Zugang zu Föderationen aus Speicher-Clouds mit Hilfe von Shibboleth und WebDAV

Sebastian Rieger[1], Yang Xiang[2], Harald Richter[3]

[1]Karlsruher Institut für Technologie (KIT),
[2]Rechenzentrum Garching (RZG),
[3]Technische Universität Clausthal (TUC)
sebastian.rieger@kit.edu, yang.xiang@rzg.mpg.de, hri@tu-clausthal.de

Abstract: Innerhalb weniger Jahre entstanden sowohl in offenen als auch in geschlossen Clouds günstige Zugriffsmöglichkeiten auf große Online-Festplatten über das Internet. Sobald jedoch die Benutzer dieser Speicher unterschiedliche Cloud-Dienstleister z.B. für institutsübergreifende Projekte oder für mehrfach verteilte Sicherheitskopien verwenden wollen, treten aufgrund der verschiedenen Benutzerkonten, Zugriffsverfahren und Zugriffsrechte Schwierigkeiten auf. Eine dienstleisterübergreifende, einheitliche Authentifizierung und Autorisierung unter Verwendung einer einzigen Benutzerkennung und eines Passworts wäre für die Benutzer der Cloud-Speicher und für deren Betreiber besser. Der vorliegende Beitrag beschreibt eine Lösung dieses Problems, die aufgrund der Verwendung eines offenen Standards (WebDAV) für den Zugriff auf Online-Filesysteme ohne zusätzliche Middleware auskommt. Die Lösung ist Shibboleth-fähig und damit kompatibel zu einem weit verbreiteten Mechanismus für verteilte Authentifizierung und Autorisierung. Sie beruht auf einer automatischen Benutzer-Lokalisierung im Internet unter Zuhilfenahme von NAPTR-Einträgen im Domain Name System und der Verwendung der E-Mail-Adresse als weltweit eindeutigen Benutzernamen. Die vorgeschlagene Lösung eignet sich für die Realisierung von Föderationen von Speicher-Clouds in denen mehrere Organisationen, z.B. Universitäten und Forschungsinstitute gemeinsam einen einheitlichen Zugriff auf mehrfach verteilte Dateisysteme im Internet bereitstellen wollen, wie sie beispielsweise für die Föderation des Landes Niedersachsen [NAAI] sowie der Max-Planck-Gesellschaft [MAAI] geplant sind.

1 Stand der Technik

In den nachfolgenden Abschnitten dieses Beitrags werden in Kapitel 1 Föderationen von Speicher-Clouds, der Zugang dazu, sowie die Authentifizierung und Autorisierung und das Problem der Lokalisierung von Benutzern beschrieben. Im anschließenden Kapitel 2 wird die Softwarearchitektur unseres Vorschlags, inkl. der Lokalisierung von Benutzern in dynamischen Föderationen dargestellt. In Kapitel 3 schließlich wird ein Fazit gezogen und zukünftige Forschungsarbeiten angegeben.

1.1 Isolierte Speicher-Clouds

Stand der Technik bei Speicher-Clouds sind isolierte Insellösungen. Die Speicher-Cloud lässt sich vom Benutzer über eine Web-Oberfläche oder über eine proprietäre Zugangsschnittstelle wie eine Online-Festplatte mit Verzeichnisstrukturen (häufig auch als sog. Buckets bezeichnet) und Dateien verwenden. Beispiele aus der jüngsten Vergangenheit für solche Speicher-Clouds sind Amazon S3 [S3], Google Storage [GS] und Microsoft Azure Storage [Azure]. Um isolierte Clouds herum sind zusätzlich Dienste und Dienstleister entstanden, die den Zugang zu und die Benutzung von Speicher-Clouds für Endanwender vereinfachen, wie z.B. DropBox [DB], Mozy [MZ] oder Ubuntu One [UO]. Ein einheitlicher de-facto oder de-jure Standard für einen dienstleisterübergreifenden Zugang auf Speicher-Clouds existiert nicht. Es wird aber bei dem Firmenkonsortium SNIA (Storage Networking Industry Association, [SNIA]) unter der Bezeichnung CDMI [CDMI] daran gearbeitet. Wann dieser Industriestandard verfügbar sein wird, ist nicht bekannt.

