DIENSTORIENTIERTE IT-SYSTEME FÜR
HOCHFLEXIBLE GESCHÄFTSPROZESSE

BAMBERG • ERLANGEN-NÜRNBERG • REGENSBURG

Christian Senk

Biometrische Authentifizierung im Kontext hochflexibler Geschäftsprozesse

Herausgeber:

Prof. Dr. Dieter Bartmann
Prof. Dr. Freimut Bodendorf
Prof. Dr. Otto K. Ferstl
Prof. Dr. Elmar J. Sinz

forFLEX ist Mitglied in abayfor

Universität Bamberg

Universität Regensburg

Universität Erlangen-Nürnberg

Christian Senk

Biometrische Authentifizierung im Kontext hochflexibler Geschäftsprozesse

forFLEX-Bericht-Nr.: forFLEX-2009-004

© Bayerischer Forschungsverbund forFLEX - Dienstorientierte IT-Systeme für hochflexible Geschäftsprozesse

Bamberg, Erlangen-Nürnberg, Regensburg 2009

Alle Rechte vorbehalten. Insbesondere ist die Überführung in maschinenlesbare Form sowie das Speichern in Informationssystemen, auch auszugsweise, nur mit schriftlicher Einwilligung von forFLEX gestattet.

Inhaltsverzeichnis

1 Problemstellung, Zielsetzung und Aufbau

Aufgrund diverser extern und intern induzierter Faktoren sehen sich Unternehmen bzw. deren Geschäftsprozesse steigenden Flexibilitätsanforderungen ausgesetzt (Ghattas und Soffer 2009; Pütz et al. 2009).

Gleichzeitig ermöglicht die voranschreitende Reifung serviceorientierter Technologien die funktionale Komplexitätsbewältigung von geschäftsprozessunterstützenden Anwendungssystemlandschaften und somit auch zunehmend die Implementierung von flexiblen inner- und inter-organisatorischen Geschäftsprozessen. In Anlehnung an die Systemtheorie bedeutet flexibel in diesem Kontext, dass Geschäftsprozesse in der Lage sind, ihre Struktur und ihr Verhalten im Rahmen ihrer Handlungsspielräume an relevante Veränderungen zielgerichtet anzupassen (Hocke 2004). Umfassen die Anforderungen an diese Anpassungsfähigkeit wahlweise Kontextsensitivität oder unvollständige Planbarkeit, so spricht man von hochflexiblen Geschäftsprozessen (hGP) (Pütz et al. 2009).

Dies impliziert per Definition einen enormen Grad an Komplexität[1] auf fachlicher Ebene, was sich am Beispiel medizinischer Versorgungsprozesse verdeutlichen lässt. Da sich die Planung des eigentlichen Ablaufs aufgrund verschiedener aufeinander aufbauender medizinischer Implikationen und der notwendigen Berücksichtigung externer Einflussfaktoren (z. B. Jahreszeit, gesetzliche Anforderungen, Abrechnungsvorschriften, etc.) üblicherweise erst während der Ausführungszeit fortführen lässt, herrscht eine enorme Vielfalt möglicher Varianten, die sich potenziell ad hoc über organisationsinterne und -externe Leistungsträger ausprägt.

Während Hochflexibilität einerseits zwar fachliche Potenziale freisetzen kann, implizieren die damit verbundenen Freiheitsgrade ein erhöhtes Risiko, dass ein Geschäftsprozess Ereignisse eintreten lässt, die aus einer nicht-funktionalen Sicht nicht eintreten dürfen. Dies stellt insbesondere im überbetrieblichen Kontext ein Problem der Informationssicherheit dar (Ghattas und Soffer 2009; Hafner und Breu 2009; Lotz et al. 2008). Da an der Ausführung einer Prozessinstanz mehrere rechtlich unabhängige Entitäten beteiligt sein können, passiert der Kontrollfluss unterschiedliche Sicherheitsdomänen, die dezentral verantwortet werden und somit individuellen Richtlinien folgen. Als Beispiel seien medizinische Behandlungsprozesse genannt, die sich dadurch auszeichnen, dass hochsensible Patientendaten virtuell durch verschiedene Versorgungseinrichtungen wandern, die unterschiedliche technische und organisatorische Sicherheitskontrollen implementiert haben. Die Sicherheit des Gesamtprozesses und der in diesem Zusammenhang verarbeiteten Daten hängt hierbei inhärent von der Verwundbarkeit des schwächsten Glieds innerhalb der

