Web-Authentifizierung
mit
OpenID

Martin Russer

Seminar Konzepte von Betriebssystemkomponenten
Departement Informatik - Lehrstuhl 4
Universität Erlangen-Nürnberg

21. Juli 2010

Inhaltsverzeichnis

1. Einleitung

Mit dem Durchbruch des Internets entwickelte sich ein „Dschungel“ an Webseiten, den sich wohl niemand nur ansatzweise hätte vorstellen können. Ein Großteil dieser Seiten beinhaltet einen Zugang für private Nutzer, zum Beispiel bei eBay, bei einem Maildienst oder in einem sozialen Netzwerk wie Facebook oder StudiVZ. Um den Schutz der privaten Daten der Nutzer zu gewährleisten, ist es nötig, den Zugang mit einer Passwortabfrage zu versehen. Da jedoch jeder Webdienst andere Vorgaben bezüglich des Login-Namens bzw. des Login-Passworts vorschreibt, ist es nicht immer möglich, den identischen Namen und Passwort zu verwenden. Viele verschiedene Nutzernamen und Passwörter sind die Folge. Hier wird der Wunsch nach einer sog. Single-Sign-On-Lösung laut, die das Ziel verfolgt, mit einer einzigen Identität den Zugriff auf mehrere Webseiten zu ermöglichen. Diese Idee gibt es nicht erst seit Zeiten von Facebook, Twitter und Co, sondern ist bereits seit der Kommerzialisierung des Internets aktuell. Mit dem 1999 eingeführten „NET Passport“ von Microsoft oder der „Security Assertion Markup Language“ (SAML - 2001) der Liberty Alliance gibt es bereits einige Ansätze um der „Passwort-Flut“ Einhalt zu gebieten; allerdings warteten diese Verfahren vergeblich auf ihren Durchbruch. [5] Die Gründe liegen vermutlich in der zentralen Speicherung von Profildaten (Sicherheitsrisiko) oder auch an der Komplexität der Verfahren. Mit dem im Jahr 2005 eingeführten OpenID [3] existiert ein weiterer Vertreter im Bereich Single-Sign-On, der vor allem durch seine Einfachheit überzeugt und bereits heute eine Vielzahl von Benutzer verbucht. Entwickelt wurde es von Brad Fitzpatrick sowie im späteren Verlauf von David Recordon. Im Jahr 2007 wurde die OpenID Foundation gegründet, die sich als Ziel die Weiterentwicklung und die Vermarktung von OpenID gesetzt hat. Im folgenden Kapitel wird der Begriff OpenID erklärt, die Funktionsweise des Systems erläutert und neben den positiven auch die negativen Aspekte beleuchtet.

2. OpenID

2.1 „Was ist OpenID?“

OpenID ist ein dezentrales Authentifizierungssystem, dass dem Benutzer erlaubt, sich mit einer einzigen Identität, dem sog. „Identifier“, auf mehreren Webseiten und Webdiensten einzuloggen. Dezentral bedeutet in diesem Sinne, dass der „Identifier“ nicht zentral bei einem einzigen OpenID-Anbieter gespeichert sein muss. Folglich können mehrere OpenID-Anbieter existieren und verwendet werden. Die Identität besteht bei OpenID aus einer URL, wie folgendes Beispiel zeigt:

https://mueller.myopenid.com

Die Struktur eines Identifiers unterscheidet sich von Anbieter zu Anbieter, entspricht aber im Großteil der Struktur des Beispiels. Dieses ist zusammengesetzt aus dem Benutzernamen „mueller“, also dem Namen, mit dem sich ein Benutzer bei einem OpenID-Anbieter angemeldet hat und der URL des Anbieters selbst, in unserem Fall „myopenid.com“. Dieser Identifier steht somit für genau einen Benutzer, der sich damit auf allen Webseiten anmelden kann, die das Login-Verfahren über OpenID unterstützen. [1]

2.2 Komponenten

Im vorherigen Abschnitt wurden die Begriffe „Benutzer“ und „Anbieter“ bereits vorweg genommen und sollen nun noch genauer erläutert werden.
Das Konzept von OpenID besteht aus drei Komponenten, dem „End-Benutzer“, dem „Konsumenten“ und dem „OpenID-Anbieter“. Ihr Zusammenspiel ermöglicht die Realisierung von OpenID. [1]

- End-Benutzer (End-User):
  Als End-Benutzer werden Nutzer von Webseiten bezeichnet, also reale Personen. In unserem Beispiel wäre das Herr Müller, der sich auf „www.zooomr.com“, eine Seite im Internet, die OpenID unterstützt, einloggen möchte.

