16 Starke Authentifizierung für den sicheren Zugriff auf IT-Ressourcen in Föderationen

Christian Senk, Dieter Bartmann

Zusammenfassung. Die Gewährleistung der Informationssicherheit bei der Ausführung hochflexibler Geschäftsprozesse erfordert in unternehmensübergreifenden Szenarien wirksame und gleichzeitig flexible Sicherheitsmechanismen. Das Föderierte Identitätsmanagement liefert Technologien für eine Zugriffskontrolle auf überbetrieblich bereitgestellte IT-Ressourcen. Gerade bei einer schwach ausgeprägten Vertrauensbeziehung zwischen Föderationsteilnehmern sowie der Implikation eines hohen Schutzbedarfs besteht die Notwendigkeit einer Zweifaktorauthentifizierung. Die föderationsweite Verfügbarkeit entsprechender Systeme kann nicht unterstellt werden. Somit schränkt die Forderung nach einer starken Authentifizierung die Strukturflexibilität eines Geschäftsprozesses potenziell ein. Eine geeignete Lösung ist die bedarfsweise Delegation einer biometrischen Authentifizierung an einen externen Dienstleister. Hierzu erfolgte die prototypische Implementierung eines Tippverhaltenserkennungsdienstes, der die Einbindung einer „Zweit"-Faktorauthentifizierung nach „Software as a Service"-Prinzipien ermöglicht. Zudem wurde eine Infrastruktur für Föderiertes Identitätsmanagement so erweitert, dass die Durchführung einer biometrischen Authentifizierung föderationsweit belegbar ist.

16.1 Problemstellung und Zielsetzung

Während der Ausführung eines Geschäftsprozesses muss stets dafür Sorge getragen werden, dass nur autorisierte Akteure Zugriff auf geschützte Ressourcen erlangen. Innerhalb von Unternehmensgrenzen lässt sich dies durch ein zentralisiertes Identitäts- und Zugriffsmanagementsystem realisieren. In überbetrieblichen Anwendungsfällen ist die Gewährleistung eines sicheren Zugriffs auf IT-Ressourcen jedoch nicht trivial. Gerade in Szenarien mit substanziellen strukturellen Flexibilitätsanforderungen sind zentralisierte Ansätze weniger sinnvoll, da sie mit hohem Aufwand für die Erstellung und die Pflege unternehmensübergreifend redundanter Benutzerkonten verbunden sind (Hommel 2007, S. 38). Dieser Nachteil lässt sich zunächst durch eine Verteilung der Benutzerverwaltung auf die jeweiligen Heimatorganisationen umgehen. Zur Umsetzung eines Identitäts- und Zugriffsmanagements zur Unterstützung (hoch-) flexibler interorganisatori-

scher Geschäftsprozesse gewinnen deswegen Technologien des Föderierten Identitätsmanagements zunehmend an Bedeutung (Hommel 2007, S. 38, Reiser 2008, S. 8 ff.). Allerdings schränken solche Ansätze die Kontrollmöglichkeiten für den Ressourceneigentümer ein. Sowohl weiter steigende Flexibilitätsanforderungen als auch die Zunahme rechtlicher und regulativer Anforderungen an die betriebliche Informationsverarbeitung implizieren so die unzureichende Eignung des hierbei unterstellten Vertrauensmodells (Senk 2010).

Zielsetzung des vorliegenden Beitrags ist die gestaltungswissenschaftliche Entwicklung (Hevner et al. 2006) eines Authentifizierungsdienstes, welcher die Sicherheit beim Zugriff auf IT-Ressourcen in Föderation erhöht und hierbei den Strukturflexibilitätsanforderungen heutiger und künftiger Geschäftsprozesse genügt. Angelehnt an die Methodik ist dieser Beitrag wie folgt aufgebaut: Abschnitt 16.2 führt als motivierendes Beispiel einen Anwendungsfall der e-Car AG ein und leitet hieraus Grundanforderungen an das zu entwickelte System ab. Abschnitt 16.3 dient der Abgrenzung begrifflicher Grundlagen sowie der Darlegung der Vorteile einer Zweifaktorauthentifizierung mittels Biometrie. Die Beschreibung des implementierten Dienstes erfolgt in Abschnitt 16.4 die Bewertung anschließend in Abschnitt 16.5. Eine Abgrenzung von verwandten Arbeiten wird in Abschnitt 16.6 vorgenommen. Abschnitt 16.7 liefert eine Zusammenfassung und einen Ausblick.

16.2 Anwendungsbeispiel „e-Car Net Partner Portal“

Die e-Car AG (siehe Kapitel 2) bietet ihren Kunden beim Neuwagenkauf äußerst flexible Konfigurations- und Gestaltungsmöglichkeiten, wie z. B. die Farb- und Motivgebung von Karosserieteilen oder die Maßanfertigung von Bedienelementen. Hierzu sieht der Prozess „Individualteilebeschaffung“ die flexible Einbindung externer Produzenten explizit vor. Dies ist nicht vollständig planbar und erfüllt somit eine Eigenschaft hochflexibler Geschäftsprozesse (hGP). Die unvollständige Planbarkeit beruht auf folgendem Sachverhalt: Die Auftragsvergabe folgt einer Ausschreibungsphase, welche über ein Marktplatz-System abgewickelt wird. Bekommt ein Produzent den Zuschlag, erlangt er die Möglichkeit, webbasiert auf ausgewählte Detailspezifikationen des betroffenen Fahrzeugmodells zuzugreifen. Hierzu wurde ein Partner-Portal implementiert. Da solche Daten Forschungs- und Entwicklungswissen der e-Car AG enthalten und Konkurrenten einen möglichen Wettbewerbsvorteil verschaffen, sind sie inhärent mit einem „sehr hohen“ Schutzbedarf und entsprechenden Zugriffskontrollanforde-

rungen behaftet. Deshalb wird eine rein passwortbasierte Authentifizierung als unzureichend erachtet. Technische Spezifikationen, wie z. B. CAD-Zeichnungen, werden unternehmensintern in Dokumentenform verarbeitet. Gemäß der geltenden Sicherheitspolitik dürfen diese Dokumente nicht physisch, also z. B. per Email, verteilt werden. Stattdessen werden sie kategorisiert in einem dedizierten Content Management System abgelegt. Dieses ermöglicht einen Lese-Zugriff per Web-Browser. Ein Zugriff eines externen Benutzers auf Spezifikationen über diese Web-Schnittstelle soll mittels starker Authentifizierung zusätzlich geschützt werden. Ein Mitarbeiter eines externen Produzenten soll nur auf Spezifikationen solcher Kategorien Zugriff haben, für welche er bei Auftragsabschluss autorisiert wurde. Über dasselbe Web-Portal sollen Partner zudem Zugriff zu allgemeinen technischen Daten erlangen, wobei deren Schutzbedarf lediglich als „moderat“ bewertet wird. Aus Flexibilitätsgründen soll hier eine weniger restriktive Nutzerauthentifizierung ermöglicht werden. Zugriffe auf IT-Ressourcen mit hohem Schutzbedarf sollen außerdem ex post eindeutig der zugreifenden Person zuordenbar sein. Die Anforderungen werden in Tab. D-3 zusammengefasst.

Anforderung	Erläuterung
Effiziente Benutzerkontenverwaltung	Schnelles und flexibles Einrichten, Pflegen und Deaktivieren der Benutzerkonten externer Partner.
Praktikable Authentifizierung	Durchsetzbarkeit eines skalierbaren, schutzbedarfsabhängigen Authentifizierungsniveaus für angemessenen Nutzungskomfort.
Strukturflexibilität der Infrastruktur	Möglichst lose Kopplung zu den heterogenen Sicherheitsinfrastrukturen der Partnerorganisationen.
Zurechenbarkeit von Zugriffen	Eindeutige Zurückführbarkeit der Zugriffe auf natürliche Personen im Rahmen durchgeführter Audits.
Mandantenbezogene Autorisierung	Zugriffsrechte für externe Benutzer werden mandantenspezifisch für bestimmte Ressourcenbereiche vergeben.

Tab. D-3: Anforderungen „e-Car Net Partner Portal“

16.3 Grundlagen

Im folgenden Abschnitt werden die Grundlagen für das Verständnis der anschließenden Systementwicklung geschaffen. Dies umfasst zunächst die Abgrenzung des Identitätsmanagementbegriffs. Es wird gezeigt, dass ein Föderiertes Identitätsmanagement Voraussetzung für den sicheren Zugriff auf IT-Ressourcen in hGP ist, hierbei allerdings die Notwendigkeit einer starken (z. B. Zweifaktor-)

Authentifizierung impliziert. Als zweiter Faktor, zusätzlich zum Passwort, eignet sich Biometrie in besonderem Maße.

