

Benutzerzentriertes ID-Management für den neuen Personalausweis



Tamara Höglér



Sneschana Sobol



Johannes Feulner



Christian Henrich



Oliver Winzenried

Neues SaaS4KMU-Forschungsprojekt +++ Sicheres Identitäts-Management in der Cloud für Privatanwender +++ Zusammenschluss regionaler IT-Unternehmen und Forschungseinrichtungen.

In den letzten Jahren hat Cloud Computing das IT-Bild grundlegend verändert: Der Trend geht weg von lokal installierten Applikationen hin zu über das Internet verfügbaren, skalierbaren Diensten. Die Verbreitung von Cloud-Computing-Lösungen ist aber nicht so weit vorangeschritten wie erwartet. Anbieter von Diensten im Internet fordern von ihren Kunden eine Vielzahl persönlicher Daten. Dies führt dazu, dass Kunden immer mehr persönliche Daten an immer mehr Anbieter geben und dabei auch immer mehr Zugangsinformationen verwalten müssen. Jetzt haben sich vier Partner des SaaS4KMU-Netzwerks zusammengeschlossen, um sich diesen Herausforderungen zu stellen und dabei die Sicherheit des neuen Personalausweises (nPA) einzubinden. In dem vom Bundesministerium für Wirtschaft und Technologie geförderten Projekt „Identitäts-Management durch den neuen Personalausweis (nPA) und OpenID“ entwickeln die vier Partner aus der TechnologieRegion Karlsruhe eine Lösung, bei der ein zentraler Server als Identitätsmanager fungiert und die verschiedenen Identitäten für Internetdienste verwaltet. Der Identitätsmanager übernimmt auch Aufgaben wie Alterskontrolle und Nachweis der Geschäftsfähigkeit, ohne dass zusätzliche Daten wie das Geburtsdatum weitergegeben werden. Die geplante Lösung soll Verbindlichkeit, Sicherheit und Benutzerfreundlichkeit kombinieren und damit den eCommerce unterstützen. Dabei wird sichergestellt, dass die Datenhoheit beim Kunden bleibt.

Um die Dienstleistungen und Anwendungen in der Cloud zu nutzen, müssen Anwender eine Vielzahl personenbezogener Daten beim jeweiligen Provider angeben. Mit der Zunahme der diversen Identitäten einer einzelnen Person im Netz steigt jedoch der Aufwand, verstreute, meist redundante Identitäten einschließlich dazugehöriger Passwörter zu verwalten. Zusätzliche Sicherheitsbedenken werden oft damit begründet, dass die – teilweise personenbezogenen – Daten nicht mehr der vollständigen Kontrolle des Anwenders unterliegen. Alle diese Faktoren können die Ausbreitung des Cloud Computing hemmen.

Ein Ansatz, dieser Problematik zu begegnen, ist die Entwicklung einer *Cloud-Computing-Lösung für das Identitäts-Management auf Basis von OpenID*. Diese soll die Ausgabe von virtuellen Identitäten auf Basis der eID-Funktion des nPA für beliebige Identitäts-Provider erlauben.

Eine derartige, innovative Lösung prototypisch zu entwickeln, ist das gemeinsame Ziel der SaaS4KMU-Partner CAS Software AG, fun communications GmbH, FZI Forschungszentrum Informatik sowie WIBU-SYSTEMS AG. SaaS4KMU ist ein Subnetzwerk des CyberForum e.V., in dem sich innovative Unternehmen aus der Region und zwei Partner aus Forschung und Lehre vernetzen, um ihre Kompetenzen im Bereich Cloud Computing zu bündeln und Mittelständlern flexible, durchgängige SaaS-Lösungen anzubieten.



