bwIDM: Anbindung nicht-webbasierter IT-Infrastrukturen an eine SAML/Shibboleth-Föderation

Saher Semaan, Richard Zahoransky

Lehrstuhl für Kommunikationssysteme
Universität Freiburg
Hermann-Herderstr. 10
79104 Freiburg
semaan@uni-freiburg.de
richard.zahoransky@rz.uni-freiburg.de

Zusammenfassung: Diese Arbeit beschreibt eine Proof-of-Concept Implementation einer Föderation aus existierenden webbasierten und nicht-webbasierter Diensten. Die Dienste der Föderation werden durch SAML / ECP gegenseitig zugänglich gemacht, ohne eine zentrale Nutzerdatenbank vorhalten zu müssen. Die einzelnen Föderationskomponenten vertrauen untereinander durch Zertifikate und Metadaten. Eine PAM-ECP-Implementierung wird gezeigt, die es ermöglicht, nicht-webbasierte Dienste mittels Shibboleth / ECP der Föderation anzuschließen. Die resultierenden Fragen des Datenschutzes, der Datenweitergabe und Sicherheit werden diskutiert.

Keywords: bwIDM, ECP, PAM, SAML, Shibboleth, SSH

1 Einleitung

Die Nutzung von organisationsübergreifenden Diensten innerhalb einer Partnerschaft verschiedener Institutionen ist für viele Forschungsdisziplinen in der heutigen Zeit unvermeidlich und sogar notwendig. Das hier vorgestellte Projekt bwIDM[1] hat das Ziel, verteilt angebotene Ressourcen und

[1] bwIDM: Föderatives Identitätsmanagement in Baden-Württemberg http://www.bwidm.de

Dienste der Universitäten des Landes Baden-Württemberg aus einem lokalen Kontext heraus zugängliche zu machen. Universitätsmitglieder sollen in der Lage sein, verschiedenste, auch nicht web-webbasierter Dienste (z.B. Desktop-Anwendungen, Grid- oder Cloud-Dienste) innerhalb und außerhalb der eigenen Universität mit ihrem lokalen Benutzeraccount zu benutzen, als wären diese Ressourcen physisch vor Ort. Hierfür soll keine landesweite zentrale Nutzerdatenbank aufgebaut werden. Stattdessen sollen die Benutzerverzeichnisse lokal an den Universitäten bestehen bleiben und durch diese betreut und gepflegt werden. Teile dieser Arbeit wurden bereits in [6] veröffentlicht.

2 Aufbau einer Föderation

Diese Arbeit konzentriert sich auf die verteilte Nutzerverwaltung und Bildung einer Föderation durch den SAML[2] Standard. Dieser beschreibt den Austausch von Nachrichten zur Autorisierung und Authentifizierung zwischen verschiedenen Organisationen, die sich gegenseitig vertrauen. Eine Implementierung dieses Standards ist durch Shibboleth[3] gegeben. SAML baut nicht auf zentrale Nutzerdatenbanken auf. Shibboleth ermöglicht es daher, lokale Identitätssysteme beizubehalten und für die Föderation nutzbar zu machen. Dies begünstigt die Datensparsamkeit, erhöht die Ausfallsicherheit und minimiert die Gefahr des Datendiebstahls. Dem gegenüber stehen organisatorische Hürden, die einmalig bewältigt werden müssen.

Innerhalb einer Föderation werden Dienste durch Service Provider (SP) geschützt. Die jeweiligen SP besitzen keine eigene Benutzerverwaltung. Stattdessen vertrauen sie auf die Aussagen von Identitätsprovidern (Identity Provider: IdP) und gewähren entsprechend Zugang zu ihrem Dienst. Zertifikate, die zwischen IdP und SP ausgetauscht werden, stellen sicher, dass die Kommunikation zwischen SP und IdP vertrauenswürdig ist. IdPs setzen auf bestehende Benutzerverzeichnisse auf. Sie sind dafür zuständig,

[2] Security Assertion Markup Language (SAML) http://www.oasis-open.org/standards, letzter Aufruf 26.04.2012

[3] What's Shibboleth? http://www.shibboleth.net/about/index.html, letzter Aufruf 26.04.2012

Benutzer zu authentifizieren und liefern dem SP auf Anfrage weitere Attribute über den Benutzer. Möchte ein Teilnehmer der Föderation die Dienste eines SP wahrnehmen und sich authentifizieren, benötigt er einen gültigen Account bei seinem lokalen IdP (siehe Bild 1). Nachdem der Benutzer authentifiziert wurde, kann der SP optional auf Grund von weiteren Attributen des Benutzers den Dienst für diesen speziellen Benutzer freigeben oder nicht.

