Policy-gesteuerte Datenfreigaben und Trust Management im organisationsübergreifenden Identitäts-Management

Anonymisierte Einreichung zur SICHERHEIT 2006

Abstract:

Interorganisationales Identitäts-Management realisiert eine verteilte Verwaltung von Dienstnutzern und deren Berechtigungen, indem Service Provider benötigte Informationen vom Identitäts-Provider des Benutzers abrufen können. Wir motivieren die Notwendigkeit benutzergesteuerter Datenfreigaben in solchen Identitäts-Föderationen anhand eines Beispiels, zeigen Defizite aktueller Implementierungen auf und demonstrieren, wie die Policy-Sprache XACML effizient für die Modellierung und Umsetzung so genannter Attribute Release Policies eingesetzt werden kann. Wir spezifizieren die policy-gesteuerte Weiterverarbeitung dieser Daten auf Service-Provider-Seite und die Umsetzung grundlegender Methoden des Trust und Reputation Managements in Identitäts-Föderationen. Die Realisierung der vorgeschlagenen Techniken wird anhand eines Prototyps beschrieben.

1 Einleitung und Problemdefinition

Während einige Dienste bewusst anonym genutzt werden sollen, sind IT-Dienstleister im Allgemeinen daran interessiert, dass nur hinreichend autorisierte Personen oder im Auftrag dieser Personen handelnde Software-Systeme (Agenten) die jeweiligen Services nutzen können. Die Autorisierung wurde traditionell mit der Identität des Benutzers verknüpft – entweder durch direkte Rechtevergabe an Benutzerkonten, oder indirekt über die Zuordnung der Benutzer zu Gruppen oder Rollen.

Moderne *Identity & Access Management (I&AM)* Systeme dienen der organisationsweit zentralen Verwaltung von Benutzern und deren Rechten. Sie bestehen in der Regel aus einem zentralen *Identity Repository*, das von autoritativen Datenquellen wie den Personal- und Kundenverwaltungssystemen der Organisation gespeist wird, und so genannten *Konnektoren* zu angeschlossenen Endsystemen und Diensten, die mit den notwendigen Benutzer- und Rechteinformationen versorgt werden, was als *Provisioning* bezeichnet wird.

Die technischen, aber auch die organisatorischen und juristischen Aspekte des organisationsinternen Identitäts-Managements sind bereits so komplex, dass sich die Implementierung von I&AM-Systemen und die Verbreiterung ihres Abdeckungsgrades häufig über mehrere Jahre hinzieht. Hinzu kommt, dass in vielen Bereichen auch identitäts-management-relevante organisationsübergreifende Prozesse über geeignete Workflows informationstechnisch unterstützt werden müssen. Dies betrifft beispielsweise Business-to-Business Outsourcing Szenarien wie On-Demand oder Utility Computing, die Zusammenarbeit mehrerer tausend Organisationen im Supply Chain Management, aber auch Anwendungs-

fälle im akademischen Umfeld wie die Bildung Virtueller Organisationen (VOs) im Rahmen von Grid Computing.

Wenn die notwendigen Kontakt- und Abrechnungsinformationen aller Benutzer bei allen Dienstanbietern vorgehalten werden, ergeben sich in der Praxis aus dieser Redundanz schnell Skalierbarkeitsprobleme und Daten-Inkonsistenzen. Im einfachsten Fall ergibt sich daraus administrativer Zusatzaufwand, falls beispielsweise die Rechnungsanschrift eines Benutzers veraltet ist. Schwerwiegender sind Fälle, in denen ehemalige Mitarbeiter einer Organisation noch monatelang Zugriff auf die IT-Systeme von Partnerorganisationen haben, da kein geeigneter Datenabgleich stattfindet.

Um diese Probleme zu vermeiden, wird in neueren Ansätzen versucht, Redundanz weitgehend zu vermeiden und Inkonsistenzen über Daten-Sychronisationsverfahren zu verhindern. Im Rahmen des *Föderierten Identitäts-Managements (FIM)* wird zwischen *Identitäts-Providern (IDPs)* und *Service Providern (SPs)* unterschieden. Jeder Benutzer hat seine Daten in der Regel bei einem einzigen IDP hinterlegt und muss sie nur dort pflegen; die SPs können diese Informationen dann über dedizierte Schnittstellen vom IDP des Benutzers abfragen. Dabei wird üblicherweise auch die Authentifizierung des Benutzers vom IDP vorgenommen; der IDP garantiert dem SP dann, dass der Benutzer erfolgreich authentifiziert wurde, so dass eine getrennte Authentifizierung beim SP nicht mehr notwendig ist – man erreicht ein organisations-übergreifendes Single Sign-On. Voraussetzung hierfür ist offensichtlich ein geeignetes Vertrauensverhältnis zwischen SP und IDP; die Menge aller Organisationen, die untereinander ein solches Vertrauensverhältnis hergestellt haben, wird als *Identitäts-Föderation* bezeichnet.

