

## Schlagwort: OpenID

### Ausgangssituation

Bei einer immer größeren Anzahl der im Internet veröffentlichten Webseiten handelt es sich um registrierungspflichtige Angebote. Exemplarisch hierfür seien Email-Dienste, Online-Shops sowie zahlreiche Communities wie z. B. StudiVZ genannt. Die Endanwender stehen damit vor der Herausforderung, sich immer mehr Zugangsdaten merken und zahlreiche Registrierungsprozesse durchlaufen zu müssen. Unter dem Schlagwort **OpenID** diskutiert man vor diesem Hintergrund einen neuen Ansatz, um den Anwendern mit einer einzigen Nutzernamen-/Passwort-Kombination den Zugriff auf registrierungspflichtige Webseiten zu ermöglichen, so die Vision (vgl. Rehman 2007).

Grundsätzlich handelt es sich bei OpenID jedoch um kein neues Phänomen. So initiierte Yahoo bereits im Jahr 1994 ein so genanntes **Single-Sign-On-System** (SSO-System), das es den Anwendern ermöglichte, mit einem Nutzerprofil auf sämtliche Yahoo-Dienste zuzugreifen (vgl. OpenID Blog Germany, 2007). Der Unterschied zwischen OpenID und den schon länger verfügbaren SSO-Systemen besteht jedoch darin, dass die Anwender ihren OpenID-Anbieter frei wählen und auf Basis der ihnen zugewiesenen OpenID die Webangebote verschiedener Unternehmen nutzen können. Der Anwender muss insofern nur einmal seine persönlichen Daten eingeben, womit langwierige Registrierungsprozesse entfallen. Gleichzeitig ist es ihm möglich darüber zu entscheiden, welche Daten an die verschiedenen Webangebote übermittelt werden.

Spätestens seit der Gründung der OpenID Foundation im Juni 2007 – die von Unternehmen wie Google, Yahoo, AOL und Microsoft unterstützt wird – wird vor diesem Hintergrund das Thema OpenID kontrovers diskutiert; teilweise stellt man sogar Vermutungen über OpenID als möglichen neuen De-facto-Standard an (vgl. Stöcker, 2008). In diesem Beitrag soll daher hinterfragt werden, welche Chancen und Risiken aus Endanwender- und Unternehmenssicht mit OpenID einhergehen.

### Funktionsweise von OpenID

Bei OpenID handelt es sich um eine Open-Source-Lösung zum dezentralen Identitätsmanagement. Dem Endanwender wird dabei – auf Basis bestehender Internet-Technologien und kryptographischer Verfahren – ein SSO-System zur Verfügung gestellt, mit dem er Zugriff auf alle

Webangebote erhält, die diesen Standard unterstützen. Die technische Funktionsweise solcher Systeme lässt sich am einfachsten am Beispiel des Registrierungs- und Anmeldeprozesses erläutern, den die Anwender für die Generierung einer OpenID und der anschließenden Anmeldung bei einem registrierungspflichtigen Webdienst durchlaufen. Er umfasst vier Schritte:

- (1) **Generierung einer OpenID:** Zur Generierung einer OpenID ist es notwendig, sich einmalig bei einem OpenID-Anbieter zu registrieren. Solche IDs vergeben neben etablierten Anbietern wie Google oder Yahoo auch kleinere auf diesen Service spezialisierte Unternehmen wie my-openID.com, ClaimID oder Videntity. Der Anmeldeprozess als solches verläuft dabei unkompliziert. Häufig reicht es aus, seinen gewünschten Benutzernamen, ein Passwort sowie eine E-Mail Adresse anzugeben (inkl. deren Verifikation). Weiterhin ist es auch denkbar, eine eigene Webseite oder ein eigenes Blog als OpenID zu verwenden. In diesem Fall müssen lediglich einige zusätzliche Zeilen in den html-Code eingefügt werden (vgl. hierzu Pötter, 2007).
- (2) **Zuweisung der OpenID:** Im Zuge der Registrierung wird dem Endanwender eine OpenID nach dem Schema `http://username.openidanbieter.com` zugewiesen, mit deren Hilfe er sich bei allen OpenID-Konsumenten anmelden kann; unter dem Begriff OpenID-Konsument werden im folgenden alle Unternehmen subsumiert, deren Webangebote eine Anmeldung mit einer OpenID unterstützen, die bei einem OpenID-Anbieter registriert wurde. Da diese Identitäten auf dem URL-Prinzip basieren, kann die OpenID auch als Link zur eigenen Webseite fungieren.
- (3) **Login mit einer OpenID:** Mit der zugewiesenen Kombination aus Nutzernamen und Passwort ist es für den Anwender möglich, die registrierungspflichtigen Webangebote von OpenID-Konsumenten zu nutzen. Bei der erstmaligen Nutzung eines neuen Webangebots ist es lediglich notwendig, der einmaligen Nutzung der beim OpenID-Anbieter hinterlegten Daten zuzustimmen.
- (4) **Informationsabfrage und -übermittlung der Nutzerdaten:** Stimmt der Anwender der Nutzung seiner Profildaten zu, erfolgt deren Abfrage vom Server des jeweiligen OpenID-Anbieters (4a). Dabei ist es wichtig zu erwähnen, dass die Endanwender für jedes neu genutzte Produkt entscheiden können, welche Informationen sie übermitteln oder nicht. Unter Umständen wird der Anwender an dieser Stelle auch zur Eingabe weiterer Daten aufgefordert, falls diese für die Nutzung des neuen Webangebots erforderlich sind (4b). Diese Zusätzin-

formationen werden jedoch nur lokal beim jeweiligen OpenID-Konsument gespeichert und nicht beim OpenID-Anbieter (in Anlehnung an Ferreyra, 2007).

