Quest Software Inc.** aufkauft - kaum dass die Anwender der **ActiveEntry** IAM-Lösung der Berliner **Völcker Informatik AG** gerade erst die Übernahme ihres Software Lieferanten durch QUEST im Juli 2010 und den Übergang zum **Quest One Identity Manager** ‚verdaut‘ hatten:

“...ROUND ROCK, Texas and ALISO VIEJO, Calif., July 2, 2012 – Dell and Quest Software today announced they have entered into a definitive agreement for Dell to acquire Quest...”

Abb. 2: Information über die Übernahme der Quest Software durch DELL auf der DELL Webseite
Quelle: [<http://www.quest.com/news-release/dell-to-acquire-quest-software-072012-817737.aspx>]

- ... sei es, dass mit der **Übernahme Novells durch Attachmate** im April 2011 die Roadmap für NOVELL Produkte neu geschrieben wurde und die NOVELL-Produkte *Identity Manager, Access Manager, Compliance Manager, Secure Login, Sentinel* und *Privileged User Management* mit **NetIQ** einen neuen Vornamen erhielten:

“... Attachmate acquired Novell in 2011. Since its acquisition, the Novell brand has had its products split distributed into four different companies:



... The identity, security and compliance products from Novell are now under the NetIQ brand name... The products that are rebranded include Novell Compliance Management Platform, Novell Privileged User Manager, Novell Sentinel, Novell Secure Login, Novell Access Manager (Novell iChain) and Novell Identity Manager...”

Abb. 3: Auszug aus Partnermitteilung Action Identity und der Attachmate Website

Quellen: <http://www.actionidentity.com/netiq>
<http://www.attachmate.com/Press/PressReleases/openletter.html>
<http://www.attachmategroup.com/de-de/news/the-attachmate-group-completes-acquisition-of-novell.html>
<http://blogs.gartner.com/earl-perkins/2011/05/19/attachmate-novell-and-the-future-for-novell-iam-customers/>

- ... oder dass nach der Übernahme **SUNs** durch **ORACLE** im Jahr 2010 aus dem früheren **SUN IDENTITY MANAGER** das Produkt **ORACLE WAVESET** wurde, das auf nahezu verlorenem Posten gegen den **ORACLE IDENTITY MANAGER (OIM)** und gegen seinen drohenden Untergang im Oracle Portfolio kämpft:

Old Name	New Name
Sun Directory Server Enterprise Edition	Oracle Directory Server Enterprise Edition
Sun OpenDS	Oracle Unified Directory
Sun Role Manager	Oracle Identity Analytics
Sun Identity Manager	Oracle Waveset
Sun OpenSSO Enterprise	Oracle OpenSSO

*“... Oracle Corporation continues to maintain this product, but with **Oracle Identity Manager as the strategic product**. Sun Identity Manager was renamed to Oracle Waveset to avoid confusion, which is actually a reversion to the original name from before Sun acquired Waveset Technologies. Waveset also incorporates connectors and adapters for interfacing to heterogenous systems, similar in principle to those included in Oracle Identity Manager...”*

Abb 4: Wikipedia-Eintrag über Oracle
Quelle: http://en.wikipedia.org/wiki/Oracle_Identity_Management

Kaum wurde im Sommer 2009 bekannt, dass SUN Microsystems von Oracle übernommen werden soll, begannen SUN-Kunden bereits um die Zukunft ihrer Investitionen in ihre bestehenden SUN IdM-Installationen zu fürchten. Mit Recht! Nach erfolgter Übernahme und vielen Monaten der Ungewissheit stand mit der Präsentation der Oracle Produkt Roadmap 2010 fest: **Dies ist der Anfang vom Ende des SUN IdM**. Oracle erklärt seinen Identity Manager (OIM) als Kernprodukt in diesem Bereich und plant, künftig nur noch die nötigsten SUN IdM-Updates auszuliefern und den Support für das Sun-Produkt 2014 gänzlich einzustellen.

Die Konsequenzen

Fakt ist, dass diese Unternehmens-Akquisitionen und Portfolio-Bereinigungen auf dem Rücken der Anwender ausgetragen werden!