Aus dem organisations-übergreifenden Datenaustausch von Identitätsinformationen ergibt sich eine Vielzahl neuer Fragestellungen hinsichtlich der technischen Umsetzung, deren Anpassung an die Geschäftsprozesse und die Einhaltung datenschutzrechtlicher Rahmenbedingungen. In diesem Artikel stellen wir die Ergebnisse unserer im Rahmen eines DFG-geförderten Projekts durchgeführten Arbeit vor, die sich mit dem Einsatz policybasierter Verfahren und der Einbeziehung von Trust Management ins föderierte Identitäts-Management befasst:

1. Wie können Benutzer Einfluß darauf nehmen, welche Service Provider welche Informationen von ihrem Identitäts-Provider abrufen können? Wie können insbesondere die Administratoren von Identitäts-Providern geeignete Voreinstellungen zum Schutz von Benutzern treffen, die sich nicht selbst darum kümmern?

2. Welche Alternativen zur a priori durchgeführten, vertraglichen Fixierung des Vertrauensverhältnises zwischen Service Provider und Identitäts-Provider und der im Rahmen von Service Level Agreements garantierten Datenqualität existieren?

Ein Szenario, das die Anwendung von FIM-Techniken und die Privacy- und Trust-Aspekte verdeutlicht, wird im folgenden Abschnitt vorgestellt. Die Verwendung von Policies zur IDP-seitigen Datenfreigabe wird in Abschnitt 3 erläutert, gefolgt von SP-seitigen Betrachtungen zur Weiterverarbeitung dieser Daten in Abschnitt 4. Die Modellierung von dynamischen Vertrauensverhältnissen zwischen Benutzern und SPs, sowie zwischen SPs und

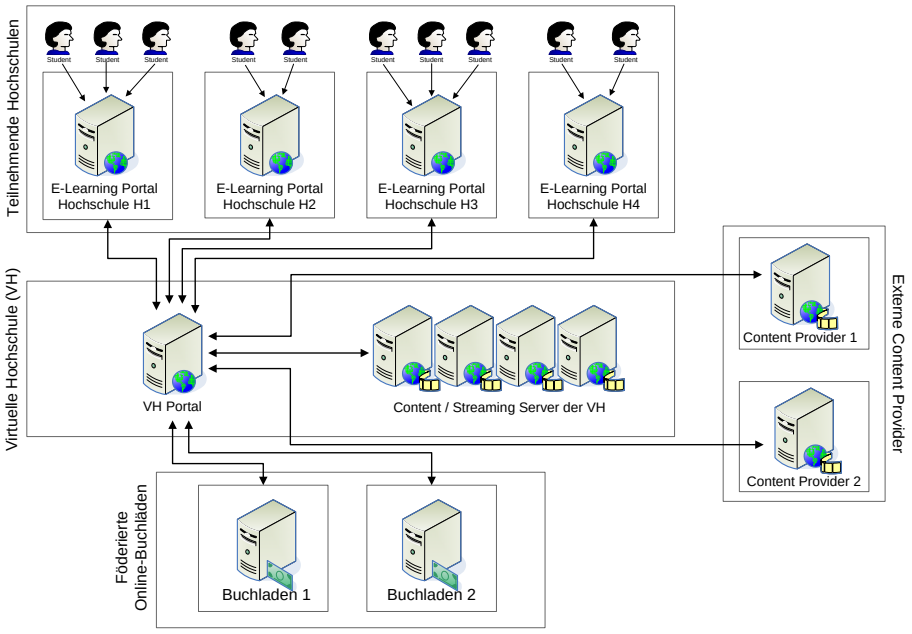

Abbildung 1: Szenario: Identitäts-Föderation für eine virtuelle Hochschule

IDPs wird in Abschnitt 5 vorgestellt. Ein Überblick über unsere prototypische Implementierung und ein Ausblick auf weitere Forschungsfragestellungen schließen diesen Artikel ab.

2 Szenario

Abbildung 1 zeigt eine Identitäts-Föderation, in deren Mittelpunkt eine Virtuelle Hochschule (VH) steht, die E-Learning Material für die Studenten der teilnehmenden realen Hochschulen anbietet. Ebenfalls an der Föderation beteiligt sind externe E-Learning-Content-Provider und Internet-Buchläden, über die bestimmte Literatur – in Analogie zu Hörerscheinen bei Präsenzveranstaltungen – verbilligt erworben werden kann.

Über FIM soll sichergestellt werden, dass nur Studenten der teilnehmenden Hochschulen auf das E-Learning System zugreifen können. Dazu müssen sich Studenten in geeigneter Weise an einem Web-Portal der Hochschule, an der sie eingeschrieben sind, identifizieren und authentifizieren, beispielsweise durch Benutzername und Passwort.