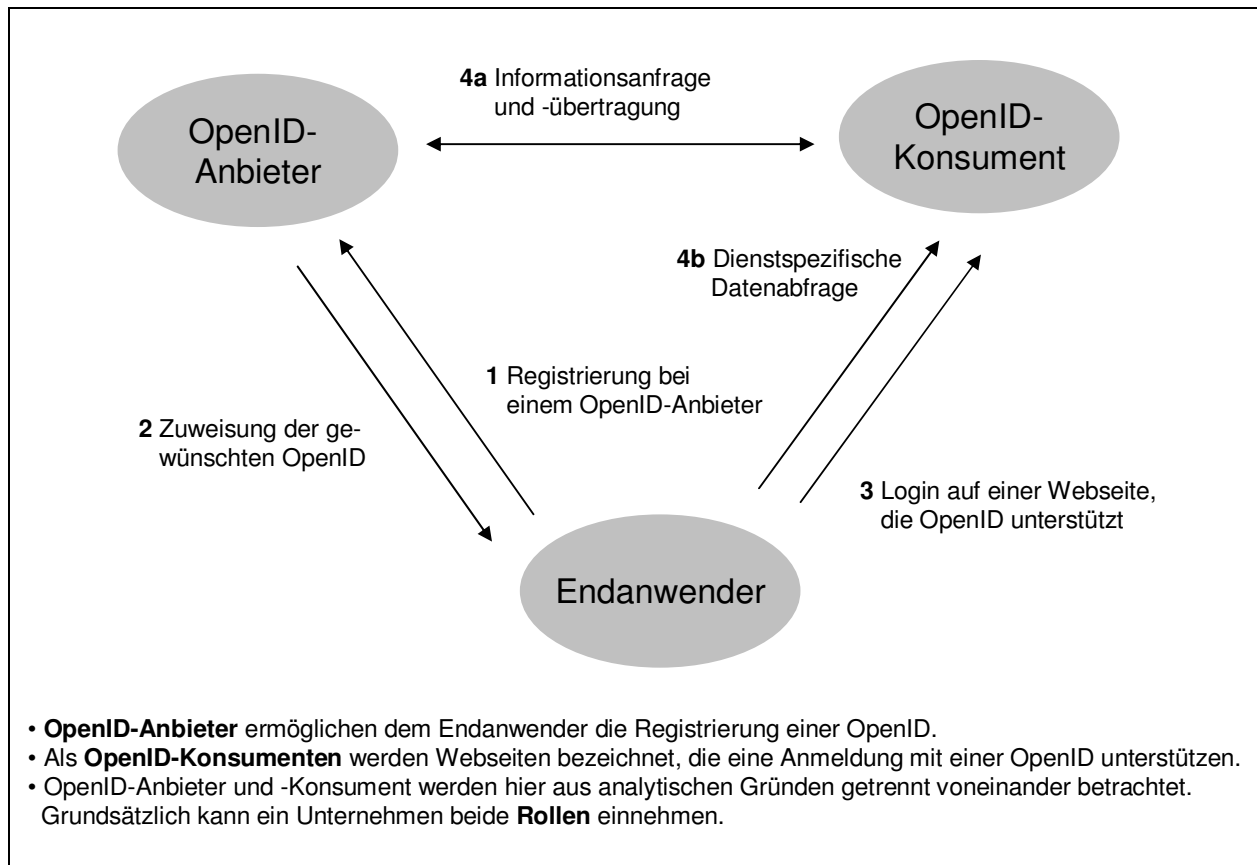


Abbildung 1: Registrierungs- und Anmeldeprozess (vgl. auch Cameron 2007 und Ferreyra 2007)

## Chancen und Risiken von OpenID aus Endanwendersicht

Die **Vorteile** des im vorangegangenen Kapitel vorgestellten SSO-System für den Endanwender liegen auf der Hand. So kann er mit einer einmaligen Registrierung Zugriff auf eine Vielzahl von Webseiten erhalten. Außerdem muss er sich lediglich eine Nutzernamen-/Passwort-Kombination merken und seine Stammdaten nur an einer Stelle pflegen; Änderungen an den Stammdaten werden automatisch an die genutzten Dienste weitergegeben. Diesen Vorteilen stehen jedoch verschiedene **Nachteile** gegenüber (vgl. auch Abb. 2):

- So besteht die Gefahr, dass die OpenID-Login Daten durch **Phishing** abgefangen werden. Ein Dritter würde damit Zugriff auf sämtliche Nutzerdaten erhalten. Es ist jedoch wichtig, an dieser Stelle zu erwähnen, dass es sich dabei um kein neues, ausschließlich OpenID betreffendes Problem handelt. Vor allem Banken, Kreditkartenunternehmen und registrierungspflichtige Internetseiten kämpfen seit jeher gegen die Angriffe von Internetkriminellen.

len. Das in Zusammenhang mit OpenID auftretende neue Problem ist lediglich der so genannte „Multiplikatoreffekt“, da die Kriminellen Zugriff auf alle vom Anwender verwendeten Webanwendungen und den damit korrespondierenden Daten erhalten (vgl. OpenID Blog Germany, 2007).

- Aus **Datenschutzgründen** ist es weiterhin als problematisch anzusehen, dass OpenID-Anbieter mit kommerzieller Ausrichtung umfangreiche Benutzerprofile erstellen und gegebenenfalls verkaufen (vgl. Pötter, 2007). Kritisch ist in diesem Zusammenhang ferner, dass es für den Auftritt als OpenID-Anbieter keiner Genehmigung durch offizielle Stellen bedarf.
- Bei nicht-kommerziellen Anbietern ist die Gefahr einer kommerziellen Verwertung der Benutzerprofile zwar geringer einzuschätzen. Allerdings stellt sich hier die Frage, inwieweit der Anbieter seinen Dienst langfristig betreiben kann. Da mit dem **Verlust einer OpenID** auch die damit generierten Daten verloren gehen, wäre darin ein ernsthaftes Problem zu sehen. Dass dieser Kritikpunkt nicht unberechtigt erscheint, zeigt auch das Beispiel der bekannten und stark frequentierten Online-Enzyklopädie Wikipedia. Sie konnte im Jahr 2006 lediglich durch Spendenaktionen gerettet werden (vgl. Kleinz, 2006).

