EGIZ

www.egiz.gv.at
E-Mail: post@egiz.gv.at
Telefon: ++43 (316) 873 5514
Fax: ++43 (316) 873 5520
Inffeldgasse 16a / 8010 Graz / Austria

eID und Sicherheit in der Cloud

Version 1.0, 20. Dezember 2012

Bernd Zwattendorfer – Bernd.Zwattendorfer@egiz.gv.at

Zusammenfassung:

Die sichere Identifizierung und Authentifizierung von Bürgerinnen bzw. Bürgern spielen im Rahmen von E-Government eine wichtige Rolle. Nachdem auch immer mehr Anwendungen – auch aus dem E-Government Bereich – in die Cloud verlagert werden, ist ein sicheres Identitätsmanagement auch in der Cloud ein essentielles Thema. Identitätsmanagement ist keine speziell neue Thematik, durch den Einsatz in der Cloud ergeben sich jedoch neue Probleme sowie Möglichkeiten. Aufbauend auf bestehenden Identitätsmodellen werden in diesem Dokument unterschiedliche Cloud Identitätsmodelle vorgestellt. Ein Fokus wird dabei auf das „Identity as a Service"-Modell gelegt, bei dem ein zentraler Identity Broker in der Cloud mehrere Identity Provider und Service Provider bedienen kann. Obwohl dieses Modell die meisten Vorteile der vorgestellten Cloud Identitätsmodelle besitzt, hat es einen entscheidenden Nachteil. In diesem Modell müssen nämlich sowohl Benutzerinnen bzw. Benutzer als auch der Service Provider für eine Identifizierung bzw. Authentifizierung ein geeignetes Vertrags- und Vertrauensverhältnis mit demselben Identity Broker besitzen. Abhilfe dagegen schafft eine Modell mit föderierten Identity Brokern („Federated Identity as a Service"-Modell), welches abschließend als neuer Ansatz vorgestellt wird.

Inhaltsverzeichnis:

Abbildungsverzeichnis

Revision History

Version	Datum	Autor(en)	
0.1	03.12.2012	Bernd Zwattendorfer	Dokumenterstellung
1.0	20.12.2012	Bernd Zwattendorfer	Fertigstellung

1 Einleitung

Das Identitätsmanagement und die sichere Authentifizierung von Bürgerinnen und Bürgern stellen im Wesentlichen keine neuen Herausforderungen dar. Im Rahmen des österreichischen E-Governments haben sich bereits bewährte Konzepte und Infrastrukturen, wie beispielsweise die österreichische Bürgerkarte oder der Portalverbund, etabliert. Generell stellen die sichere Identifizierung und Authentifizierung häufig vorkommende und notwendige Prozesse dar, um Benutzerinnen bzw. Benutzern Zugriff auf ein bestimmtes Service oder eine bestimmte Ressource gewähren zu können, welche üblicherweise nicht für die Allgemeinheit bestimmt und frei zugänglich ist. Um Identitäten generell sicher zu verwalten, existieren bereits seit Jahren einige Ansätze. Angefangen von LDAP [LDAP], Kerberos [Kerberos], über Web-basierte Ansätze wie SAML [SAML] oder Shibboleth[1] um nur einige Beispiele zu nennen. Aber auch zahlreiche EU-Projekte haben sich bereits mit der sicheren Verwaltung von Identitäten befasst. Bekannte Projekte sind FIDIS[2], PRIME[3] oder PrimeLife[4], im grenzüberschreitenden Kontext vor allem STORK[5] bzw. aktuell STORK 2.0[6].

Die meisten dieser Identitätsmanagement-Ansätze verwenden einen sogenannten Identity Provider, der Identitäts- sowie Authentifizierungsdaten einer Benutzerin bzw. eines Benutzers einem Service Provider, welcher geschützte Ressourcen nur nach sicherer Identifizierung und Authentifizierung bereitstellen möchte, zur Verfügung stellt. Über die Jahre haben sich auch unterschiedliche Ansätze für die Verwendung eines Identity Providers herauskristallisiert. In Abschnitt 2 werden gängige traditionelle Identitätsmodelle beschrieben.

Nachdem Cloud Computing immer mehr an Wichtigkeit gewinnt, spielt ein sicheres Identitätsmanagement auch bei Cloud Applikationen eine essentielle Rolle. Im Rahmen des Cloud Computing haben sich deshalb auch bereits unterschiedliche Cloud Identitätsmodelle entwickelt, welche im Abschnitt 3 genauer vorgestellt werden. Als das Modell mit den meisten Vorteilen hat sich das „Identity as a Service“-Modell herauskristallisiert. In diesem Modell arbeitet der Identity Provider vollständig in der Cloud, wodurch die Vorteile des Cloud Computing am besten ausgenützt werden können. Dieses Modell, welches auch als Identity Broker-Modell bezeichnet wird, wird in Abschnitt 4 detaillierter diskutiert.

Das Cloud Identity Broker-Modell, in dem der Identity Broker mehr oder weniger als Hub zwischen ein oder mehreren Identity Providern bzw. Service Providern als Intermediär agiert, hat jedoch einen entscheidenden Nachteil. Benutzerinnen bzw. Benutzer und der Service Provider müssen beide ein Vertrauens- bzw. Vertragsverhältnis mit demselben Identity Broker besitzen, damit eine Identifizierung bzw. Authentifizierung stattfinden kann. Dadurch entsteht eine starke Abhängigkeit zum zentralen Identity Broker, sowohl für Benutzerinnen bzw. Benutzer als auch für den Service Provider. Um diesen Nachteil entgegen zu wirken, wird in Abschnitt 5 ein föderierter Ansatz von unterschiedlichen Identity Brokern vorgestellt. Dabei können sowohl Benutzerinnen bzw. Benutzer als auch der Service Provider eine Affiliation zu jeweils einem anderen Identity Broker besitzen, und die Identity Broker tauschen Identitäts- und Authentifizierungsdaten untereinander aus. Dieses Modell behält dabei die Vorteile des Identity Broker-Modells, eliminiert dabei aber dessen Nachteile.

[1] http://shibboleth.net

[2] http://www.fidis.net

[3] https://www.prime-project.eu

[4] http://primelife.ercim.eu

[5] https://www.eid-stork.eu

[6] http://www.eid-stork2.eu

2 Traditionelle Identitätsmodelle

Im Rahmen des Internets bzw. des WWW haben sich über die Jahre unterschiedliche Identitätsmodelle entwickelt, wie eine Identifizierung und Authentifizierung durchgeführt werden kann. Innerhalb dieses Abschnitts werden gängige Identitätsmodelle, wie sie derzeit im WWW Einsatz finden, vorgestellt.

In den meisten Fällen erfolgt die Identifizierung und Authentifizierung einer Benutzerin bzw. eines Benutzers über einen sogenannten Identity Provider, welcher die Identitäts- und Authentifizierungsdaten anschließend an einen Service Provider weiterleitet. Der Service Provider verwaltet in diesem Fall die geschützte Ressource bzw. Dienstleistung, auf welche die Benutzerin bzw. der Benutzer zugreifen möchte. Abhängig von den übermittelten Daten des Identity Providers erlaubt oder verweigert der Service Provider den Zugriff. Obwohl viele Identitätsmodelle im WWW auf diesem Ansatz mit Identity und Service Provider aufbauen, verfolgen nicht alle denselben methodologischen Ansatz. So gibt es beispielsweise Unterscheide, wo die Identitätsdaten der Benutzerin bzw. des Benutzers gespeichert werden. Basierend auf der Unterscheidung von Palfrey und Gasser [PaGa07] werden in diesem Abschnitt gängige und traditionelle Identitätsmodelle vorgestellt. Unterscheidungskriterium dabei ist der Speicherort der Identitätsdaten (zentral, benutzer-zentriert, oder föderal).