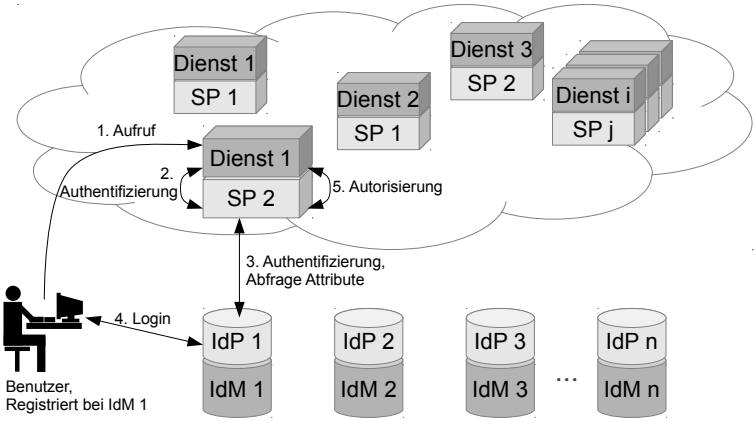

Bild 1: Ein Benutzer meldet sich für einen Dienst innerhalb einer Föderation an einem SP an. Der SP leitet den Anfragenden an seinen lokalen IdP weiter. Dort meldet sich der Benutzer an, worauf der IdP die Authentifizierung an den SP weiterreicht.

Möchte eine Institution der Föderation beitreten, muss sie mindestens ein SAML2 fähigen IdP einrichten und die dazugehörigen Metadaten erzeugen. Diese beschreiben und beweisen die Identität des Ausstellers. Hierfür enthalten die Metadaten Informationen über die unterstützen Protokolle und die Kontaktdaten des Ansprechpartners für den Problemfall. Um sichere Verbindungen zu ermöglichen, beinhalten die Metadaten zusätzlich die

CA-Zertifikate[4] für den jeweiligen Host. Sowohl IdP als auch SP machen sich über Metadaten bekannt.

Um die Verteilung der Metadaten zu erleichtern, lassen sich Discovery-Services (DS) innerhalb einer Föderation einsetzen. Dieser Dienst erfüllt zwei Aufgabe. Er aggregiert die Metadaten der Teilnehmer und verteilt diese. Zweitens nutzt der DS die Informationen aus den Metadaten, um Authentifizierungsanfragen von Personen verschiedener Institutionen an den korrekten IdP weiterzuleiten.

3 Funktion

SAML im allgemeinen und die Implementierung durch Shibboleth zielen im wesentlichen auf die Bereitstellung von Web-Anwendungen durch einen Web-Browser. Der SAML[5] Standard bietet mit dem Enhanced Client or Proxy (ECP) Profil eine Unterstützung für nicht web-basierte Dienste an. Folgend werden beide Varianten beschrieben

3.1 Aufruf eines Webdienstes

Das Bild 2 zeigt grafisch die Funktionsweise von SAML bzw. Shibboleth durch die Verwendung eines Browsers. Greift ein Benutzer auf eine durch Shibboleth geschützte Ressource zu, prüft das Shibboleth-Modul (der SP), auf ein gültigen Session-Cookie. Existiert kein solches Cookie, setzt der SP sein eigenes Cookie und leitet den Browser auf die Webseite des Heimat-IdP oder auf die Webseite des DS. Landet der Benutzer auf der Seite des DS, wählt er von dort den IdP seiner Organisation aus (nicht im Bild dargestellt). Der Benutzer gibt daraufhin sein Passwort direkt auf der Webseite des IdP ein. SP oder DS benötigen kein Wissen über das Passwort. Nach der Passworteingabe ist der Benutzer authentifiziert und der IdP sendet seine Antwort in einer SAML-Assertion zusammen mit dem vom SP

[4] Im Rahmen dieses Projekts werden die Zertifikate über DFN-PKI bereitgestellt (https://www.pki.dfn.de).

