



ERFOLGREICHER EINZUG VON STANDARDPROTOKOLLEN IN DIE TELEKOMMUNIKATION

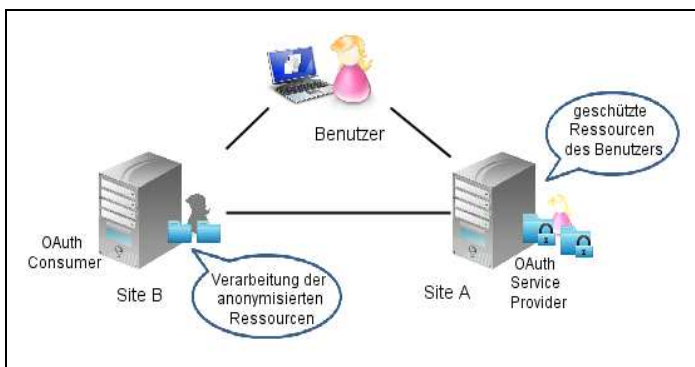
# Vernetzung auf sicheren Pfaden



Das Protokoll OAuth hält nach seinem Erfolg bei sozialen Netzwerken auch Einzug in die Telekommunikationsbranche. Doch was verbirgt sich genau hinter OAuth? Welche Vorteile bietet es und welche sind wichtig für die Telekommunikationsbranche? Erschließen sich neue Möglichkeiten? Wie geht es mit OAuth weiter? Diese und weitere Fragen versucht der folgende Artikel zu beantworten.

**Stefanie Dronia**

OAuth ist in der Version 1.0a ein von der IETF standardisiertes Protokoll für sichere Authentifizierung und Autorisierung von Anwendungen im Internet ([1]). Es erlaubt einem Benutzer den Zugriff auf seine privaten Ressourcen auf einer Web-Site A (OAuth Service Provider) für eine zweite Web-Site B (OAuth Client) zu autorisieren ohne Web-Site B seine Zugangsdaten (Benutzername und Passwort) preiszugeben.



**Das ist die zentrale Eigenschaft von OAuth:**

Die Zugangsdaten und die Benutzeridentität bleiben der Client-Applikation gegenüber verborgen.

Es gibt eine Reihe von Gründen, seine Zugangsdaten nicht überall und mit jedem zu teilen. Die Offenlegung des eigenen Email-Accounts (Benutzername und insb. Passwort) für ein soziales Netzwerk zum Verschicken von Nachrichten entspricht der Bekanntgabe der PIN der eigenen EC-Karte. Letzteres würde wohl niemand ernsthaft in Erwägung ziehen. Im Internet jedoch sind sich viele der Tragweite nicht bewusst, was sie wem anvertrauen. OAuth stellt einen Ausweg aus dieser Misere bereit. Doch wie kann man sich das vorstellen? Um auf das Beispiel mit der EC-Karte zurück zu kommen: Hier es ist schlicht und einfach die eigene Unterschrift. Nur mit dieser wird z.B. ein Restaurant autorisiert, seine Rechnung abzubuchen. Die Verwendung der EC-Karte wird auf eine bestimmte Transaktion, einen Empfänger und einen bestimmten Betrag eingeschränkt. Für das Restaurant ist also nur ein stark beschränkter Zugriff möglich.

Im Internet ändert sich die Welt: Kaum jemand interessiert sich tiefgehend für verwendete Protokolle und Standards. Umso wichtiger ist die Gewährleistung einer erhöhten Privatsphäre und Sicherheit für den

Benutzer. OAuth ist eine große Chance, dies zu erreichen.