16.3.1 Identitätsmanagement

Die Disziplin des Identitätsmanagements (IdM) bildet die Grundlage für den sicheren Zugriff auf IT-Ressourcen und umfasst hierbei alle erforderlichen Maßnahmen, um Benutzer von Informationssystemen, bzw. Akteure in Geschäftsprozessen, zu erkennen und ihnen genau die zur Ausführung ihrer Tätigkeit notwendigen Zugriffe zu ermöglichen (Dierstein 2004, S. 347 f.; Eckert 2009, S. 189 ff.; Hommel 2007, S. 14 f.; Mezler-Andelberg 2008, S. 14 f.). Die Basisfunktionen des IdM sind somit zunächst die Authentifizierung, also die Bestimmung oder Überprüfung einer Benutzeridentität, sowie die Autorisierung, d. h. die Zuweisung und Überprüfung von Zugriffsrechten von Benutzern auf bestimmte (IT-) Ressourcen (Hommel 2007, S. 14 f.; Mezler-Andelberg 2008, S. 27 ff.). Die Überwachung einer Ressource sowie die Entscheidung, ob ein Subjekt für einen Zugriff tatsächlich autorisiert ist, wird als Zugriffskontrolle bezeichnet (Schläger 2008, S. 33). Aufbauend auf diesen Funktionen werden Zugriffe protokolliert, um diese eindeutig bestimmten Subjekten zurechnen und retrospektiv auswerten zu können. Diese Zurechnungsfunktion ist wiederum die Basis für eine betriebswirtschaftliche Leistungsverrechnung (Accounting i. e. S.) sowie das Auditing (Hommel 2007, S. 261 f.). Im Rahmen von Audits werden Zugriffsrechte sowie erfolgte Zugriffe auf die Einhaltung interner und externer Vorgaben geprüft (Hommel 2007, S. 261 f.; Mezler-Andelberg 2008, S. 189 ff.).

16.3.2 Basismodelle des Identitätsmanagements

Zur Umsetzung eines Identitätsmanagements haben sich drei Basismodelle herausgebildet, wobei sich davon nur das letzte für hGP in Verbundstrukturen eignet (Senk 2010). Die Modelle werden im Folgenden kurz beschrieben:

Innerbetriebliches Identitäts- und Zugriffsmanagement

Das Konzept des innerbetrieblichen Identitäts- und Zugriffsmanagements (engl. „Identity & Access Management“, IAM) beschreibt die applikationsübergreifende Zentralisierung des IdM. Hierzu wird ein zentrales Identitätsverzeichnis durch sog. führende Systeme (z. B. HR, CRM) mit relevanten Informationen bestehender interner und externer Benutzer gespeist. In der Praxis wird dieses Verzeich-

nis meist als Dienst auf Basis des LDAP-Protokolls realisiert. Zielsysteme, d. h. geschützte unternehmensinterne IT-Ressourcen (Dienste oder Applikationen), beziehen benötigte Benutzerdaten aus dem zentralen Identitätsverzeichnis direkt über die verfügbaren Verzeichnisdienstschnittstellen oder indirekt über geeignete Konnektoren. Dies induziert sowohl Kosten- als auch Qualitätsvorteile. Zudem ermöglicht die applikationsübergreifend zentralisierte Datenhaltung ein unternehmensweites „Single Sign-On“ (SSO). (Hommel 2007, S. 15 ff.)

Nutzerzentriertes Identitätsmanagement

Das nutzerzentrierte IdM (engl. „User-centric Identity Management“, UCIM) sieht einen Benutzer selbst als autonome Verwaltungsinstanz für seine Identität. Er verwaltet eine beliebige Anzahl unterschiedlicher digitaler Identitäten und entscheidet fallbezogen, unter welcher Identität er gegenüber einem IT-System auftritt und welche Informationen er über sich preisgibt. Technisch erfolgt dies beispielsweise über das OpenID-Protokoll. (Arias Cabarcos et al. 2009, S. 179; Hommel 2007, S. 57 ff.)

Föderiertes Identitätsmanagement

Das Föderierte Identitätsmanagement (engl. „Federated Identity Management“, FIM) beschreibt das verteilte IdM in einem Verbund aus administrativ unabhängigen Organisationen. Dieser Verbund wird als Föderation (engl. „Identity Federation“) bezeichnet. Verantwortlich für die Authentifizierung und die digitale Identität eines Benutzers in der Föderation ist dessen Heimatorganisation, der sog. „Identity Provider“ (IdP). Organisationen, welche innerhalb der Föderation IT-Ressourcen anbieten, werden als „Service Provider“ (SP) bezeichnet. Versucht ein Benutzer auf IT-Ressourcen eines SP zuzugreifen, so muss er vom IdP, also seiner Heimatorganisation, zunächst authentifiziert werden. Der IdP bestätigt anschließend dem SP protokollbasiert, dass er für diesen Benutzer und dessen Identität bürgt. Auf der Grundlage dieser Bestätigung (engl. security assertion) trifft der SP die Zugriffsentscheidung. Da sich der Benutzer nicht direkt beim SP sondern bei seiner Heimatorganisation authentifiziert, ist er dem SP nicht zwangsweise a priori bekannt. Dies bedeutet, dass der SP den Aussagen des IdP vertrauen muss. Eine bestehende organisatorische Vertrauensbeziehung zwischen allen IdP und SP ist also Voraussetzung für FIM. Vertrauensbeziehungen basieren hierbei i. d. R. auf expliziten Föderationsvereinbarungen (BSI 2010). Diese stellen hierbei Mindestvorgaben an die Sicherheitsmechanismen sämtlicher Föderationsmitglieder (BSI 2010). Das so entstehende Vertrauensgefüge

wird als Circle of Trust (CoT) bezeichnet und kann statisch oder dynamisch ausgeprägt sein. Die „Security Assertion Markup Language“ (SAML) (Wisniewski et al. 2005) und WS-Federation (Bajaj et al. 2003) stellen mögliche Ausprägungen von FIM dar. (Boursas 2009, S. 15 f.; Hommel 2007, S. 37 ff.; Tsolkas und Schmidt 2010, S. 259 ff.)

Identitätsmanagement für überbetriebliche hochflexible Geschäftsprozesse

Maßgebliche Anforderungen für ein überbetriebliches IdM zur Unterstützung von hGP sind (1) die Strukturflexibilität der notwendigen Infrastruktur sowie (2) ein hinreichend hohes Maß an Kontrolle über die Identitätsdaten zugreifender Subjekte (Senk 2010). So ist die Korrektheit und Qualität dieser Daten Voraussetzung für eine fundierte Zugriffsentscheidung, aber auch notwendig, um Zugriffe ex post eindeutig zuordnen und somit Compliance-Konformität nachweisen zu können (Dierstein 2004; Senk 2010).

Diese beiden Anforderungen erfüllt lediglich das FIM-Konzept (Senk 2010). Während IAM zwar die zentrale und somit direkte Kontrolle von Identitätsdaten ermöglicht, induziert es im Rahmen einer überbetrieblichen Anwendung einen hohen Aufwand für die Benutzerkontenverwaltung, welcher die mögliche strukturelle Flexibilität einschränkt (Hommel 2007; Senk 2010). UCIM hingegen bietet zwar ein sehr hohes Maß an nutzerseitiger Anwendungsflexibilität, bietet aufgrund des fehlenden organisatorischen Vertrauensmodells bestehender Ausprägungen nur eingeschränkte Möglichkeiten zur Sicherstellung der Korrektheit und Qualität von Identitätsattributen im betrieblichen Kontext (Arias Cabarcos et al. 2009, S. 179; Hommel 2007, S. 58 f.; Senk 2010).

Da FIM explizit für einen überbetrieblichen Einsatz konzipiert wurde, weist es so prinzipiell auch die beste Eignung für solche Anwendungsfälle auf (Hommel 2007, S. 37 ff.). Da allerdings zwischen SP und Benutzer über den IdP lediglich ein transitives Vertrauensverhältnis besteht und zwischen IdP und SP in der Praxis nur generische Vereinbarungen getroffen werden können, stellt der Nutzer bzw. dessen Authentifizierung bei einem hohen Schutzbedarf einer IT-Ressource ein mögliches Sicherheitsrisiko dar (Senk 2010; Thomas et al. 2008, S.72). Der belegbare Ausweis einer angemessenen Authentifizierungsstärke trägt hierbei zur Erhöhung der Transparenz bei Zugriffsentscheidungen sowie der Informationssicherheit in Föderationen bei (Senk 2010; Thomas et al. 2008, S. 72).

16.3.3 Zweifaktorauthentifizierung mittels Biometrie

Eine passwortbasierte Authentifizierung ist für den Zugriff auf IT-Ressourcen in Föderationen zur Unterstützung von hGP unzureichend, da hierdurch kein starkes Sicherheitsniveau erreicht werden kann (Hoonakker et al. 2009, S. 462; St. Clair et al. 2006, S. 51). Dies liegt an den begrenzten menschlichen Möglichkeiten im Umgang mit komplexen bzw. technisch hinreichend sicheren Passwörtern, einer so entstehenden organisatorischen Verwundbarkeit (Cowan et al. 2008) sowie an der nur schwachen künstlichen Bindung dieses Authentifizierungsfaktors an den Nutzer (Oppliger 1998; Smith 2002). Eine Möglichkeit zur Stärkung des Authentifizierungsniveaus ist die Ergänzung bestehender Verfahren um einen zweiten Faktor wie Besitz (z. B. USB-Token) oder Biometrie (z. B. Fingerabdruck). Hierbei spricht man von Zweifaktorauthentifizierung (Bakdi 2007, S. 11 ff.; Graevenitz 2006, S. 2; Jain et al. 2004, S. 7 ff.).