2.1 Zentraler Ansatz

In diesem Identitätsmodel werden die Identitätsdaten von Benutzerinnen und Benutzern in einer zentralen Datenbank entweder beim Identity Provider oder beim Service Provider, welcher dann gleichzeitig die Funktion eines Identity Providers übernimmt, gespeichert und verwaltet. Bevor eine Benutzerin bzw. ein Benutzer ein Service nutzen kann, muss sie bzw. er sich erfolgreich beim Service bzw. Identity Provider registrieren. Nach erfolgreicher Registrierung kann eine Benutzerin bzw. ein Benutzer die gewünschten Dienstleistungen in Anspruch nehmen. Die Authentifizierung erfolgt dabei über den Identity Provider, welcher nach erfolgreicher Authentifizierung die Identitäts- und Anmeldedaten der Benutzerin bzw. des Benutzers an den Service Provider weiterleitet. Da in diesem Fall die Daten der Benutzerin bzw. des Benutzers zentral beim Identity Provider verwaltet werden, hat die Benutzerin bzw. der Benutzer keinen Einfluss darauf, welche Daten wirklich vom Identity Provider zum Service Provider übertragen werden. Abbildung 1 veranschaulicht dieses zentrale Identitätsmodell. Typische Vertreter, die dieses Identitätsmodell umsetzen, sind etwa Google Accounts Authentication[7] oder Facebook[8].

[7] https://developers.google.com/accounts/

[8] http://facebook.com/

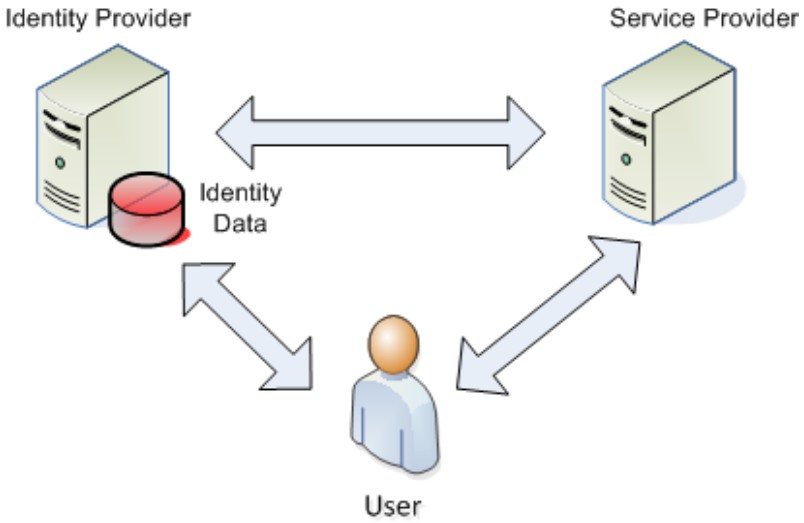

Abbildung 1 - Zentrales Identitätsmodell

2.2 Benutzer-zentrierter Ansatz

In diesem Modell bleibt die Benutzerin bzw. der Benutzer immer im Besitz ihrer bzw. seiner Identitätsdaten. Die Identitätsdaten werden dabei in der Umgebung des Benutzers, z.B. auf einer Smart Card, gespeichert und die Benutzerin bzw. der Benutzer stimmt explizit zur Weitergabe der Daten an den Service Provider zu. Typische Implementierungsbeispiele für dieses Modell wären einzelne eID Systeme unterschiedlicher Länder, wie es beispielsweise auch die österreichische Bürgerkarte darstellt. Wesentlicher Vorteil dieses Modells ist, dass ein direkter Kommunikationskanal zwischen der Benutzerin bzw. dem Benutzer und dem Service Provider entsteht, sodass eine Ende-Zu-Ende-Sicherheit gewährleistet werden kann. Abbildung 2 veranschaulicht wiederum dieses benutzer-zentrierte Modell.

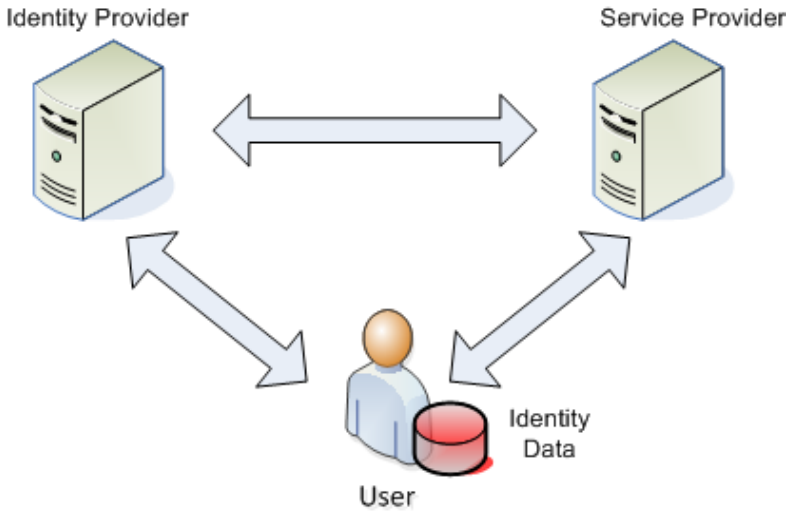

Abbildung 2 - Benutzer-zentriertes Identitätsmodell

2.3 Föderierter Ansatz

Beim föderierten Identitätsmodell sind die Identitätsdaten der Benutzerin bzw. des Benutzers über mehrere Identity Provider verteilt gespeichert. Die Identity Provider sind dabei über geeignete Vertrauensverhältnisse auf organisatorischer Ebene miteinander verknüpft. Üblicherweise sind die Datenbanken der einzelnen Identity Provider, die die Identitätsdaten der Benutzerin bzw. des Benutzers gespeichert haben, so miteinander verknüpft, dass Daten

einfach zwischen den Identity Providern ausgetauscht werden können. Die Zuordnung der Daten zu einer Benutzerin bzw. zu einem Benutzer erfolgt dabei meistens über einen gemeinsamen Identifikator. Shibboleth ist ein bekanntes und vor allem im universitären Bereich breit eingesetztes Konzept, welches sich des föderierten Ansatzes bedient. Abbildung 3 illustriert diesen Ansatz mit den verteilt gespeicherten Identitätsdaten.

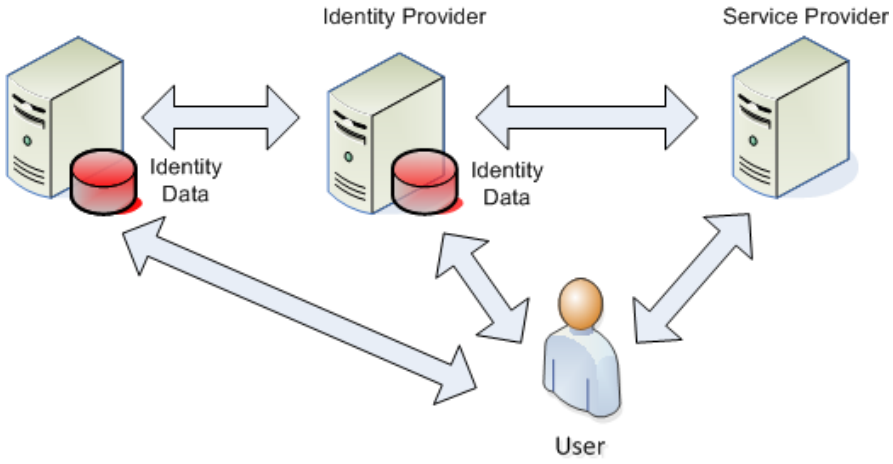

Abbildung 3 - Föderiertes Identitätsmodell

3 Cloud Identitätsmodelle

Identitäten und Authentifizierung spielen jedoch nicht nur bei klassischen Web Applikationen, sondern auch in der Cloud eine gewichtige Rolle. Die klassischen bzw. traditionellen Modelle können daher auch teilweise in die Welt der Clouds übertragen werden. Gopalakrishnan [Go09] oder Cox [Co12] klassifizieren beispielsweise solche Cloud Identitätsmodelle in ihren Publikationen. Unterscheidungskriterium ist hauptsächlich, wo Identitätsdaten von Benutzerinnen und Benutzern verwaltet werden.