- Konsument (Relying-Party):
  Unter einerm Konsumenten versteht man eine Webseite oder einen Webdienst, der private Ressourcen eines End-Benutzers beinhaltet, die durch einen Login geschützt sind. Dies kann ein Blog, ein soziales Netzwerk etc. sein.
  (Beispiele: www.blogger.com, www.sourceforge.net, …)

- OpenID-Anbieter (OpenID-Provider):
  OpenID-Anbieter stellen den Dienst der Anmeldung mittels einer (einzigen) URL zur Verfügung. Ist man einmal bei einem Anbieter angemeldet, kann man diesen Account für diverse Webseiten verwenden, die OpenID unterstützen. Es gibt sowohl Anbieter, die speziell auf OpenID ausgerichtet sind, wie zum Beispiel „www.myopenid.com“, als auch Anbieter, die ihr Angebot um OpenID erweitert haben. Dies sind beispielsweise „www.google.com“ oder „www.yahoo.com“. Folglich ist es oft gar nicht nötig, ein OpenID-Konto anzulegen, da man bereits eines besitzt, ohne davon gewusst zu haben.

2.3 Funktionsweise

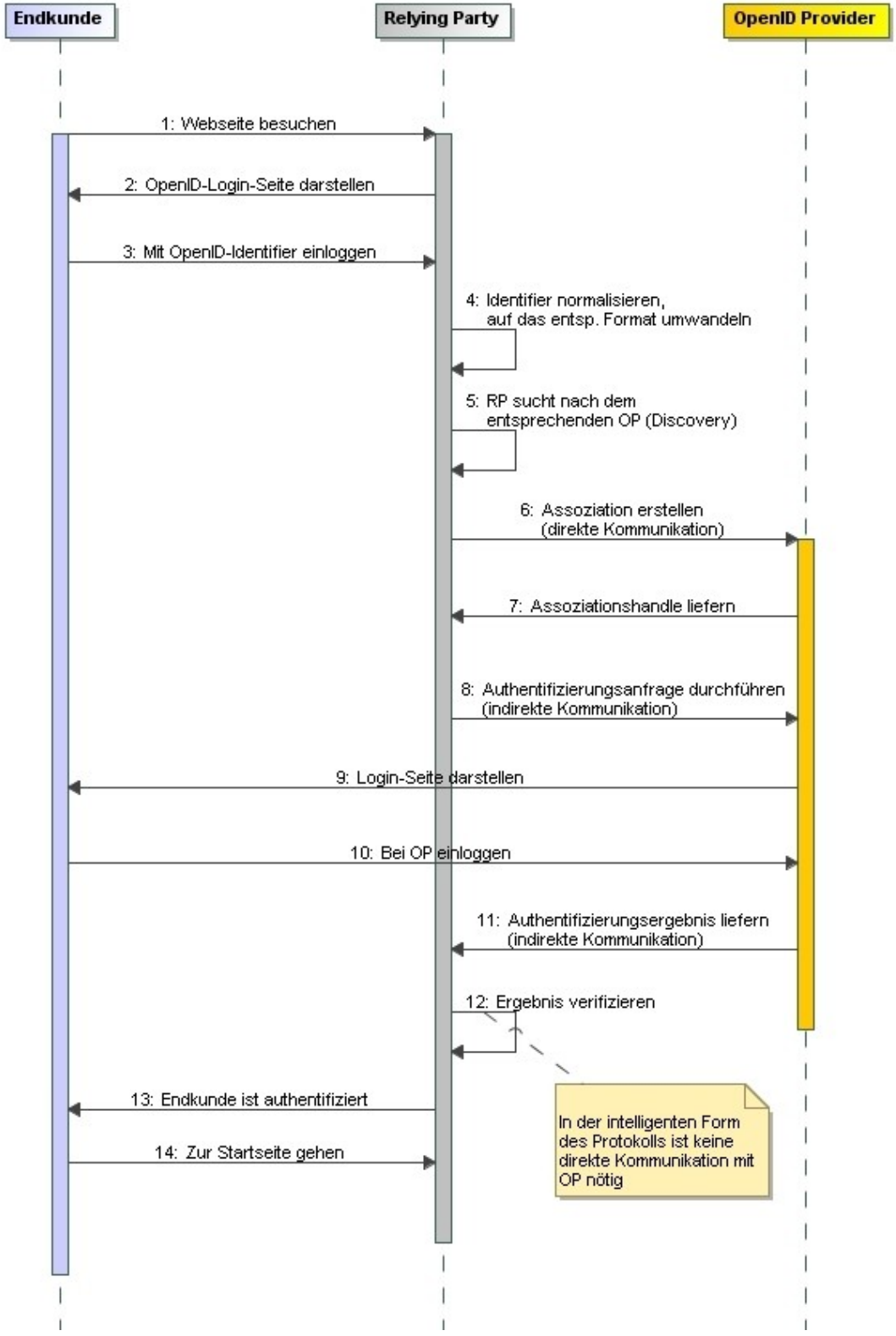

Abbildung 1: Ablauf einer Authentifizierung

Im Allgemeinen geht es um die Umleitung des Benutzer-Logins einer Webseite auf einen Anbieter, um sich dort zu authentifizieren[1]. Auf *Abb. 1* ist die Funktionsweise grafisch dargestellt. Im folgenden Beispiel wird der Ablauf anhand eines Beispiels erläutert:
Herr Müller besucht die Webseite „zooomr.com“ und möchte sich dort einloggen, um auf seine geschützten Daten zuzugreifen (1). Dazu sucht er die Login-Maske auf, die für OpenID vorgesehen ist (2), trägt seine OpenID-URL (https://mueller.myopenid.com) ein und bestätigt mit „Enter“ (3). Nun wird der Login-Vorgang gestartet. Intern wird „zooomr.com“ den Identifier normalisieren, d. h. der Nutzername „mueller“ und der Anbieter „myopenid.com“ werden extrahiert (4). Mit dem gewonnenen Anbieter-Namen