



© Julien Eichinger - Fotolia.com

## FÖDERIERTES IDENTITÄTS- MANAGEMENT

### Unternehmensübergreifend sichere Wertschöpfungsketten

Kooperationen über Unternehmensgrenzen hinweg gewinnen durch sich verändernde Wertschöpfungsstrukturen zunehmend an Bedeutung. Beinahe »normal« ist es inzwischen die eigenen IT-Systeme gegenüber Externen zu öffnen. IT-Lösungen wie Cloud-Services oder Kooperationsportale ermöglichen es, unternehmensübergreifende Geschäftsprozesse effizient zu gestalten und somit grundsätzlich die Kosten signifikant zu senken. Gleichzeitig ist dabei jedoch zu gewährleisten, dass nur jeweils autorisierten Akteuren Zugriff auf sensible Ressourcen gewährt wird. Innerhalb eines Unternehmens wird dies durch ein zentralisiertes Identitätsmanagement realisiert. Sollen jedoch auch externe Partner in das Identitätsmanagement eingebunden werden, entstehen zahlreiche neue Herausforderungen.

Die Komplexität des Identitätsmanagements und damit die Sicherheitsanforderungen sowie der Administrationsaufwand steigen deutlich an – etwa durch die Erstellung und Pflege unternehmensübergreifend redundanter Benutzerkonten. Es droht die Gefahr, dass die mittels Kooperation erzielten Effizienzgewinne durch Sicherheitslücken und deutlich gesteigerten Ressourcenbedarf teuer erkaufte werden. Als Ausweg bietet sich ein **Föderiertes Identitätsmanagement (FidM)** an.

### Fraunhofer-Institut für Arbeits- wirtschaft und Organisation IAO

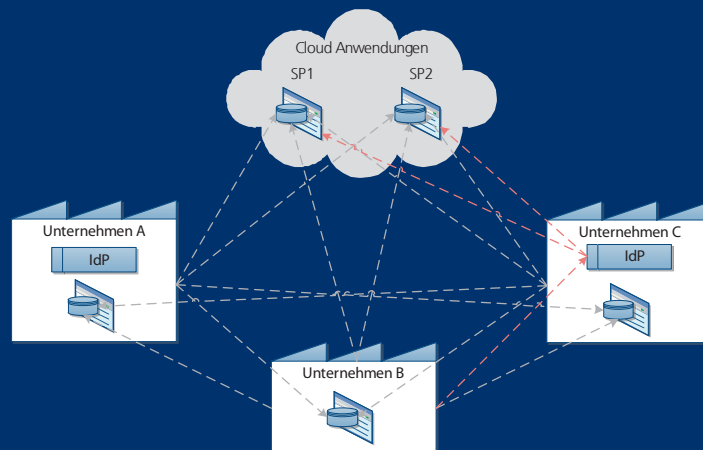
Nobelstraße 12  
70569 Stuttgart

### Ansprechpartner

Dr. Michael Kubach  
Telefon +49 711 970-2428  
michael.kubach@iao.fraunhofer.de

Dr. Heiko Roßnagel  
Telefon +49 711 970-2145  
heiko.rossnagel@iao.fraunhofer.de

[www.swm.iao.fraunhofer.de](http://www.swm.iao.fraunhofer.de)  
[www.ikt.iao.fraunhofer.de](http://www.ikt.iao.fraunhofer.de)



## Ihre Vorteile durch Föderiertes Identitätsmanagement

Die Grundfunktionen eines Föderierten Identitätsmanagements decken sich mit denjenigen eines herkömmlichen Identitätsmanagements (IdM). Dieses ist die Basis für einen sicheren Zugriff auf IT-Ressourcen, indem es alle Maßnahmen umfasst, um Benutzer von IT-Systemen zu erkennen und ihnen die aufgabenspezifisch notwendigen Zugriffe zu ermöglichen. Föderiertes Identitätsmanagement ermöglicht das verteilte IdM in administrativ unabhängigen Organisationen.

Verantwortlich für die Authentifizierung und die digitale Identität eines Benutzers ist der Identity Provider, etwa seine Heim- oder eine dritte Organisation. Die Daten jedes einzelnen Mitarbeiters müssen somit nicht mehr zentral erfasst und gepflegt werden.

Mittels Föderiertem Identitätsmanagement lassen sich dann wirtschaftliche Vorteile mit gesteigertem Komfort und Sicherheitslevel sowohl für das Einzelunternehmen als auch für seine Kooperationspartner verbinden. Beispielsweise lässt sich ein Single-Sign-On für unterschiedliche Kooperationspartner bei verwandten, aber eigenständigen IT-Ressourcen mit geringerem Aufwand für die Registrierung und Deregistrierung von Benutzern betreiben. Verlässt ein Mitarbeiter das Unternehmen oder wechselt das Projekt, so muss dies nur bei dem für ihn zuständigen Identity-Provider vermerkt werden. Automatisch wird dann der Zugriff auf alle IT-Ressourcen im Unternehmensverbund angepasst. Die Identität der

Benutzer ist im gesamten Verbund stets aktuell und muss nicht bei jedem einzelnen Service-Provider gepflegt werden.

Der einzelne Benutzer schließlich kann mittels eines Token, etwa der firmeneigenen PKI-Karte, auf alle IT-Ressourcen zugreifen: So müssen die Unternehmen nicht zahlreiche Tokens – Keygeneratoren, unterschiedliche PKI-Karten und Passwörter – für jeden einzelnen Dienst vorhalten. Sicherheitsrisiken, beispielsweise durch auf Zetteln am Bildschirm notierte Passwörter, werden entschärft.

## Herausforderungen eines föderierten Identitätsmanagement

Erfahrungen aus bereits erfolgreich abgeschlossenen Projekten zum Föderierten Identitätsmanagement zeigen, dass die praktischen Herausforderungen weniger in der technischen Umsetzung als in der Überwindung organisatorischer Hürden bestehen. Schließlich sind die Sicherheitspolicies aus unterschiedlichen, rechtlich eigenständigen Organisationen zu berücksichtigen, hinter welchen auch jeweils spezifische Interessen von Akteuren wie den Fach-, IT- und Rechtsabteilungen stehen.

Aufgrund unserer Erfahrung in vorangegangenen Projekten können wir neutral und fundiert Lösungen erarbeiten. Darüber hinaus bieten wir Unterstützung, indem wir Sie durch die Vielzahl existierender technischer Lösungsalternativen navigieren.

## Wir bieten Ihnen

- Workshops mit Ihren Mitarbeitern, um ein gemeinsames Verständnis für die Problemfelder zu schaffen und die Anwender an der Lösungsentwicklung zu beteiligen
- Anforderungsanalyse und Auswahl einer maßgeschneiderten FIDM-Lösung unter Abwägung von Sicherheits- wie Wirtschaftlichkeitsaspekten
- Wissenschaftliche Expertise sowie Neutralität aufgrund unserer Anbieterunabhängigkeit und langjährigen Erfahrung in Forschungs- und Praxisprojekten