

Statement of the Month

Düsseldorf, im Februar 2006

Federation ist Vertrauenssache: Unternehmensübergreifendes Identity Management

Endlich ist es geschafft. Durch die Einführung einer Identity Management (IdM) Lösung hat die Hersteller AG die Kosten der Benutzerverwaltung gesenkt, Richtlinien, Standards und Vorschriften erfüllt, und den Benutzerkomfort durch Self-Services erheblich gesteigert. Es wäre Zeit sich zurückzulehnen, wenn da nicht ein nagendes Restproblem wäre. Externe Mitarbeiter von Partnern und Zulieferern verursachen einen großen Anteil des verbleibenden Administrationsaufwands. Dies ist umso ärgerlicher, da diese Benutzer bereits in den IdM-Systemen ihrer eigenen Unternehmen verwaltet werden und nun auf teilweise komplizierten Wegen in die bestehende IdM Infrastruktur integriert werden müssen. Jörg Senekowitsch, Senior Architect, und Harald Meyer, Principal Architect bei Novell, untersuchen, wie sich dieser Aufwand verringern lässt:

Es gibt tatsächlich eine einfache Lösung - die sogenannte „Federation“ von Benutzern. Im Grunde genommen bedeutet dies nichts weiter, als dass man der Verwaltung der Benutzer beim Partner selbst vertraut und zur Authentisierung eines Benutzers auf die beim Partner verwalteten und gespeicherten Daten zurückgreift.

Ein Beispiel verdeutlicht die Zusammenhänge: Max Mustermann arbeitet bei der Zuliefer AG. Seine Aufgabe besteht unter anderem darin, über das Zuliefererportal die Zulieferung von Komponenten zu steuern. Bisher musste Max dazu im Portal oder in der IdM-Infrastruktur der Hersteller AG registriert werden. Bei der Registrierung erhielt Max einen Benutzernamen und ein Passwort von der Hersteller AG, mit dem er sich von nun an am Portal authentisieren kann. Hat Max sein Passwort mal vergessen, kann er sich bei der Hotline der Hersteller AG melden und ein neues Passwort erhalten. Zu diesem Zweck sind weitere Details über Max bei der Hersteller AG hinterlegt, damit er sich gegenüber dem Hotline-Mitarbeiter legitimieren kann. So steht einer zufriedenen Zusammenarbeit zwischen Max als Vertreter der Zuliefer AG und der Hersteller AG nichts mehr im Wege.

Schwieriger wird die Situation, wenn Max für eine längere Zeit ausfällt. Dann muss ein Kollege von Max aus der Zuliefer AG aushelfen. Ist dieser Kollege bisher nicht bei der Hersteller AG registriert, erfolgt wieder ein Registrierungsprozess und die damit verbundene Vergabe von Benutzernamen und Passwort. Aber der Kollege vertritt Max nur für eine gewisse Zeit. Wenn Max wieder die Aufgaben der Zuliefer AG übernimmt, muss die Autorisierung des Kollegen für den Zugriff auf die Daten der Hersteller AG entfernt werden. Auch der Zugang von Max muss zeitnah beendet werden, sollte Max die Zuliefer AG einmal verlassen. Dazu müssen entsprechende Verwaltungsprozesse bei der Hersteller AG angestoßen werden. Auslöser sind in diesem Fall externe Ereignisse bei der Zuliefer AG, von denen die Hersteller AG unter Umständen zu spät erfährt.

Noch schlechter stellt sich die Situation aus der Sicht der Zuliefer AG dar. Diese muss nicht nur intern Max verwalten, sondern auch alle seine Zugänge zu den Systemen der Kunden der Zuliefer AG. Da Max nicht nur für die Hersteller AG zuständig ist, sondern auch für zehn weitere Unternehmen, bedeutet dies einen erheblichen Aufwand. Hin und wieder teilen sich Kollegen von Max die Arbeit, die Mitarbeiter erhalten neue Zuständigkeiten oder es ergeben sich andere Veränderungen. Entstehen dabei Auswirkungen auf die Zugangsberechtigung zu den Systemen

der Kunden, muss dies den Herstellern unverzüglich angezeigt werden.