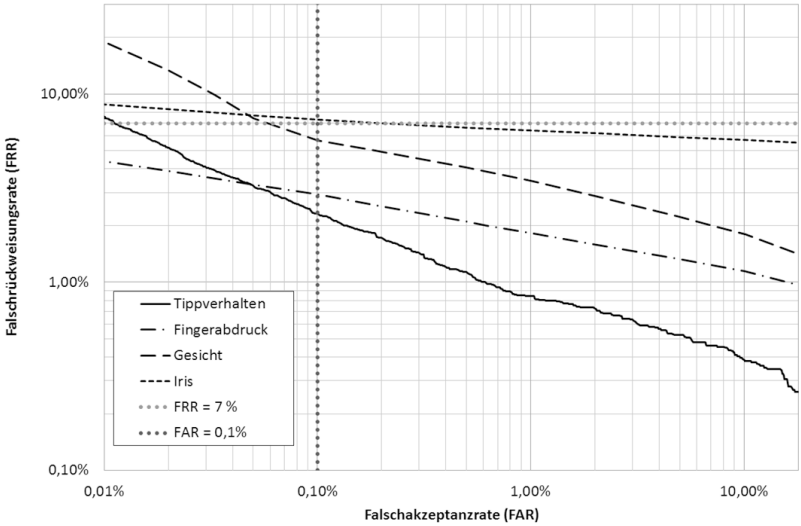

Abb. D-7: Vergleich der Erkennungsleistung ausgewählter biometrischer Systeme[27]

[27] Repräsentativ für die Tippverhaltenserkennung wurde ein System der Psylock GmbH herangezogen. Die zugehörigen Fehlerraten wurden vom Hersteller zu Verfügung gestellt (Stand: 2010). Die weiteren Daten stammen aus der im Jahre 2005 vom Bundesamt für Sicherheit in der Informationstechnik durchgeführten Studie BioP II.

Insbesondere die Biometrie eignet sich zur Realisierung des zweiten Faktors, also einer „Faktor-Zwei-Authentifizierung“ (F2A). Biometrische Authentifizierung bezeichnet hierbei die automatisierte Identifikation oder Verifikation einer Person anhand differenzierender verhaltensbasierter oder physiologischer Merkmale. Hierdurch wird eine potenziell höhere Authentifizierungsstärke erreicht als bei wissens- oder besitzbasierten Verfahren, welche durch eine lediglich künstlich erzeugte Personenbindung charakterisiert sind (Bakdi 2007, S. 12). Die Effektivität der Authentifizierung wird nicht mehr auf der organisatorischen Ebene durch den verantwortungsbewussten Umgang des Nutzers mit dem Authentifizierungsfaktor (z. B. Passwort, Hardware-Token) bestimmt, sondern auf technischer Ebene durch die Sicherheit und Erkennungsleistung des biometrischen Systems. Voraussetzung für eine biometrische Authentifizierung ist immer eine vorgelagerte Trainingsphase (Enrollment). Das Authentifizierungssystem registriert dabei das jeweilige Merkmal des Benutzers als Referenzdatensatz. Technisch bedarf es hierbei eines Sensors zur Digitalisierung des Merkmals. Während eines Authentifizierungsvorganges gibt der Nutzer eine weitere Probe seines Merkmals ab. Stimmt diese gemäß einer zuvor spezifizierten statistischen Toleranz mit dem Referenzdatensatz überein, so gilt die Authentifizierung als erfolgreich. Die Erkennungsleistung eines biometrischen Systems wird hierbei im Wesentlichen durch zwei Fehlerraten bestimmt, der Falschakzeptanz- (FAR) und der Falschrückweisungsrate (FRR). Eine „Detection Error Tradeoff“ (DET)-Kurve, die diese beiden Raten einander gegenüberstellt, ermöglicht die Vergleichbarkeit unterschiedlicher Systeme. (Graevenitz 2006, S. 2; Jain et al. 2004, S. 7 ff.)

Biometrische Authentifizierungssysteme erlangen derzeit zunehmend einen Reifegrad, der den breiten Praxiseinsatz ermöglicht (IBG 2009). Beispiele hierfür sind die Erkennung des Gesichts, der Iris, des Fingerabdrucks oder des Tippverhaltens, welche in Abb. D-7 auf der Basis marktgängiger Systeme einander gegenübergestellt werden. Die abgebildeten DET-Kurven zeigen, dass praktisch alle Systeme bei einer FAR von 0,1% eine FRR kleiner als 7% aufweisen; somit ist allen Lösungen gemäß der Vorgaben des BSI und der Common Criteria for Information Technology Security Evaluation ein für den Praxiseinsatz geeignetes Sicherheitsniveau zu bescheinigen (Biometric Evaluation Methodology Working Group 2002; BSI 2005). Einschränkend ist zu erwähnen, dass die verfügbaren Daten für die drei erstgenannten Verfahren 2005 erhoben wurden während die Messungen zur Tippverhaltenserkennung von 2010 stammen.

16.4 Systemkonzeption und Implementierung

Gegenstand des folgenden Abschnitts ist die Entwicklung einer Infrastruktur für FIM, welche eine bedarfsweise Zweifaktorauthentifizierung mittels Biometrie realisiert. Zur Authentifizierung über einen zweiten Faktor im Kontext hGP erweist sich der Bezug eines Dienstes nach dem „Software as a Service“-Prinzip als geeignet. Hierfür werden Entwurfsprinzipien spezifiziert. Es wird zudem gezeigt, dass zur Umsetzung eines entsprechenden Authentifizierungsdienstes die Tippverhaltenserkennung prädestiniert ist. Anschließend erfolgt die Beschreibung der entwickelten generischen Infrastruktur sowie des implementierten Dienstes.

16.4.1 Implikationen für den Architekturentwurf

Wie in Abschnitt 16.3.2 beschrieben, unterstellt FIM, dass die jeweilige Heimatorganisation für die betriebliche Identität eines Nutzers verantwortlich ist. Eine Fragmentierung der Identität eines (betrieblichen) Benutzers führt zudem zu technischen und organisatorischen Problemen (Hommel 2007). Deswegen ist es sinnvoll, dass der IdP auch für die Authentifizierung über einen zusätzlichen Faktor die Verantwortung behält (Hommel 2007, S. 57 f.; Olden 2010, S. 171 ff.). Dies führt aus der Sicht einer Föderation zu einer Reduktion auf folgende Architekturmuster:

Dezentralisierte biometrische Authentifizierung

Die Heimatorganisation des Benutzers betreibt im Rahmen ihres eigenen zentralisierten IAM autonom eine eingebettete biometrische Authentifizierungsinfrastruktur. Benutzer können so bei Bedarf, z. B. zusätzlich zur bestehenden passwortbasierten Identitätsbestimmung, biometrisch authentifiziert werden. In interorganisatorischen Szenarien muss das betriebliche IAM in der Lage sein, einem Dienst-Anbieter (SP) protokollbasiert eine vollzogene biometrische Benutzerauthentifizierung zu bestätigen, damit die Aussage im Rahmen des Vertrauensmanagements des SP verwertet werden kann. Während die organisationsinterne Integration einer biometrischen Authentifizierungsinfrastruktur mit den bestehenden zentralisierten IAM-Systemen ein praktisches Problem darstellt, müssen organisationsübergreifend Methoden zur Etablierung von Transparenz und Vergleichbarkeit der Ergebnisqualität unterschiedlicher Systeme geschaffen werden. Derzeitige Vorhaben zur Standardisierung und Zertifizierung biometri-

scher Verfahren und Systeme liefern hier einen möglichen Beitrag (Bitkom 2010; ISO 2009; TeleTrusT Deutschland e. V. und AG 6 2006).