Neben diesen offenen Speicher-Clouds werden gemäß [Frei10] bei IT-Infrastrukturen im wissenschaftlichen Umfeld zunehmend geschlossene Clouds eingesetzt. Letztere basieren oftmals auf Open Source Implementierungen von Speicher-Clouds (vgl. Eucalyptus Walrus [WALR]) und zeichnen sich dadurch aus, dass den Anwendern innerhalb einer geschlossenen Benutzergruppe ein einheitlicher und vereinfachter Zugriff ermöglicht wird, der instituts- und damit ortsunabhängig ist. Für die Realisierung des Zugriffs erfordert dies i.d.R. eine einheitliche Authentifizierung und Autorisierung (AA) über proprietäre Anwendungen. Ein Beispiel dafür ist die AA-Infrastruktur (AAI) des DFN [DAAI]. Die technische Grundlage für eine AAI bildet häufig der SAML-Standard [SAML] dessen Implementierung in Form von Shibboleth [Mor04] insbesondere in wissenschaftlichen IT-Infrastrukturen weit verbreitet ist.

1.2 Föderationen von Speicher-Clouds

Die natürliche Erweiterung von isolierten Speicher-Clouds sind Verbünde daraus. In [Xia02] wurde eine entsprechende Föderation von Speicher-Clouds beschrieben, die auf REST [REST] beruht. REST basiert wiederum auf HTTP, es verwendet aber u.a. Uniform Resource Identifiers (URIs) anstelle von Uniform Resource Locators (URLs) und neben HTML auch XML in der Response. Der Nachteil dieser Lösung war jedoch, dass Client-seitig zusätzliche Middleware für den Zugriff auf den im Netz verfügbaren Online-Filesystemen erforderlich war.

Das vorliegende Paper beschreibt einen neuen Ansatz, um ohne zusätzliche Middleware auf Föderationen von Speicher-Clouds zugreifen zu können. Dazu wird der WebDAV-Standard [rfc4918] verwendet, der ebenfalls eine Erweiterung von HTTP darstellt, die aber substantiell über REST hinausgeht. Für die vorgeschlagene Lösung wurde ein Shibboleth-fähiger WebDAV-Client entwickelt, der anstelle einer Web-Browser-basierten Benutzerlokalisierung, sowie einer statischen Authentifizierung und Autorisierung (AA) eine sog. dynamische Föderation verwendet, wie sie in [Xia02] beschrieben wurde.

Dadurch können Endanwender auch in zeitlich veränderlichen Föderationen direkt auf unterschiedliche Cloud-Betreiber zugreifen, ohne eine gesonderte Middleware zu verwenden und ohne sich erneut anmelden zu müssen (= Single Sign-On). Die hier vorgeschlagene Lösung erlaubt, das native WebDAV-Modul mod_dav [Mdav] des Apache Web-Servers eines Shibboleth-unterstützenden Cloud-Dienstleisters als WebDAV-Server einzusetzen, ohne dass dafür Erweiterungen auf der Server-Seite oder ein Web-Browser für die Verwendung von Shibboleth auf der Client-Seite notwendig wären.

Andere Forschergruppen wie [BeB06] und [Sch08] arbeiten ebenfalls an der Unterstützung von Shibboleth für WebDAV, allerdings auf Seiten des Servers. Eine frühere, Web-Browser-basierte Lösung wurde bereits in [NA07] vorgestellt. Für Grid-Umgebungen wurde eine ähnliche, auf iRODS aufsetzende Lösung in [iRODS] beschrieben.

1.3 Zugang zum Online-Filesystem

Dienstleister für offene Speicher-Clouds haben i.d.R. eine proprietäre Zugangsschnittstelle (vgl. Amazon S3 oder Google Storage REST API), die nur über spezielle Clients genutzt werden kann. Durch letztere werden alle Dateizugriffe auf die bekannten HTTP-Methoden PUT, GET, POST und DELETE abgebildet (vgl. [Xia02]). Einige Cloud Storage Provider bieten darüber hinaus auch einen WebDAV-basierten Zugriff an. Dieser ermöglicht den Benutzern das Lesen, Schreiben und Löschen von Dateien ohne die Verwendung eines speziellen Clients oder einer proprietären API. Dies diente unserer Lösung als Vorbild. Abbildung 1 zeigt, wie der Zugang zweier Beispielanwender zu WebDAV-basierten Online-Filesystemen erfolgt, die in unterschiedlichen Speicher-Clouds angesiedelt sind.