Gopalakrishnan schlussfolgert, dass drei unterschiedliche Identitätsmanagement-Konzepte in der Cloud unterschieden werden können. Das erste Konzept (Trusted IDM Pattern) sieht vor, dass das Identitätsmanagement-System bzw. der Identity Provider in der vertrauenswürdigen Umgebung des Cloud Service Providers, der auch die entsprechende Applikation hostet, läuft. Dieses Konzept eignet sich eher für kleine und nicht hoch-skalierbare Clouds, wie es z.B. eine Private Cloud darstellen kann. Im Gegensatz dazu sieht sie das zweite Konzept (External IDM Pattern) eher für hoch-skalierbare Clouds, also Public Clouds, geeignet. In diesem Konzept wird das Identitätsmanagement-System bzw. der Identity Provider extern zur Cloud betrieben. Dabei werden die Identitätsdaten vom externen Identity Provider über eine definierte Schnittstelle, wie es z.B. SAML [SAML] ist, an den Cloud Service Provider übergeben. Das dritte von ihr vorgestellte Identitätsmanagement-Konzept in der Cloud wird als „Interoperable IDM Pattern“ bezeichnet. Das Identitätsmanagement-System bzw. der Identity Provider unterstützt dabei mehrere unterschiedliche Authentifizierungsmechanismen und -technologien und kann breit von mehreren Cloud Service Providern eingesetzt werden.

Im Gegensatz zu dieser Klassifizierung beschäftigt sich Cox [Co12] nur mit Identitätsmodellen für die Public Cloud. Seiner Meinung nach ist ein Identitätsmanagement im Rahmen einer Private Cloud trivial, da das Identitätsmanagement-System bzw. der Identity Provider unter der Obhut der Organisation, welche die Private Cloud betreibt, steht und somit kein externes Vertrauensverhältnis zu anderen Identity Providern besteht. Im Wesentlichen definiert Cox vier unterschiedliche Modelle und legt den Schwerpunkt bei der Klassifizierung auf die Bereitstellung von Identitäten. In seinem ersten Modell erstellt und managet der Cloud Service Provider die Identitäten für das Unternehmen, welches ein Cloud Service in Anspruch nimmt. Es gibt dabei keine externe Verknüpfung zu Benutzerinnen- bzw. Benutzer-Daten des Unternehmens. Das zweite Modell von Cox behandelt die Synchronisation von Identitäten bzw. Benutzerinnen- oder Benutzer-Daten. Dabei werden die Identitätsdaten des Unternehmens in das Identitätsmanagement-System des Cloud Service Providers übernommen. Es erfolgt also ein Transfer der Daten des Unternehmens zum Cloud Service Provider. Das dritte Modell bedient sich eines föderierten Ansatzes, welcher bereits bei den traditionellen Modellen in Abschnitt 2.3 beschrieben wurde. In diesem Fall werden die Identitätsdaten immer noch von der Organisation selbst in ihrer Umgebung verwaltet, die Daten jedoch über eine externe Schnittstelle dem Cloud Service Provider zur Verfügung gestellt. Die bereits existierenden Identitätsdaten von Benutzerinnen und Benutzern beim Cloud Service Provider werden dabei mit den bei der Organisation verwalteten Identitätsdaten verknüpft. Das vierte Modell von Cox ist ähnlich dem dritten Modell von Gopalakrishnan (Interoperable IDM Pattern), dass im Wesentlichen alle Eigenschaften der drei anderen von Cox vorgestellten Modelle vereinheitlicht.

Neben Gopalakrishnan und Cox hat sich auch Goulding [Go10] in einem Whitepaper mit unterschiedlichen Identitätsmodellen in der Cloud beschäftigt. Er trifft dabei eine Unterscheidung nach Anwendungsfällen, je nach dem von welchem Provider die Identitätsdaten bereitgestellt werden. Beim ersten Modell werden die Identitätsdaten von einer Organisation über eine externe Schnittstelle dem Cloud Service Provider bereitgestellt. Im zweiten Modell wird das Identitätsmanagementsystem des Cloud Service Provider um die

Identitätsdaten der Organisation ergänzt. In seinem dritten Modell werden die Identitätsdaten von einem Cloud Service Provider, der sich besonders auf ein Identitätsmanagement spezialisiert hat, von der Cloud mehreren unterschiedlichen Service Providern bereitgestellt.

Auch die Cloud Security Alliance (CSA) [CSA11] hat sich mit unterschiedlichen Architekturen für ein Identitätsmanagement in der Cloud befasst. Im sogenannten „Hub-and-Spoke“-Modell werden Identitäten von einem zentralen Broker bzw. Proxy verwaltet, der auch mehrere unterschiedliche Identity Provider und Service Provider vereint. Im „Free-Form“-Modell ist der Service Provider selbst für die Verwaltung von Identitäten bzw. unterschiedlichen Identity Providern verantwortlich. Das dritte von der CSA beschriebene Modell ist ein hybrider Ansatz, der die Vorteile des „Hub-and-Spoke“-Modells und des „Free-Form“-Modells vereint.

Im Folgenden werden die beschriebenen unterschiedlichen Cloud Identitätsmodelle als Basis herangezogen und eine Einteilung in drei Modelle getroffen. Für diese unterschiedlichen Modelle existieren bereits Implementierungen, welche auch in den entsprechenden Unterabschnitten erwähnt werden. Zusätzlich zu der Unterscheidung werden auch Vor- und Nachteile der einzelnen Modelle diskutiert.

3.1 Identität in der Cloud

Das Modell „Identität in der Cloud“ ist das einfachste Cloud Identitätsmodell. In diesem Modell übernimmt der Cloud Service Provider, der auch die Cloud Applikation hostet, die Funktion und Rolle des Identity Providers. Der Cloud Service Provider besitzt also sein eigenes Identitätsmanagement-System, welches die Identifizierung und Authentifizierung für die Cloud Applikationen regelt. Somit sind die Identitätsdaten *in der Cloud* gespeichert. Abbildung 4 veranschaulicht dieses „Identität in der Cloud“-Modell.

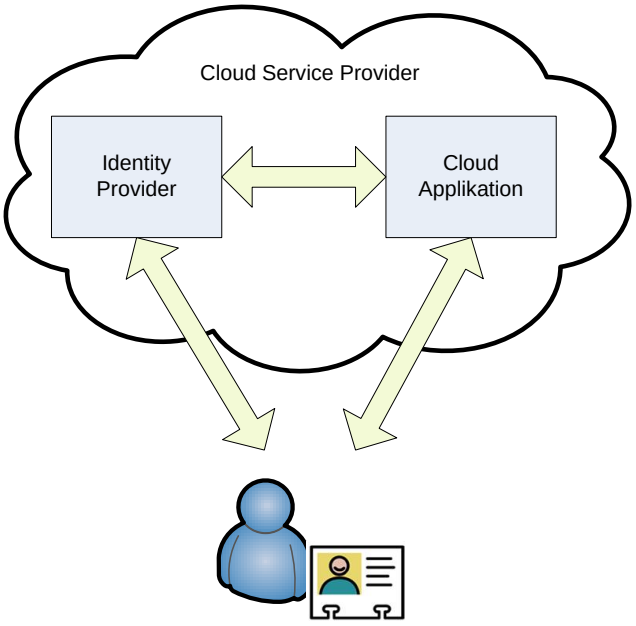

Abbildung 4 - Identität in der Cloud

Dieses Modell kann als spezielles Modell des zentralen Ansatzes aus Abschnitt 2.1 angesehen werden, wo der Service Provider und Identity Provider quasi miteinander verschmelzen. Dieses Modell wird auch von Gopalakrishnan [Go09] und Cox [Co12] ausführlich diskutiert. Typische praktische Implementierungen dieses Modells sind die beiden Cloud Service Provider Google und Salesforce.com. Beide Cloud Service Provider

hosten und verwalten ihr eigenes Benutzerinnen- bzw. Benutzer-Management für ihre angebotenen Software as a Service[9] (SaaS) Applikationen.