Zentralisierte biometrische Authentifizierung

Verfügt eine Organisation nicht über eine dedizierte, für den föderierten Einsatz geeignete biometrische Authentifizierungskomponente, so besteht die Möglichkeit, die biometrische Authentifizierung durch einen externen Dienstleister zu beziehen, der für Betrieb und Wartung des Authentifizierungssystems verantwortlich ist. Das derartige Outsourcing von IT-Sicherheitsfunktionen wird allgemein als „Managed Security Service" (MSS) bezeichnet, welches auf unterschiedliche Arten erfolgen kann (Ding et al. 2005; Khalid Kark 2010):

- **Application Service Providing (ASP):** In Analogie zum ASP-Modell betreibt ein Dienstleister eine angepasste Systeminstanz für genau einen Kunden und stellt diesem die Authentifizierungsfunktionalität über dedizierte bzw. vereinbarte Schnittstellen zur Verfügung.
- **Software as a Service (SaaS):** Im Zuge der fortschreitenden Entwicklung des „Cloud Computings" (Buxmann et al. 2008, S. 500 ff.; Krcmar 2009, S. 698 f.) werden sicherheitsbezogene Dienste zunehmend auch nach SaaS-Prinzipien über Internetschnittstellen angeboten und genutzt. In solchen Fällen spricht man von „Security as a Service" (SECaaS) (Hafner et al. 2009). In Analogie zeichnet sich eine SECaaS-Lösung für den Dienstnehmer dadurch aus, dass sie als vollständig virtualisierte multimandantenfähige Ressource nutzbar ist, und dieser nur das bezahlt, was er auch tatsächlich nutzt (Baun et al. 2010, S. 37 f.; Münzl et al. 2009, S. 24; Krcmar 2009, S. 698 f.). Der derartige Bezug eines Authentifizierungsdienstes wird als „Authentication as a Service" (AaaS) bezeichnet (Forrester Research 2009, S. 1).

16.4.2 Authentication as a Service

Aufgrund der geringeren technischen und organisatorischen Abhängigkeit des Dienstnehmers zum Dienstanbieter und der somit höheren erreichbaren Strukturflexibilität innerhalb der Föderation, ist für den Bezug eines Authentifizierungsdienstes im Kontext hGP das SaaS-Modell dem ASP-Modell vorzuziehen. Aus diesem Grund folgt die prototypische Implementierung SaaS-Prinzipien.

Abgeleitet aus den Designprinzipien für SaaS-Dienste von LA und KIM (2009, S. 280) ergeben sich folgende technische Architekturanforderungen für AaaS-Systeme:

- **Anwendungsbezogene Dienst-Granularität:** Die Granularität eines AaaS-Dienstes muss sowohl funktionale Vollständigkeit als auch eine übergreifende Wiederverwendbarkeit ermöglichen. Funktional umfasst dies zunächst Methoden für die Benutzerregistrierung und die eigentliche Benutzererkennung, aber auch für die Administration des Dienstes.
- **Multi-Mandantenfähigkeit:** Um eine abnehmerspezifische Konfiguration und eine klare Datentrennung gewährleisten zu können, muss das System Mandantenfähigkeit explizit vorsehen. Zudem muss einem Mandanten eine dedizierte Konfigurationsschnittstelle zur Verfügung gestellt werden.
- **Standardisierte Netzwerkschnittstellen:** Der AaaS-Dienst muss über standardisierte Netzwerkschnittstellen in das Zielsystem des Abnehmers integrierbar sein. In betrieblichen Umgebungen impliziert dies die Verwendung von Standards wie SAML oder „WS-Federation".
- **Thin-Client-Anwendung:** Ein weiteres impliziertes Erfordernis ist die Umsetzung einer Thin-Client-Architektur. Systemelemente werden hierbei soweit wie möglich zum Betreiber ausgelagert. Dies schränkt die Menge der für die Umsetzung von AaaS geeigneten Authentifizierungsverfahren auf Ansätze ein, welche eine möglichst hohe relative Hardwareunabhängigkeit aufweisen. Die erforderlichen (Hardware-) Systeme dürfen somit in ihrer Anwendung nicht auf dedizierte Authentication Service Provider beschränkt sein und sind idealerweise im Einsatzkontext bereits deckend vorhanden. Dies prädestiniert wenige besitzbasierte Methoden (z. B. auf der Basis von Mobiltelefonen) sowie biometrische Verfahren, welche ein Merkmal über nicht-dedizierte Sensoren digitalisieren, die also unabhängig vom Authentifizierungszweck den Benutzern bereits verfügbar sind. Dies umfasst die Tippverhaltenserkennung über Standard-PC-Tastaturen sowie die Spracherkennung über eine geeignete Telefonanlage (Senk 2010). Weiterhin sind Verfahren mit dedizierten Sensoren geeignet, sofern deren breite Verfügbarkeit im Einsatzkontext unterstellt werden und diese gleichzeitig über eine standardisierte Kommunikationsschnittstelle (z. B. gemäß BioAPI) verfügen (Steffens 2009, S. 298).

Abb. D-8 beschreibt eine hieraus abgeleitete Systemarchitektur für AaaS zur Erweiterung bestehender IAM-Infrastrukturen für die Authentifizierung interner Benutzer über einen zusätzlichen Faktor. Aus technischer Sicht lagert das be-

triebliche IAM, welches zentralisiert Personen-, Autorisierungs- sowie Authentifizierungsdaten verwaltet, lediglich die partielle biometrische Identität bestimmter Nutzer an einen AaaS-Anbieter aus und leitet den Benutzer bei Bedarf an diesen zur Durchführung einer biometrischen Authentifizierung über, um so die resultierende Authentifizierungsbestätigung intern weiter zu verarbeiten und die partielle Identität des Benutzers zu ergänzen. Mitarbeiter, Kunden und Partner haben lediglich Zugriff auf die Enrollment- und Authentifizierungsschnittsttellen. Dieser erfolgt idealerweise Browser-basiert. Administratoren auf Mandantenseite pflegen technische und leistungsbezogene Parameter des Systems und binden vorhandene Schnittstellen in die eigene IAM-Infrastruktur ein.

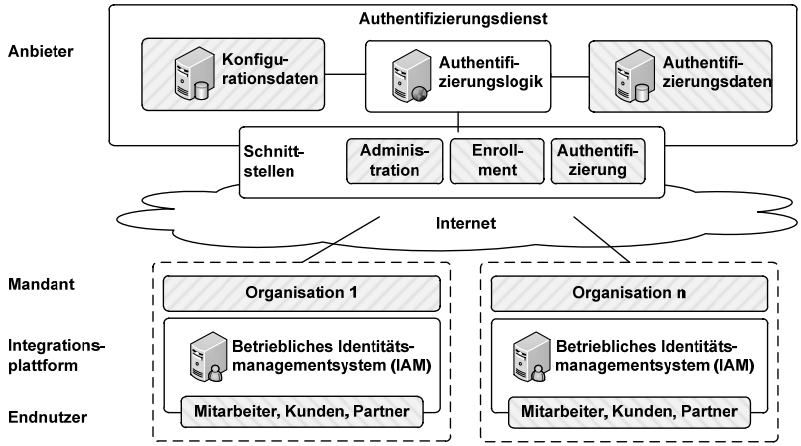

Abb. D-8: Authentication as a Service-Systemarchitektur für betriebliche Abnehmer

In Analogie zu SaaS kann diese Bezugsform insbesondere für kleine und mittlere Unternehmen relevant sein, für welche der autonome Betrieb einer derartigen Lösung nicht wirtschaftlich wäre (Buxmann et al. 2008, S. 500 ff.; Gartner 2008; Krcmar 2009, S. 698). Dies kann der Fall sein, wenn die biometrische Authentifizierung nicht deckend eingesetzt wird, also beispielsweise nur bei Zugriff auf besonders sensible Daten oder aufgrund expliziter (föderierter) Vereinbarungen. Studien von GARTNER (2008) und FORRESTER RESEARCH (2009) zufolge steigt zudem die Praxisrelevanz solcher Sicherheits- bzw. Authentifizierungsdienste.

16.4.3 Umsetzung mittels Tippverhaltenserkennung

Die technische Umsetzbarkeit eines biometrischen Authentifizierungssystems gemäß der spezifizierten AaaS-Architektur soll im Folgenden anhand der Tippverhaltensbiometrie gezeigt werden. Das Tippverhalten jedes einzelnen Menschen auf einer Tastatur ist, als stark vom Verhalten geprägtes biometrisches Merkmal, einerseits durch einfache, tagesformabhängige, stark schwankende Charakteristika, wie der Geschwindigkeit des Tippens, dem Tipprhythmus und der Präzision des Tippprozesses bestimmt (Bartmann et al. 2007, S. 2; Bergando et al. 2002, S. 367). Andererseits existieren aber auch tieferliegende Charakteristika, wie beispielsweise die Rechts- und die Linkshändigkeit, bezeichnende, wiederkehrende Tippfehler und ein eventuell damit verbundenes Korrekturverhalten oder die Fingerfertigkeit beim Tastengreifen (Bakdi 2007, S. 84 ff.). Diese prägenden Charakteristika treten im Bereich von Millisekunden auf. Folglich kann das menschliche Tippverhalten auch nicht antrainiert oder einfach weitergegeben werden (Chang 2006, S. 647 f.; Sung und Cho 2006, S. 654). Das Drücken sowie das Loslassen einer Taste und die dazu gehörenden Halte- und Übergangsdauern sind die direkten Messergebnisse des Tippverhaltens (Bakdi 2007, S. 65; Chang 2006, S. 648). Aus diesen lassen sich weitere, komplexe Charakteristika ableiten (Bakdi 2007, S. 6, 39, 67 ff.; Sung und Cho 2006, S. 654). Die zusätzliche Extraktion dieser Merkmale aus den ursprünglichen Messdaten ermöglicht es dann, eine höhere Verfahrensleistungsfähigkeit zu erzielen (Bakdi 2007, S. 91). Biometrische Verfahren auf der Grundlage des Tippverhaltens analysieren folglich eine Vielzahl von Charakteristika des menschlichen Tippens und können sowohl in Form eines textungebundenen Verfahrens als auch in Form eines textgebundenen Verfahrens arbeiten (Bakdi 2007, S. 25 f.; Dotzler 2010, S. 53). Textungebundene Verfahren können das Tippverhalten anhand der Eingabe beliebiger Texte untersuchen (Bakdi 2007, 25 f.). Für den Enrollmentprozess, in dem das Verfahren das Tippverhalten eines Merkmalsträgers erlernt, sowie für die eigentlichen Authentifizierungsprozesse, finden beliebige und unterschiedliche Zeichenketten Verwendung (Bakdi 2007, S. 25 f.). Textabhängige Verfahren müssen im Gegensatz dazu stets denselben Eingabetext verwenden, sowohl für das Enrollment als auch für alle späteren Authentifizierungsvorgänge. Das Erkennungsverfahren ist hier fest mit der speziellen Tippvorlage verknüpft, mit welcher der Nutzer das System anfangs trainiert. Beide Verfahrensansätze eignen sich sehr gut zur Absicherung des Zugangs zu logischen Ressourcen am PC-Arbeitsplatz. Die Aufzeichnung der Tastaturereignisse erfolgt über eine Softwarekomponente, welche in beliebige Webseiten eingebettet wer-