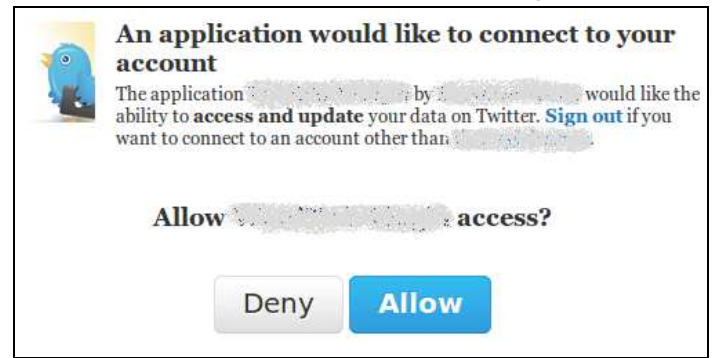
Die steigende Anzahl von Webservices führt zur Vernetzung vieler Anwendungen im Web um etwas Neues zu schaffen. Benutzer haben viele Web-Sites für unterschiedliche Zwecke, so z.B. eine Site zum Ablegen von Fotos, eine für Videos, eine für Email usw. Um alle Sites gemeinsam nutzen zu können, ist irgendeine Form der Integration notwendig. Die verschiedenen Sites schützen jedoch den Zugang zu den Ressourcen des Benutzers. In der Regel sind Benutzername und Passwort der Schlüssel für den Zugang. Dieser wiederum ist zu mächtig, um ihn anderen Sites preiszugeben. Einmal ausgehändigt, ist es schwierig, ihn anschließend zu widerrufen. Einzig die Änderung von Benutzername und Passwort wäre eine Option. Das würde aber den Zugang für alle Sites auf einen Schlag unmöglich machen.

### Wo setzt nun OAuth an?

OAuth ist für Benutzer völlig transparent. Bei richtiger Umsetzung merkt der Benutzer nicht, dass OAuth als Protokoll verwendet wird. Wesentliche Erkennungsmerkmale sind, dass der Benutzer sich beim ihm bekannten Provider authentifiziert und der Autorisierung eines Clients explizit zustimmt.

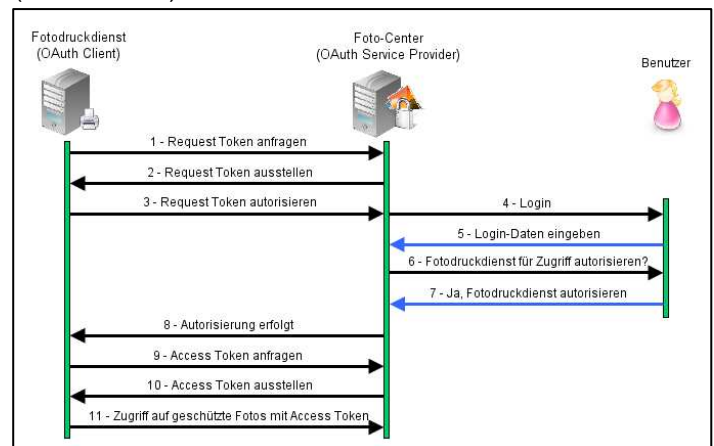
Ein Beispiel zur Veranschaulichung von OAuth: Der Benutzer möchte gerne Fotos bei einem Fotodruckdienst drucken lassen. Dafür ruft er einen Fotodruckdienst auf und gibt an, dass er Fotos drucken lassen möchte. Der Fotodruckdienst fragt nach den Fotos und der Benutzer wählt aus einer Liste von Foto-Centern dasjenige aus, bei dem seine Fotos hinterlegt sind. Der Druckdienst schickt nun den Benutzer zu seinem Foto-Center, um für den Zugriff auf die Fotos autorisiert zu werden. Der Benutzer meldet sich mit seinen Zugangsdaten beim Foto-Center an (er authentifiziert sich) und wird anschließend vom Foto-Center gefragt, ob er dem Druckdienst Zugriff auf seine Fotos geben möchte. Wenn dies der Fall ist (er autorisiert den Druckdienst für den Zugriff), wird er zurück zum Fotodruckdienst geschickt, der nun auf die Fotos beim Foto-Center zugreifen kann. In keinem Schritt gibt der Benutzer seine Identität oder seinen Account dem Fotodruckdienst preis. Die untenstehende Abbildung zeigt beispielhaft eine Seite, wie die Autorisierung eines

Clients bei Twitter beim Benutzer eingeholt wird.