Vorteile von OpenID aus Endanwendersicht	Nachteile von OpenID aus Endanwendersicht
Zahlreiche Webseiten sind mit einer Nutzernamen-/Passwort-Kombination nutzbar → Registrierungsaufwand entfällt	Gefahr des Datenmissbrauchs durch Phishing → Ein Dritter erhält unter Umständen Zugriff auf sämtliche Nutzerdaten
Stammdaten werden an einem Ort verwaltet	OpenID-Anbieter können umfangreiche Benutzerprofile erstellen → Gefahr des gläsernen Kunden
	Nicht-kommerzielle Anbieter können aus dem Markt ausscheiden → Verlust der mit einer OpenID korrespondierenden Nutzerdaten

Abb. 2: Vor- und Nachteile von OpenID aus Endanwendersicht

## Chancen und Risiken von OpenID aus Unternehmenssicht

Wie einleitend bereits erörtert, können Unternehmen sowohl als OpenID-Anbieter als auch als **OpenID-Konsument** auftreten. Letztgenannte erhoffen sich dadurch den Registrierungsaufwand für den Endanwender zu verringern und auf diesem Wege mehr Nutzer als in der Vergangenheit in ihre Anwendungen zu kanalisieren. Vor allem kleine Internetunternehmen und Startups implementieren vor diesem Hintergrund OpenID, zumal für sie die Rolle als OpenID-Anbieter – ne-

ben Branchengrößen wie Yahoo und Google – nicht in Betracht kommt. Ein Problem für OpenID-Konsumenten ist jedoch in der Verfügbarkeit von anonymen OpenIDs zu sehen, die man ohne eine Anmeldung bei einem OpenID-Anbieter erhalten und als Login bei allen OpenID-Konsumenten nutzen kann; der Bezug solcher IDs ist z. B. über die Seite [www.jkg.in/openid](http://www.jkg.in/openid) möglich. Die OpenID als solche wird dabei zufällig generiert, womit eine Identifikation des Endanwenders nicht mehr möglich ist. Diese Art von IDs ist aus rechtlichen Gesichtspunkten jedoch fragwürdig, da die Rückverfolgung der Urheber bei der Veröffentlichung von illegalen Inhalten nicht mehr möglich ist. Ebenso kritisch ist aus Unternehmenssicht anzumerken, dass in diesem Fall weder eine Personalisierung von Werbung noch andere verkaufsfördernde Maßnahmen (z. B. Cross-/Up-Selling) möglich sind.

**OpenID-Anbieter** können im Vergleich zu OpenID-Konsumenten sehr umfassende Benutzerprofile erstellen. So werden deren Server automatisch kontaktiert, wenn sich ein Anwender mit seiner OpenID bei einem OpenID-Konsumenten anmeldet. Speichert man diese Daten und wertet sie in Kombination mit den in den Profilen hinterlegten Daten aus, erhält man nicht nur umfangreiche Benutzerprofile, sondern auch weit reichende Informationen bezüglich des Surfverhaltens der Anwender. Da es sich dabei um sensible Daten handelt, ist eine der größten Herausforderung für OpenID-Anbieter daher darin zu sehen, die Datenintegrität zu gewährleisten und potenzielle Hackerangriffe abzuwehren. Dies kann z. B. durch die Implementierung von Smartcards erfolgen, denkbar ist aber auch der Einsatz von Zertifikaten (vgl. z. B. [www.certifi.ca](http://www.certifi.ca)) oder biometrischen Verfahren (z. B. Fingerabdrücke, Iris-Scan, Stimmerkennung, etc.) (vgl. OpenID Blog Germany, 2007).

Abschließend ist es an dieser Stelle wichtig darauf hinzuweisen, dass Unternehmen sowohl als OpenID-Anbieter als auch als OpenID-Konsument auftreten können. In der Wirtschaftspraxis bestehen zum gegenwärtigen Zeitpunkt aber noch keine namhaften Beispiele, die eine solche Doppelrolle einnehmen. So treten Unternehmen wie Yahoo und AOL zwar als OpenID-Anbieter auf. Allerdings ist es bislang nicht möglich, mit einer solchen OpenID die registrierungspflichtigen Dienste dieser Unternehmen zu nutzen, womit die Idee dieses SSO-Systems faktisch untergraben wird.