versucht der Konsument eine Verbindung zum Anbieter „myopenid.com“ herzustellen, um – soweit möglich – eine Beziehung zwischen Konsument und Anbieter (eine sogenannte Assoziation) in Form eines Geheimschlüssels herzustellen (6+7). Der Schlüssel ermöglicht die Beibehaltung des Zustandes, so dass bei späterer Kommunikation kein direkter Informationsaustausch stattfinden muss. Daraufhin startet die Authentifizierungsannahme (8), in dem Herr Müller an seinem OpenID-Anbieter weitergeleitet wird (9). Dort gibt er seinen Benutzernamen und sein Passwort, welche er bei der Anmeldung beim OpenID-Anbieter gewählt hat, ein (10). Durch eine Weiterleitung (Redirect) erhält „zooomr.com“ das Ergebnis der Authentifizierung und kann überprüfen, ob Herr Müller einen korrekten Login ausgeführt hat (11). In manchen Fällen wird nochmal zusätzlich eine direkte Verbindung zum Anbieter aufgebaut, um eine Bestätigung zu erhalten (12). Andernfalls wird der Geheimschlüssel aus Schritt (6+7) verwendet, um das Authentifizierungsergebnis zu verifizieren. War das Ergebnis erfolgreich, erreicht Herr Müller seine Daten, als hätte er einen „Standard-Login“ auf „zooomr.com“ verwendet (13). [1] [6]

2.4 Integration bei einer Registrierung

Nachdem die Arbeitsweise von OpenID erläutert wurde, sollten noch einige Fragen bezüglich der Integration besprochen werden. Man stelle sich folgendes Szenario vor:

- Herr Müller hat bereits diverse Accounts bei Webdiensten, die OpenID unterstützen, möchte jedoch zukünftig diese mit Hilfe einer einzigen OpenID-Identität verwalten.

oder

- Herr Mueller besitzt bereits ein Konto bei einem OpenID-Anbieter, und möchte sich nun bei einer Webseite anmelden, die OpenID unterstützt. Kann er dort einfach seine OpenID-URL verwenden oder muss er sich zuerst „normal“ anmelden?