Der wesentliche Vorteil dieses Modells ist, dass der Kunde oder die Organisation, welche Cloud Dienstleistungen bezieht, keine eigene Benutzerinnen- bzw. Benutzerverwaltung aufsetzen muss, sondern sich vollkommen auf das bestehende System des Cloud Service Providers verlassen kann. Die Nutzung dieses bestehenden Systems spart sowohl Kosten als auch wird der Wartungsaufwand verringert, da Accounts direkt beim Cloud Service Provider erstellt und gewartet werden. Nichtsdestotrotz ergibt sich dadurch der Nachteil, dass die Organisation weniger Kontrolle über die gespeicherten Benutzerinnen- bzw. Benutzerdaten besitzt, weil alle Daten beim Cloud Service Provider gespeichert werden. Ein zusätzlicher Aufwand kann entstehen, wenn die Identitätsdaten von einem bestehenden Identitätsmanagementsystem der Organisation mit dem System des Cloud Service Providers synchronisiert werden sollen. Dieser Fall wird von Cox [Co12] ausführlich diskutiert.

3.2 Identität zur Cloud

Beim „Identität zur Cloud“-Modell wird im Wesentlichen das traditionelle zentrale Identitätsmodell aus Abschnitt 2.1 in die Welt des Cloud Computing übertragen. In diesem Fall wird das Identitätsmanagement, welches vom Cloud Service Provider benötigt wird, an einen externen Identity Provider ausgelagert. Der einzige Unterschied zum traditionellen Identitätsmodell ist, dass es sich bei dem Service Provider nicht um einen klassischen Web-Dienstanbieter, sondern um einen cloud-basierten Dienstanbieter handelt. In weiterer Folge wird für dieses spezielle Modell angenommen, dass der Identity Provider wie im traditionellen Identitätsmodell nicht cloud-basierend ist. Der Fall des Identitätsmodells mit cloud-basiertem Identity Provider wird im nächsten Abschnitt 3.3 genauer behandelt. Der Fall des „Identität zur Cloud“-Modells wird in Abbildung 5 illustriert.

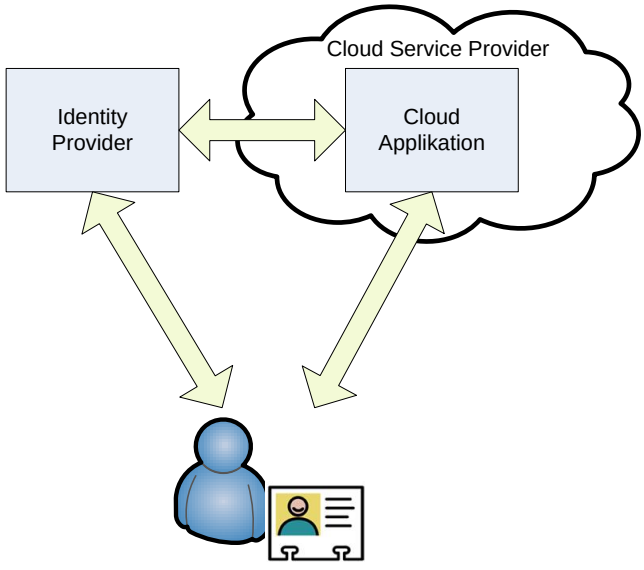

Abbildung 5 - Identität zur Cloud

In diesem Modell ist der Identity Provider für die komplette Benutzerinnen- bzw. Benutzerverwaltung verantwortlich, also z.B. für das Erstellen oder Entfernen von Identitäten und Accounts, Benutzerinnen- bzw. Benutzerauthentifizierung, etc. Der Cloud Service Provider ist hingegen nur für die Cloud Applikation verantwortlich und konsumiert Identitätsdaten bzw. Identitätsinformationen vom externen Identity Provider. Anders

[9] Software as a Service (SaaS) bezeichnet ein Cloud Service Modell, wo Software vom Cloud Service Provider als Dienstleistung den Endkunden angeboten wird.

ausgedrückt, werden Identitätsdaten *zu der Cloud* transferiert. Der Transfer von Identitätsdaten zwischen dem Identity Provider und dem Cloud Service Provider erfolgt üblicherweise über standardisierte Schnittstellen und Protokolle. Protokolle, welche speziell für den sicheren Austausch von Identitäts- und Authentifizierungsinformationen ausgelegt sind, sind beispielsweise SAML [SAML], OpenID[10], oder OAuth[11].

Viele bestehende Cloud Service Provider, im besonderen Public Cloud Service Provider wie z.B. Google oder Salesforce.com, setzen bereits auf dieses Cloud Identitätsmodell mit der externen Identitätsbereitstellung. Sowohl Google als auch Salesforce.com setzen beispielsweise auf SAML oder OpenID für ihre externen Schnittstellen. Im Gegensatz zu Salesforce.com unterstützt Google auch noch eine externe Authentifizierung via OAuth. Die Verwendung solcher Schnittstellen ermöglicht nicht nur die Abbildung des zentralen Ansatzes traditioneller Identitätsmodelle, sondern auch des föderierten Ansatzes, wie er in Abschnitt 2.3 beschrieben ist. Ein Cloud Provider, welcher nicht nur auf externe Authentifizierung, sondern auch auf sichere Authentifizierung mittels eIDs setzt, ist Fabasoft. Fabasoft[12] unterstützt für ihre Cloud Applikation FolioCloud die Authentifizierung mittels Bürgerkarte, neuen deutschen Personalausweis, und SwissID.

Bei Anwendung dieses Modells ist der wesentliche Vorteil, dass bereits existierende Identitätsmanagement-Systeme z.B. einer Organisation oder eines Unternehmens für eine externe Identifizierung und Authentifizierung an Cloud Services wiederverwendet werden können. Im Gegensatz zum vorherigen Modell (Identität in der Cloud) ist kein neues Benutzerinnen- bzw. Benutzer-Management beim Cloud Service Provider oder eine Migration der Identitätsdaten zum Cloud Service Provider notwendig. Während die Applikation in der Cloud betrieben wird, bleibt das Identitätsmanagement unter der Obhut der jeweiligen Organisation. Ein Nachteil dieses Modells wäre beispielsweise die Interoperabilität (auf technischer aber auch semantischer Ebene) der zwischen den beiden Providern ausgetauschten Identitätsdaten. Aus diesem Grund setzen viele Provider auf standardisierte Schnittstellen. Obwohl solch standardisierte Schnittstellen ein gewisses Maß an Interoperabilität garantieren sollten, ergibt sich oft aufgrund der jeweiligen Implementierung ein unterschiedliches Verhalten. Dieses unterschiedliche Verhalten wurde bereits in einem anderen EGIZ-Projekt (MOAs in der Cloud [Zw12]) festgestellt und analysiert. Als weiterer Nachteil kann die Auswahl des Identitätsmanagement-Protokolls festgehalten werden, falls nur bestimmte Protokolle vom Cloud Service Provider unterstützt werden. Wird ein Protokoll nicht vom externen Identitätsmanagement-System der Organisation unterstützt, so kann es zu zusätzlichem Implementierungsaufwand und Kosten auf der Seite der Organisation bzw. des Unternehmens kommen. Semantische Interoperabilität könnte ein weiteres Problem darstellen, falls die vom externen Identity Provider zur Verfügung gestellten Attribute nicht vom Cloud Service Provider entsprechend verstanden bzw. interpretiert werden können. Hierfür ist ein spezielles Mapping bzw. gemeinsames Verständnis über die ausgetauschten Attribute zwischen Identity Provider und Cloud Service Provider notwendig.