Um diese für alle beteiligten Unternehmen aufwändigen Prozesse in den Griff zu bekommen, haben die Hersteller AG und die Zuliefer AG sich auf eine Federation-Lösung geeinigt. Dabei verwaltet die Zuliefer AG den Zugang zur Hersteller AG eigenverantwortlich. Max benötigt nun keinerlei Benutzernamen und Passwort mehr, um sich bei der Hersteller AG anzumelden. Einzig seine gültige Anmeldung bei der Zuliefer AG und eine von der Zuliefer AG erteilte Berechtigung ist ausreichend, um Zugang zum System der Hersteller AG zu erhalten. Da die Zuliefer AG ähnliche Verträge mit den anderen Herstellern geschlossen hat, entsteht auch dort kein Verwaltungsaufwand mehr. Eine Vertretung von Max kann einfach innerhalb der Zuliefer AG durch Vergabe einer entsprechenden Berechtigung an eine andere Person erfolgen. Ein Ausscheiden von Max führt aufgrund der entzogenen Zugangsberechtigung zu den Systemen der Zuliefer AG automatisch auch zu einem Entzug aller Zugangsberechtigungen zu den Kunden-Systemen.

Wenn Max sich nun am Mitarbeiterportal der Zuliefer AG anmeldet, werden ihm entsprechend seiner jeweiligen Berechtigungen Links zu den verschiedenen Herstellerportalen angeboten. Ein Klick auf einen solchen Link erzeugt in einer IdM-Komponente der Zuliefer AG eine Bestätigung, dass Max Mustermann tatsächlich am Portal der Zuliefer AG angemeldet ist und fügt der Bestätigung weitere Informationen hinzu: beispielsweise eine Signatur, den Namen desjenigen, der die Bestätigung ausgestellt hat, den Namen von Max, seine Rolle in der Zuliefer AG bezüglich der Interaktion mit der Hersteller AG, den Zeitpunkt seiner Anmeldung und ein Ablaufdatum der Bestätigung. Dann wird diese Bestätigung zum späteren Abruf unter einem eindeutigen Schlüssel abgelegt. Dieser Schlüssel wird nun dem Link zum Portal der Hersteller AG hinzugefügt. Die IdM-Infrastruktur der Hersteller AG extrahiert den Schlüssel und kontaktiert auf einem separaten Kanal die Zuliefer AG um die zugehörige Bestätigung abzuholen. Die Bestätigung ist eine Art digitale Urkunde, deren Korrektheit wird geprüft und anhand der von der Zuliefer AG übermittelten Informationen fällt die Entscheidung, den Benutzer (hier Max) entsprechend seiner von der Zuliefer AG zugeteilten Rolle zur Interaktion mit den Systemen der Hersteller AG zuzulassen.

Alle Parteien, Hersteller AG, Zuliefer AG und Anwender profitieren von diesem Vorgehen. Die Hersteller AG muss sich, nachdem die Beziehung zu den Authentisierungssystemen bei der Zuliefer AG hergestellt sind, nie mehr um die Verwaltung von Benutzern aus der Zuliefer AG beschäftigen. Die Zulassung erfolgt ausschließlich aufgrund der von der Zuliefer AG verwalteten Daten und der bei der Hersteller AG hinterlegten Sicherheitsrichtlinien.

Die Zuliefer AG muss nach der einmaligen Installation und Konfiguration der Federation-Partner, keinerlei weitere Verwaltungsaufgaben jenseits der bestehenden Aufgaben durchführen. Zu den bestehenden Aufgaben zählen die Vergabe von Berechtigungen - etwa der Zugang zu Hersteller-Systemen - sowie die Verwaltung von Passwörtern. Diese Aufgaben fallen ohnehin in jedem Fall an. Eine wichtige Vereinfachung und damit verbunden Kosteneinsparung geschieht durch den Wegfall der Benachrichtigungen an die Hersteller, da beispielsweise bei einem Entzug der Zugangsberechtigung zu den Systemen der Zuliefer AG auch automatisch die Zugänge zu den Hersteller-Systemen entzogen werden.