den kann. Dies prädestiniert sie folglich auch für die Realisierung eines Web-basierten Authentifizierungsdienstes (Olden 2010; Pope und Bartmann 2010, Senk 2010). Tab. D-4 stellt ausgewählte Verfahren vergleichend gegenüber. Die Bewertung erfolgt in Anlehnung an DOTZLER (2010), POPE und BARTMANN (2010) sowie SENK (2010). Wesentliches Bewertungskriterium für starke Authentifizierungsverfahren im Kontext überbetrieblicher hGP ist die Strukturflexibilität, ohne welche die flexible Bildung von Föderationen nicht möglich ist (Senk 2010). Diese ist bei unterstellter Telearbeitsplatzinfrastruktur nur für die Tippverhaltensbiometrie gegeben. Ferner grenzt sich die Tippverhaltenserkennung von den genannten alternativen biometrischen Verfahren insbesondere durch die Skalierbarkeit des Verfahrens, die Praktikabilität sowie die Nicht-Zudringlichkeit ab. Damit eignet sich das Verfahren sehr gut zur Umsetzung eines F2A-Dienstes in flexiblen Föderationen.

	Verfahren				
Bewertungs-kriterien	**Passwort**	**HW-Token**	**Finger-abdruck**	**Stimme**	**Tippver-halten28**
Nicht-Übertragbarkeit des Authentifizierungsmerkmals	nein	nein	ja	ja	ja
Überwindungssicherheit des Verfahrens	schwach	stark	mittel	mittel	mittel-hoch
Strukturflexibilität (relative HW-Unabhängigkeit)	ja	nein	nein	kontext-abhängig	kontext-abhängig
Skalierbarkeit der Stärke des Verfahrens	mittel	schwach	mittel	mittel	hoch
Praktikabilität (Registrierung und Authentifizierung)	hoch	mittel	mittel	mittel	mittel-hoch
Nicht-Zudringlichkeit und Datenschutzfreundlichkeit	hoch	hoch	niedrig	mittel	hoch

Tab. D-4: Vergleichende Bewertung ausgewählter Authentifizierungsverfahren

Aus Praktikabilitätsgründen (Bakdi 2007, S. 26) wird für das zu implementierende Gesamtsystem ein textgebundenes Tippverhaltenserkennungssystem im

[28] Annahme eines marktgängigen textgebundenen Tippverhaltenserkennungsverfahrens

Verifikationsmodus herangezogen, welches den Autoren zu Forschungszwecken von der Psylock GmbH[29] zu Verfügung gestellt wurde.

16.4.4 Architekturentwurf

In Anlehnung an den föderierten Anwendungsfall wurde eine Makro-Systemarchitektur zur Einbindung externer Authentifizierungsdienste nach SaaS-Prinzipien spezifiziert. Diese umfasst die vier Entitätstypen IdP, SP, Authentication Service Provider sowie Trusted Third Party (TTP) (Abb. D-9). Die Schnittstellen zwischen den Entitäten unterteilen sich hierbei nach vorgelagerten und zugriffsbezogenen Prozessschritten:

Vorgelagerte Prozessschritte:

1. Für die spätere Signierung (partieller) Authentifizierungsbestätigungen verwendet der Authentication Service Provider einen (privaten) Signierschlüssel. Der zugehörige (öffentliche) Prüfschlüssel wird einer vertrauenswürdigen dritten Instanz (TTP) übermittelt.
2. Der IdP legt sich als Mandant beim Authentication Service Provider an. In diesem Zusammenhang werden für die kryptografisch gesicherte Übertragung zukünftiger Nachrichten Schlüssel ausgetauscht. Zudem erhält der IdP notwendige Schnittstellenspezifikationen und bindet diese an geeigneter Stelle in sein FIM-System ein.
3. Der SP gibt ein Profil für den Sicherheitsdatenverkehr innerhalb der Föderation bzw. zwischen SP und IdP vor. Jeder IdP muss seine FIM-Systeme dementsprechend konfigurieren. (Hommel 2007, S. 234 f.; Wisniewski et al. 2005, S. 4)

[29] Für Details zum System und zum Praxispartner, vgl. http://www.psylock.com

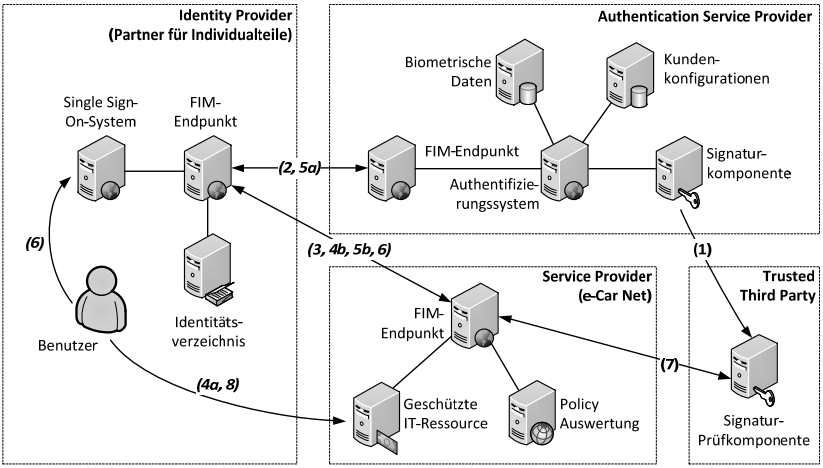

Abb. D-9: Architektur der Föderationsinfrastruktur

Zugriffsbezogene Prozessschritte:

4. Beim Versuch eines IdP-seitigen Benutzers auf eine geschützte IT-Ressource eines SP zuzugreifen (4a), ermittelt der SP standardmäßig aus dem spezifischen Schutzbedarf Anforderungen an die Qualität der Benutzerauthentifizierung und übermittelt diese Anforderung an den IdP (4b).
5. Daraufhin wird der Benutzer vom SSO-System des IdP aufgefordert, sich gemäß diesen Vorgaben zu authentifizieren (5a). Der IdP prüft diese Anforderungen und bindet bei Bedarf einen potenziell beliebigen externen Authentifizierungsdienst ein. In diesem Fall wird der Benutzer sowohl intern (passwortbasiert) als auch extern (2. Faktor) jeweils partiell authentifiziert. Die Bestätigung der durchgeführten F2A wird in signierter Form an den IdP übermittelt (5b).
6. Der IdP bestätigt für den zugreifenden Benutzer die durchgeführte 2.-Faktor-Authentifizierung und hängt die vom Authentication Service Provider dediziert signierte F2A-Bestätigung an.
7. Der SP validiert über die TTP und den dort hinterlegten Prüfschlüssel die gesendete F2A-Bestätigung.
8. Im positiven Fall wird geprüft, ob der Benutzer für den Zugriff autorisiert ist und ihm der Zugriff anschließend gewährt oder verweigert.