Rolle des Unternehmens	Vorteile	Nachteile
OpenID-Konsument	<p>Senkung der Hemmschwelle zur Nutzung registrierungspflichtiger Webangebote → Anwender können sich mit ihrer bestehenden OpenID anmelden</p> <p>Stammdaten des Anwenders werden beim ersten Login automatisch in die eigene Datenbank integriert</p>	<p>Anonyme OpenIDs erlauben keine Identifikation und Rückverfolgung des Endanwenders → Vermarktungsprobleme</p> <p>OpenID-Konsumenten müssen auf die Sicherheitsmaßnahmen des Anbieters vertrauen</p>
OpenID-Anbieter	<p>Generierung umfangreicher Surfprofile zur Personalisierung von Werbung und Webseiten</p>	<p>Teilweise können hohe Kosten für Sicherheitsvorkehrungen entstehen, um einen Datenmissbrauch zu verhindern</p> <p>Unklare Haftungsfragen, wenn die Daten „gehackt“ werden</p>

Abb. 3: Vor- und Nachteile von OpenID aus Unternehmenssicht

## Zukunftspotenzial von OpenID

Wenngleich in jüngerer Zeit intensiv in der Wirtschaftspresse über OpenID berichtet wurde, befindet sich diese Technologie nach wie vor in einem frühen Entwicklungsstadium. Zum gegenwärtigen Zeitpunkt unterstützen vordergründig kleine und unbekanntere Webseiten eine Anmeldung mit einer OpenID; eine genaue Aussage über deren Anzahl ist aufgrund der unterschiedlichen Angaben – sie reichen von 500 (vgl. OpenID Directory, 2008) bis zu 10.000 Webangeboten (vgl. GoogleWatchBlog, 2008) – zum jetzigen Zeitpunkt nicht möglich. Die großen Wettbewerber im Internetgeschäft wie AOL oder Yahoo treten bislang lediglich als Anbieter von OpenID auf, lassen aber keinen Zugriff auf ihre eigenen Webangebote mit solchen IDs zu. Vielmehr bedarf es weiterhin einer separaten Registrierung. Inwieweit sich OpenID vor diesem Hintergrund tatsächlich als neuer Standard durchsetzt, lässt sich zum gegenwärtigen Zeitpunkt noch nicht genau abschätzen, nicht zuletzt aufgrund der zahlreichen konkurrierenden Alternativen wie Bandit ([www.bandit-project.org](http://www.bandit-project.org)), Higgins ([www.eclipse.org/higgins](http://www.eclipse.org/higgins)), LID ([lid.netmesh.org](http://lid.netmesh.org)) oder Yadis ([yadis.org](http://yadis.org)).

Dr. Christian Maaß,  
Dipl.-Kff. Isabelle Adelt,  
Oliver Wagner  
Gütersloh

## Literaturempfehlungen

- Cameron, K. (2007): Integrating OpenID and Infocard. URL: <http://www.identityblog.com/?p=659>, abgerufen am 07.03.2008.
- Ferreya, D. (2007) OpenID for Dummies. URL: <http://webwe usability.wordpress.com/2007/02/20/openid-rocks/>, abgerufen am 07.03.2008.
- Kleinz, T. (2006): 350.000 Dollar für Wikipedia. Heise Online. URL: [www.heise.de/newsticker/meldung/print/68099](http://www.heise.de/newsticker/meldung/print/68099), abgerufen am 27.02.2008.
- OpenID Blog Germany (2007) OpenID Historie. URL: <http://openidgermany.de/openid-historie/>, abgerufen am 22.02.2008.
- Pötter, C. (2007): OpenID und der gläserne Surfer. URL: <http://www.neunetz.com/2007/04/08/openid-und-der-glaeserne-surfer/>, abgerufen am 22.02.2008.
- Rehman, R. (2007): OpenID <http://www.openidbook.com/>, abgerufen am 26.02.2008.
- Stöcker, C. (2008): IT-Giganten wollen den Web-Ausweis. Spiegel Online, <http://www.spiegel.de/netzwelt/web/0,1518,druck-533988,00.html>; abgerufen am 22.02.2008.