Bei der Nutzung der VH kann diese dann einerseits Informationen über den Studenten bei dessen Heimat-Hochschule abrufen. Andererseits ist die Virtuelle Hochschule selbst eine autoritative Datenquelle, der die externen Content-Provider und Buchläden vertrau-

en, wenn beispielsweise entschieden werden muss, ob ein Benutzer berechtigt ist, ein bestimmtes Buch verbilligt zu kaufen.

Offensichtlich muss es geeignete Mechanismen geben, um festlegen zu können, welche an der Föderation beteiligten SPs welche Informationen über den Benutzer abrufen dürfen. Zum Beispiel können für die VH die Attribute *Name*, *Matrikelnummer*, *Geburtsdatum* und *Studiengang* für die Erstellung von „Scheinen" bei erfolgreicher Kursteilnahme notwendig sein. Diese Daten werden aber vom Internet-Buchladen nicht benötigt und sollten diesem nicht zur Verfügung gestellt werden. Andererseits würde dieser wiederum eine Lieferanschrift und Zahlungsinformationen wie die Kreditkarten- oder Konto-Daten für Lastschriftverfahren benötigen, die für das E-Learning System irrelevant sind.

Ferner ist bei einer Auswahl aus mehreren an der Föderation beteiligten Buchläden zu betrachten, welchen davon ein Benutzer wählt. Diese Wahl kann beispielsweise von seinem Einverständnis mit den allgemeinen Geschäftsbedingungen und Lieferkonditionen abhängen, aber auch davon, ob und wie viele andere aus seiner Heimat-Hochschule diesem Service Provider bereits vertrauen.

Auf der anderen Seite ergibt sich für den SP durch die Teilnahme an der Föderation noch keine Verpflichtung, beliebige Kunden zu beliefern. Das Akzeptieren einer Bestellung wird vielmehr von bisherigen Erfahrungen mit diesem Kunden bzw. seinem IDP abhängen, sowie von seiner Kreditwürdigkeit, die beispielsweise von Scoring Services wie der Schufa abgerufen werden kann.

Zu untersuchen ist deshalb einerseits, wie Benutzer festlegen können, welche SPs auf welche ihrer Daten zugreifen können, und andererseits, wie Aspekte des dynamischen Trust und Reputation Managements im Datenmodell zu berücksichtigen sind.

3 Policygesteuerte Datenfreigabe

Die Liberty Alliance, eines der Standardisierungsgremien für Protokolle und Dienste im FIM-Umfeld, hat den Begriff *Attribute Release Policies (ARPs)* geprägt [Was04]. Sie fordert, dass Benutzer Regeln in Form von Policies aufstellen können sollen, die die Freigabe von Benutzerdaten (attribute release) durch den IDP steuern. Allerdings werden weder in den Spezifikationen der Liberty Alliance noch in denen der beiden anderen FIM-Standards, OASIS SAML [CKPM05] und WS-Federation [KA03], konkrete Aussagen über Format, Syntax und Semantik dieser ARPs getroffen. Eine Verfeinerung dieser Anforderungen, ebenfalls ohne konkrete ARP-Spezifikation, ist Gegenstand diverser Forschungsarbeiten im Umfeld von Privacy Enhancing Technologies [Pfi02, BLLS03, BS00, BLK+01].

Weil darüber hinaus eine Implementierung von ARPs keine verpflichtende Anforderung für die Konformität zu diesen Standards ist, weisen aktuelle Produkte meist keinerlei entsprechende benutzergesteuerte Datenschutz-Mechanismen auf. Eine Ausnahme bildet die im Hochschulumfeld weit verbreitete und als de facto Standard geltende, auf SAML basierende Open Source Software Shibboleth [CCE+05]. Sie erlaubt Administratoren, in der Granularität einzelner Datenfelder (Attribute) festzulegen, an welche SPs welche Daten

freigegeben werden sollen; Benutzer haben darüber hinaus die Möglichkeit, diese Voreinstellungen individuell zu modifizieren und zu ergänzen [Can04, NS04]. Diese letztere Möglichkeit existiert derzeit nur theoretisch, da geeignete web-basierte Management-Interfaces für Endnutzer erst noch im Entstehen sind.