16.4.5 Prototypische Implementierung

Auf der Basis eines vom Praxispartner Psylock GmbH zur Verfügung gestellten Erkennungssystems zur tippverhaltensbasierten Benutzererkennung (Psylock Authentication Server, PAS) wurde ein AaaS-konformer Dienst prototypisch implementiert. Abb. D-10 zeigt die Architektur in vereinfachter Form. Für einen IdP verfügt der Dienst über zwei dedizierte Schnittstellen:

- **Web Service:** Es wurde ein Web Service `PreloaderWS` mit den Methoden `getCore()` und `getConfig()` implementiert: Die erlauben die dynamische Einbettung einer `Recorder`-Komponente in die Infrastruktur des Dienstnehmers sowie das Laden mandantenspezifischer Einstellungen wie den zu tippenden Eingabesatz. Der `Recorder` dient der Aufzeichnung der Tastaturereignisse während der Abgabe einer Tippprobe eines Benutzers über einen Web-Browser. Dieser wird vom Authentication Service Provider geladen und IdP-seitig zunächst gespeichert. Eine Prüfroutine garantiert hierbei die Verwendung der jeweils aktuellsten Version.
- **SAML:** Zum Austausch von Authentifizierungsnachrichten wurde eine SAML-Schnittstelle ergänzt. SAML beschreibt bereits ein umfassendes XML-Framework für solche Zwecke, welches eine einheitliche Semantik besitzt und spezifische Sicherheitsaspekte adressiert (Wisniewski et al. 2005). SAML ist ein offener Standard und wird deshalb der alternativen WS-Federation-Spezifikation vorgezogen. Zur Realisierung wurde die Open-Source-Implementierung Shibboleth IdP[30] angepasst und dem PAS vorangestellt. Sobald ein Benutzer die Abgabe einer Tippprobe abschließt, sendet der IdP einen `SAML authentication request`, welcher neben der Mandantenkennung (z. B. @e-car.net) die eindeutige Benutzerkennung sowie parametrisierbare Vorgaben an die zu erbringende Authentifizierungsqualität enthält. Hierzu sieht SAML explizit das Konstrukt `AuthenticationContext` sowie 25 bereits spezifizierte Schemata vor (Cahill et al. 2005, S. 21 ff.). Im vorliegenden Fall wurde das generische Schema `Unspecified` verwendet. Um das Mapping einer Anfrage auf einen konkreten Mandanten und dessen Dienstkonfiguration im PAS vornehmen zu können, wurde der Shibboleth IdP um eine Datenbank erweitert.

[30] Für eine detaillierte Beschreibung, vgl. SHIBBOLETH, http://shibboleth.internet2.edu/

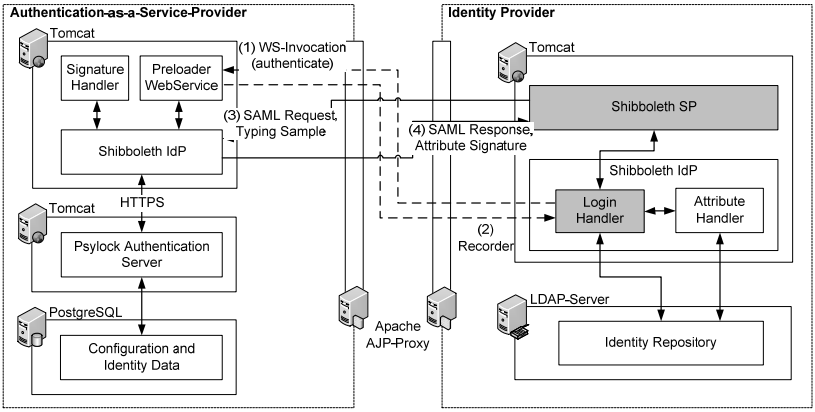

Abb. D-10: Schnittstelle zwischen Identity Provider und Authentication Service Provider

Zudem wurde ein `SignatureHandler` implementiert, der u. a. die biometrischen Authentifizierungsbestätigungen explizit signiert und als Attribut der SAML-Antwort anhängt. Dies ist notwendig, um auch nach einer Weiterverarbeitung der SAML-Bestätigung durch den IdP zweifelsfrei nachweisen zu können, dass eine externe Authentifizierung durch den Schlüsselinhaber erfolgreich durchgeführt und die Bestätigung nicht unautorisiert manipuliert wurde (Fox 1999, S. 620 ff.). SAML sieht selbst keine Mechanismen für eine solche Ende-zu-Ende-Integrität vor. Sobald dem Dienst die SAML-Anfrage des IdP sowie die logisch angehängte Tippprobe vorliegt, wird die Anfrage dem entsprechenden Mandanten zugeordnet und die Tippprobe dem Psylock Authentication Server zur Prüfung gegeben. Anschließend versendet der Dienst eine SAML-Antwort an den Dienstnehmer. Die Antwort besteht aus einer Authentifizierungsbestätigung (`AuthnStatement`) und einer Attributbestätigung (`AttributeStatement`). Die Authentifizierungsbestätigung besagt, dass der Benutzer nach den Vorgaben des `AuthenticationContext` authentifiziert wurde. Die Attributbestätigung liefert weitere qualitäts- oder sicherheitsinduzierende Informationen wie im Beispiel Details zum Authentifizierungsverfahren oder die dedizierte Signatur.

Auf der Seite des Dienstnehmers (IdP) wurde die Sicherheitsinfrastruktur hinsichtlich der Nutzung externer Authentifizierungsdienste erweitert. Hierbei wurde unterstellt, dass der IdP als Mitglied einer Föderation bereits ein Shibboleth IdP-System betreibt. Dieses ist mit dem betriebsinternen Identitätsverzeich-

nis[31] verbunden. Die Authentifizierung eines Benutzers wird über die Shibboleth `LoginHandler`-Komponente gesteuert. Standardmäßig unterscheidet diese jedoch nicht zwischen der Authentifizierung mit einem und mit zwei Faktoren. Deswegen erfolgt bei einer Authentifizierungsanfrage eines SP an den IdP ergänzend eine Prüfung des `SAML AuthenticationContext`. Lautet die Vorgabe `PasswordProtectedTransport`, so erfolgt eine interne passwortbasierte Benutzererkennung. Bei der Vorgabe `Unspecified` wird die Steuerung an eine neu entwickelte alternative `LoginHandler`-Komponente übergeben, welche explizit für die Durchführung einer Zweifaktorauthentifizierung zuständig ist und die Logik der Standard-Login-Komponente erweitert. Dies umfasst den clientseitigen Aufruf der zwei Schnittstellen des Authentifizierungsdienstes:

- **Web Service:** Die beiden Methoden des PreloaderWS-Web Service werden zur Einbettung der Aufzeichnungskomponente in die betriebsinterne Login-Portal-Seite sequentiell aufgerufen. Alternativ können an dieser Stelle auch (webfähige) Aufzeichnungs- oder Eingabekomponenten anderer interner oder externer Authentifizierungsdienste statisch oder dynamisch eingebunden werden (z. B. zur Eingabe eines Einmalpassworts oder zur Steuerung einer Sprachaufzeichnung) Abb. D-11 die vom entwickelten `LoginHandler` erzeugte Authentifizierungsseite. Die Umrandung kennzeichnet den dynamisch eingebundenen Recorder. Falls ein Benutzer kein biometrisches Profil beim referenzierten Dienst besitzt, wird dies während der Eingabe der Benutzerkennung dynamisch erkannt und anstelle des Recorders eine Umleitung zur Enrollment-Seite aktiviert.
- **SAML:** Sobald der Benutzer seine Kennung, sein Passwort und seine Tippprobe bestätigt, wird IdP-intern eine Überprüfung des Passworts vorgenommen. Verläuft diese positiv, so stößt der `LoginHandler` eine ergänzte Komponente (Shibboleth SP) an, welche eine SAML-Anfrage an den Authentifizierungsdienst erstellt und sendet. Parallel hierzu erfolgt die Sendung der Tippprobe. Der Shibboleth SP meldet die Antwort des Authentifizierungsdienstes an den `LoginHandler` zurück. Dieser fordert im negativen Fall eine erneute Benutzerauthentifizierung. Bei erfolgreicher Zweifaktorauthentifizierung wird die Authentifizierungsbestätigung an einen `AttributeHandler` weitergereicht.

[31] Implementiert mit OpenLDAP, vgl. http://www.openldap.org/

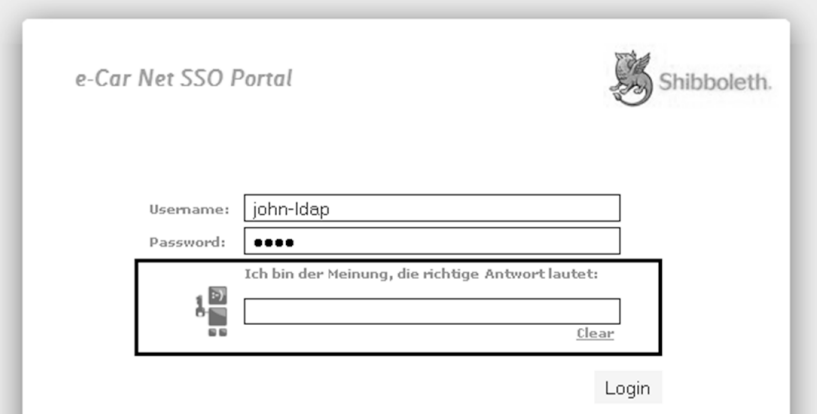

Abb. D-11: Screenshot der Shibboleth IdP Single Sign-On Login-Seite

Der `AttributeHandler` erzeugt und sendet standardmäßig eine SAML-Authentifizierungsbestätigung an den SP, welcher die IT-Ressource schützt, auf die der Benutzer des IdP Zugriff erlangen möchte. Der Shibboleth IdP wurde so konfiguriert, dass er neben dem `AuthenticationContext` Attribut sowohl die biometrische Authentifizierungsbestätigung als auch die zugehörige Signatur und den öffentlichen Schlüssel des Authentication Service Providers anhängt. Den öffentlichen Schlüssel und die signierte Authentifizierungsbestätigung kann der SP über den Web Service `CACertificate` der implementierten TTP prüfen und somit Ende-zu-Ende-Integrität sicherstellen (Fox 1999, S. 620 ff.).