[1] Komplexität wird nach Piller (2000) als „[…] das Zusammentreffen einer strukturellen Vielschichtigkeit, resultierend aus der Anzahl und Diversität der Elemente eines Systems sowie deren gegenseitige Verknüpfung und der dynamischen Veränderlichkeit der gegenseitigen Beziehungen der Systemelemente" verstanden.

entstehenden Prozesskette ab und entzieht sich somit der vollständigen Kontrolle durch den jeweiligen Geschäftsprozessverantwortlichen (Haffner und Breu 2009; Schläger und Nowey 2006). Die Einhaltung relevanter rechtlicher und regulatorischer Anforderungen (IT-Compliance) kann aus diesem Grund per se nicht vollständig gewährleistet werden und basiert zu einem Großteil auf der Vertrauensbeziehung zu den beteiligten Entitäten (Reiser 2008).

Ein fundamentales Problem ist hierbei die Authentifizierung. Verbreitete passwortbasierte Verfahren weisen inhärente Schwächen auf, da sie perfekte Sicherheit auf organisatorischer Ebene unterstellen. Auch besitzbasierte Ansätze sind nur bedingt für die Sicherung hochflexibler Geschäftsprozesse geeignet. Gegenstand der vorliegenden Arbeit ist deswegen die Untersuchung von Möglichkeiten zur sicherheitstechnischen Härtung von hochflexiblen Geschäftsprozessen durch geeignete biometrische Authentifizierungsdienste.

Der Aufbau der Arbeit gestaltet sich wie folgt: In Kapitel 2 werden die grundlegenden Charakteristika hochflexibler Geschäftsprozesse beschrieben, um auf die bestehende Sicherheitsproblematik hinzuführen und die tragenden Rolle der Nutzer-Authentifizierung darzustellen. Eine Diskussion der Eignung verschiedener Authentifizierungsmethoden erfolgt in Kapitel 3. Zielsetzung des vierten Abschnitts ist die Bewertung ausgewählter biometrischer Authentifizierungsverfahren und die Identifikation der Tippverhaltensbiometrie als technische Lösung der betrachteten Authentifizierungsproblematik. Kapitel 5 stellt die Untersuchung möglicher Architekturkonzepte auf infrastruktureller Ebene dar. Abschließend liefert der sechste Abschnitt eine Zusammenfassung und einen Überblick über weitere notwendige Forschungsarbeiten.

2 Allgemeine Sicherheitsbetrachtung hGP

2.1 Charakteristika von hGP

Unter einem Geschäftsprozess im Allgemeinen versteht man eine zeitlich-logische Abfolge fachlicher Aktivitäten, die verteilt durch organisatorische und technische Aufgabenträger, d. h. durch Personen oder Anwendungssysteme (Sinz 1999), und unter Verbrauch weiterer Unternehmensressourcen ausgeführt werden. Ergebnis eines Geschäftsprozesses ist die Erstellung einer spezifischen Leistung, die für einen Prozesskunden einen messbaren Mehrwert liefert (Österle und Winter 2003; Schmelzer und Sesselmann 2008). Gegenstand eines Geschäftsprozesses als Teil des betrieblichen Informationssystems ist somit eine betriebswirtschaftlich motivierte Informationsverarbeitung (IV), an der Personen zur Verwendung oder Interpretation beteiligt sind (Lehner 1995; Moormann und Schmidt 2007).

Die Anforderungen an hGP lassen sich anhand folgender drei Merkmale ableiten (Pütz et al. 2009):

(1) Planbarkeit von Geschäftsprozessstruktur und -verhalten
(2) Zeitliche Beziehung zwischen der Planungs- und Ausführungsphase
(3) Kontextsensitivität des Prozesses

Hochflexibilität ist hierbei konkret gegeben, wenn (a) ein Geschäftsprozess als nur *unvollständig planbar* charakterisiert werden kann und folglich Ausführungs- und Planungsphase überlappen oder wahlweise (b) Struktur und Verhalten des Prozesses dynamisch *von in- und externen Kontextfaktoren beeinflusst* werden (Pütz et al. 2009).

Während sich Verhaltensflexibilität hierbei auf den rein fachlichen Kontrollfluss eines Geschäftsprozesses bezieht, der sich an einem spezifischen Geschäftsvorfall orientiert, beschreibt Strukturflexibilität den Anspruch eines Prozesses, dynamisch neue Gestaltungsobjekte in diesen Fluss einbinden zu können. Dies können bspw. Aufgabenträger sein, denen zur Laufzeit, d. h. nach der Instanziierung eines Geschäftsprozesses, kontextabhängig einzelne fachliche Aktivitäten logisch zugewiesen werden.