[5] Ab der Version 2.0

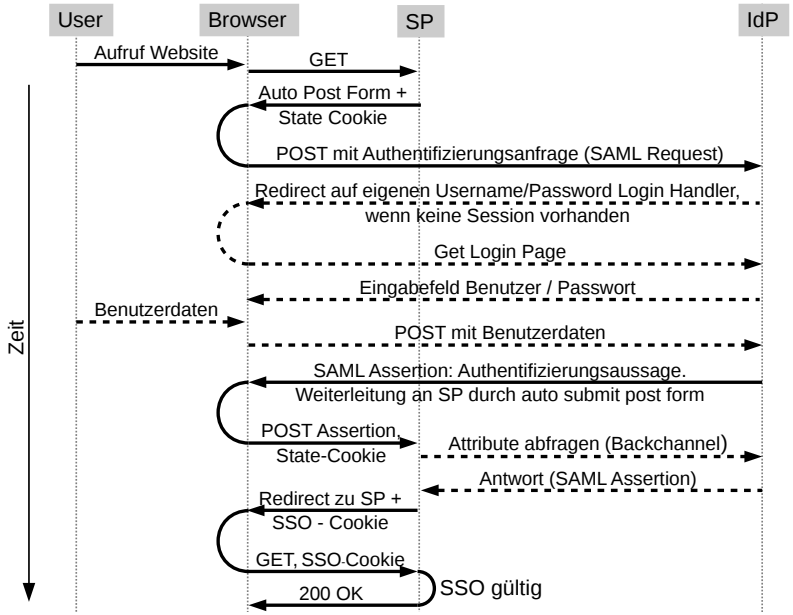

Bild 2: Single-Sign-On Anmeldung mit SAML2 [7].

generierten Session-Cookie über den Browser zurück an den SP. Die digital unterschriebene SAML-Assertion repräsentiert die Authentifizierung des Nutzers am IdP. Ein letzter Redirect führt den Browser zurück zu dem SP. Das vom Browser vorgezeigte Session-Cookie ist dem SP diesmal bekannt und der Benutzer ist somit gegenüber dem SP authentifiziert. Der SP kann nun entsprechend seinen Regeln die Autorisierung durchführen.

3.2 Enhanced Client or Proxy

Enhanced Client or Proxy (ECP) ist ein Unterprofil des SAML-Standards [6], um Anwendungen, die außerhalb eines Browsers arbeiten in eine Föderati-

[6] http://wiki.oasis-open.org/security/SAML2EnhancedClientProfile, Working Draft 04

on einzubinden. Da ein nicht-webbasierter Dienst nicht zwingend Browser-Redirects nutzen oder HTML-Seite anzeigen kann, muss dieser auf andere Weise die Authentifizierung durchführen [3]. Ein Dienst, der das ECP-Profil unterstützt, kann mit SP und IdP kommunizieren und direkt SAML-Assertions verarbeiten. Um einen Dienst ECP-fähig zu machen sind Änderungen und Anpassungen notwendig, sowohl Server- als auch Clientseitig.

Möchte ein Benutzer auf einen ECP-fähigen Dienst zugreifen, verlangt der Dienst vom SP eine Authentifizierungsanfrage für den Heimat-IdP des Benutzers. Die Antwort vom SP ist eine SAML-Nachricht mit der entsprechenden, unterschriebenen Anfrage an den IdP als Inhalt. Der Dienst leitet die SAML-Nachricht an den entsprechenden IdP. Daraufhin prüft der IdP die Identität des Benutzers, beispielsweise über eine Passwortabfrage. Für eine erfolgreiche Authentifizierung muss der ECP-fähige Dienst diese Passwortabfrage an den Benutzer weiterleiten und die Eingabe zurück an den IdP senden. Ist die Identität durch den IdP geprüft, sendet dieser sein Ergebnis wieder als SAML-Nachricht zurück an den Dienst. Die Nachricht leitet der Dienst an den SP. Der SP prüft den Inhalt und teilt dem Dienst mit, ob sich der Benutzer erfolgreich authentifiziert hat, beziehungsweise gibt den entsprechenden Service frei.

4 Datenschutz und Sicherheit

SAML nutzt Zertifikate zur Überprüfung von Identitäten, gewährleistet Vertraulichkeit durch Verschlüsselung, und stellt sicher, dass die Überprüfung des Passworts direkt bei der Heimatorganisation erfolgt. Somit gewährleistet Shibboleth mit dem SAML-Protokoll, dass

- Die Prüfung des Passworts am IdP und nicht am SP erfolgt.
- Die Passwörter nicht im Klartext zum IdP übertragen werden.
- Man-in-the-middle Angriffe durch Nutzung von SSL/TLS erschwert sind [2].
- Der Nutzer der Datenweitergabe von Attributen durch den IdP aktiv zustimmen muss.