### Doch was passiert technisch?

Nachdem der Benutzer sein Foto-Center ausgewählt hat, beginnt der so genannte OAuth Autorisierungsprozess (manchmal auch OAuth Dance genannt). Eine Sequenz von auf dem REST-Architekturstil basierenden http-Requests und html-Seiten wird durchlaufen. Wie die untenstehende Grafik illustriert, wird eine Reihe von Schritten durchgeführt, bei denen der Benutzer jedoch nur in den Schritten 5 und 7 (blaue Pfeile) aktiv ist.



Zuerst (1) erfragt der Fotodruckdienst, der OAuth Client, beim Foto-Center, dem OAuth Service Provider, ein Request- Token an. Der Service Provider stellt dem Client das Request- Token aus (2). Dieses Token repräsentiert eine einzelne Autorisierungstransaktion. Als nächstes (3) bittet der Client um Autorisierung des Request-Tokens. Der Service Provider (das Foto-Center) fordert den Benutzer auf (4), sich ihm gegenüber zu authentifizieren. Der Benutzer tut dies z. B. mit seinem Benutzernamen und Passwort (5). Der Service Provider fragt den Benutzer (6), ob der Client in seinem Namen auf seine Ressourcen – hier im Beispiel die Fotos – zugreifen darf. Der Benutzer stimmt zu (7) – er autorisiert den Client. Der Service Provider meldet die Autorisierung an den Client zurück (8), der daraufhin ein Access-Token anfragt (9). Der Service Provider stellt das Access-Token aus

(10). Mit diesem Token greift der Client im Namen des Benutzers auf die Ressourcen beim Service Provider zu (11).

Das Access-Token stellt somit den Schlüssel dar, mit dem ein Client auf die geschützten Ressourcen eines Benutzers bei einem Service Provider zugreifen darf – ohne dabei die Zugangsdaten oder Identität des Benutzers zu kennen. Der Schlüssel ist eingeschränkt auf einen Gültigkeitszeitraum, die Ressourcen, den Client und den Benutzer. Wenn das Token für eine lange Gültigkeit ausgestellt wurde, kann es im Client gespeichert und in späteren Sitzungen wieder verwendet werden. Der Benutzer kann die Autorisierung jederzeit beim Service Provider widerrufen.

### **Die Anwendungsgebiete von OAuth sind weitläufig**

Die weiteste Verbreitung – wie auch seinen Ursprung – findet OAuth in Applikationen, die auf soziale Netzwerke, z.B. Facebook oder Twitter, zugreifen. Auch Google und Yahoo! schützen Ressourcen mit OAuth. XING beispielsweise verwendet OAuth bei seiner mobilen Applikation um ein automatisches Login des Benutzers durchzuführen. Applikationen, die auf Services der Deutschen Telekom, z.B. Mediacenter oder Email@t-online.de, zugreifen, setzen OAuth als langlebige Authentifizierungs- und Autorisierungsmethode ein. Dabei werden mobile Applikationen ebenso wie Web- und Desktop-Applikationen angeboten.

Neben der delegierten Autorisierung, dem klassischen OAuth-Anwendungsgebiet, wird das OAuth-Token auch für die Benutzerauthentifizierung beim Service Provider verwendet. Die genannten Anbieter haben OAuth in ihre APIs integriert und stellen sie Entwicklern von Webservices, Desktop- und mobilen Anwendungen zur Verfügung. Zur Integration von OAuth in Client-Applikationen können zahlreiche Open-source-Bibliotheken für eine Vielfalt von Programmiersprachen verwendet werden, z.B. Java, PHP, C# und Objective C.

### **Welche Vorteile bietet OAuth der Telekommunikationsbranche? Lassen sich dabei neue Anwendungsgebiete erschließen?**

Der klassische Grund für die Einführung von OAuth bei Telekommunikationsunternehmen ist die Bereitstellung von eigenen Diensten für den Zugriff von außen. Diese Dienste stellen den Service Provider im OAuth-Sinn dar. Es können Anwendun-

gen (die OAuth Clients) entwickelt werden, die im Namen und auf Rechnung eines Kunden Dienste wie z.B. SMS oder Konferenzruf bereitstellen. Der Dienst kann aus dem OAuth Access-Token Informationen ableiten, die z.B. für die Rechnungsstellung erforderlich sind.