Um die Leistungsfähigkeit von Geschäftsprozessen zu steigern, wird ein möglichst hoher Grad an Prozessintegration und -automation angestrebt (Kupsch 2006; Masak 2006). Da nur wenige geeignete Systeme zur technischen Implementierung von hGP existieren (Pütz et al. 2009), sind hier hohe performanzsteigernde Automatisierungspotenziale zu erwarten. Als Beispiel seien erneut medizinische Versorgungsprozesse genannt, die oft ohne den integrierten Einsatz von Informationstechnologie (IT) ausgeführt werden. IT dient hier primär zur lokalen Prozessdokumentation oder der Unterstützung standardisierter, interner Abläufe. Potenziale entstehen in einem solchen Fall sowohl durch die modellgetriebene Koordinationsautomation mittels Prozess bzw. Workflow Engines als auch durch die (Teil-) Automation einzelner Aktivitäten auf der Basis lose gekoppelter fachlicher Services einer dienstorientierten Architektur (Serviceorientierte Architektur, SOA).

Aufgrund der zunehmenden Reife von Technologien, die eine dienstorientierte Umsetzung von Geschäftsprozessen ermöglichen, entstehen neue Flexibilitätsspielräume und besonders im überbetrieblichen Kontext gleichzeitige Kontrollrisiken auf technischer Ebene.

Da die Ausführung eines Workflows organisationsintern zentral durch eine Prozess Engine gesteuert wird, ist diese für die Einbindung und Durchsetzung bestimmter Sicherheitsdienste verantwortlich. Gleichzeitig ermöglicht die Laufzeitumgebung eine zentrale Kontrolle sämtlicher Zugriffe. In kooperativen Szenarien verknüpfen verschiedene Entitäten mit unterschiedlichen autonomen Laufzeitumgebungen ihre Workflows dynamisch zu einem übergreifenden Geschäftsprozess (Hafner und Breu 2009). Für solche Prozesse existiert i. d. R. keine zentrale Steuerungsinstanz. Die Sicherheit des Gesamtprozesses hängt somit dezentralisiert vom Zusammenwirken der beteiligten, potenziell heterogenen Sicherheitsdomänen sowie der implementierten Sicherheitsdienste ab (Ghattas und Soffer 2009; Hafner und Breu 2009). Die Herausforderung liegt somit darin, den gesamten, also domänenübergreifenden Geschäftsprozess sicherheitstechnisch zu härten, d. h. Sicherheitsdienste bzw. -mechanismen zu implementieren, die prozessweit ein transparentes Mindestmaß an Restriktion und Kontrolle für Geschäftsprozesssicherheit erzwingen.

2.2 Schutz- und Ordnungsmäßigkeitsziele

Wesentlich für Geschäftsprozesse die potenziell durch Anwendungssysteme unterstützbar sind, ist die technische Verarbeitung von Informationen. Diese Informationen unterliegen spezifischen Schutzbedarfen, die Gegenstand der Geschäftsprozesssicherheit sind. Entsprechend müssen Sicherheitsmechanismen implementiert werden, die Struktur und Verhalten eines Geschäftsprozesses so einschränken, dass spezifizierte Sicherheitsziele und -anforderungen eingehalten werden (Lotz et al. 2008). Während zur Erhöhung von Sicherheit dem Geschäftsprozess also potenziell Freiheitsgrade entzogen werden, impliziert die Anforderung der Flexibilität die Bereitstellung zusätzlicher fachlicher Freiheitsgrade sowohl auf Struktur- als auch auf Verhaltensebene. Entsprechend sind die Ziele Flexibilität und Sicherheit konträr, was bedeutet, dass ein maximal flexibler Geschäftsprozess keiner maximalen Sicherheit unterliegen kann. Zielsetzung muss es deswegen sein, den Einfluss und die Wirkung von Sicherheitsmechanismen dynamisch so zu dosieren, dass die Flexibilitätsbedarfe des Geschäftsprozesses möglichst wenig behindert werden. Die Erfüllung der für den Geschäftsprozess relevanten Schutzziele der Informationssicherheit (engl. security) bleibt hierbei jedoch essenziell.

Unter Informationssicherheit versteht man die „Eigenschaft eines funktionssicheren Systems, nur solche Systemzustände anzunehmen, die zu keiner unautorisierten Informationsveränderung oder -gewinnung führen“ (Eckert 2009). Im Rahmen einer Informationsverarbeitung muss der Zugriff so auf autorisierte Subjekte beschränkt und entsprechend kontrolliert werden (Eckert 2009).