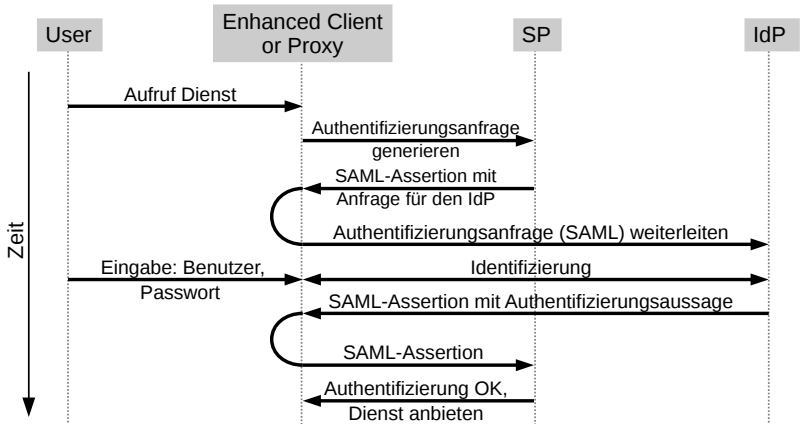

Bild 3: Vereinfachte Arbeitsweise von ECP. Ein nicht webbasierter Dienst kann durch das ECP-Profil föderationsfähig gemacht werden [5].

Der zuletzt genannte Punkt ist (in Deutschland) ein wichtiges Kriterium des Datenschutzes[7]. Die dem IdP angeschlossenen Datenbanken halten in vielen Fällen weitere Eigenschaften zu den Benutzeraccounts bereit. Die Weitergabe dieser Attributen an eine fremde Institution fällt unter das Datenschutzgesetz[8] und muss vom Accountinhaber ausdrücklich für jeden Dienst erlaubt sein. Konkret bedeutet dies, dass der IdP nach der Abfrage des Benutzerpassworts prüfen muss, ob die Authentifizierungsanfrage von einem SP stammt, dem der Nutzer bereits seine Einwilligung zur Datenabfrage gegeben hat. Sollte dies nicht zutreffen, darf der IdP die Attribute erst nach der Einverständnis des Benutzers an den SP senden. Eine Implementierung dieser Funktionalität ist durch uApprove[9] bereits gegeben. uApprove setzt auf den IdP auf und zeigt dem Benutzer eine zusätzliche Webseite wäh-

[7] §§ 4 ff. Bundesdatenschutzgesetz (BDSG), Online verfügbar: http://www.gesetze-im-internet.de/bdsg_1990/

[8] § 5 Verwaltungs- und Benutzungsordnung (VB) Universität Freiburg

[9] http://www.switch.ch/aai/support/tools/uApprove.html uApprove von SWITCH, letzter Aufruf: 26.04.2012

rend dem Login-Vorgang, auf der er informiert wird, welche Attribute der SP abfragen möchte. Der Nutzer kann dem Vorgang aktiv zustimmen oder den Login-Prozess beenden. Das Bild 4 zeigt die Abfrage der Erlaubnis zur Datenweitergabe.

Bild 4: uApprove zeigt dem Benutzer, welche Attribute der SP vom IdP verlangt und holt die Berechtigung des Benutzers ein (Browser-Screenshot).

uApprove funktioniert nur für Webdienste, da andere Dienste nicht zwingend in der Lage sind, HTML-Seiten darzustellen. In diesem Fall kann die Weitergabe der Attribute nicht durch den Benutzer überprüft und unterbunden werden.
Einem Dienst, der über ECP an die Föderation angebunden werden soll, stehen damit zwei Problemen gegenüber:

1. Wie geschildert, kann ein Benutzer eines ECP-fähigen Dienstes der Abfrage von Attributen währende des Login-Prozess nicht zustimmen.

2. Je nach Konzeption des Dienstes, muss dem Server, der den Dienst bereitstellt, das Föderationspasswort zugänglich sein.

Auf beide genannte Punkte wird im Folgenden anhand eines implementierten, ECP-fähigen SSH-Servers näher eingegangen. Diese prototypische Implementierung steht exemplarisch für weitere, ECP-fähige Dienste.