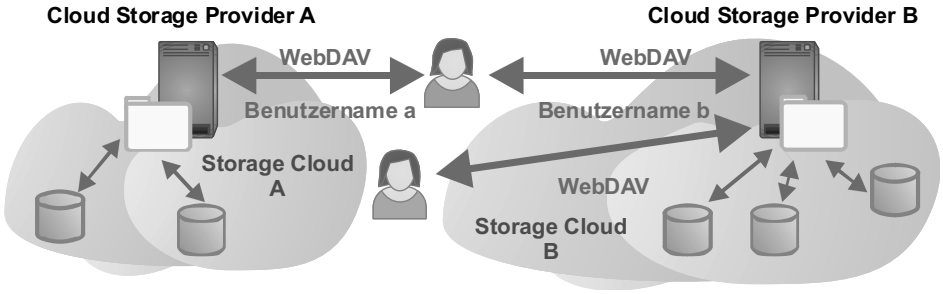

Abbildung 1: Zugang zu WebDAV-basierten Online-Filesystemen in unterschiedlichen Speicher-Clouds.

Die AA erfolgt typischerweise mit Hilfe von Benutzernamen und Passwort. Die Verwendung von Zertifikaten, PINs oder TANs sind im Anwender-Bereich eher unüblich. Für unterschiedliche Cloud Storage Provider müssen Benutzer jedoch i.d.R. verschiedene Benutzernamen und Passwörter verwalten, da jeder Cloud-Betreiber seine Benutzer separat verwaltet und ggf. unterschiedliche Anforderungen an die verwendeten Passwörter stellt. Außerdem ist in Bezug auf die aktuell verfügbaren Anbieter kein Single Sign-On über Cloud-Grenzen hinweg möglich.

Darüber hinaus basiert die Autorisierung von Lese- und Schreibzugriffen bei WebDAV auf den im Kontext des Web-Servers limitierten Zugriffsmöglichkeiten, sowie auf den Rechten, die im darunterliegenden Dateisystem definiert sind. Diese Rechte werden hierbei nicht auf die Benutzernamen, sondern auf eine eindeutige Identifikation (ID) des Benutzers abgebildet. In Windows-Umgebungen bildet beispielsweise der Security Identifier (kurz SID) eine solche ID [SID]. Unix verwendet gemäß des POSIX Standards stattdessen den User Identifier [UID], welcher im Gegensatz zum SID nicht global eindeutig ist. Bei der gleichzeitigen Benutzung mehrerer Speicher-Clouds entsteht daher in Bezug auf die Abbildung der Benutzernamen auf die ID für die Betreiber der Speicher-Cloud ein Problem, das beispielsweise durch die vollständige Verlagerung der Autorisierung in den Web- bzw. WebDAV-Server gelöst werden kann.

1.4 Authentifizierung und Autorisierung in Föderationen

Bei SAML-basierten [SAML] Föderationen benutzen die Diensterbringer (Service Provider, SP) für die AA sog. Identity Provider (IdP) und lagern die Aufgabe, den Benutzer zu authentifizieren, komplett in den IdP aus. Ein prominentes Beispiel für eine Föderation im wissenschaftlichen Umfeld bildet die AA-Infrastruktur des DFN (= DFN-AAI) [DAAI]. Betrachten wir zur Erläuterung der DFN-AAI einen Mitarbeiter der Max-Planck-Gesellschaft. Dieser wird über den für ihn zuständigen IdP authentifiziert und autorisiert. Der IdP ist an seinem Heimatinstitut angesiedelt, innerhalb dessen der Benutzer einen eindeutigen Benutzernamen und eine wohldefinierte Menge an Zugriffsrechten hat. Aufgrund der Mitgliedschaft der MPG in der DFN-AAI kann der Benutzer jedoch unter Verwendung seines Benutzernamens auch auf Dienstleistungen zuzugreifen, die von Instituten außerhalb der MPG angeboten werden, sofern diese Institute ebenfalls an der DFN-AAI teilnehmen. Da in einer Föderation nur der für den Benutzer zuständige IdP die AA durchführt, wird Single Sign-On auch für den Spezialfall einer Föderation über Cloud-Grenzen hinweg möglich. Cloud Service Provider (CSP) einer Speicher-Cloud, verwenden den jeweils zuständigen IdP einer Föderation für die AA. Diese Methode ist in Abbildung 2 dargestellt.