1 Bedeutung: sich auszuweisen, seine Identität bestätigen

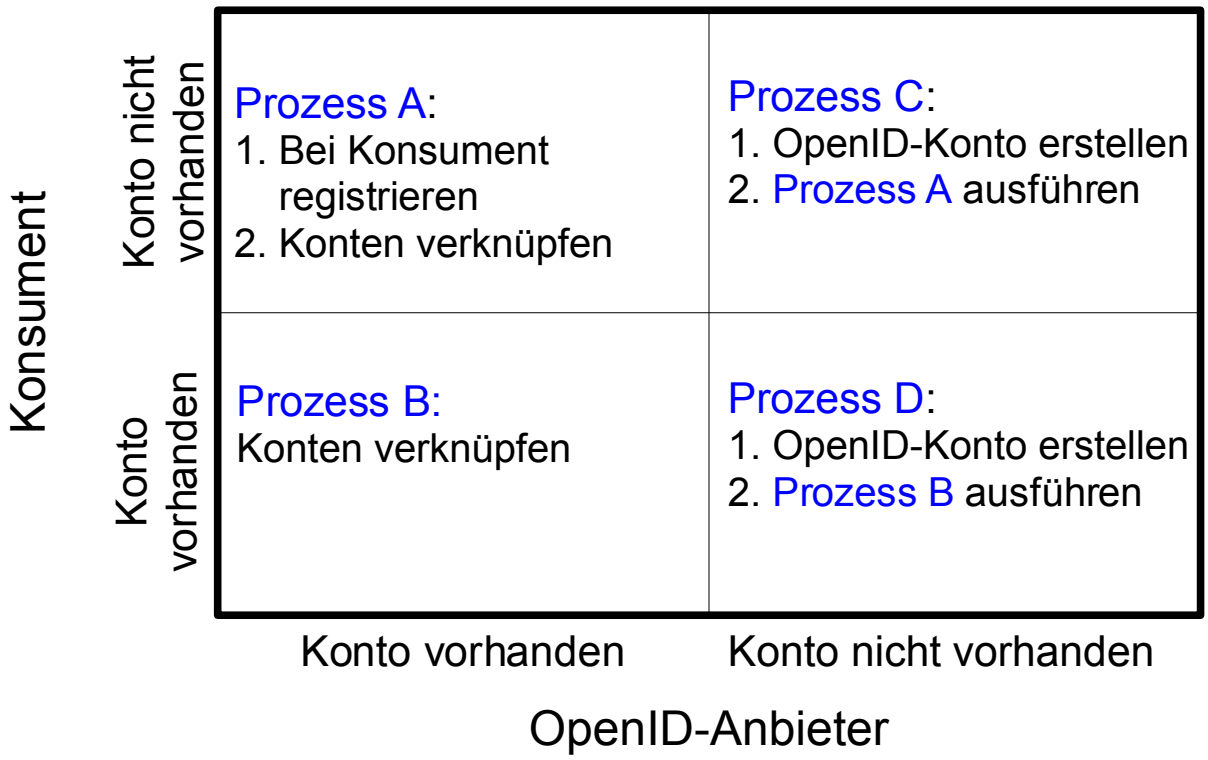

Abbildung 2: Integration bei einer Registrierung

In *Abb. 2* werden die verschiedenen Fälle der Integration dargestellt.
Sofern noch kein Konto bei einem OpenID-Anbieter vorhanden ist (Prozesse C und D), muss dieses zuerst erstellt werden. Herr Müller muss also einen Zugang beim Anbieter seiner Wahl anlegen. Ist dies geschehen, hängt der Folgeschritt davon ab, ob bereits ein Konto bei einem Konsumenten existiert oder nicht. Falls Herr Müller also bereits bei „zooomr.com“ registriert ist (Prozess B), werden die Konten miteinander verknüpft. Daraufhin kann sich Herr Müller in Zukunft mit seinem OpenID Account anmelden. Wäre nun Herr Müller noch nicht bei „zooomr.com“ angemeldet (Prozess A), kann er nun besonders komfortabel fortfahren. Es wird automatisch ein Registrierungsprozess auf zooomr.com durchgeführt, indem die Daten von Herr Müller direkt aus dem OpenID-Konto in das neue zooomr-Konto übertragen werden (OpenID Attribute Exchange). OpenID spezifiziert die erforderlichen Funktionalitäten. Diese werden im nächsten Abschnitt erklärt. [1] [3]

2.5 Spezifikationen

Spezifikationen erweitern OpenID um unterschiedliche Aspekte des Identitätsmanagements zu ermöglichen. Im Folgenden werden einige dieser Spezifikationen dargestellt:

- OpenID Assertion Quality Extension 1.0 [3]
  Diese Spezifikation überprüft die Qualität der Attribute, um sicherzustellen, dass eine

angegebene E-Mail-Adresse ein gültiges Format besitzt oder ob diese wirklich dem Benutzer gehört.