Ein ECP-fähiger Dienst erhält eine hohe Benutzerakzeptanz, wenn der Client zum bedienen des Dienstes wie gewohnt bedienbar ist [1]. Für den hier gezeigten Proof-of-Concept ist das der Fall. Der SSH-Client bedarf keiner Modifikation und verhält sich für den Anwender wie gewohnt. Auf der Server-Seite wurde ein Pluggable Authentication Module (PAM) [4] entwickelt, dass die Authentifizierung durch ECP am SP und IdP durchführt. Das bedeutet, dass nur der SSH-Server ECP-fähig ist und nur dieser die Authentifizierung mit dem SP und IdP abwickeln kann. Damit der Server die Authentifizierung im Namen des Benutzers durchführen kann, benötigt dieser das vom Benutzer gelieferte Passwort, wie es in Bild 5 beschrieben ist. Hierdurch erhält der ECP-fähige Server Zugang zu dem Benutzeraccount:

- Der ECP-fähige Dienst nimmt das Benutzerpasswort selbst entgegen und hat somit unkontrollierten Zugriff auf den Benutzeraccount.
- Der Dienst ist in der Lage den IdP nach Attributen abzufragen, ohne die Herausgabe dieser Attribute vom Benutzer erlauben zu lassen.

Diese beiden Punkte entsprechen weder dem SAML-Standard noch dem Datenschutzgesetz. Die demonstrierte Beispielimplementierung bietet den Föderationsmitglieder mehrere Möglichkeiten, den SSH-Server zu nutzen. Somit lassen sich beide genannten Probleme umgehen. Eine vorgeschaltete Login-Seite stellt sicher, das der Benutzer sein Föderationspasswort dem SSH-Server nicht preisgeben muss und gewährleistet, dass der Benutzer der Weitergabe seiner Attribute zustimmen muss. Im Folgenden werden verschiedene Ansätze zur Ermöglichung eines ECP-fähigen SSH-Dienstes diskutiert. Darauf aufbauend wird die momentane Implementierung des Proof-of-Concepts eingehender beschrieben. Die Tabelle 1 zeigt eine Übersicht der hier diskutierten, möglichen Varianten eines ECP-fähigen SSH-Dienstes an.

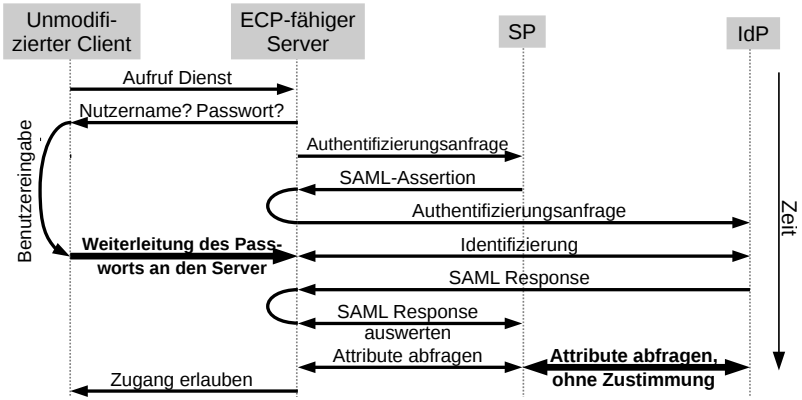

Bild 5: Kommunikationsschema eines ECP-fähigen Dienstes. Da der Client nicht ECP-fähig ist, kann nur der Server die Authentifizierung mit der Föderation durchführen. Hierfür muss dem Server das Passwort des Benutzers verfügbar sein. Dies entspricht nicht dem SAML2-Standard. Die Weitergabe der Attribute ohne Zustimmung des Benutzers entspricht nicht dem Datenschutzgesetz.

	Eigenes Home-Dir	Passwort verborgen	Abfragen d. Attribute	alternativer Login
Anonymer Zugang	-	-	-	-
Sofortiger Login	x	-	-	-
Anmelden m. Prüfung	x	-	x (ohne Zustimmung)	-
Register Seite	x	x	x	x

Tabelle 1: Übersicht der vorgestellten Login-Möglichkeiten

4.1 Anonymer Zugang

Mitglieder der Föderation könnte ermöglicht werden, sich mit ihrem Nutzernamen und ihrem Benutzerpasswort der Heimatorganisation direkt am ECP fähigen SSH-Server anzumelden. Das Benutzerpasswort muss dem SSH-Server anvertraut werden, damit dieser den Heimat-IdP fragen kann, ob der Benutzer ein Account innerhalb der Föderation besitzt. Ist die Antwort vom IdP positiv, wird der Zugriff auf ein dienstlokales Gastkonto ohne persistentem Heimatverzeichnis gewährt. Dieser Ansatz bedingt keiner lokalen Datenhaltung. Da der SSH-Server keine Attribute abfragen muss, ist diese Variante konform mit dem Datenschutz. Die Autorisierung des Dienstes kann allerdings nur sehr grob erfolgen.