Im Wesentlichen erfordert dies die Verfolgung der klassischen drei Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit, die sich konkret auf die Sicherheit der Strukturelemente (Schutzobjekte) des IV-Systems bzw. des Geschäftsprozesses beziehen (Dierstein 2004): [2]

- **Vertraulichkeit**: Vermeidung der Möglichkeit unautorisierter Informationsgewinnung (Eckert 2009; Shirey 2000)
- **Integrität**: Vermeidung der Möglichkeit unautorisierter und unbemerkter Datenmanipulation (Eckert 2009; Shirey 2000)
- **Verfügbarkeit**: Vermeidung der Möglichkeit einer unautorisierten Beeinträchtigung authentifizierter und autorisierter Subjekte in der Wahrnehmung ihrer Berechtigungen (Eckert 2009)

Dierstein (2004) erweitert die schutzobjektzentrierte Sicherheitsbetrachtung um Ziele der Ordnungsmäßigkeit, die das Geschäftsprozessverhalten adressieren. Diese umfassen die Zurechenbarkeit und die Revisionsfähigkeit. Unter Zurechenbarkeit versteht man die Eigenschaft eines IV-Systems, alle Vorgänge und Ergebnisse definierbaren Verursachern

[2] In der Literatur werden weitere Schutzziele unterschieden. Diese lassen sich auf Ordnungsmäßigkeitsziele oder Schutzfunktionen zurückführen. (Kronschnabl 2008)

zuzuordnen. Revisionsfähigkeit bzw. Rechtverbindlichkeit ist gegeben, wenn diese Vorgänge und Ergebnisse im Rechtsverkehr Dritten gegenüber beweisbar sind. (Dierstein 2004)

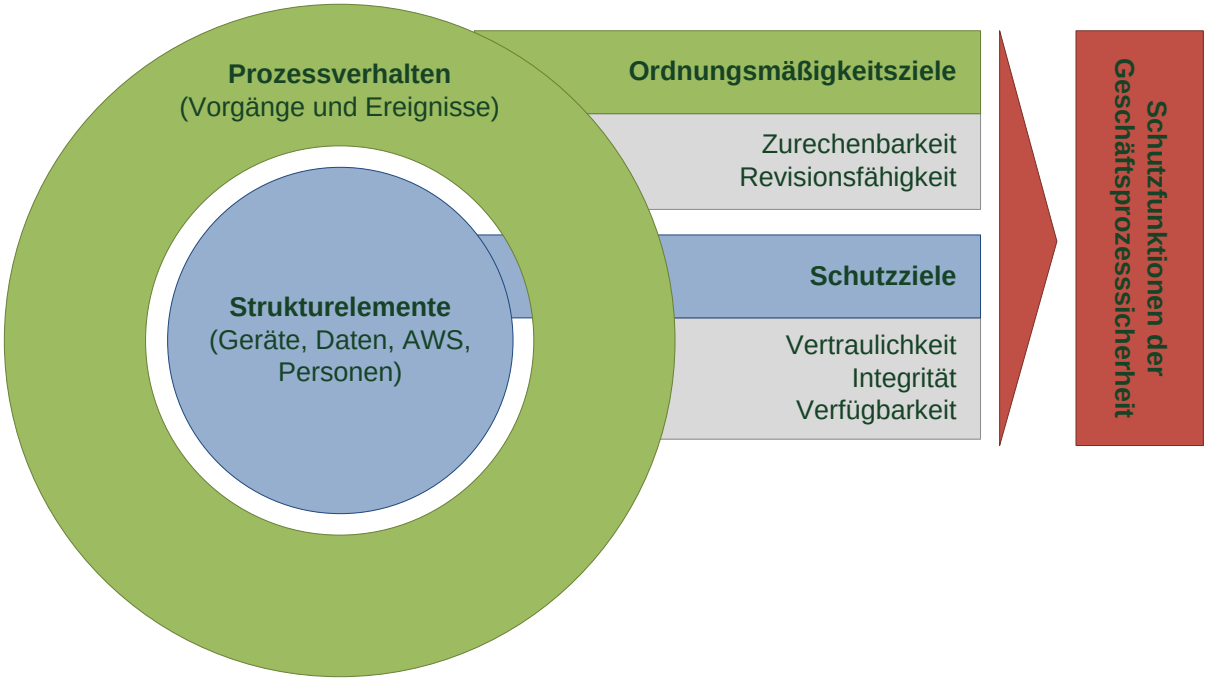

Abbildung 1: Schutzfunktionen und Geschäftsprozesssicherheit
Quelle: in Anlehnung an (Dierstein 2004)

Die Sicherheit von Geschäftsprozessen umfasst sowohl Schutz- als auch Ordnungsmäßigkeitsziele. Um diese effektiv verfolgen zu können, müssen die generischen Schutzfunktionen wie Authentifizierung, Autorisierung, Zugriffskontrolle, Protokollierung und Überwachung durch entsprechende Sicherheitsmechanismen umgesetzt werden. Abbildung 1 illustriert diesen Zusammenhang.