Darüber hinaus sind die Ausdrucksmöglichkeiten von Shibboleth ARPs stark begrenzt. Beispielsweise kann die Freigabe von Daten an einen SP nicht von einem Zweck abhängig gemacht werden; somit ist keine Unterscheidung zwischen dem reinen Browsen einer Webseite zu Recherchezwecken und dem tatsächlichen Bestellen von Produkten möglich. Im Rahmen dieser Arbeit sollte deshalb ein für ARPs geeignetes Policy-Format gefunden werden, das insbesondere die folgenden Kriterien erfüllt:

- Interoperabilität: Statt der Definition einer neuen Policy-Sprache soll nach Möglichkeit auf bereits existierende Standards zurückgegriffen werden.
- Unabhängigkeit vom Datenschema: Das im Rahmen von Identitäts-Föderationen eingesetzte Datenschema kann frei gewählt werden. Die Verwendung von Standards wie P3P [RC99, BK01] oder dem zugehörigen APPEL [Lan02], die auf die Verwendung eines eigenen, stark E-Commerce-lastigen Datenschemas angewiesen sind, ist im Rahmen von FIM im Allgemeinen nicht möglich.
- Unterscheidung zwischen verschiedenen Datenfreigabe-Zwecken und verschiedenen Rollen der Benutzer. Im vorgestellten Szenario kann eine Person beispielsweise sowohl Student als auch Mitarbeiter der Hochschule sein; die Datenfreigaben und Autorisierungen der Person können von der Rolle abhängen, in der sie aktuell agiert.
- Unterstützung so genannter Obligationen, d.h. von Aktionen, die beim Evaluieren von ARPs vom IDP durchgeführt werden müssen; beispielsweise sollen sich Benutzer mittels E-Mails oder Logfiles über versuchte Datenzugriffe von SPs informieren lassen können.
- Ausdrucksfähige Policy-Conditions, um beispielsweise die Freigabe bestimmter Attribute von der Freigabe anderer Attribute abhängig machen zu können. Ebenso sollen Benutzer aus Usability-Aspekten Gruppen von Attributen bilden können, um beispielsweise ihre Lieferanschrift, bestehend aus Name, Straße, PLZ und Ort kollektiv freigeben oder sperren zu können.
- Verteilte Policy-Administration, da oftmals unternehmens-weite Richtlinien existieren, die standort- und abteilungsspezifisch verfeinert und von unterschiedlichen Personen gepflegt werden. Diese von Administratoren voreingestellten Werte sollten bis zu einem gewissen, ebenfalls konfigurierbaren Grad von den Endnutzern individuell angepasst werden können.

Mehrere moderne Policy-Sprachen eignen sich für die Formulierung von ARPs. Unsere Wahl fiel letztendlich auf die eXtensible Access Control Markup Language (XACML, [Mos05]), da sie gegenüber akademischen Ansätzen wie Ponder [DDLS01] den Vorteil hat, bereits in anderen Zusammenhängen erfolgreich im FIM-Umfeld eingesetzt worden zu sein [LPL+03, Maz04, CO02] und hinsichtlich vieler praxisrelevanter Details wie der

```
<Policy id="xacmlARP1" RuleCombiningAlg="first-applicable">
  <Description> Kreditkartendaten an Online-Buchhandlung </Description>
  <Rule id="KreditkarteAnBuchhandlung" effect="permit">
    <ResourceMatch MatchId="string-equal">
          idp.example.com/hansmustermann/privat/creditCardNumber
    </ResourceMatch>
    <Subject>
      <SubjectMatch MatchId="string-equal" AttributeValue="shop.example.com">
        <SubjectAttributeDesignator AttributeId="service_provider" />
      </SubjectMatch>
      <SubjectMatch MatchId="string-equal" AttributeValue="bookshop">
        <SubjectAttributeDesignator AttributeId="service" />
      </SubjectMatch>
      <SubjectMatch MatchId="string-equal" AttributeValue="purchase">
        <SubjectAttributeDesignator AttributeId="purpose" />
      </SubjectMatch>
    </Subject>
    <Action>
      <ActionMatch MatchId="string-equal" AttributeValue="read">
        <ActionAttributeDesignator AttributeId="action-id" />
      </ActionMatch>
    </Action>
    <Obligation Id="Log" FulfillOn="Permit">
        <AttributeAssignment Id="text">
          Kreditkartendaten wurden an folgenden Dienstleister übermittelt:
          <SubjectAttributeDesignator AttributeId="service_provider" />
        </AttributeAssignment>
    </Obligation>
  </Rule>
  <Rule id="SonstNichtsFreigeben" effect="deny"/>
</Policy>
```

Abbildung 2: Beispiel für eine XACML-basierte Attribute Release Policy

Namensgebung für Provider-Identifikatoren verbindliche Konzepte vorzuweisen, die bei anderen Policy-Sprachen fehlen.

Da XACML eine sehr generische Policy-Sprache ist, haben wir die Semantik ihrer einzelnen Elemente, insbesondere der Subjects, Resources, Actions, Conditions und Obligations für FIM-ARPs spezifiziert. Abbildung 2 zeigt ein Beispiel für eine XACML-ARP, in der die Kreditkarten-Daten des Benutzers nur genau dann freigegeben werden, wenn sie konkret für die Bestellung bei einem bestimmten Service Provider eingesetzt werden sollen.