3.3 Identität von der Cloud

In diesem dritten Cloud Identitätsmodell werden Identitäten von einem Identity Provider bereitgestellt, der selbst auch in der Cloud betrieben wird. Im Prinzip werden daher Identitäten *von der Cloud* einem Service Provider als Cloud Service zur Verfügung gestellt. Aus diesem Grund wird dieses Modell gerne auch als „Identity as a Service“-Modell bezeichnet. Das Modell „Identität von der Cloud“ ist in der folgenden Abbildung 6 dargestellt.

[10] http://openid.net

[11] http://oauth.net

[12] http://www.fabasoft.com

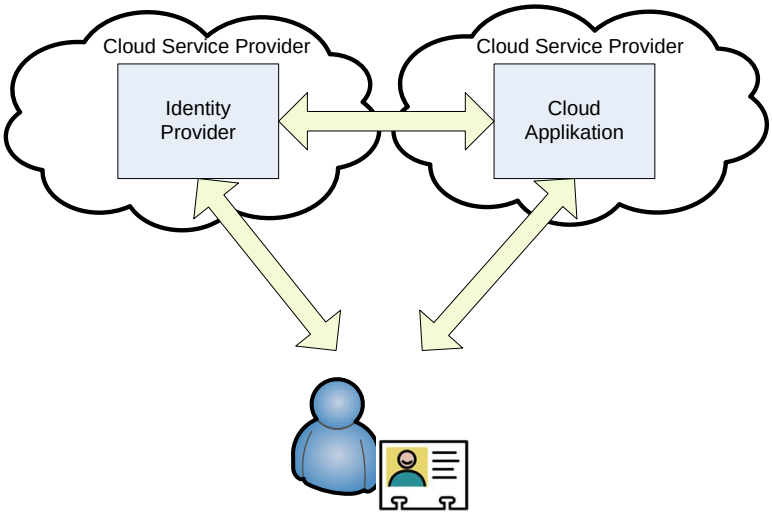

Abbildung 6 - Identität von der Cloud

In diesem Modell werden sowohl die Applikation als auch der Identity Provider in der Cloud betrieben. Im Gegensatz zum „Identität in der Cloud“-Modell aus Abschnitt 3.1 muss der Identity Provider nicht notwendigerweise vom selben Cloud Service Provider betrieben werden, der auch die Applikation hostet. Nichtsdestotrotz kann auch ein Cloud Service Provider sowohl Identity Provider als auch die Applikation betreiben. Die Vorbedingung ist jedoch, dass die Benutzerinnen- bzw. Benutzerverwaltung von der Applikation getrennt ist.

Im Allgemeinen ist dieses Cloud Identitätsmodell unabhängig vom darunterliegenden Cloud Deployment Modell. Im Prinzip kann dieses „Identity as a Service“-Modell in einer Public, Private, oder Community Cloud betrieben werden. Durch die mögliche Verknüpfung unterschiedlicher Cloud Deployment Modelle (Der Identity Provider kann mittels eines anderen Modells als der Cloud Service Provider betrieben werden.) kann dieses Modell auch als dein hybrides Cloud Deployment Modell angesehen werden. Obwohl hier nur ein Cloud Service Provider als Identitäten-konsumierende Applikation eingezeichnet ist, lässt sich dieses Modell auch auf traditionelle Web-basierende Applikationen anwenden.

Diese Modell bietet vor allem Kostenvorteile und weniger Wartungsaufwand, da das Identitätsmanagement an einen Cloud Service Provider, der sich auf das Identitätsmanagement als Service spezialisiert hat, ausgelagert wird. Der wesentliche Vorteil dieses Modelles ist jedoch die Trennung der Cloud Service Provider. Das heißt, dass der Cloud Service Provider der Applikation und der des Identity Providers nicht unbedingt ident sein müssen. Das erlaubt Organisationen eine größere Auswahlmöglichkeit, welchem Cloud Service Provider sie ihr Identitätsmanagement anvertrauen wollen. Gründe für die Wahl eines speziellen Identity Providers könnten beispielsweise die Einhaltung von Datenschutzregulierungen oder das Speichern der Identitätsdaten in einem gewünschten Land sein. Ein klarer Nachteil dieses Modells ist natürlich, dass Identitätsdaten in die Cloud ausgelagert werden und somit dem Cloud Service Provider ein hohes Maß an Vertrauen geschenkt werden muss. Zusätzlich ergibt sich das Problem, dass eventuell Identitätsdaten von der Organisation in die Cloud migriert und zum Cloud Service Provider transferiert werden müssen.

4 Cloud Identity Broker Modell

Das „Identity as a Service“-Modell ist ein vielversprechendes Modell für ein Identitätsmanagement in der Cloud. Im vorigen Abschnitt wurde nur ein allgemeiner Überblick und die generelle Idee dieses Modells präsentiert, dass Identitäten von der Cloud bereitgestellt werden. Bezieht man sich jedoch auf die Publikationen von der Cloud Security Alliance [CSA11] oder Huang [Hu10], so kann das „Identity as a Service“-Modell mehr als ein Identity Broker-Modell angesehen werden. In diesem Fall agiert der Identity Provider in der Cloud als zentraler Identity Broker zwischen mehreren Service und Identity Providern. Anders ausgedrückt, spielt der Identity Broker eine Art Hub zwischen mehreren Service und Identity Providern. Abbildung 7 gibt einen detaillierteren Überblick über dieses „Identity as a Service“-Modell mit zentraler Identity Broker-Funktionalität.