Max Mustermann muss sich nun nicht mehr für jeden Hersteller den Benutzernamen und das Passwort merken. Seine Authentisierung bei der Zuliefer AG reicht aus, um Zugang zu den Systemen der Hersteller zu erhalten, sofern er die notwendigen Berechtigungen innerhalb der Zuliefer AG besitzt.

Folgende Voraussetzungen müssen erfüllt sein. Der Austausch der Benutzer- und Berechtigungsinformationen zwischen den IdM-Systemen der verschiedenen Unternehmen erfolgt über ein Standard-Internetprotokoll, die so genannte Security Assertion Markup Language (SAML). Dieses Protokoll ist seit kurzem in der Version 2.0 freigegeben und erste Produkte, die die Übertragung der Informationen steuern, stehen zur Verfügung. Frühere Produkte, basierend auf den älteren Standards SAML 1.0 und SAML 1.1, hatten mit erheblichen

Interoperationsproblemen zu kämpfen, so dass der Einsatz über Unternehmensgrenzen hinweg schwierig war.

Eine weitere Voraussetzung ist, dass im vorliegenden Fall die Hersteller AG bereit ist, den Authentisierungssystemen und Prozessen der Zuliefer AG zu vertrauen. Dies ist jedoch mehr ein vertragliches und organisatorisches als ein technisches Problem. Für Situationen, in denen die Hersteller AG der Authentisierung beim Partner nicht vertraut, steht seit kurzem auch das so genannte „federate Provisioning“ zur Verfügung, bei der die Verwaltung der Benutzer wie Max immer noch bei der Zuliefer AG liegt, die Daten von Max aber physikalisch im IdM-System der Hersteller AG gespeichert werden.

Das Beispiel zeigt: Mit Identitätsmanagement lassen sich Partner enger anbinden, Prozesse effizienter gestalten und der Zutritt zu unterschiedlichen Systemen für Benutzer vereinfachen - ohne Einbußen bei der Sicherheit.

Über Novell

Novell, Inc. (Nasdaq: NOVL) ist seit mehr als 20 Jahren im Markt und entwickelt und vertreibt „Software for the Open Enterprise“. Mit offener, Standard-basierter Software unterstützt Novell mehr als 50.000 Unternehmen und Institutionen in 43 Ländern dabei, ihre IT-Umgebungen einfacher und sicherer zu gestalten und zu verwalten sowie besser zu integrieren. Novell Kunden erhalten die Kontrolle über ihre IT-Infrastruktur zurück und senken die Kosten. Dabei werden sie weltweit von 5.200 Novell Mitarbeitern, 5.000 Partnern und technischen Support Centers unterstützt.

Seit 1986 ist Novell durch die Novell GmbH in Düsseldorf auch auf dem deutschen Markt vertreten. Von diesem Standort aus werden Vertrieb und Marketing für Deutschland, Österreich und die Schweiz koordiniert - Niederlassungen befinden sich in Berlin, Frankfurt, München, Nürnberg, Wien, Zürich und Genf. Weitere, ausführliche Informationen über Novell Lösungen, Produkte und Services stehen im Internet zur Verfügung unter www.novell.com oder www.novell.de.

Weitere Informationen:

Ulrike Beringer
Manager Public Relations
Novell GmbH
Phone +49 (0) 89 206 002 118
eMail: <mailto:uberinger@novell.com>
Internet: <http://www.novell.com>

Novell Presseservice
vibrio Kommunikationsmanagement Dr. Kausch GmbH
Markus Pflugbeil
Senior PR Consultant
Phone +49 (0) 89 32 15 18 62
Fax +49 (0) 89 3 21 51 77
eMail: <mailto:markus.pflugbeil@vibrio.de>
Internet <http://www.vibrio.de>