Shibboleth-ARPs lassen sich verlustfrei in XACML-ARPs konvertieren, so dass bei unserer in Abschnitt 6 beschriebenen Implementierung Abwärtskompatibilität gewährleistet ist.

4 Policygesteuerte Weiterverarbeitung der Identitäts-Daten

Das Gegenstück zu den Attribute Release Policies beim Service Provider sind die so genannten *Attribute Acceptance Policies (AAPs)*. Aktuelle AAP-Implementierungen, zum Beispiel in Shibboleth, weisen neben einer sehr eingeschränkten Ausdrucksfähigkeit das Problem auf, dass sie für jeden Dienst separat spezifiziert werden müssen. Dies ist zwar

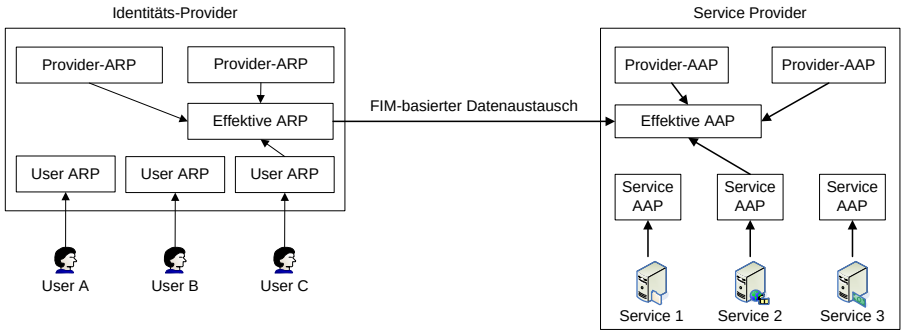

Abbildung 3: Zusammenspiel von Attribute Release und Acceptance Policies

für E-Commerce Websites in der Regel ausreichend, bedeutet für Identitäts-Föderationen, in denen Service Provider mehrere Dienste anbieten, allerdings administrativen Zusatzaufwand und komplexeres Change Management.

Unser AAP-Konzept ist in Abbildung 3 dargestellt und zielt auf eine Unterscheidung zwischen provider-weiten und service-spezifischen AAPs ab, die sich gegenseitig ergänzen. Diese Aufteilung bringt diverse Vorteile aus Sicht des Service Managements mit sich:

- An zentraler Stelle können AAPs definiert werden, die für alle Dienste gelten. Provider-weite Vorgaben, beispielsweise hinsichtlich der über Kunden zur Verfügung stehenden Kontakt- und Abrechnungsdaten, können so effizient umgesetzt werden, ohne die lokalen Dienst-Administratoren in ihrer Flexibilität einzuschränken.
- Die Überprüfung der Vollständigkeit der vorliegenden Daten muss nicht mehr von jedem Service separat implementiert werden. Dies ist insbesondere dann notwendig, wenn nicht-FIM-spezifische Services über FIM provisioniert werden sollen; beispielsweise wird somit die Einspeisung von FIM-Daten in lokale I&AM-Systeme und damit die Integration von FIM-Diensten in die bereits vorhandenen lokalen Geschäftsprozesse erleichtert.
- Daten, die nicht für die Erbringung eines bestimmten Dienstes erforderlich sind, können aus Datenschutzgründen verworfen oder anonymisiert werden, bevor sie den Dienst erreichen. Diese Möglichkeit ist dann relevant, wenn proprietäre Dienstimplementierungen mehr Daten vom IDP anfordern als eigentlich notwendig und der Benutzer zu permissive ARPs konfiguriert hat.
- Auf Fehlersituationen wie das Fehlen von zur Diensterbringung notwendigen Attributen kann unmittelbar und mit FIM-Mitteln reagiert werden. So könnte der Benutzer beispielsweise von seinem IDP über das Auftreten des Fehlers informiert und auf die Notwendigkeit weiterer Datenfreigaben aufmerksam gemacht werden, ohne dass dieser Fehler erst im Dienst auftritt und möglicherweise zu unklaren Fehlermeldungen führt.

```
<Policy id="SiteARP_CC" RuleCombiningAlg="first-applicable" prio="100">
  <Description> Abgelaufene Kreditkarten ablehnen </Description>
  <Rule id="Check_CC_expiry" effect="deny">
    <Target>
         <AnyResource/> <!-- auf alle Dienste anwenden -->
         <AnyAction/>   <!-- auf alle Aktionen anwenden  -->
         <!-- auf Benutzer mit angegebener Kreditkarte anwenden -->
         <SubjectMatch AttributeValue="\d+">
           <SubjectAttributeDesignator AttributeId="CreditCardNumber"/>
         </SubjectMatch>
    </Target>
    <Condition FunctionId="time-greater">
         <EnvironmentAttributeSelector AttributeId="current-time">
         <SubjectAttributeDesignator AttributeId="CreditCardExpiry"/>
    </Condition>
    <Obligation Id="Log" FulfillOn="Deny">
        <AttributeAssignment Id="text">
          Abgelaufene Kreditkarte abgelehnt, Benutzer:
          <SubjectAttributeDesignator AttributeId="subject-id" />
        </AttributeAssignment>
    </Obligation>
  </Rule>
  <Rule id="acceptOtherwise" effect="permit"/>
</Policy>
```