4.2 Sofortiger Zugang mit Heimatverzeichnis und eindeutigem Namen

Zusätzlich zur oben beschrieben Methode, ist es möglich eine eindeutige Zuweisung der Benutzer durch eine randomisierte, aber persistenten Identität (PersistentID) zu ermöglichen. Solch eine persistentID wird vom Heimat-IdP für jeden Benutzer generiert und an die SP geliefert. Diesem Ansatz sind die gleichen Nachteile behaftet wie dem Anonymen Zugang. Durch eine dienstlokale Datenbank ist es allerdings möglich, den Benutzern ein persistentes Heimatverzeichnis zuzuordnen. Auch wenn sich der Nachname eines Nutzers ändern sollte, bleibt die PersistentID erhalten.

4.3 Anmelden mit Prüfung der Attribute

Die beschriebenen Methoden lassen sich so erweitern, dass der SSH-Server zusätzlich die Attribute der Benutzer beim IdP erfragt. Somit ließe sich stets die Zugangsberechtigung prüfen - allerdings wäre die Abfrage der Attribute ohne Zustimmung und die Herausgabe durch den IdP ein Bruch des Datenschutzes.

4.4 Zugang über Registrierungsseite

Um sowohl den Datenschutz zu beachten und nicht auf die Herausgabe des Föderationspassworts zu bestehen, funktioniert die Implementierung des Proof-of-Concepts nach folgendem Schema: Vor dem ersten nutzen des SSH-Server muss der Nutzer mit seinem Browser auf eine Registrierungsseite navigieren. Somit lässt sich sicherstellen, dass ein Nutzer, der den SSH-Zugang erwünscht, der Datenweitergabe aktiv zustimmt. Daraufhin erstellt die Seite einen Eintrag in einer dienstlokalen Datenbank. Dem SSH-Server ist nach dieser Prozedur der Benutzer bekannt. Die Registrierungsseite zeigt dem Benutzer ein einmalig gültiges Passwort an, dass für den SSH-Login verwendbar ist. Nach jedem Login wird das Passwort neu gesetzt. In zukünftigen Versionen bietet die Seite eine Option, dass der Benutzer sein öffentlichen Schlüssel hinterlegen kann. Somit entfällt die Eingabe des Einmal-Passworts. Eine Weitergabe des Passworts an den SP ist nicht mehr nötig. Die Zustimmung des Benutzers zur Weitergabe von Attributen kann eingeholt werden und die Heimatverzeichnisse auf dem SSH-Server sind persistent. Benutzer können sich de-registrieren falls sie ihr Konto auf dem SSH-Server löschen möchten. Die hinterlegten Attribute und Daten werden dann vollständig gelöscht. Im folgenden wird die detaillierte Funktionsweise geschildert.

5 Funktionsweise SSH-Login

Der Proof-of-Concept besteht aus einem selbst entwickeltem PAM-Modul, einer PostgreSQL-Nutzerdatenbank und mehreren PHP-Modulen, entwickelt von Universität Karlsruhe (KIT) und Universität Konstanz. In diesem Abschnitt wird auf die SSH Proof-of-Concept Implementierung näher eingegangen.

5.1 Registrierung über Webseite

Ein potentieller Nutzer des SSH-Servers öffnet zur erstmaligen Freischaltung des Diensts die Registrierungsseite mit seinem Browser. Die Seite ist durch Shibboleth geschützt. Nur Föderationsmitglieder haben darauf Zu-

griff. Das Benutzerpasswort wird durch Browserweiterleitung direkt am IdP eingegeben und ist dem SP nicht zugänglich. Wie im Bild 6 (Schritt 4) gezeigt, stimmt der Benutzer aktiv der Weitergabe seiner Attribute zu oder beendet alternativ die Sitzung.