Ein anderer Grund OAuth einzuführen ist die sichere und benutzerfreundliche Authentifizierung von Kunden auf mobilen Endgeräten, wie Smartphones oder auch Endgeräten für IPTV. Schnell geht ein solches Gerät verloren oder wird unüberlegt anderen Personen zur Nutzung überlassen. Sind Zugangsdaten auf dem Gerät gespeichert, kann der unehrliche Finder damit sehr viel Schaden auch in finanzieller Hinsicht anrichten.

Grundsätzlich sollte man annehmen, dass es für Telekommunikationsunternehmen möglich sein sollte, die Authentifizierung des Endgeräts und somit des Benutzers anhand der SIM-Karte im Gerät bzw. anhand von Netzwerkinformationen durchzuführen. Prinzipiell ist das möglich - solange der Zugang zum Netzwerk über das eigene Netzwerk (z.B. GPRS oder HSDPA) erfolgt. Smartphones verfügen jedoch in der Regel über eine WLAN-Schnittstelle und verwenden diese auch vorrangig für die Verbindung mit dem Internet, da dort die verfügbare Bandbreite höher ist. Die zugehörigen Verbindungsinformationen reichen leider nicht mehr aus, um gewohnte Authentifizierungsmechanismen anzuwenden. Die Authentifizierung anhand von Netzwerkinformationen kann nicht mehr zuverlässig angewendet werden. Die Integration von OAuth in die Anwendungen auf den Geräten hingegen wirkt als eine zuverlässige Sicherheitsschraube. Des Weiteren ist anzumerken, dass mittels OAuth der Zugriff auch mit Identitäten erfolgen kann, die vom mit der SIM-Karte assoziierten Benutzer abweichen.

Um OAuth als Standardverfahren zu etablieren, muss Sicherheit bei den Stakeholdern der Anwendungen einen hohen Stellenwert erhalten. Bisher ist dies leider noch nicht gegeben. Bei der Integration von OAuth erfolgt die Authentifizierung des Benutzers und das Einholen seiner Zustimmung über einen Web-Browser. Dabei kommen sichere und etablierte Verfahren aus dem Internet und des Telekommunikationsunternehmens, z. B. zertifizierte https-Verbindungen, zum Einsatz. Wenn der Browser zusätzlich in die Architektur einer Anwendung integriert werden soll, werden häufig ablehnende Anmerkungen, wie „viel zu kompliziert und zu

aufwändig“ (Entwicklungskontext) oder „nicht benutzerfreundlich – noch ein Fenster“ (Marketing/Produktdesign), geäußert.

Die Bedeutung der Vorteile, die OAuth zusammen mit etablierten Verfahren zur sicheren Authentifizierung bietet, erhält leider noch nicht die verdiente Anerkennung. Um OAuth als Standard-Verfahren in Telekommunikationsunternehmen zu etablieren, ist noch ein weiter Weg zu bestreiten, den zahlreiche Diskussionen begleiten.

### Wohin entwickelt sich der Standard (OAuth 2.0)?



Die aktuelle Version 1.0a des OAuth-Standards wurde im Oktober 2007 von der IETF verabschiedet. Es ist einige Zeit vergangen, in der Erfahrungen, aber auch Kritikpunkte gesammelt werden konnten. Vielen erscheint der Autorisierungsprozess als zu lang und zu umständlich. Auch wird permanent Kritik an der Anwendung kryptographischer Verfahren (Client-Seite) und dem Vorhalten größerer Datenmengen für die Bestimmung und Verifizierung gültiger OAuth-Requests (Service Provider-Seite) geäußert. OAuth 1.0a ermöglicht den Zugriff auf eine Ressource über einen einzelnen Service. Applikationen, die verschiedene Services bzw. Ressourcen integrieren möchten, können nur mit Mehraufwand realisiert werden. Der Autorisierungsprozess, und somit auch die Autorisierung durch den Benutzer, muss für jeden Service separat erfolgen. Diese Einschränkung erweist sich vor allem für die Telekommunikationsbranche als ein gravierender Nachteil von OAuth 1.0a. Das Protokoll wurde entwickelt, um in einzelne Sites integriert zu werden. Ein Einsatz in großen Umgebungen mit einem zentralen Identitätsmanagement-System und vielen Sites wurde nicht bedacht.