- OpenID Provider Authentication Policy Extension 1.0 (PAPE) [3]
  Mit PAPE kann eine Webseite festlegen, wie sich ein Benutzer bei einem OpenID-Anbieter zu registrieren hat, beispielsweise mit einer Absicherung gegen Phishing (siehe Abschnitt 2.4) oder dass mehrere Faktoren zur Authentifizierung verwendet müssen.

- OpenID Authentication 2.0 [3]
  Diese Spezifikation stellt den Hauptteil im Protokoll von OpenID dar und regelt den Ablauf und die Rahmenbedingungen einer Authentifikation, wie sie bereits in Abschnitt 2.3 erklärt wurde.

- OpenID Simple Registration Extension 1.0 (SReg) [3]
  SReg ist ein wichtiger Bestandteil des OpenID-Protokolls und definiert einen Austausch von Attributen zwischen Anbieter und Konsument, wodurch eine direkte Registrierung mit einem OpenID Konto ermöglicht wird. Folgende Attribute können über SReg übertragen werden:

Attribut	Bedeutung	Beispiel
openid.sreg.nickname	Benutzer-Name	„mueller“
openid.sreg.email	E-Mail-Adresse	„mueller@web.de“
openid.sreg.fullname	Richtiger Name	„Thomas Müller“
openid.sreg.dob	Geburtstag	„YYYY-MM-DD“ auch 1980-00-00 möglich
openid.sreg.gender	Geschlecht	„M“ (oder „F“)
openid.sreg.postcode	Postleitzahl, Zipcode, ...	„91052“ sollte zum Land passen, muss aber nicht
openid.sreg.country	Land	„DE“
openid.sreg.language	Sprache	„ger“ oder „deu“
openid.sreg.timezone	Zeitzone	„Europe/Berlin“

Tabelle 1: Tabelle über SReg-Attribute

- OpenID Attribute Exchange (AE) [3]
  AE kann man als Weiterentwicklung von SReg bezeichnen. Es ermöglicht ebenfalls den Austausch von Identitätsattributen, jedoch ohne Beschränkung der Attributtypen.

Folglich können unbegrenzt eigene Attribute hinzugefügt und auch erweitert werden. Weiterhin kann der Benutzer entscheiden, welche Daten an welche Website (Konsument) übermittelt werden sollen.

2.6 Sicherheit und Kritik

Die wohl häufigste Kritik, die in Zusammenhang mit OpenID erwähnt wird, ist die Anfälligkeit gegenüber Phishing. [1]

> **„Phishing** [ˈfɪʃɪŋ] werden Versuche genannt, über gefälschte WWW-Adressen an Daten eines Internet-Benutzers zu gelangen.“ [8]

Der Grund hierfür ist die Tatsache, dass eine Weiterleitung zur OpenID-Anbieter-Seite stattfindet. Eine Konsumenten-Seite kann somit den Benutzer an eine falsche Webseite weiterleiten, die äußerlich der des Anbieter entspricht. Loggt sich der Benutzer dort mit seinem Namen und Passwort ein, kann man die Informationen sehr leicht abgreifen.
Um gegen Phishing vorzugehen, gibt es verschiedene Ansätze. Einige OpenID-Anbieter stellen besondere Login-Verfahren zur Verfügung, die eine Phishing-Attacke deutlich erschweren. [1]

- ImageShield:
  Dieser Dienst wird von myvidoop.com zur Verfügung gestellt und macht die Benutzung eines Passworts überflüssig. Anstatt einer Eingabe-Maske für Name und Passwort erscheint dem Benutzer eine Anordnung von Bildern. Der Benutzer selbst definiert sich eine Gruppe von Bilder-Kategorien, z.B. Auto, Essen, Filme. Nun müssen nur die zugehörigen Buchstaben der Bilder eingegeben werden, hier: V,X,F. Wird man auf eine Seite weitergeleitet, auf der nicht alle oder keine Bilder der Kategorien zu sehen sind, liegt die Vermutung eines Phishing-Versuchs nahe.