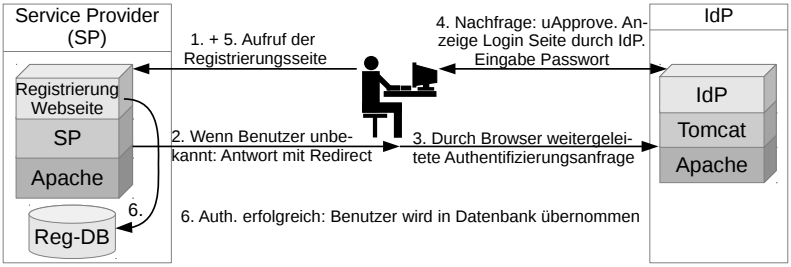

Bild 6: Notwendige Registrierung, um den ECP-fähigen SSH-Server zu nutzen. Die Registrierungsseite ist durch Shibboleth mit uApprove geschützt. Der Benutzer muss der Weitergabe seiner Attribute aktiv zustimmen. Der Browserredirect garantiert, dass der SP kein Zugriff auf das Benutzerpasswort bekommt.

5.2 Registrierungsseite

Nach der Zustimmung wird der Browser zurück auf die Registrierungsseite geleitet. Da der Benutzer nun eine gültige SAML-Session besitzt, zeigt die Webseite die vom IdP gelieferten Attribute an. Mit einem Klick auf einen “registrieren”-Knopf werden die gelieferten Attribute gespeichert. Zusätzlich wird zu jedem Account eine User-ID, Username und temporäres Passwort (One-Time-Passwort: OTP) generiert und hinterlegt. Das temporäre Passwort wird im Browser angezeigt. Die Registrierung ist damit abgeschlossen. Der Benutzer hat mit den angezeigten Daten nun Zugriff auf den SSH-Server, wie bereits in Abschnitt 4.4 erwähnt. In einer zukünftigen Version der Registrierungsseite wird es möglich sein, dass der Benutzer direkt sein öffentlichen Schlüssel hinterlegt.

5.3 Einloggen auf den SSH-Server

Das im Rahmen des bwIDM-Projekts entwickelte PAM-Modul untersucht jeden SSH-Login-Versuch. Stammt der einloggende Benutzer aus der Föderation, prüft das Modul die Eingabe des temporären Passworts. Alternativ kann sich der Benutzer über sein privaten Schlüssel einloggen. Stimmt das temporäre Passwort oder der Schlüssel, erfolgt eine Abfrage der Attribute am Heimat-IdP des Benutzers. Da der SP dem IdP bakannt ist, entspricht der IdP der Anfrage und liefert die Attribute aus. Nur wenn dort noch ein aktiver Account besteht, wird dem Login-Versuch stattgegeben. Falls das temporäre Passwort zum einloggen verwendet wurde, wird ein neues generiert. Durch die Verwendung dieser alternativen Loginvarianten benötigt der SSH-Server kein Zugriff auf das persönliche Passwort. Zusätzlich kann sich der Benutzer auch mit seinem Benutzerpasswort der Heimatorganisation anmelden - nimmt dann allerdings in kauf, dass das Passwort am SSH-Server einsehbar ist. Die Zuweisung von Föderationsaccounts zu lokalen Benutzernamen übernimmt der Name Service Switch (NSS) von Linux und nutzt hierfür die von der Registrierungsseite befüllte PostgreSQL-Datenbank. Dem System ist somit das Heimatverzeichnis, die UID und GID bekannt.

5.4 Ausscheiden eines Mitgliedes aus der Föderation

Scheidet ein Mitglied aus der Föderation aus, ist es sinnvoll, die hinterlegten Daten ebenfalls zu löschen. Die Löschung von Daten auf Wunsch des Benutzer ist durch die Verwendung der Registrierungsseite möglich. Auf dieser Seite ist dem Benutzer die Möglichkeit geboten, seine gespeicherten Daten einzusehen und zu löschen.
Da die Nutzerdaten bei jedem Login geprüft werden, kann auf Statusänderungen eines Benutzers reagiert werden, ohne dass es einer manuellen, lokalen Datenbankpflege benötigt. Das PAM-Modul prüft bei jedem Login eines authentifizierten Nutzers dessen Attribute. Dabei wird geprüft, ob dem Nutzer immer noch die nötigen Rechte innerhalb der Föderation zugewiesen sind und der Benutzer immer noch Teil der Föderation ist. Zugang wird gewährt, wenn sowohl die Zugangsdaten als auch die zugewiesene At-