Seit geraumer Zeit wird OAuth in der Version 2.0 spezifiziert. Der zugehörige Draft liegt in Version 10 ([3]) bei der IETF vor. Grundlegende Veränderung gegenüber dem aktuellen Standard ist die Unterscheidung von Anwendungsfällen, die die Eigenschaften verschiedener Endgeräte berücksichtigen. Abläufe speziell für Web-Applikationen, User-Agents (in Webseiten integrierte Applikationen), native Applikationen (z.B. Mobile Apps, Desktop-Anwendungen, auf Spielkonsolen oder IPTV-Boxen) und auf Basis vorhandener Vertrauensverhältnisse werden betrachtet. Resultat ist ein vereinfachter und angepasster Ablauf, um ein Zugriffstoken zu erhalten. Weiterhin stellt OAuth 2.0 die Möglichkeit bereit, über einen einzigen

Autorisierungsprozess den Zugriff auf mehrere Ressourcen zu erhalten. Der Integration verschiedener Services in einer einzigen Applikation sind dadurch große Hürden genommen. Die Vernetzung von Services schreitet voran.

Der neue OAuth-Standard wird auf einer öffentlichen Mailing-Liste bei der IETF entwickelt, bei der jeder mitmachen kann - und viele machen mit. Dieses demokratische Vorgehen ist bei anderen Standardisierungsorganisationen selten zu finden und weist zahlreiche Vorteile auf. Experten mit verschiedensten Schwerpunkten können sich ohne unternehmenspolitische Kabale und Hürden über technische Aspekte und neue Anwendungsfälle austauschen. Beiträge können jederzeit und von überall geäußert werden. Barrieren wie Beitrittsgebühren oder eine Zustimmung zu juristischen Klauseln bestehen nicht.

Leider besitzt dieses Vorgehen auch Nachteile. In einigen Fällen, zumeist Detailfragen, ist es schwierig, einen gemeinsamen Konsens zu finden. Viele vertreten den Anspruch, dass die eigenen Bedürfnisse maximal berücksichtigt werden. Entscheidungen werden dadurch oft verzögert. Weiterhin ist zu beobachten, dass sich die Anforderungen aus dem Telekommunikationsbereich selten mit den Anforderungen aus dem Bereich der sozialen Netzwerke decken.

Der heutige Stand von OAuth 2.0 (Version 10 des Drafts) ist bereits weitaus besser als OAuth 1.0a. Obwohl er noch nicht abgeschlossen ist, wird er bereits in der Praxis umgesetzt. Der Weg bis hierhin war die Arbeit aller Beteiligten zweifellos wert.

### Unsere Erfahrungen in der Telekommunikationsbranche

Unsere Erfahrungen in aktuellen Projekten mit OAuth sind durchweg positiv. Die Integration in eine vorhandene Landschaft von Identitätsmanagement-Systemen (IdM) ist aus technischer Sicht unproblematisch. Es unterstützt das Architekturprinzip des offenen Dreiecks, das vorteilhaft für große Umgebungen ist. Systeme, die nach Authentifizierung und Autorisierung Zugriffstoken ausstellen, werden von denjenigen entkoppelt, die nach Vorweis von Zugriffstoken Dienste anbieten. Sie können die Zugriffstoken selbständig verifizieren. Dadurch können Services entwickelt werden, die kanalunabhängig (mobil, web, IPTV) sind und sogar in internen wie Wholesale-Szenarien eingesetzt werden können.