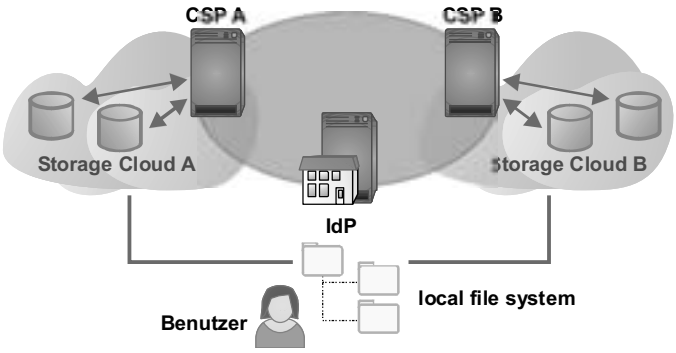

Abbildung 2: Single Sign-On in Föderationen aus Speicher-Clouds mit Hilfe eines Identity Providers (IdP).

Aufgrund des Verbundes mehrerer Partner und aufgrund besserer Skalierbarkeit existieren in einer Föderation mehrere IdPs. Diese müssen innerhalb der Föderation und bei den einzelnen CSPs in der Speicher-Cloud verwaltet werden. Um diese Verwaltung zu vereinfachen, kann in einer Cloud ein Identity-Dienst, dessen Funktion als „Identity as a Service“ (IDaaS) bezeichnet wird, verwendet werden. In dem Szenario aus CSP, IdPs und zentralem Identity-Dienst bildet der Identity-Dienst mit den IdPs eine sternförmige Topologie und wirkt für die CSPs als Proxy der IdPs. Der Vorteil, der sich für die CSPs aus der sternförmigen Topologie ergibt, ist die Vereinfachung der AA, da nur zum zentralen Identity-Dienst ein Vertrauensverhältnis bestehen muss. Insgesamt entsteht eine mehrfache Indirektion des Vertrauens gemäß des Transitivitätsgesetzes, beginnend mit dem Vertrauensverhältnis vom CSP zum zentralen Identity-Dienst, von dort zu den einzelnen IdPs und schließlich zu den Benutzern. Diese Indirektion ist in Abbildung 3 dargestellt und wurde in [Xia02] beschrieben.

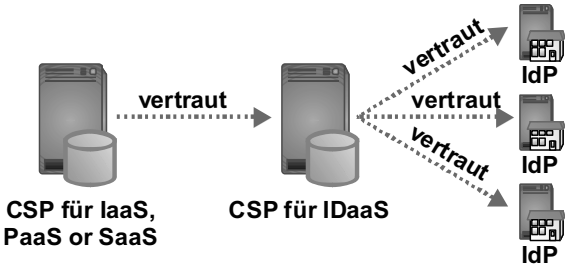

Abbildung 3: Mehrfache Indirektion des Vertrauens für AA in einer Föderation gemäß [Xia02].

1.5 Lokalisierung des Benutzers im Internet

Im Folgenden wird davon ausgegangen, dass der SAML-basierte Shibboleth Standard für die AA verwendet wird. Dieser bildet auch die Basis für unsere in Kapitel 2 vorgeschlagene Lösung für den föderativen Zugriff auf Speicher-Clouds. Shibboleth verwendet für die Lokalisierung des Benutzers, d.h. für die Ermittlung von dessen Heimatorganisation einen sog. Discovery Service (DS). Der DS stellt eine Web-Seite mit fester und a priori bekannter URL bereit, auf die der Benutzer zugreift. Während des Zugriffs auf den SP wird der Benutzer auf diese Web-Seite umgeleitet. Auf der Anmelde-Web-Seite wird dem Benutzer eine Liste von Organisationen bzw. IdPs präsentiert, die an der Föderation teilnehmen. Der Benutzer wählt seine Heimatorganisation und damit auch den für ihn zuständigen IdP. Dann wird der Web-Browser des Benutzers über eine HTTP Redirection an denjenigen IdP weitergeleitet, bei dem er seinen Benutzernamen und Passwort eingeben muss, um die Authentifizierung durchzuführen. Sind mehrere Föderationen z.B. unter Verwendung von eduGAIN [EduG] zu einer sog. Konföderation zusammengefasst, ähnlich wie dies auch bei der bereits skizzierten Föderation von Speicher-Clouds der Fall ist, so werden die Discovery Services der Konföderation sowie der darin enthaltenen Föderationen kaskadiert, d.h., der Benutzer meldet sich im Sinne einer Anmeldehierarchie an.