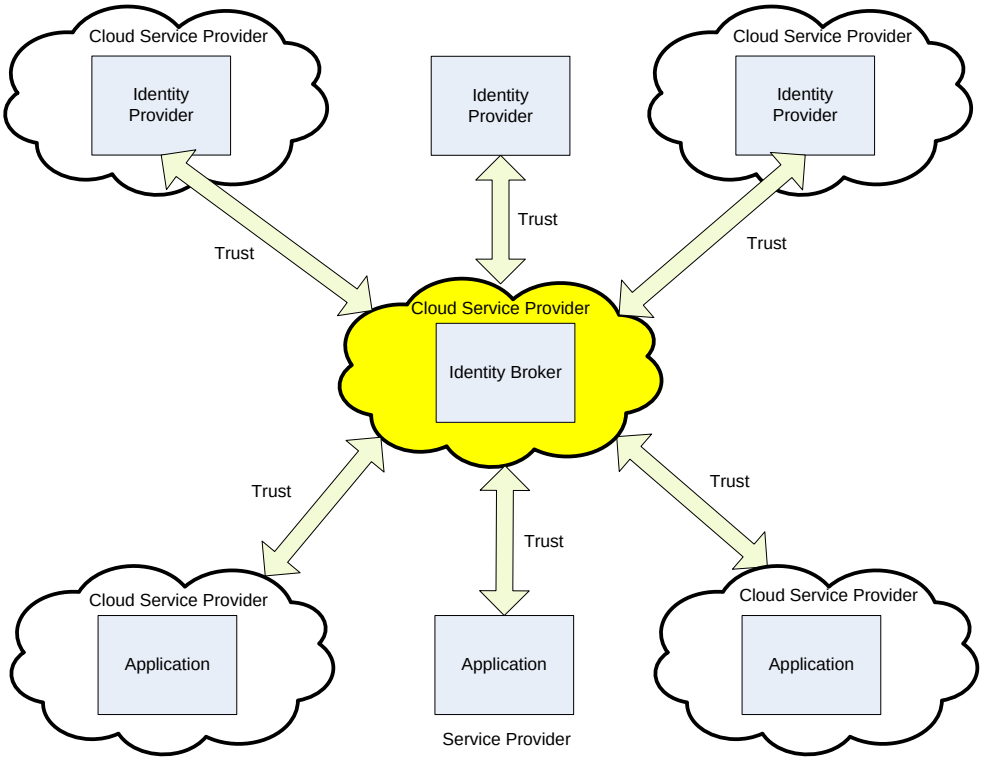

Abbildung 7 - Identity as a Service Modell mittels zentralem Identity Broker

Die Grundidee dieses Modells ist es, den Service Provider von mehreren und unterschiedlichen Identity Providern zu entkoppeln. Im Gegensatz zu Abhängigkeiten zu mehreren und unterschiedlichen Identity Providern hat ein Service Provider nur mehr eine starke Abhängigkeit zum Identity Broker. Dies hat Vorteile sowohl auf technischer als auch organisatorischer Ebene. Auf technischer Ebene muss der Service Provider nur das Kommunikationsprotokoll mit dem Identity Broker implementieren, andere Protokolle oder Schnittstellen für den Datenaustausch anderer Identity Provider kann er ignorieren. Die Implementierung anderer Protokolle bzw. die Kommunikation mit anderen Identity Providern übernimmt der Identity Broker. Um den Implementierungsaufwand beim Service Provider trotzdem so gering wie möglich zu halten, bietet der Identity Broker üblicherweise standardisierte Schnittstellen und Protokolle (z.B. SAML, OpenID, etc.) für den sicheren Datenaustausch an. Der Vorteil auf organisatorischer Ebene ist, dass unterschiedliche Vertrauensverhältnisse zwischen dem Service Provider und mehreren Identity Providern zu einem starken Vertrauensverhältnis zusammengefasst werden, nämlich zwischen dem Service Provider und dem Identity Broker. Der Identity Broker übernimmt in diesem Fall die unterschiedlichen Vertrauensverhältnisse mit den Identity Providern. Man kann auch den

Identity Broker als Vermittler für die Vertrauensverhältnisse zwischen dem Service Provider und den Identity Providern bezeichnen. Das Vorhandensein nur eines Vertrauensverhältnisses erleichtert das vertragliche Modell des Service Providers. Nichtsdestotrotz hat dieses Identity Broker Modell einen wesentlichen Nachteil. Bricht der Identity Broker zusammen oder ist aus irgendeinem Grund nicht erreichbar, so sind die Service Provider vom externen Identitätsmanagement-System abgeschnitten. Dieses Risiko ist aber jetzt nicht nur speziell auf dieses Modell zu beziehen, sondern kann auch in anderen, z.B. traditionellen Identitätsmodellen gefunden werden, wo die Identifizierung und Authentifizierung an einen externen Identity Provider ausgelagert wird.

Das Cloud Identity Broker Modell ist nicht neu und wurde bereits von mehreren Organisationen und Unternehmen implementiert. Als Beispiel dafür wäre das Produkt „Cloud SSO“[13] von Intel zu erwähnen, das eine fertige Implementierung des Identity Broker Modells bietet. Intel Cloud SSO offeriert eine starke Benutzerinnen- bzw. Benutzer-Authentifizierung bei über 100 unterschiedlichen SaaS-Applikationen sowie den Zugriff auf unterschiedliche Identity Provider bzw. Stores. Für dessen Realisierung setzt Intel auf bestehende und weitverbreitete Förderationsschnittstellen, die von den jeweiligen SaaS-Providern angeboten werden. Eine weitere Implementierung des Identity Broker-Modells sind die Resultate des SkIDentity[14]-Projekts. Das SkIDentity Projekt fokussiert sich speziell auf sichere Authentifizierungsmechanismen und eIDs, sodass beispielsweise Anmeldungen mittels österreichischer Bürgerkarte oder dem neuen deutschen Personalausweis bei Cloud Service Providern möglich sind. Unterschied zum Intel Cloud SSO Produkt ist hier, dass nicht auf bestehende Schnittstellen der Cloud Service Provider zurückgegriffen wird, sondern der Cloud Service Provider ein eigenes Konnektor-Modul für eine SkIDentity-Authentifizierung installieren muss. Andere Produkte, die auch dieses Identity Broker-Modell implementieren, sind beispielsweise RadiantOne's Cloud Federation Service[15], McAfee's Cloud Identity Manager[16], VMWare's Horizon[17], oder Fugen's Cloud ID Broker[18].

Obwohl dieses Modell viele Vorteile besitzt, so können auch einige Nachteile identifiziert werden. Ein wesentlicher Nachteil ist, dass sowohl Benutzerinnen bzw. Benutzer als auch der Service Provider sich beide auf den gleichen zentralen Identity Broker verlassen müssen. Das heißt, dass Benutzerinnen bzw. Benutzer und Service Provider ein Vertrauensverhältnis mit demselben Identity Provider, in diesem Fall dem Identity Broker, besitzen müssen. Betrachtet man nur die Vertrauensverhältnisse, so ist dieses Modell ähnlich dem traditionellen zentralen Identitätsmodell aus Abschnitt 2.1, welches paarweise Vertrauensverhältnisse verwendet. Ein vermitteltes Vertrauensverhältnis (Brokered Trust) kommt nur zwischen dem Service Provider und den unterschiedlichen Identity Providern ins Spiel.

Ein weiterer Nachteil dieses Modells ist, dass sowohl Benutzerinnen bzw. Benutzer als auch der Service Provider von den Funktionen und Eigenschaften des Identity Brokers abhängig sind. Einerseits sind Service Provider davon abhängig, welche Schnittstellen und Kommunikationsprotokolle der Identity Broker unterstützt. Stellt beispielsweise der Identity Broker den Support bzw. die Unterstützung für eine bestimmte Schnittstelle ein, so ist der Service Provider von dem Identity Service abgeschnitten und muss viel Aufwand einsetzen, um ein anderes Protokoll oder eine andere Schnittstelle zu implementieren. Andererseits sind auch Benutzerinnen bzw. Benutzer auf gewisse Art und Weise vom Identity Broker

[13] http://www.intelcloudsso.com

[14] http://www.skidentity.com

[15] http://www.radiantlogic.com/products/radiantone-cfs

[16] http://www.mcafee.com/uk/products/cloud-identity-manager.aspx

[17] http://www.vmware.com/products/desktop_virtualization/horizon-application-manager/overview.html

[18] http://fugensolutions.com/cloud-id-broker.html

abhängig, nämlich von der Anzahl und Art von Identity Providern, die der Identity Broker unterstützt. Möchte beispielsweise eine Benutzerin bzw. ein Benutzer sich über einen speziellen Identity Provider anmelden oder einen speziellen Authentifizierungsmechanismus einsetzen, welcher vom Identity Broker nicht unterstützt wird, so ist eine Anmeldung am Service Provider einfach nicht möglich. Die Benutzerin bzw. der Benutzer hat also nicht wirklich eine freie Entscheidungsmöglichkeit bei der Auswahl des Identity Providers und ist von der Unterstützung des Identity Brokers abhängig.

Um diesen Nachteilen entgegen zu wirken, wird ein neues Identitätsmodell für die Cloud vorgeschlagen. Dieses Modell setzt auf den traditionellen föderierten Ansatz wie in Abschnitt 2.3 beschrieben. Das sogenannte „Federated Identity as a Service“-Modell wird im folgenden Abschnitt genauer erläutert.