Dem Themenkomplex Sicherheit wird jedoch allzu oft von Entwicklungseinheiten außerhalb von IdM-Abteilungen wenig bis keine Beachtung geschenkt. Oft muss die Verwendung von OAuth und weiterer Sicherheitsverfahren den Projekten aufgezwungen werden. Um auch dort Sicherheitsbewusstsein aufzubauen und Sensibilisierung hinsichtlich dieses Themas zu erzeugen, werden verschiedene proaktive Maßnahmen ergriffen. Kompetente Ansprechpartner machen in ausführlichen Beratungsgesprächen die verantwortlichen Projektmitarbeiter zu Verbündeten. Anschauliche Dokumentationen für den Erstkontakt mit OAuth und darauf aufbauende API-Dokumentation erleichtern die Integration in die Anwendung für Entwickler erheblich.

Stehen alle Beteiligten auf der gleichen Seite, so ist eine große Hürde für den erfolgreichen Projektverlauf aus dem Weg geräumt. Das gemeinsame Ziel „der zufriedene und vertrauende Kunde“ rückt in Reichweite.

Weiterhin ist es wichtig, die bestehenden und neue Anforderungen der Telekommunikationsbranche an OAuth hinsichtlich Anwendungsfällen und Sicherheitsanforderungen zu identifizieren. Das Eintreten für diese Anforderungen auf der IETF-Mailingliste bei der Entwicklung des neuen OAuth-Standards ist selbstverständlich. Er entwickelt sich dadurch in eine Richtung, die den Ansprüchen der Telekommunikationsbranche Rechnung trägt.

## Fazit

Telekommunikationsunternehmen sind, im Gegensatz zu sozialen Netzwerken, Anbieter zahlreicher Dienste und tragen dafür hohe Kostenrisiken. Sie stellen somit andere Sicherheitsanforderungen an Technologien und Protokolle. OAuth 2.0 bietet für sie viele Möglichkeiten und erfüllt deren Anforderungen. Es kann in großen Umgebungen angewendet werden und ebnet den Weg, unterschiedliche Dienste in einzelne Client-Applikationen zu integrieren.

Eine Bereitstellung von Diensten über öffentliche Schnittstellen ist in diesem Kontext notwendig. Daher ist es erforderlich, die klassischen Ansätze der Perimeter-basierten Sicherheit um eine nutzer- und anwendungsbezogene Sicht zu ergänzen. OAuth 2.0 unterstützt dies, denn die Authentifizierung und Autorisierung der Clients kann an den Anwendungsschnittstellen auf Basis von Tokens erfolgen. Der Kunde autorisiert eine einzelne Applikation statt wie

bisher jeden Zugriff auf einen Dienst. Die Entwicklung von Clients, die über das Internet auf Dienste von Telekommunikationsunternehmen zugreifen und so miteinander vernetzen, wird möglich.

Wird OAuth auch fester Bestandteil anderer Protokolle, z.B. IMAP für Emails, wird es sich noch stärker etablieren und zu einem nicht mehr weg zu denkenden Standard werden. Sollte der neue Standard nicht alle von Telekommunikationsunternehmen notwendigen Eigenschaften enthalten, so bleibt die Möglichkeit, individuelle Erweiterungen zu entwickeln. Diese bedienen die eigenen Bedürfnisse nach maximaler Sicherheit bei optimierter Benutzerfreundlichkeit mit minimalem Zusatzaufwand, um die eigenen Dienste anbieten zu können.

Es bleibt der optimistische Blick auf den neuen OAuth 2.0-Standard und die Neugier darauf, wie er sich vor allem in der Telekommunikationsbranche ausbreiten wird.

Quellen:

[1] <http://oauth.net/core/1.0a>

[2] <http://hueniverse.com/oauth/>

[3] <http://tools.ietf.org/id/draft-ietf-oauth-v2-10.html>

## Über den Autor

Stefanie Dronia ist Consultant bei der SYRACOM Consulting AG und im Bereich Telekommunikation tätig. Sie ist Autorin des Buches „Sequentielle Quadratische Programmierung“, erschienen im VDM Verlag Dr. Müller, 2008

### Kontakt:

**SYRACOM Consulting AG**

**Stefanie Dronia**

Otto-von-Guericke-Ring 15

65205 Wiesbaden

Germany

Phone: +49 (0) 6122 – 9176 0

[stefanie.dronia@syracom.de](mailto:stefanie.dronia@syracom.de)

[www.SYRACOM.de](http://www.SYRACOM.de)