Der Benutzer wählt hierbei zunächst im DS der Konföderation seine Föderation aus. Anschließend wird er an den DS dieser Föderation umgeleitet, bei dem er seine Heimatorganisation resp. seinen IdP selektiert. Diese Auswahl ist für einen WebDAV-Zugriff ohne Web-Browser nicht praktikabel. Der Benutzer wünscht sich hier, wie in Abbildung 2 dargestellt, eine direkte Anbindung in Form eines virtuellen Dateisystems, ohne beim Zugriff auf Verzeichnisse und Dateien zusätzlich einen Web-Browser öffnen zu müssen, bzw. zwischen Datei-Explorer und Web-Browser zu wechseln. Eine erneute separate Anmeldung für jeden Storage Provider, z.B. bei einer Aggregation mehrerer Dateisysteme über mehrere CSPs, wäre ebenfalls benutzerunfreundlich.

Zusätzlich versagt diese Methode, wenn sich die Zahl der IdPs in einer Speicher-Cloud schnell ändert, oder wenn die Zahl der Speicher-Clouds in einer Föderation zeitlich variiert. Für diesen komplizierteren Fall kann die AA über eine in [Xia01] beschriebene dynamischen Discovery-Prozedur erfolgen: Zuerst wählt der Benutzer, wie bereits beschrieben, den CSP an. Danach gibt er jedoch anstelle der Auswahl seiner Heimatorganisation als Benutzernamen direkt seine E-Mail-Adresse ein, und ein erweiterter Discovery Service sendet basierend auf der Domain der E-Mail Adresse eine DNS-Anfrage an den zuständigen DNS-Server. Das Ergebnis der Anfrage ist ein DNS NAPTR-Eintrag, in dem zuvor der für den Benutzer verantwortliche IdP verbucht wurde. Der NAPTR-Eintrag wird dann vom Cloud-Dienstleister ausgewertet und mit dessen Information der richtige IdP konsultiert, der die AA durchführt ([Xia02]). Durch die dynamische Discovery-Prozedur können Benutzer auch über die Grenzen einer Föderation hinweg lokalisiert werden. Dies wird in [Xia02] auch als dynamische Föderation bezeichnet.

Der geschilderte Vorgang ist in Abbildung 4 gezeigt. Der Benutzer erhält nach einmaliger erfolgreicher Anmeldung an seinem IdP über alle SPs innerhalb der dynamischen Föderation ein Single Sign-On.

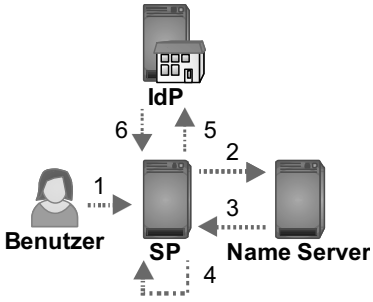

Abbildung 4: AA mit Hilfe eines DNS NAPTR-Eintrags in zeitlich veränderlichen Föderationen.

Das Konzept eignet sich auch für Benutzer, die mehrere Identitäten bei unterschiedlichen IdPs haben. Diese können durch die Angabe Ihrer E-Mail-Adresse selbst entscheiden, welche Identität sie bei der Anmeldung am SP verwenden wollen.

2 Zugang zu Speicher-Clouds mit Shibboleth und WebDAV

In diesem Kapitel wird die Architektur eines Shibboleth-fähigen WebDAV-Clients für den Zugang zu Föderationen von Speicher-Clouds beschrieben.

Der Client basiert auf einer Erweiterung des WebDAV-Clients Sardine [Sard], der als Open Source zur Verfügung steht, und ist als Swing-basierte Java-Anwendung realisiert. Der implementierte Prototyp erlaubt den Zugriff auf Dateiverzeichnisse, deren Inhalten, sowie das Kopieren einzelner Dateien zwischen WebDAV-Server und lokalem Rechner mittels „Drag & Drop“. Sardine benutzt den Apache HTTP Client [HC] für den Zugriff auf den Web-Server. Um eine AA per Shibboleth zu ermöglichen, wurde eine zusätzliche Methode für die Verbindung zum WebDAV-Server realisiert. Diese Methode verarbeitet die für Shibboleth erforderlichen Weiterleitungen (HTTP Redirects) bei der AA, sowie die Auswahl des IdPs unter Verwendung der in Kapitel 1.5 "Lokalisierung des Benutzers im Internet" erläuterten dynamischen Discovery-Prozedur. Dabei entfällt die manuelle Auswahl des IdPs und wird durch die automatisierte Ermittlung des zuständigen IdPs anhand der E-Mail-Adresse ersetzt. Die Methode extrahiert die SAML-Antwort (inkl. Relay State), die der IdP nach der erfolgreichen Authentifizierung des Benutzers erzeugt, und sendet diese (per SAML HTTP POST Profile) an den CSP zurück. Ferner wurde Sardine von uns um eine Sitzungsverwaltung erweitert, die die vom SP und vom IdP erstellten HTTP-Sitzungs-Cookies [rfc2965] während der Verwendung des Clients analog zur Sitzungsverwaltung eines Web-Browsers speichern.