Abbildung 4: Beispiel für eine XACML-basierte Attribute Acceptance Policy

Die bereits für ARPs eingesetzte Policy-Sprache XACML ist auch für die Modellierung und Umsetzung von AAPs sehr gut geeignet. Wir haben wiederum die AAP-spezifische Semantik der XACML-Elemente spezifiziert; Abbildung 4 zeigt eine XACML-AAP, bei der Kreditkarten-Daten für alle Services verworfen werden, sofern das Gültigkeitsdatum der Kreditkarte bereits überschritten wurde.

5 Einbezug von Trust und Reputation Management

Vertrauen ist ein Eckpfeiler von Föderiertem Identitäts-Management (FIM): Service Provider (SPs) verlassen sich auf die Korrektheit der ihnen vom Identitäts-Provider (IDP) gelieferten Daten und Endnutzer sind darauf angewiesen, dass ihr IDP nicht mehr als die von ihnen freigegebenen Daten herausgibt.

Der IDP ist in der Regel die Organisation, für die ein Endnutzer arbeitet, oder der Internet-Provider bzw. die Online-Bank von Privatpersonen. Vertrauensbeziehungen zwischen SPs und IDPs einer Föderation werden derzeit in der Regel out-of-band geschlossen, beispielsweise vertraglich in Form eines Service Level Agreements, das auch Garantien hinsichtlich der Datenqualität enthält.

Diese Form von Trust Management (TM) ist relativ statisch, da die Teilnehmer an einer Föderation und ihr aufgebrachtes Vertrauen nur einer geringen Fluktuation unterliegen. Weitere TM-Aspekte wie die zuverlässige Authentifikation von Benutzern und Service Providern sowie die Integrität und Vertraulichkeit übertragener Daten werden von den FIM-Protokollen abgedeckt, beispielsweise auf Basis von SSL und Zertifikaten. Unser Ziel ist es, diese statische Trust-Komponente dynamisch zu ergänzen; wir bringen dazu wie nachfolgend beschrieben Aspekte des Reputation Managements ins FIM-Umfeld ein.

Reputation Management zielt darauf ab, den Grad des eigenen Vertrauens in einen Dritten davon abhängig zu machen, welche positiven oder negativen Erfahrungen man selbst oder als vertrauenswürdig eingestufte Andere mit ihm gemacht haben, gegebenenfalls über einen bestimmten Zeitraum hinweg. Ein Beispiel für praktisches Reputation Management findet sich in den Bewertungssystemen von Online-Auktionshäusern.

Es existieren verschiedene Ansätze, wie aus den diversen Eingabeparametern und konfigurierbaren Gewichten letztendlich der Vertrauensgrad, als *Trust Level* bezeichnet, ermittelt wird. Welcher Algorithmus sich am Besten eignet, ist stark abhängig vom Anwendungsspektrum der Identitäts-Föderation und wird hier nicht näher betrachtet.

Die Verwendung von Trust Levels in FIM-Szenarien ist ein zweistufiger Prozess:

1. Benutzer müssen, zum Beispiel über Web-Interfaces bei ihrem IDP, die Möglichkeit erhalten, für jeden Service die Eingabeparameter für die Berechnung des Trust Levels festlegen zu können. IDP-Administratoren können Voreinstellungen vornehmen, die damit Empfehlungen beispielsweise auf Basis vertraglicher Beziehungen zum SP umsetzen können. Analog dazu können SP-Administratoren derartige Einstellungen für einzelne Benutzer, alle ein bestimmtes Kriterium erfüllende Benutzer oder ganze IDPs vornehmen.

2. In die Attribute Release bzw. Acceptance Policies können Default-Regeln aufgenommen werden, die mit Schwellwerten arbeiten. Dies führt dazu, dass beispielsweise Datenfreigaben für den Fall, dass sie nicht service-spezifisch a priori vorgenommen wurden, genau dann durchgeführt werden, wenn der dynamisch berechnete Trust Level einem SP gegenüber einen bestimmten Schwellwert überschreitet. Analog dazu kann der SP die von einem Scoring Service zur Laufzeit gelieferte Kreditwürdigkeit des potentiellen Kunden einfliessen zu lassen und ihm bei Unterschreiten eines Schwellwerts beispielsweise nur die Lieferung per Vorauskasse statt auf Rechnung oder per Bankeinzug anbieten.