16.5 Bewertung des Prototyps

Anhand eines Anwendungsfalls wurden in Abschnitt 16.2 Anforderungen spezifiziert, gegen welche eine Systembewertung erfolgte. Das Ergebnis zeigt zusammenfassend Tab. D-5. Die ersten vier Anforderungen gelten als vollständig erfüllt. Die Anforderung der mandantenbezogenen Autorisierung wurde nicht erfüllt, da diese durch ein entsprechendes Zugriffskontrollkonzept beim IdP adressiert werden muss. Der beschriebene Prototyp eines AaaS-Dienstes am Beispiel der Tippverhaltenserkennung belegt die technische Umsetzbarkeit des AaaS-Konzepts mit Biometrie. Das Verfahren eignet sich insbesondere aufgrund der hohen Praktikabilität und der Hardwareunabhängigkeit bei gegebener Telearbeitsplatzinfrastruktur. Außerdem implementiert das System des Praxispartners ausgereifte Mechanismen zur Steigerung von Qualität und Sicherheit. Die Erweiterung der FIM-Infrastruktur war notwendig, um die Ende-zu-Ende-Integrität der

vom Dienstleister ausgestellten biometrischen Authentifizierungsbestätigung gewährleisten zu können. Der Prototyp wird derzeitig weiterentwickelt. So verfügt das System bisher nicht über eine vollständig implementierte Mandantenschnittstelle, welche einem betrieblichen Administrator ein ausgereiftes Konten- und Nutzermanagement ermöglicht. Zudem wird gegenwärtig eine Funktion ergänzt, welche für ein sicheres Benutzer-Enrollment technisch ein 4-Augen-Prinzip erzwingt. Weiterhin induziert der Betrieb eines solchen Dienstes in einer offenen Cloud-Umgebung allgemeine und verfahrensspezifische Sicherheitsrisiken, welche eingängig untersucht und berücksichtigt werden müssen. Zudem erfolgt eine Validierung anhand weiterer ausgewählter Anwendungsfälle.

16.6 Abgrenzung zu verwandten Forschungsarbeiten

Während sich die vorliegende Arbeit auf den Schutz browserbasiert zugreifbarer IT-Ressourcen in Föderationen beschränkt, beschreibt Senk (2010) ein Konzept zur Durchsetzung starker Authentifizierung beim Zugriff auf IT-Ressourcen, welche im Kontext hGP physisch über Unternehmensgrenzen hinweg verteilt werden (z. B. Versendung digitaler Dokumente per Email). Referenzarchitekturen für FIM und IAM, welche dieser Arbeit zugrunde gelegt wurden, spezifiziert Hommel (2007). Olden (2010) entwickelte einen Tippverhaltenserkennungsdienst für das SSO privater Benutzer in OpenID-Umgebungen und stellt mögliche Lösungen für ausgewählte Qualitäts- und Sicherheitsprobleme vor. Eine datenschutzrechtliche Bewertung der Tippverhaltensbiometrie erfolgt in Dotzler (2010). Bakdi (2007) beschreibt tippverhaltensbasierte Erkennungsverfahren.

Anforderung	Erfüllt?	Erläuterung
Effiziente Zugriffskontenverwaltung beim SP	Ja	In FIM erfolgt beim SP keine Verwaltung einzelner Benutzerkonten, es erfolgt lediglich ein Schlüsselmanagement auf Organisationsebene.
Praktikabilität der Benutzerauthentifizierung	Ja	Der Authentifizierungsaufwand wird für den Benutzer flexibel an den Schutzbedarf der Ressource angepasst. Die Authentifizierung über einen zusätzlichen zweiten Faktor erfolgt nur bei erhöhtem Schutzbedarf. Das integrierte Tippverhaltenserkennungsverfahren zeichnet sich durch vergleichsweise hohe Praktikabilität aus. Der Benutzer erfährt während der F2A keine Umleitung zu einer dritten Instanz.
Strukturflexibilität der Sicherheitsinfrastruktur	Ja	Partnerorganisationen müssen selbst keine dedizierten internen Systeme zur Durchführung einer F2A betreiben Die Integration und die Nutzung des beschriebenen Authentifizierungsdiensts nach dem SaaS-Modell sind kostenflexibel und mit wenig Aufwand verbunden. Die spezifizierte Architektur ermöglicht die flexible Nutzung unterschiedlicher Authentifizierungsdienste unabhängiger Anbieter. SAML ist plattformunabhängig und weit verbreitet.
Zurechenbarkeit von Zugriffen auf IT-Ressourcen	Ja	Durch die Durchführung einer Zweifaktorauthentifizierung wird eine hohe Personenbindung erreicht. Die Identität der zugreifenden Person wird bei derzeitiger Konfiguration aus dem Identitätsverzeichnis des IdP abgerufen und dem SP zu Protokollierungszwecken übermittelt, ohne dass diese für die Autorisierung von Relevanz ist. Die übermittelte Identität kann auch durch ein Pseudonym ersetzt werden. In diesem Fall erfordert die Zurechnung einzelner Zugriffe die Kooperation des jeweiligen IdP.
Mandantenbezogene Autorisierung	Nein	Die Anforderung, dass Zugriffsrechte mandantenbezogen vergeben werden, wurde nicht umgesetzt und erfordert ein geeignetes Zugriffskontrollkonzept. Die hierfür erforderlichen Attribute sind allerdings bereits Bestandteil der SAML-Bestätigungen des implementierten Systems.

Tab. D-5: Anwendungsfallbezogene Bewertung des Systems

16.7 Fazit

Biometrie ist eine Zukunftstechnologie, die Potenziale hinsichtlich der Stärkung überbetrieblicher Vertrauensbeziehungen mittels Zweifaktorauthentifizierung bietet. AaaS stellt hierbei eine probate zentralisierte Lösung für den Bezug der partiellen F2A im Kontext von hGP dar. Die technische Durchführbarkeit wurde durch die Entwicklung eines Prototyps auf Basis der Tippverhaltenserkennung aufgezeigt. Dieses Verfahren eignet sich aufgrund der Verwendung handelsüblicher Tastaturen als Sensor und der hieraus resultierenden hohen relativen Hardwareunabhängigkeit in Telearbeitsplatzumgebungen in besonderem Maße für die Umsetzung eines webbasierten biometrischen Authentifizierungsdienstes. Zudem wurde eine FIM-Infrastruktur so erweitert, dass die Durchführung einer Authentifizierung über den zweiten Faktor organisationsübergreifend beweisbar bleibt, um so die Möglichkeiten zur Zugriffskontrolle auf IT-Ressourcen in Föderationen zu erweitern und das erreichbare Sicherheitsniveau somit zu erhöhen.

Der Prototyp wird, wie in Abschnitt 16.5 beschrieben, weiterentwickelt und validiert. Zudem werden derzeitig Untersuchungen zur Akzeptanz von SECaaS- und AaaS-Lösungen durchgeführt. Weitere offene Forschungsthemen betreffen die semantische und quantitative Beschreibung von Authentifizierungsqualität sowie ein hierauf aufbauendes Management von Vertrauensbeziehungen.

16.8 Literatur

Arias Cabarcos P, Almenárez Mendoza F, Marín-López A, Díaz-Sánchez D (2009) Enabling SAML for Dynamic Identity Federation Management. In: Wozniak J, Konorski J, Katulski R, Pach A (Hrsg.) Wireless and Mobile Networking. Springer Boston.

Bajaj S, Della-Libera G, Dixon B, Dusche M, Hondo M, Hur M, Kaler C, Lockhart H, Maruyama H, Nadalin A, Nagaratnam N, Nash A, Prafullchandra H, Shewchuk J (2003) Web Services Federation Language (WS-Federation). Version 1.0. http://specs.xmlsoap.org/ws/2003/07/secext/WS-Federation.pdf. Abruf am 2011-03-15.

Bakdi I (2007) Benutzerauthentifizierung anhand des Tippverhaltens bei Verwendung fester Eingabetexte. Universitätsverlag, Regensburg.

Bartmann D, Bakdi I, Achatz M (2007) On the Design of an Authentication System Based on Keystroke Dynamics Using a Predefined Input Text. International Journal of Information Security and Privacy 1(2):1–12.