Dadurch wird ein Single Sign-On sowohl über unterschiedliche CSPs als auch über die Grenzen einzelner Clouds hinweg realisiert. Die Autorisierung der Benutzer erfolgt anhand von Attributen, die der IdP an den jeweiligen SP übermittelt. Diese Attribute können in unterschiedlichen im Apache Web-Server konfigurierten sog. Locations, die die WebDAV Verzeichnisstruktur abbilden, oder im SP selbst für die Autorisierung verwendet werden.

Die skizzierte Lösung kann mit gängigen Web-Servern wie z.B. Apache oder Microsoft IIS für den WebDAV-basierten Zugriff auf entfernte Dateien und Verzeichnisse verwendet werden. Innerhalb des für den Test unseres Prototyps verwendeten Apache Web-Servers sind hierfür die Module mod_dav und mod_davfs vorhanden. Für die Authentifizierung benutzt mod_dav wiederum das Apache Modul mod_auth und dessen Authentifizierungserweiterungen. Aus der Sicht des Apache Servers bildet der Shibboleth SP eine solche Authentifizierungserweiterung (mod_shib). Verwendet man diese für eine Location des Apache Web-Servers, die mittels mod_dav für WebDAV eingerichtet wurde, so wird der Benutzer beim ersten Zugriff mit einem Web-Browser auf diese Location automatisch an den Discovery Service und von dort nach entsprechender Auswahl an den IdP seiner Heimatorganisation weitergeleitet. Nach erfolgreicher AA erfolgt eine Umleitung zurück an den SP. Dieser erlaubt, sofern die Zugriffsrechte vorhanden sind, den Zugriff auf die in der Location vorhanden Verzeichnisse und Dateien. Veränderungen an den Dateien und Verzeichnissen sind mit gängigen Web-Browsern allerdings nicht möglich. Hierfür wird unser WebDAV-Client benutzt.

Um ein Funktionieren auch bei zeitlich veränderlichen Föderationen über Speicher-Clouds zu ermöglichen, verfügt jeder IdP und SP über einen sog. Trust Estimation Service (TES) [Xia01]. Der TES wurde von uns als Erweiterung in Shibboleth integriert. Wie Abbildung 5 zeigt, fungiert der TES für Shibboleth wie ein externer Discovery Service. Der TES ist als standalone Tomcat-Anwendung implementiert und wurde mit den Standard-Shibboleth Komponenten verbunden.

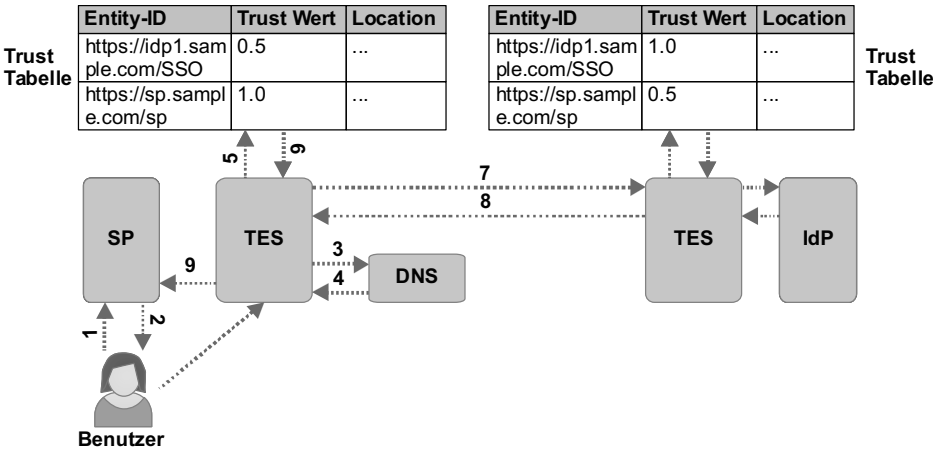

Abbildung 5: Integration eines sog. Trust Estimation Service in die Shibboleth.