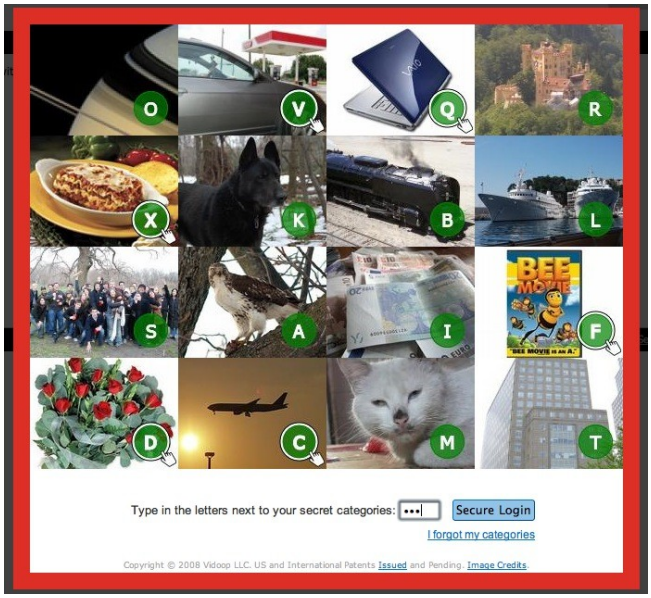

Abbildung 3: ImageShield Beispiel

- PhoneFactor:
  Wie der Name bereits vermuten lässt, wird der Login um einen Anruf erweitert. Wird ein Benutzer zu einem OpenID-Anbieter weitergeleitet, bekommt er zusätzlich einen Anruf des Anbieters, der die Echtheit der Seite bestätigt. Nun gibt man am Telefon sein

Passwort ein um die Authentifizierung abzuschließen. Dieser Dienst ist jedoch nur für einen Festnetzanschluss der deutschen Telekom und einem Account bei „myopenid.com“ als Anbieter verfügbar.

- VeriSign VIP Credentials
  „VeriSign.com“ bietet einen sogenannten VIP Token Generator an, ein Gerät, dass zusätzlich zu Benutzernamen und Passwort bei Bedarf einen neuen Token[2] generiert, um den Login besser zu schützen. Hierfür sind allerdings einmalig 30$ zzgl. Versand zu bezahlen.

Weiterhin wurde mit Version 2.0 OpenID um „direct identity“ erweitert. Statt der OpenID gibt der Nutzer auf einer Website nur noch seinen OpenID-Anbieter an und kann dann dort entscheiden, mit welcher OpenID er sich bei dieser Website anmelden will. So lassen sich unterschiedliche Identitäten für einzelne Websites nutzen. Zudem kann auf diese Weise Phishing besser verhindert, da der Nutzer sich zuvor direkt bei seinem OpenID-Anbieter anmeldet und nicht von einer Website zu diesem weitergeleitet wird. [7]

Ein weiterer Kritikpunkt liegt in der möglichen Speicherung von Bewegungsdaten. Aufgrund der zentralen Kontrolle über das OpenID-Konto, besteht für den Anbieter die Möglichkeit, einen Verlauf der Anmeldungen an den Konsumenten-Seiten zu erstellen. Neben neuen OpenID-Anbietern haben auch längst die Internet-Riesen wie Google, Yahoo und Facebook ihr Angebot um OpenID erweitert, wodurch sich ein Wettkampf um die Gunst der Benutzer und somit ihren Profil-Daten entwickelt hat.

3. Zusammenspiel mit OAuth

OpenID und OAuth werden häufig in einem Atemzug erwähnt. Bei OAuth handelt es sich um ein dezentrales Autorisierungssystem[3]. Es gewährt Webseiten sowie Dritt-Anwendungen Zugriff auf eigene Daten, die auf einer anderen Webseite liegen, ohne dabei die die eigene Identität bzw. das eigene Passwort zu übermitteln. [4] Zum Beispiel kann man einem Druck-Dienst im Web den Zugriff auf die eigenen Facebook-Bilder gewähren, ohne dabei dem Druck-Dienst das Passwort für Facebook zu übermitteln. Auch hier wird mit Hilfe einer Weiterleitung der Zugriff kontrolliert. Hier kommt OpenID ins Spiel, denn das Gewähren der Zugriffe über OAuth kann nun mittels einer einzigen ID vollzogen werden.
Zusammengefasst ermöglicht dies die Regelung der Authentifizierung (OpenID) und

2 Hier: Ein Code, der zusätzlich zu Benutzer-Name und Passwort eingegeben werden muss.
3 Unter Autorisierung versteht man die Zuteilung von Rechten.