Die manuell spezifizierten Eingabeparameter können in Benutzerattributen untergebracht und somit einfach in den XACML Conditions der ARPs bzw. AAPs genutzt werden. Aus Gründen der Nachvollziehbarkeit von dynamischen Datenfreigaben sollten die im jeweiligen Fall verwendeten Eingabeparameter für den Algorithmus zur Trust Level Berechnung mitprotokolliert und dem Endnutzer zur Einsicht angeboten werden.

6 Prototypische Implementierung

Abbildung 5 zeigt die Architektur unserer prototypischen Implementierung am Beispiel des Identäts-Providers (IDP):

1. Vom Service Provider (SP) eingehende Attributsanfragen werden nicht mehr durch direktes Nachschlagen der Attribute im Identity Repository bearbeitet, sondern an einen von uns entwickelten XACML Policy Enforcement Point (PEP) weitergeleitet.

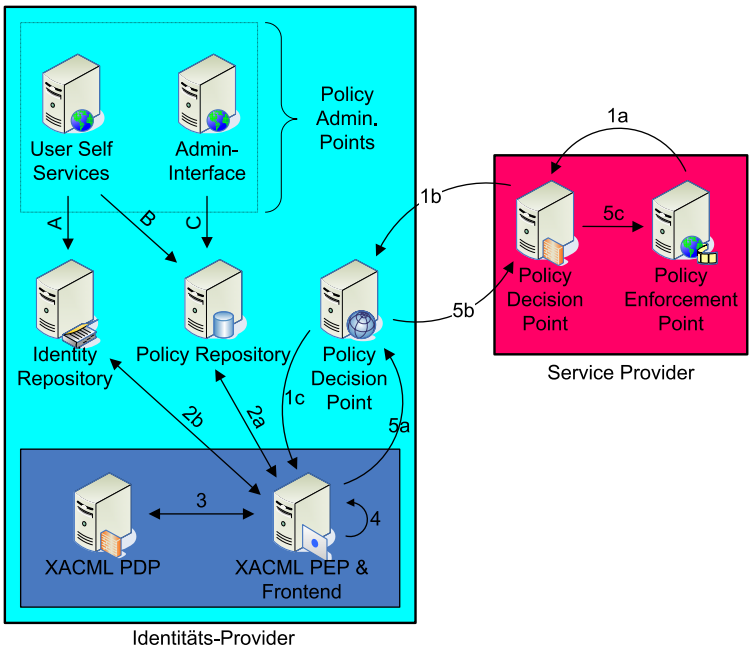

Abbildung 5: Identitäts-provider-seitige Architektur

2. Der XACML PEP bezieht einerseits die relevanten Attribute Release Policies (ARPs) aus einem Policy Repository und andererseits die Werte aller Benutzerattribute, da diese von XACML Conditions in den ARPs benötigt werden könnten. Aus den einzelnen ARPs wird ein XACML PolicySet zusammengestellt; die Attributswerte fliessen dabei als XACML-ResourceContent-Element mit ein. Benutzer und Administratoren können ihre Daten und ARPs über dedizierte Web-Interfaces verwalten (Pfeile A–C).

3. Das PolicySet wird anschließend von einem beliebigen standard-konformen XACML Policy Decision Point (PDP) ausgewertet. Wir verwenden hierfür die Open Source Implementierung von Sun [Pro04].

4. Als Antwort erhält unser XACML PEP die Entscheidungen über die Freigabe der einzelnen Attribute und die optionalen XACML obligations, die zu erfüllen sind; sie betreffen das Informieren des Benutzers über erfolgreiche oder abgelehnte Attributszugriffe durch SPs in Form von E-Mails oder Logfiles.

5. Die freigegebenen Attribute werden zurückgegeben und wie bisher an den SP übermittelt.

Da nur IDP-interne Workflows erweitert werden und keine Modifikationen an FIM-Protokollen notwendig sind, ist diese Vorgehensweise nicht nur auf SAML, sondern auch auf die Li-

berty Alliance und WS-Federation Architekturen anwendbar.

Unsere Implementierung für die SAML-basierte Open Source Software Shibboleth [CCE+05] in Version 1.2 ersetzt die dort integrierten Behandlungsroutinen für ARPs und AAPs. Wir planen, die angekündigte Version 2.0 von Shibboleth so zu erweitern, dass zwischen verschiedenen ARP/AAP-Varianten gewählt werden kann und unsere XACML-basierte Implementierung beizusteuern.

7 Zusammenfassung und Ausblick

Ausgehend vom einem Beispiel für eine Identitäts-Föderation haben wir eingangs die Notwendigkeit benutzergesteuerter Datenfreigabe-Mechanismen aufgezeigt. Für diesen Zweck ist die Methodik des verteilten, policy-basierten Managements sehr gut geeignet. Nach der Vorstellung unserer Ziele bei der policy-basierten Umsetzung haben wir gezeigt, wie die Policy-Sprache XACML sowohl für Attribute Release als auch für Attribute Acceptance Policies eingesetzt werden kann und welche Vorteile dies insbesondere auf Service Provider Seite mit sich bringt.