Das Dilemma, in dem sich die HP-, NOVELL-, VÖLCKER- und SUN – Kunden seitdem befinden: Sie haben erhebliche Mittel in die Lizenzen, Implementierung und Softwarepflege der Lösung gesteckt, um nun von vorn beginnen zu müssen. Sie sehen sich von der technologischen Weiterentwicklung ihrer Lösung abgeschnitten, der Support wird über kurz oder lang eingestellt.

Darüber hinaus befinden sie sich plötzlich in einer Zusammenarbeit mit einem Partner, den sie sich nicht ausgesucht haben und der in vielen Bereichen ‚anders tickt‘. Oft verliert der Kunde den direkten Draht und seitherige Ansprechpartner, die Kommunikation ist schwieriger oder umständlicher, Preise von Dienstleistungen werden angehoben...

„Abreißen und neu aufbauen“ - das bedeutet meist nochmals beträchtliche Kosten für Lizenzen, Integration und Betrieb.

Die Alternativen

Sind die betroffenen IAM-Kunden zwar einerseits der Entwicklung des Anbietermarktes machtlos ausgeliefert, so besitzen sie nun andererseits die Macht der Wahl – der Wahl einer Lösung, die ihre Anforderungen und Erwartungen optimal erfüllt (wenn nicht gar übersteigt) und dies zu fairen Lizenz-, Migrations- und Betriebskosten. Der Punkt ist erreicht, an dem die Karten neu gemischt und neue Wege eingeschlagen werden können, um das Beste aus der Situation zu machen. Denn ein UPGRADE auf das Produkt des AUFKÄUFERS ist nicht die einzige, beste, zukunftsfähigste und vor allem nicht kostengünstigste Option für sie. Es gibt ALTERNATIVEN.

Betrachtet man z.B. den SUN → Oracle Fall, gibt es vordergründig mehrere brauchbare Optionen. Die von Oracle naturgemäß empfohlene bzw. forcierte *'Identity Management Upgrade Strategy'* scheint SUN-Kunden insbesondere aus Kostengründen nicht automatisch zu überzeugen. Sie erfordert eine erhebliche Investition, da die Architektur der beiden Produkte gravierend unterschiedlich und der Übergang somit mehr als aufwendig ist.

Denkbar wäre auch, auf der seitherigen SUN Plattform zu bleiben und sich - wenigstens für ein paar weitere Jahre - des Supports der SUN-Lösung durch einen der darauf spezialisierten Dienstleister zu bedienen, was technologisch gesehen jedoch kurzfristig einem Stillstand und längerfristig einem Rückschritt gleichkommt.

Die erfolversprechendste Strategie ist sicher ein – wenn auch schmerzhafter - klarer Schnitt und der Blick nach vorn. IAM-Kunden können dem unfreiwilligen AUS ihrer Lösung eine positive Seite abgewinnen, indem sie jetzt die Gelegenheit ergreifen, ihre alte Technologie über Bord zu werfen und sie kostengünstig durch eine innovative Lösung der nächsten Generation zu ersetzen. Denn Tatsache ist eben auch, dass die Entwicklung seit Einführung der erwähnten IAM-Produkte in großen Schritten vorangegangen ist.

Die Lösung

Dieser Plan, das Blatt zu wenden, gelingt, wenn Anbieter und Produkt folgende Voraussetzungen erfüllen:

- Der IAM-Anbieter verfügt über ein durchdachtes Migrationskonzept für einen geordneten, schrittweisen und unterbrechungsfreien Übergang.
- Er besitzt ferner eine langjährige Security und IAM-Expertise, IAM-Projektkenntnisse sowie idealerweise entsprechende Erfahrungen aus einem bereits realisierten Migrationsprojekt.
- Er bietet neben Kauf (Lizenzierung) und Miete seiner Software weitere Betriebsarten wie Managed IAM Services und SaaS bzw. Security-as-a-Service sowie die Möglichkeit des Wechsels zwischen diesen Betriebsarten. Um Kosten und Risiken zu minimieren, sollte er einen Proof of Concept in einer „Secured Private Cloud“ – bei größeren Unternehmen und Konzernen verbunden mit einem nachfolgenden Umstieg auf eine On-Site-Installation – realisieren können.
- Das neue Produkt ist kein 1:1 Ersatz des Vorgänger-Produkts sondern stellt eine erweiterte Produkt Suite von Identity & Access Komponenten mit größerer Funktionsbreite bereit, mit der ein höherer Automatisierungsgrad erzielt und weiterer Nutzen generiert werden kann.
Beispiele: Berechtigungsverwaltung in dynamischen Team- bzw. Projektstrukturen oder temporären Pools von Nutzern (Pool Ressourcen Management, beispielsweise für Filespaces, Mailgruppen, SharePoint), Administration von Mitarbeiterrechten als Primary, Shadow und Delegierte User, Privileged User Management, Mobile Device Management, Integriertes Single Sign-On mit gesicherter Authentifikation etc.)
- Es deckt alle benötigten Funktionen weitestgehend in einer STANDARD-Ausführung ab, fügt sich in gegebene Geschäftsprozesse ein und erfüllt die vorliegenden Revisionsanforderungen.
- Kundenspezifische Anpassungen sollten minimiert bzw. ganz vermieden werden können.
- Das Produkt ergänzt das bestehende IAM um einen leistungsfähigen Business Layer mit vordefinierten und anpassungsfähigen Prozessen sowie einem praxiserprobten Rollenreferenzmodell und intelligenten Regelwerk, das die Abläufe den Richtlinien des Anwenders entsprechend steuert, und sorgt so für eine effizientere Nutzer- und Berechtigungsverwaltung.

Das mittelständische Softwareunternehmen **iSM – Institut für System-Management GmbH** – ist seit mehr als 14 Jahren am Markt. Seine Identity & Access Management Lösung **bi-Cube**® ist erfolgreich bei namhaften international aufgestellten Kunden aus unterschiedlichen Branchen im Einsatz und erfüllt die genannten Voraussetzungen für ein erfolgreiches Migrationsprojekt.

„Identity & Access Management ist unsere Kernkompetenz und täglich Brot. Deshalb können sich unsere Kunden auch 100% auf uns verlassen“ argumentiert Barbara Müller Philipps Sohn, Geschäftsführerin Marketing & Sales des iSM.

Das iSM hat als Hersteller der IAM-Lösung **bi-Cube**® ein Migrationsverfahren erarbeitet, das es ermöglicht, relativ aufwands- und kostenneutral von anderen Tools wie dem Sun Identity Manager auf **bi-Cube**® zu migrieren. Das standardisierte Vorgehens- bzw. Migrationsmodell ermöglicht dabei einen reibungsfreien Umstieg und bedeutet gleichzeitig ein Upgrade des Funktionsumfangs der eingesetzten Lösung.

Das Consultingteam des Herstellers unterstützt die Migration und bietet somit Sicherheit und Qualität eines Produkts „made in Germany“. Ohne Backdoor-Bedenken und ohne den Einsatz von Implementierungspartnern eines ausländischen Lieferanten wird ein unkomplizierter und sicherer Ablauf gewährleistet.

Mit **bi-Cube**[®] kann mindestens **80% Automatisierung** der User- und Berechtigungsverwaltung in Verbindung mit einer umfassenden Erfüllung aller Compliance-Anforderungen erreicht werden.

Allgemeine Informationen zum aktuellen Migrationsprojekt **SUN IdM** → **bi-Cube**[®] IAM bei der **TOGNUM AG** (MTU), Friedrichshafen, sind zu finden auf www.secu-sys.de. Für detaillierte Auskünfte steht ihnen das Team und Management des iSM jederzeit zur Verfügung.

Ein Umstieg auf **bi-Cube**[®] wird 2013 durch attraktive Migrationskonditionen unterstützt.



Autor:

Barbara Müller Philipps Sohn
Geschäftsführerin Marketing & Vertrieb
iSM – Institut für System-Management GmbH

ism@secu-sys.de
<http://secu-sys.de>

Tel. 0381/ 37 57 30
Fax 0381/37 57 329



Pressekontakt:

Jessica Brach
Marketing & PR
iSM – Institut für System-Management GmbH

jessica.brach@secu-sys.de
<http://secu-sys.de>

Tel. 0381/ 37 57 30
Fax 0381/37 57 329