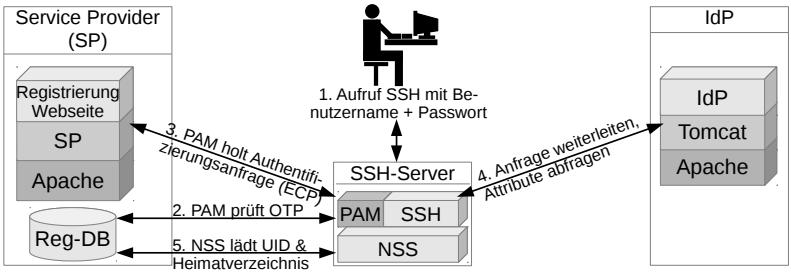

Bild 7: Das PAM bearbeitet den SSH-Loginversuch und prüft die Gültigkeit des Benutzereintrags über ECP am IdP. Hierfür kann der Benutzer sein OTP oder seinen Public Key nutzen. Würde der Benutzer sein persönliches Kennwort für den Login nutzen, hätte der SSH-Server ungeschützten Zugriff auf dieses.

tribute gültig sind. Ändern sich die Attribute, werden diese Änderungen in der dienst-lokalen Datenbank übernommen. Scheidet ein Teilnehmer aus der Föderation aus, verweigert auch der SSH-Server den Zugang.

6 Fazit

In dieser Arbeit wurde ein Überblick der SAML-Föderation gegeben. Es wurde gezeigt, dass SAML bzw. Shibboleth konform mit den herrschenden Datenschutzbestimmungen sind. Da gewisse Dienste nicht web-fähig gemacht werden können, besteht die Notwendigkeit, eine Authentifizierung ohne die Anzeige von HTML-Seiten und Weiterleitungen mittles HTTP-Redirects durchzuführen. Das in SAML integrierte ECP-Profil bietet diese Funktionalität. Anhand eines exemplarischen, ECP-fähigem SSH-Dienst wurde gezeigt, dass nicht web-fähige Dienste über ECP in eine Föderation integrierbar sind. Eine im Rahmen des bwIDM-Projekts entwickelte Registrierungsseite ermöglicht einem Benutzer seine Datenfreigabe einzusehen und der Datenweitergabe zuzustimmen. Ebenfalls ist dem Nutzer die Möglichkeit gegeben, alternative Techniken für den Login zu nutzen. Die Weitergabe des Föderationspassworts an den Dienst ist nicht nötig. So bleiben

die Datenschutzbestimmungen berücksichtigt und ein ECP-fähiger Dienst darf konform mit den geltenden Bestimmungen auf die Attribute eines Benutzers zugreifen.

Literaturverzeichnis

[1] M. Amberg, M. Hirschmeier und D. Schobert. Dart - Ein Ansatz zur Analyse und Evaluierung der Benutzerakzeptanz. In *Wirtschaftinformatik Proceedings 2003*.

[2] T. Gross. Security analysis of the saml single sign-on browser/artifact profile. In *Computer Security Applications Conference, 2003. Proceedings. 19th Annual*, Seiten 298 – 307, Dez. 2003.

[3] J. Köhler, S. Labitzke, M. Simon, M. Nussbaumer und H. Hartenstein. FACIUS: An Easy-to-Deploy SAML-based Approach to Federate Non Web-Based Services. In *IEEE International Conference on Trust, Security and Privacy in Computing and Login-Node Communications (TrustCom-2012)*, Liverpool, UK, Juni 2012.

[4] A. G. Morgan. Pluggable authentication modules for linux: An implementation of a user-authentication api. *Linux J.*, 1997(44es), Dez. 1997.

[5] OASIS. Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0. Technical report, OASIS Standard, Mrz 2005.

[6] M. Simon, M. Waldvogel, S. Schober, S. Semaan und M. Nussbaumer. bwIDM: Föderieren auch nicht-webbasierender Dienste auf Basis von SAML. In *DFN Forum Kommunikationstechnologien*, volume 5 von *Lecture Notes in Informatics (LNI - Proceedings, GI-Edition)*, Seiten 119–128, Germany, Regensburg, Mai 2012.

[7] SWITCH. Expert aai demo. Online verfügbar: http://www.switch.ch/aai/demo/2/expert.html, Letzter Aufruf 25.04.2012.