Die Benutzeroberfläche der erreichten Lösung ist in Abbildung 6 dargestellt.

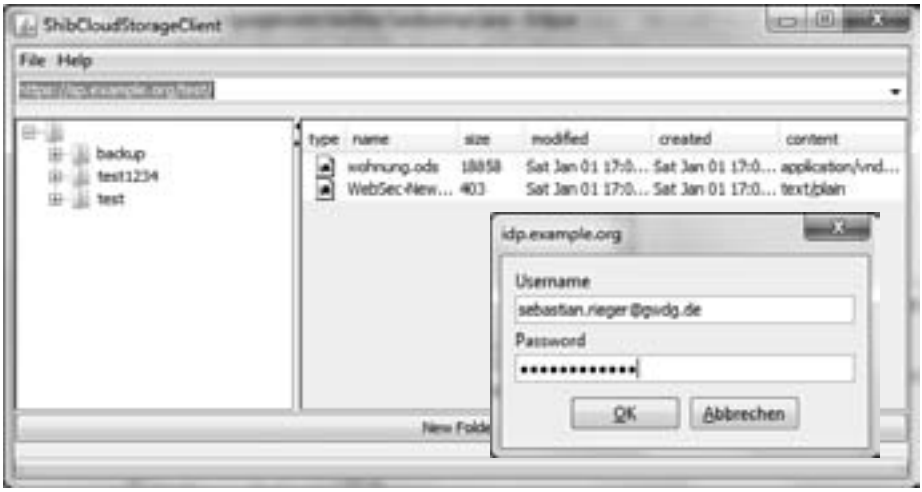

Abbildung 6: Benutzeroberfläche für den Zugang zu Föderationen von Speicher-Clouds.

3 Fazit und Ausblick

Die vorgestellte Lösung ermöglicht eine einheitliche Authentifizierung für Speicher-Clouds. Der implementierte Shibboleth-fähige WebDAV-Client erlaubt dabei durch die Verwendung einer dynamischen Discovery-Prozedur ein Single Sign-On über mehrere Cloud Storage Provider, d.h. mehrere Speicher-Clouds hinweg. Das Lesen und Schreiben auf den Online-Festplatten erfolgt durch die Verwendung von WebDAV ähnlich wie in einem virtuellen Dateisystem. Dies ermöglicht einen einheitlichen Zugriff auf verteilte Dateisysteme für die Realisierung von standortübergreifenden Speicher-Clouds, wie sie beispielsweise innerhalb der MPG-AAI [MPAAI] und Nds-AAI [NAAI] geplant sind. In Zukunft wird evaluiert, wie die Abbildung von Benutzernamen auf eindeutige IDs für die Zugriffsrechte des Dateisystems ohne die explizite Verlagerung der Autorisierung in den Web-Server oder in den Shibboleth-fähigen Service Provider realisiert werden kann. Darüber hinaus soll geprüft werden, inwieweit sich objektbasierte Online-Filesysteme (z.B. auf Basis von NoSQL-Datenbanken) für die Integration in ein virtuelles Dateisystem bei Föderationen von Speicher-Clouds eignen, die für ihre Datenreplikation bereits global eindeutige Identifikation verwenden (vgl. das virtuelle Dateisystem GridFS für MongoDB [Monfs]).

Literaturverzeichnis

[ACL] Access Control List: http://de.wikipedia.org/wiki/Access_Control_List (6. Januar 2011).

[Azure] Windows Azure Storage: http://www.microsoft.com/windowsazure/windowsazure/ (6. Januar 2011).

[BeB06] Bellembois, T.; Bourges, R.: The open-source ESUP-Portail WebDAV storage solution, http://www.esup-portail.org/download/attachments/43515911/ESUP-Web-DAV.pdf (6. Januar 2011).

[CDMI] Cloud data management interface. SNIA Web Site, April 2010: http://cdmi.sniacloud.com/ (6. Januar 2011).

[DAAI] DFN-AAI – Authentifikations- und Autorisierungs-Infrastruktur: https://www.aai.dfn.de (6. Januar 2011).

[DB] Dropbox: http://www.dropbox.com/ und http://de.wikipedia.org/wiki/Dropbox (6. Januar 2011).