Für beide Policy-Varianten haben wir demonstriert, wie sich grundlegende Aspekte von Trust und Reputation Management auf Basis von Schwellwert-Verfahren für Trust Levels einsetzen lassen. Abschließend haben wir die Architektur unseres Prototyps und seine Integration in Shibboleth vorgestellt.

Im Rahmen unserer weiteren Forschungstätigen werden wir insbesondere die Integration von FIM-Daten in service-provider-seitige Geschäftsprozesse untersuchen. Das Ziel ist hierbei insbesondere eine stärkere Integration von FIM- und I&AM-Komponenten, die von den aktuellen Standards und Implementierungen nur unzureichend abgedeckt wird.

Literatur

[BK01] Oliver Berthold and Marit Köhntopp. Identity management based on P3P. In *International workshop on Designing privacy enhancing technologies*, pages 141–160, New York, NY, USA, 2001. Springer-Verlag New York, Inc.

[BLK+01] Kathy Bohrer, Xuan Liu, Dogan Kesdogan, Edith Schonberg, Moninder Singh, and Susan Spraragen. Personal Information Management and Distribution. In *4th International Conference on Electronic Commerce Research ICECR-4*, 2001.

[BLLS03] Kathy Bohrer, Stephan Levy, Xuan Liu, and Edith Schonberg. Individualized Privacy Policy Based Access Control. In *Proceedings 6th International Conference on Electronic Commerce Research*, ICECR, 2003.

[BS00] Piero A. Bonatti and Pierangela Samarati. Regulating Service Access and Information Release on the Web. In *Proceedings of CCS '00, Athens*. ACM Press, 2000.

[Can04] Scott Cantor. Shibboleth v1.2 Attribute Release Policies. `http://shibboleth.internet2.edu/guides/deploy-guide-origin1.2.html#2.e.`, 2004.

[CCE+05] Scott Cantor, Steven Carmody, Marlena Erdos, Keith Hazelton, Walther Hoehn, and Bob Morgan. Shibboleth Architecture, working draft 09. http://shibboleth.internet2.edu/docs/, 2005.

[CKPM05] Scott Cantor, John Kemp, Rob Philpott, and Eve Maler (Eds.). Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0. OASIS Security Services Technical Committee Standard, March 2005.

[CO02] David Chadwick and Alexander Otenko. The PERMIS X.509 Role Based Privilege Management Infrastructure. In *Proceedings of the 7th ACM Symposium on Access Control Models and Technologies*, SACMAT, pages 135–140. ACM Press, 2002.

[DDLS01] Nicodemos Damianou, Naranker Dulay, Emil Lupu, and Morris Sloman. The Ponder Policy Specification Language. *Lecture Notes in Computer Science*, 1995, 2001.

[KA03] Chris Kaler and Anthony Nadalin (Eds.). Web Services Federation Language (WS-Federation). Web services specification document, BEA, IBM, Microsoft, Verisign, RSA Security, 2003.

[Lan02] Marc Langheinrich (Ed.). A P3P Preference Exchange Language — APPEL 1.0. http://www.w3.org/TR/P3P-preferences/, 2002.

[LPL+03] Markus Lorch, Seth Proctor, Rebekah Lepro, Dennis Kafura, and Sumit Shah. First Experiences Using XACML for Access Control in Distributed Systems. In *Proceedings of the ACM Workshop on XML Security*. ACM Press, 2003.

[Maz04] Paul Mazzuca. Access Control in a Distributed Decentralized Network: An XML Approach to Network Security. Honors Thesis, Dartmouth College, 2004.

[Mos05] Tim Moses (Ed.). OASIS eXtensible Access Control Markup Language 2.0, core specification. OASIS XACML Technical Committee Standard, 2005.

[NS04] Sidharth Nazareth and Sean Smith. Using SPKI/SDSI for Distributed Maintenance of Attribute Release Policies in Shibboleth. Technical Report TR2004-485, Department of Computer Science, Dartmouth College, Hanover, HN 03744 USA, 2004.

[Pfi02] Birgit Pfitzmann. Privacy in browser-based attribute exchange. In *Proceedings of the ACM Workshop on Privacy in Electronic Society (WPES 2002)*, pages 52–62. ACM Press, 2002.

[Pro04] Seth Proctor. Sun's XACML implementation. http://sunxacml.sf.net/, 2004.

[RC99] Joseph Reagle and Lorrie F. Cranor. The Platform for Privacy Preferences. In *Communications of the ACM*, volume 42, pages 48–55. ACM Press, 1999.

[Was04] Thomas Wason (Ed.). Liberty ID-FF Architecture Overview v1.2. Liberty Alliance Specification, 2004.