5 Federated Identity as a Service Modell

Das „Federated Identity as a Service“-Modell löst das Problem der Abhängigkeit von ein und demselben Identity Broker sowohl für Benutzerinnen bzw. Benutzer als auch für Service Provider. In diesem Modell müssen Benutzerinnen bzw. Benutzer und Service Provider nicht auf denselben Identity Broker für eine Authentifizierung setzen. Beide können eine Vertrags- und Vertrauensverhältnis mit unterschiedlichen Identity Brokern eingehen, was die Flexibilität erhöht. Die unterschiedlichen Identity Broker können auch jeweils auf die unterschiedlichen individuellen Bedürfnisse von Benutzerinnen bzw. Benutzern oder von Service Providern eingehen. Beispiele für solche Bedürfnisse wären nationale Regulierungen oder Gesetze. Obwohl kein direktes Vertrauensverhältnis mit ein und demselben Identity Broker für Benutzerinnen bzw. Benutzer und dem Service Provider besteht, so können sich durch Föderation der Identity Broker Benutzerinnen bzw. Benutzer trotzdem am Service Provider anmelden. Abbildung 8 zeigt dieses föderierte „Identity as a Service“-Modell.

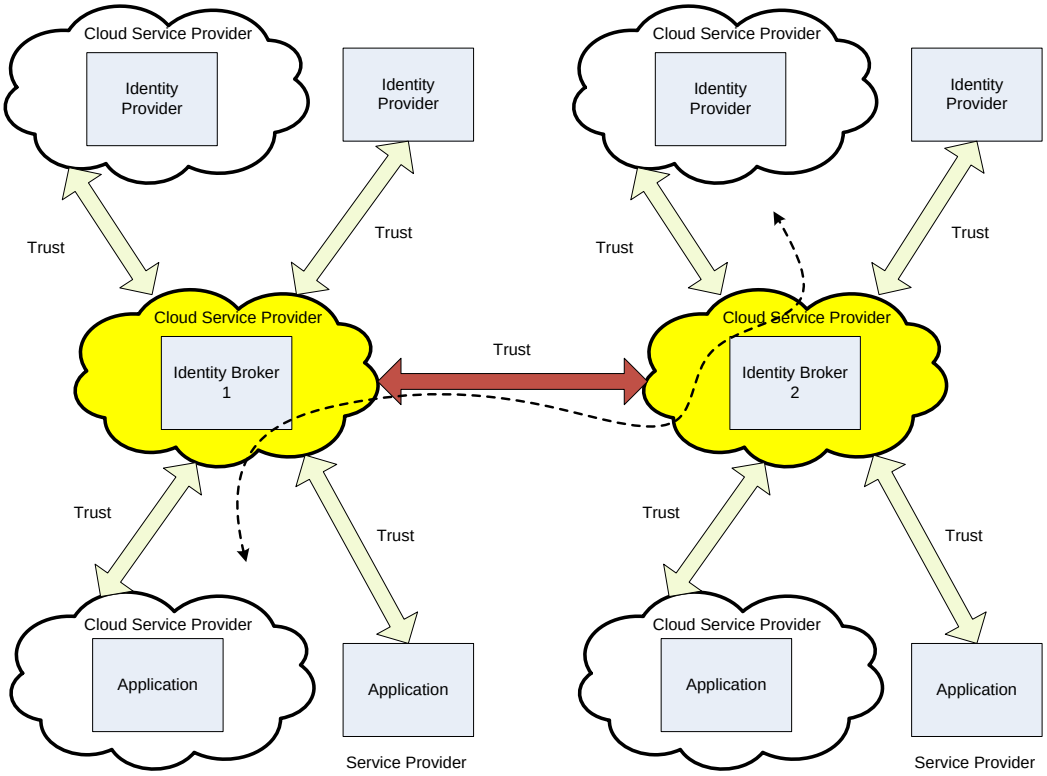

Abbildung 8 - Federated Identity as a Service Model

In diesem föderierten Ansatz ist es möglich, dass der Service Provider eine Vertragsbeziehung mit dem Identity Broker 1 besitzt, während die Benutzerin bzw. der Benutzer hingegen eine Vertragsbeziehung dem Identity Broker 2 hat. Beide Identity Broker haben ebenfalls ein entsprechendes Vertrauensverhältnis bzw. eine Vertragsbeziehung untereinander. Daher unterstützt dieses Modell das sogenannte „Brokered Trust Model“ [BoElKa+04] über mehrere Identity Broker.

Betrachtet man den Informations- und Prozessfluss aus Abbildung 8 etwas genauer, so kontaktiert eine Benutzerin bzw. ein Benutzer in einem ersten Schritt jenen Service Provider, von dem sie bzw. er eine geschützte Ressource oder Service nutzen möchte. Nachdem diese Ressource geschützt ist, wird von der Benutzerin bzw. dem Benutzer eine entsprechende Authentifizierung benötigt. Für eine entsprechende Identifizierung bzw. Authentifizierung besitzt der Service Provider ein Vertragsverhältnis mit dem Identity Broker 1. Im Gegensatz zu den meisten zuvor beschriebenen Identity Modellen, hat die Benutzerin

bzw. der Benutzer in diesem Modell kein Vertragsverhältnis mit demselben Identity Broker wie die Service Provider (Identity Broker 1), sondern mit dem Identity Broker 2. Dieser unterstützt im Gegensatz zum Identity Broker 1 jenen Identity Provider, den die Benutzerin bzw. der Benutzer auch für eine Authentifizierung bei dem ausgewählten Service Provider nutzen möchte. Um diesen Identity Provider auch nutzen zu können, wird die Benutzerin bzw. der Benutzer an Identity Broker 2 weitergeleitet. Danach initiiert der Identity Broker 2 den Identifizierungs- und Authentifizierungsprozess mit dem gewünschten Identity Provider. Die Benutzerin bzw. der Benutzer authentifiziert sich dabei beim Identity Provider mit seinem gewünschten Authentifizierungsmechanismus. War der Authentifizierungsvorgang erfolgreich, so werden entsprechende Identitäts- und Authentifizierungsdaten der Benutzerin bzw. des Benutzers an den Identity Broker 2 übermittelt. Anschließend leitet Identity Broker 2 die Daten an den Identity Broker 1 weiter, welcher sie schlussendlich an den Service Provider transferiert. Basierend auf den empfangenden Daten erlaubt bzw. verbietet der Service Provider den Zugriff auf die geschützte Ressource. Im Prinzip gibt es in diesem Modell drei Kommunikationskanäle, wo Identitätsdaten ausgetauscht werden, nämlich zwischen:

1. Identity Provider und Identity Broker 2
2. Identity Broker 2 und Identity Broker 1
3. Identity Broker 1 und Service Provider

Für den Kommunikationskanal zwischen Identity Provider und Identity Broker 2 bzw. Identity Broker 1 und Service Provider können einfach existierende Identitätsprotokolle wie z.B. SAML oder OAuth verwendet werden. Im Gegensatz dazu muss noch evaluiert werden, welches Identitätsprotokoll für den Kommunikationskanal zwischen Identity Broker 1 und 2 am besten geeignet ist bzw. ob nicht ein neues eigenständiges Protokoll designed werden sollte.

Im Folgenden zählen wir Anforderungen auf, die notwendigerweise erfüllt werden müssen, um so ein „Federated Identity as a Service“-Modell aufzubauen. Es wird dabei in funktionale, technische, organisatorische und ökonomische Aspekte unterschieden.

5.1 Funktionale Anforderungen

Auf jeden Fall müssen in diesem Modell die beiden Identity Broker Basis-Funktionalitäten eines Identitätsmanagements bereitstellen. Dazu gehören unter anderem die Registrierung von Benutzerinnen bzw. Benutzern, das Sammeln und Überprüfen von Attributen, sowie das Bereitstellen, Überprüfen und Verwalten von Authentifizierungsinformationen. Weiters ist die Vision dieses Modells, dass nicht nur natürliche Personen unterstützt werden, sondern auch juristische Personen. Vielmehr sollen damit nicht nur klassische Transkationen zwischen einer natürlichen Person und einem Service Provider, sondern auch andere Transaktionen z.B. zwischen zwei natürlichen Personen in diesem Netzwerk abgebildet werden.