Baun C, Kunze M, Nimis J, Tai S (2010) Cloud computing. Web-basierte dynamische IT-services. 2. Aufl. Springer, Berlin; Heidelberg.

Bergando F, Gunetti D, Picardi C (2002) User Authentication through Keystroke Dynamics. ACM TISSEC 5(4):367–397.

Biometric Evaluation Methodology Working Group (2002) Biometric Evaluation Methodology. http://www.cesg.gov.uk/policy_technologies/biometrics/media/bem_10.pdf. Abruf am 2010-07-24.

Bitkom (2010) BITKOM-Umfrage zeigt Offenheit für Biometrie im Betrieb. http://www.bitkom.org/de/presse/8477_62477.aspx. Abruf am 2010-07-24.

Boursas L (2009) Trust-based access control in federated environments, München. http://mediatum2.ub.tum.de/doc/680428/document.pdf.

Bundesamt für Sicherheit in der Informationstechnik (BSI) (2005) Untersuchung der Leistungsfähigkeit von biometrischen Verifikationssystemen - BioP II. http://www.bsi.bund.de/literat/studien/biop. Abruf am 2010-07-24.

Bundesamt für Sicherheit in der Informationstechnik (BSI) (2010) SOA-Security-Kompendium. Sicherheit in Service-orientierten Architekturen. Version 2.0. https://www.bsi.bund.de/cae/servlet/contentblob/486838/publicationFile/44002/SOA-Security-Kompendium_pdf.pdf. Abruf am 2010-07-24.

Buxmann P, Hess T, Lehmann, S. (2008) Software as a Service. Wirtschaftsinformatik 50(6):500–503.

Cahill CP, Hughes J, Lockhart H, Beach M, Metz R, Randall R, Wisniewski T, Reid I, Austel P, Hondo M, McIntosh M, Nadalin T, Ragouzis N, Cantor S, Morgan B, Davis PC, Hodges J, Hirsch F, Kemp J, Madsen P, Anderson S, Mishra P, Linn J, Philpott R, Moreh J, Anderson A, Maler E, Monzillo R (2005) Authentication Context for the OASIS Security Assertion Markup Language (SAML) V2.0. OASIS Standard, 15 March 2005. http://docs.oasis-open.org/security/saml/v2.0/saml-authn-context-2.0-os.pdf. Abruf am 2011-03-15.

Chang W (2006) Keystroke Biometric System Using Wavelets. In: Proc. of ICB.

Cowan N, Morey CC, Chen Z, Gilchrist AL, Saults JS (2008) Theory and Measurement of Working Memory Capacity Limits. In: Ross BH (Hrsg.). Academic Press.

Dierstein R (2004) Sicherheit in der Informationstechnik. Der Begriff IT-Sicherheit. Informatik Spektrum 27(4):343–353.

Ding W, Yurcik W, Yin X (2005) Outsourcing Internet Security: Economic Analysis of Incentives for Managed Security Service Providers. In: Deng X, Ye Y (Hrsg.) Internet and Network Economics. Springer Berlin / Heidelberg.

Dotzler F (2010) Datenschutzrechtliche Aspekte und der Einsatz biometrischer Systeme in Unternehmen: Eine exemplarische Betrachtung von Systemen auf der Grundlage des biometrischen Merkmals Tippverhalten. Kölner Wissenschaftsverlag, Köln.

Eckert C (2009) IT-Sicherheit. Konzepte, Verfahren, Protokolle. Oldenbourg, München.

Forrester Research (2009) Authentication-As–A-Service: A commissioned study conducted by Forrester Consulting on behalf of VeriSign. http://www.verisign.co.uk/static/auth-as-a-service.pdf. Abruf am 2010-07-24.

Fox D (1999) Zum Problem der Gültigkeitsprüfung von Schlüsselzertifikaten. In: Bundesamt für Sicherheit in der Informationstechnik (Hrsg.) Tagungsband 6. Deutscher IT-Sicherheitskongreß des BSI 1999. SecuMedia, Ingelheim.

Gartner (2008) Gartner Says Security Delivered as a Cloud-Based Service Will More Than Triple in Many Segments by 2013. www.gartner.com/it/page.jsp?id=722307. Abruf am 2010-07-24.

Graevenitz G von (2006) Erfolgskriterien und Absatzchancen biometrischer Identifikationsverfahren. Lit, Kassel.

Hafner M, Mukhtiar M, Breu R (2009) SeAAS - A Reference Architecture for Security Services in SOA. J. UCS 15(15):2916–2936.

Hevner AR, March ST, Park J, Ram S (2006) Design science in information systems research. In: Information systems. Wiley, Chichester [u. a.].

Hommel W (2007) Architektur- und Werkzeugkonzepte für föderiertes Identitäts-Management. Dr. Hut, München.

Hoonakker P, Bornoe N, Carayon P (2009) Password Authentication from a Human Factors Perspective: Results of a Survey among End-Users. In: Human Factors and Ergonomics Society 54rd Annual Meeting.

International Biometric Group (IBG) (2009) State of Biometric Standards. IBG, New York.

ISO (2009) Security Evaluation Of Biometrics. ISO, Geneva.

Jain A, Ross A, Prabhakar S (2004) An Introduction to Biometrics Recognition. Circuits and Systems for Video Technology, IEEE Transaction 14(1):4–20.

Khalid Kark (2010) Market Overview: Managed Security Services. http://www.verizonbusiness.com/resources/analystreports/ar_forrester_managed_security_services2010_en_xg.pdf. Abruf am 2011-03-16.

Krcmar H (2009) Informationsmanagement. 5. Aufl. Springer, Heidelberg.

La H, Kim S (2009) A Systematic Process for Developing High Quality SaaS Cloud Services. In: Proc. of CloudCom, Springer.

Lotz V, Pigout E, Fischer PM, Kossmann D, Massacci F, Pretschner A (2008) Towards Systematic Achievement of Compliance in Service-Oriented Architectures: The MASTER Approach. Wirtschaftsinformatik 50:383–391.

Mezler-Andelberg C (2008) Identity Management. Eine Einführung. Grundlagen, Technik, wirtschaftlicher Nutzen. Dpunkt, Heidelberg.

Münzl G, Przywara B, Reti M, Schäfer J, Sondermann K, Weber M, Wilker A (2009) Cloud Computing. Evolution in der Technik, Revolution im Business. BITKOM-Leitfaden. http://www.bitkom.org/files/documents/BITKOM-Leitfaden-CloudComputing_Web.pdf. Abruf am 2011-03-21.

Olden M (2010) Biometric authentication and authorisation infrastructures. Dissertation. Universität Regensburg, Regensburg.

Oppliger R (1998) Internet and Intranet security. Artech House, Boston.

Pope JA, Bartmann D (2010) Securing online transactions with biometric methods. International Journal of Electronic Marketing and Retailing 3(2):132–144.

Reiser H (2008) Ein Framework für föderiertes Sicherheitsmanagement. Habilitation. LMU München, München.

Schläger C (2008) Attribute based infrastructures for authentication and authorisation. Eul, Lohmar ; Köln.

Senk C (2010) Securing Inter-organizational Workflows in Highly Flexible Environments Through Biometrics. In: Proc. of ECIS, Pretoria.

Smith RE (2002) Authentication. From passwords to public keys. Addison-Wesley, Boston.

St. Clair L, Johansen L, Enck W, Pirretti M, Traynor P, McDaniel PT (2006) Password Exhaustion. Predicting the End of Password Usefulness. In: Bagchi A, Atluri V (Hrsg.) Information systems security. Second international conference, ICISS 2006, Kolkata, India, December 19-21, 2006; proc. Springer, Berlin.

Steffens F (2009) Biometrie nach dem Baukastenprinzip mit BioAPI 2.0. Datenschutz und Datensicherheit - DuD 33:295–298.

Sung K, Cho S (2006) GA SVM Wrapper Ensemble for Keystroke Dynamics Authentication. In: Proc. of ICB.

TeleTrusT Deutschland e. V., AG 6 (2006) Identifikationsverfahren: Bewertungskriterien zur Vergleichbarkeit biometrischer Verfahren. Kriterienkatalog. TeleTrusT, Erfurt.

Thomas I, Menzel M, Meinel C (2008) Using quantified trust levels to describe authentication requirements in federated identity management. In: Damiani E, Proctor S (Hrsg.) Proceedings of the 2008 ACM Workshop on Secure Web Services. October 31, 2008, Alexandria, Virginia. ACM Press, New York, N.Y.

Tsolkas A, Schmidt K (2010) Rollen und Berechtigungskonzepte. Ansätze für das Identity- und Access-Management im Unternehmen. Vieweg-Teubner, Wiesbaden.

Wisniewski T, Nadalin T, Cantor S, Hodges J, Mishra P (2005) SAML V2.0 Executive Overview. http://www.oasis-open.org/committees/download.php/13535/sstc-saml-exec-overview-2.0-cd-01-2col.pdf. Abruf am 2010-08-12.