[EduG] eduGAIN: http://www.edugain.org/ (6. Januar 2011).

[Frei10] Freitag, S: Erweiterung einer D-Grid-Ressource um eine Compute-Cloud-Schnittstelle. In (Müller, P.; Neumair, B.; Dreo Rodosek, G., Hrsg.): Proc. 3. DFN-Forum Kommunikationstechnologien, Konstanz 2010. Gesellschaft für Informatik, Bonn, 2010; S. 13-22.

[GS] Google Storage: http://code.google.com/intl/de-DE/apis/storage/ (6. Januar 2011).

[HC] Apache HttpComponents: http://hc.apache.org/ (6. Januar 2011).

[iRODS] Zhang, S.; Coddington, P.; Wendelborn, A.: Davis: A generic interface for iRODS and SRB, 10th IEEE/ACM International Conference on Grid Computing, Banff, 2009.

[Mdav] Apache Module mod_dav: http://httpd.apache.org/docs/2.0/mod/mod_dav.html (6. Januar 2011).

[Monfs] MongoDB GridFS Specification: http://www.mongodb.org/display/DOCS/GridFS+Specification (6. Januar 2011).

[Mor04] Morgan, R. L.; Cantor, S.; Hoehn, W.; Klingenstein, K.: Federated Security: The Shibboleth Approach, EDUCAUSE Quarterly, Vol. 27, 2004, S. 12-17.

[MAAI] Max-Planck-Gesellschaft - MPG-AAI: https://aai.mpg.de (6. Januar 2011).

[MZ] Mozy: http://mozy.com und http://en.wikipedia.org/wiki/Mozy (6. Januar 2011).
[NA07] Ngo, L.; Apon, A.: Using Shibboleth for Authorization and Authentication to the Subversion Version Control Repository System, Fourth International Conference on Information Technology - ITNG '07, Las Vegas, 2007.
[NAAI] Nds-AAI: Authentifizierungs- und Autorisierungs-Infrastruktur für Niedersachsen: http://www.daasi.de/projects/ndsaai.html (6. Januar 2011).
[REST] Roy T. Fielding. Architectural Styles and the Design of Network-based Software Architectures. PhD thesis, University of California, Irvine, 2000 und http://de.wikipedia.org/wiki/Representational_State_Transfer (6. Januar 2011).
[rfc2965] Kristol, D.; Montulli, L.: HTTP State Management Mechanism, ftp://ftp.rfc-editor.org/in-notes/rfc2965.txt (6. Januar 2011).
[rfc4918] Dusseault, L. et al.: HTTP Extensions for Web Distributed Authoring and Versioning (WebDAV), ftp://ftp.rfc-editor.org/in-notes/rfc4918.txt (6. Januar 2011).
[S3] Amazon Simple Storage Service (Amazon S3), http://aws.amazon.com/de/s3/, abgerufen am: 6.1.2011.
[SAML] OASIS: Security Services (SAML) TC: www.**oasis**-open.org/committees/security/ (6. Januar 2011).
[Sard] sardine - an easy to use webdav client for java: http://code.google.com/p/sardine/ (6. Januar 2011).
[Sch08] DataFinder: A Python Application for Scientific Data Management, EuroPython 2008: The European Python Conference, Vilnius, 2008.
[SID] Security Identifier: http://de.wikipedia.org/wiki/Security_Identifier (6. Januar 2011).
[SNIA] Storage Networking Industry Association: http://www.snia.org und http://de.wikipedia.org/wiki/Storage_Networking_Industry_Association (6. Januar 2011).
[UID] Benutzerkennung: http://de.wikipedia.org/wiki/Benutzerkennung (6. Januar 2011).
[UO] Ubuntu one: https://one.ubuntu.com/ (6. Januar 2011).
[WALR] Interacting with Walrus (2.0) - Storage Service: http://open.eucalyptus.com/wiki/EucalyptusWalrusInteracting_v2.0 (6. Januar 2011).
[Xia01] Xiang, Y.; Kennedy, J.A.; Richter, H.; Egger, M.: Network and Trust Model for Dynamic Federation, The Fourth International Conference on Advanced Engineering Computing and Applications in Sciences, Florence, 2010.
[Xia02] Xiang, Y.; Rieger, S.; Richter, H.: Introducing a Dynamic Federation Model for RESTful Cloud Storage, The First International Conference on Cloud Computing, GRIDs, and Virtualization, Lisbon, 2010.