Das dargestellte Modell sollte benutzer-zentriert ausgelegt sein und eine Authentifizierung sollte nicht unbedingt auf Basis von Attributen alleine, sondern eher auf Basis einzelner Claims erfolgen. Die Verwendung von Claims erlaubt es besonders die Privatsphäre von Benutzerinnen bzw. Benutzern zu schützen, da nur die minimalste Menge an persönlichen Informationen Preis gegeben wird (z.B. nur die Bestätigung, dass eine Benutzerin bzw. ein Benutzer älter als 18 ist anstatt des kompletten Geburtsdatums). Zusätzlich sollte von den einzelnen Identity Brokern Single Sign-On (SSO) unterstützt werden können.

5.2 Technische Anforderungen

Wesentliche technische Anforderungen sind Sicherheit sowie der Datenschutz der beteiligten Personen. Dafür ist die Verwendung eines entsprechenden Trust Protokolls notwendig, welches auch das „Brokered Trust Model“ entsprechend abbildet. Zusätzlich sollte bestehende Infrastruktur einfach wiederverwendet werden können und so gut es geht auf

bestehende Standards gesetzt werden. Die einzelnen Identity Broker sollen auch geeignete APIs bereitstellen, um Erweiterungen und eventuelle neue Geschäftsmodelle einfach zu ermöglichen. Abschließend kann auch gesagt werden, dass eine Implementierung eines solchen Modells unterschiedliche Clients einer Benutzerin bzw. eines Benutzers unterstützen sollte, um so auch eine gewisse Ortsunabhängigkeit zu gewährleisten.

5.3 Organisatorische Anforderungen

Die Verwendung von Standards ist nicht nur eine technische, sondern auch eine organisatorische Anforderung. Standards ermöglichen Interoperabilität. So sollte versucht werden, existierende Standards zu verwenden und keinen eigenen, zusätzlichen zu erfinden.

Auf organisatorischer Ebene muss speziell auf die Verwendung eines geeigneten Trust Frameworks geachtet werden, um ein gemeinsames Verständnis speziell zwischen den Identity Brokern zu gewährleisten. Speziell auf semantischer Ebene ist ein gemeinsames Verständnis für die ausgetauschten Attribute unerlässlich. Ein Beispiel für solch ein gemeinsames Verständnis wäre die Einführung von Authentifizierungslevels, wie es das STORK-Framework [HuLeEe09] gemacht hat. Letztendlich müssen auch geeignete Prozesse eingeführt werden, um die ausgetauschten Attribute bzw. Daten auch verifizieren zu können.

5.4 Rechtliche Anforderungen

Die Einhaltung rechtlicher Anforderungen ist speziell notwendig, wenn nationale Identitätsmanagement-Systeme, wie es die österreichische Bürgerkarte beispielsweise darstellt, in so einem Modell involviert sind. Dabei müssen die Identity Broker auf die Einhaltung nationaler Richtlinien und Gesetze eingehen. Die Einhaltung von Datenschutzrichtlinien wird vermutlich eines der wichtigsten rechtlichen Anforderungen sein. Jedoch müssen hier nicht nur unbedingt Gesetze betroffen sein, sondern auch bilaterale Verträge oder Nutzungsbedingungen z.B. des Service Providers können in diesen Bereich fallen.

5.5 Ökonomische Anforderungen

Die Teilnahme an einem solchen Netzwerk wird vermutlich nicht kostenlos geschehen können. Daher müssen entsprechende Preis- bzw. Abrechnungsmodelle entwickelt werden. Vielmehr müssen auch Anreize geschaffen werden, um Unternehmen bzw. Personen dazu zu bringen, in diesem Netzwerk teilzunehmen. Um die Entwicklung von Geschäftsmodellen zu vereinfachen, sollten vor allem die Identity Broker entsprechende APIs bereitstellen, um einfach neue Geschäftsmodelle generieren zu können.

6 Zusammenfassung

Identitätsmanagement und die sichere Identifizierung und Authentifizierung spielen eine wichtige Rolle in vielen Bereichen, vor allem aber auch im Bereich des E-Governments. Identitätsmanagement ist an sich keine neue Thematik, deshalb haben sich über die Jahre auch einige Identitätsmodelle entwickelt. Obwohl dieses Modelle bereits ziemlich ausgereift sind, ergeben sich bei Anwendung im Cloud Computing neue Problematiken. Es haben sich daher zum Großteil auch eigene Cloud Identitätsmodelle entwickelt. Das Modell mit den meisten Vorteilen dabei ist das „Identity as a Service"-Modell, bei dem Identitäten von einem Identity Provider in der Cloud bereitgestellt werden. Aktuelle Implementierungen dieses Modells setzen hauptsächlich auf ein Identity Broker-Modell, wo ein Identity Broker in der Cloud mehrere Identity Provider und Service Provider bedienen kann. Dieses Modell hat aber einen entscheidenden Nachteil, nämlich, dass sowohl Benutzerinnen bzw. Benutzer als auch Service Provider die Abhängigkeit mit demselben Identity Broker für eine Identifizierung Authentifizierung besitzen müssen. Diesen Nachteil – bei gleichzeitiger Beibehaltung der Vorteile des Identity Broker-Modells - umgeht das „Federated Identity as a Service"-Modell. In diesem Modell können unterschiedliche Identity Broker miteinander kommunizieren und somit besteht keine Abhängigkeit für Benutzerinnen bzw. Benutzer und Service Provider zu ein und demselben Identity Broker. In diesem Modell können also beide ein Vertrags- bzw. Vertrauensverhältnis zu einem unterschiedlichen Identity Broker besitzen. Für die Umsetzung eines solchen Modells sind jedoch zahlreiche Anforderungen, z.B. auf organisatorischer, technischer, oder rechtlicher Ebene zu lösen. Die Anforderungen wurden teilweise in diesem Dokument skizziert. In einem Folgeprojekt sollen die Anforderungen dabei genauer spezifiziert und Teile dieses Modells zu Demonstrationszwecken implementiert werden.

Referenzen

[BoElKa+04]	Boyen, S., Ellison, G., Karhuluoma,, G., MacGregor, W., Madsen, P., Sengodan, S. Shinkar, S. and Thompson,, P.: Trust Models Guidelines. Draft. OASIS, 2004
[Co12]	Cox, P.: How to Manage Identity in the Public Cloud. InformationWeek reports, März, 2012
[CSA11]	Cloud Security Alliance: SECURITY GUIDANCE FOR CRITICAL AREAS OF FOCUS IN CLOUD COMPUTING V3.0, 2011
[Go09]	Gopalakrishnan, A.: Cloud Computing Identity Management. SETLabs Briefings, vol. 7, no. 7, pp. 45-55, 2009.
[Go10]	Goulding, J.: Identity and Access Management for the Cloud: CA's strategy and vision. Whitepaper, CA Cloud Business Unit, Mai 2010
[Hu10]	Huang, H. Y., Wang, B., Liu, X. X., and Xu, J. M.: Identity Federation Broker for Service Cloud. 2010 International Conference on Service Sciences (pp. 115–120), 2010
[HuLeEe09]	Hulsebosch, B., Lenzini, G. and Eertink, H.: D2.3 - Quality authenticator scheme. STORK Deliverable, 2009
[LDAP]	Sermersheim, J.: Lightweight Directory Access Protocol (LDAP): The Protocol. RFC 4511. Internet Engineering Task Force (IETF), 2006
[Kerberos]	Neuman, C., Yu, T., Hartman, S. and Raeburn, K.: The Kerberos Network Authentication Service (V5). RFC 4120. Internet Engineering Task Force (IETF), 2005
[PaGa07]	J. Palfrey, U. Gasser: Digital Identity Interoperability and eInnovation, Case Study, November 2007, Berkman Publication Series
[SAML]	Lockhart, H., Campbell, B: Security Assertion Markup Language (SAML) V2.0 Technical Overview. OASIS Committee Draft 02, 2008
[Zw12]	Zwattendorfer, B.: MOAs in der Cloud, 2012