Autorisierung (OAuth) im Web mittels eines einzigen Zugangs. [2]

4. Ausblick

Wie schon bei den in der Einleitung erwähnten Vorgängern (NET Passport / SAML) entscheidet auch bei OpenID letztendlich die Akzeptanz der Website-Betreiber und der Anwender über den Erfolg. Neben den Bemühungen um Sicherheit und vor allem die einfache Handhabung spricht auch folgende Statistik (Abb.4) von Scott Kveton (OpenID Foundation) für den Erfolg von OpenID und lässt eine erfolgreiche Zukunft vermuten. Während im Januar des Jahres 2007 ca. 1,125 Konsumenten-Seiten existierten, war es sechs Monate später bereits fast die vier-fache Anzahl.

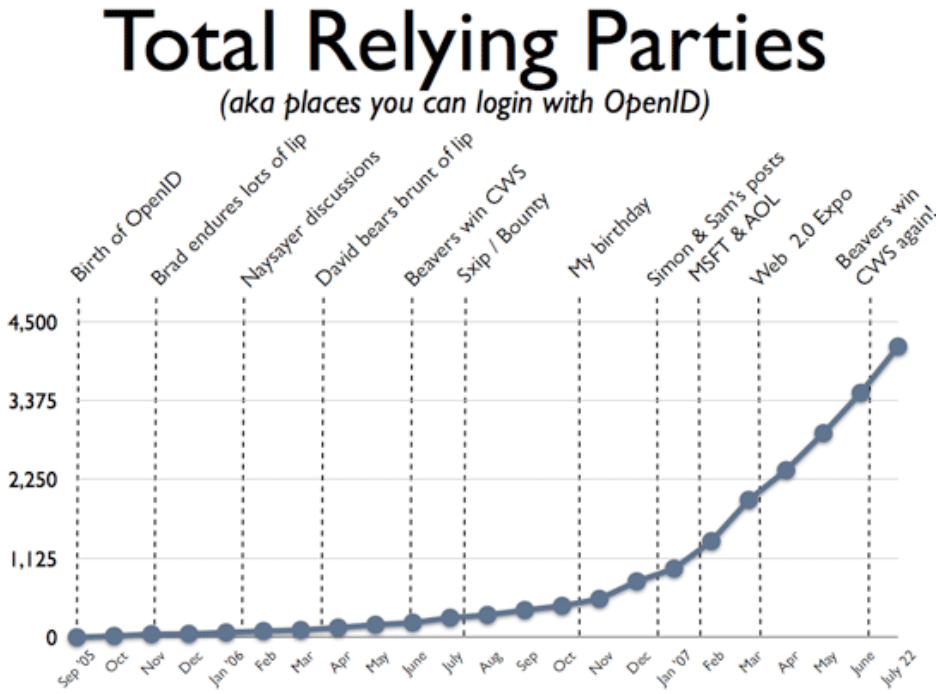

Abbildung 4: Anzahl der Konsumenten

5. Bilderverzeichnis

6. Literaturverzeichnis

[1] Artikel: “Identity Management: Authentifizierungsdienste mit OpenID“ von Lofi Dewanto; Aufgerufen am 18/06/2010; http://www.heise.de/developer/artikel/Identity-Management-Authentifizierungsdienste-mit-OpenID-227202.html

[2] Artikel: „OAuth-OpenID: You’re Barking Up the Wrong Tree if you Think They’re the Same Thing“; Aufgerufen am 20/06/2010; http://softwareas.com/oauth-openid-youre-barking-up-the-wrong-tree-if-you-think-theyre-the-same-thing

[3] www.openid.net; Aufgerufen am 20/06/2010

[4] www.oauth.net; Aufgerufen am 22/06/2010

[5] Artikel: „Netzweite Identitäten mit OpenID“ von Martin Raepple; Aufgerufen am 19/06/2010; http://www.springerlink.com/content/755180g7h7741187/

[6] Buch: „Get Ready For OpenID“ von Rafeeq Ur Rehman; Conformix Technologies Inc.

[7] Artikel: „OpenID 2.0 ist fertig“ von Jens Ihlenfeld; Aufgerufen am 19/06/2010; http://www.golem.de/0712/56417.html

[8] Wikipedia; Eintrag „Phishing“; Aufgerufen am 21/06/2010; http://de.wikipedia.org/wiki/Phishing