Quelle: WIBU-SYSTEMS AG

Mit der geplanten Lösung werden neben der *anwenderseitigen Identitätenverwaltung* auch *anbieterseitige Herausforderungen* des Identitäts-Managements (ID-Management) handhabbar, beispielsweise der Altersnachweis und der Nachweis der Geschäftsfähigkeit bei Diensten und Leistungen, die einer Altersbeschränkung unterliegen.

Die Motivation für den Einsatz des nPA für ein benutzerzentriertes ID-Management ist vielfältig. So ist der nPA aufgrund seiner zu erwartenden Verbreitung ein geeignetes und gleichzeitig sicheres Mittel, um den genannten Herausforderungen gerecht zu werden. Der große Nutzen in der Weiterentwicklung und der Kombination des nPA mit benutzerzentrierten Ansätzen ergibt sich aus der Synergie der technologischen Ansätze: Der nPA profitiert von der Möglichkeit, seine bewusst eingeführten Beschränkungen hinsichtlich der hoheitlich darauf bereitgestellten Anwenderdaten zu erweitern. Das geht durch die offenen Ansätze der benutzerzentrierten Verfahren nahezu unbegrenzt, jedoch innerhalb der vorgegebenen Datenschutzrichtlinien. Umgekehrt profitieren die benutzerzentrierten Identitätsverfahren vom hohen, staatlich abgesicherten Sicherheitsniveau des nPA.

Im eCommerce-Markt wird nach wie vor nach einem Konzept gesucht, das Sicherheit, Verbindlichkeit und Einfachheit in idealer Weise miteinander verbindet. Hier kann durch die Kombination standardisierter, offener Protokolle mit dem nPA eine direkte Zuordnung der Identität einer Person und dessen Zusatzinformationen wie Rollen und Rechten zu einer Person gewährleistet werden. Die geplante Lösung ist besonders für Cloud-Plattformen wie CAS Open extrem wichtig, da diese Systeme die technologische Basis für Cloud-Dienste und eCommerce-Lösungen darstellen. Die wichtige Mittlerfunktion zwischen nPA und virtueller Identität im benutzerzentrierten Identitätsmanagement wird durch das CodeMeter DRM-System von WIBU-SYSTEMS gewährleistet. Die CodeMeter Schutz- und Autorisierungsfunktionen bilden die Basis für die erforderliche IT-Sicherheit bei der Verwaltung und der Nutzung der virtuellen Identitäten in einem offenen System. Eine auf Grundlage von CAS Open entwickelte Security-Middleware soll Entwicklern von Cloud-Anwendungen einen komfortablen Zugang zu den Mechanismen des benutzerzentrierten Identitätsmanagements bieten.

Um sicherzustellen, dass der Kunde die Kontrolle über seine persönlichen Daten behält, entwickeln die Projektpartner neuartige Sicherheitsmechanismen zum Schutz dieser Daten. Dazu speichert der Identitätsmanager die Kundendaten so, dass er diese nur in Kooperation mit dem Kunden entschlüsseln kann. Dies stellt sicher, dass bei einem Verlust der Kundendaten diese nicht missbraucht werden können, weil sie nicht im Klartext, sondern nur verschlüsselt vorliegen.

Die geplante Lösung ist besonders in dem immer stärker steigenden eCommerce-Markt extrem wichtig. In ihm wird nach wie vor nach einem Konzept gesucht, das Sicherheit, Verbindlichkeit und Einfachheit in idealer Weise miteinander kombiniert. Die notwendige Akzeptanz bei den Anwendern kann aber nur erreicht werden, wenn das zu entwickelnde Gesamtkonzept in jedem Detail auch als vertrauenswürdig (besonders auch von technischen Laien) anerkannt wird.

CyberForum e.V.
E-Mail: hoegler@cyberforum.de

CAS Software AG
E-Mail: sneschana.sobol@cas.de

fun communications GmbH
E-Mail: johannes.feulner@fun.de

FZI Forschungszentrum Informatik
E-Mail: henrich@fzi.de

WIBU-SYSTEMS AG
E-Mail: info@wibu.com