Eine zentrale Rolle nimmt hierbei die Zugriffskontrolle ein. Die Informationsverarbeitung muss gemäß den spezifizierten Schutzzielen auf autorisierte Nutzer eingeschränkt werden. Zurechenbarkeit und Revisionsfähigkeit erfordern zudem retrospektiv die Transparenz der einzelnen Zugriffe und deren eindeutige Zurückführbarkeit auf den jeweiligen Nutzer.

Im Rahmen der Zugriffskontrolle ist zunächst zu ermessen, inwieweit ein Subjekt Rechte auf eine geschützte Ressource ausüben darf, um diese Entscheidung anschließend durchzusetzen. Als Grundlage dienen die Ergebnisse der Autorisierung und der Authentifizierung. Im Rahmen der Autorisierung erfolgt vorab eine logische Zuweisung von Rechten und Privilegien für bestimmte Subjekte im Sinne eines Regelwerks. Durch eine effektive, d. h. personenbindende Nutzer-Authentifizierung wird die Authentizität des Subjektes bzw. dessen Identität sichergestellt, so dass das richtige Regelwerk zur Zugriffszeit angewandt und auch ex post Zurechenbarkeit und Revisionsfähigkeit gewährleistet werden kann.

3 Authentifizierung im Kontext hGP

3.1 Begriffsbestimmung

Unter Authentifizierung (engl. authentication[3]) versteht man im Allgemeinen die logische Assoziierung eines Subjekts mit einer digitalen Identität anhand einer Menge differenzierender Merkmale. Könnte ein Subjekt jede beliebige Identität annehmen oder vortäuschen, so wären logische Zugriffsrestriktionen auf Autorisierungsebene unnötig, da diese willkürlich umgangen werden könnten. Aus diesem Grund ist Authentifizierung Voraussetzung für eine effektive Zugriffskontrolle. In hochgradig regulierten Fachdomänen (z. B. Gesundheitswesen) besteht die Anforderung einer starken Authentifizierung, da eine digitale Identität eindeutig mit einer natürlichen Person logisch verknüpfbar sein muss. Die Stärke der Authentifizierung wird hierbei durch die Personenbindung impliziert, also den Grad der Wahrscheinlichkeit mit dem die ermittelte digitale Identität konsistent mit der tatsächlichen, also der zivilen Identität ist. Methoden zur Feststellung der Identität einer Person können prinzipiell nach drei[4] Faktoren klassifiziert werden (Jain und Ross 2007; Smith 2002):

(1) Identitätsnachweis durch Wissen
(2) Identitätsnachweis durch Besitz
(3) Identitätsnachweis durch Biometrie

Diese Faktoren umfassen jeweils unterschiedliche Methoden und weisen spezifische Vor- und Nachteile bzgl. der erreichbaren Authentifizierungsstärke auf. Eine Kombination von zwei oder mehr Faktoren (Zwei-/ Multifaktor-Authentifizierung) ermöglicht zudem eine weitere Erhöhung der Personenbindung.

3.2 Implizierte Anforderungen durch den Kontext hGP

Authentifizierung im betrieblichen Umfeld kann (a) der physischen Zutrittskontrolle oder (b) der logischen Zugriffskontrolle zu Systemen oder Ressourcen dienen. Im Kontext hGP wird der zweite Fall unterstellt, da die verteilte IT-gestützte Verarbeitung fachlicher Ressourcen durch menschliche Aufgabenträger (Nutzer) im Vordergrund steht. Es wird zudem angenommen, dass jeder potenzielle Nutzer im Regelfall logisch über einen oder mehrere netzwerkfähige stationäre oder mobile Rechner am hGP partizipieren kann und entsprechende Fähigkeiten hierzu besitzt.

---

[3] Unter *authentication* werden im Englischen die deutschen Begriffe Authentifizierung und Authentisierung zusammengefasst. Authentisierung beschreibt hierbei die Preisgabe der Identitätsmerkmale durch das jeweilige Subjekt und nicht deren Prüfung und grenzt sich somit von der Authentifizierung ab.

[4] In der Literatur wird als möglicher vierter Faktor der Identitätsnachweis durch Verortung, z. B. über GPS-Koordinaten, genannt. Aufgrund mangelnder Praxisrelevanz erfolgt allerdings keine explizite Betrachtung. (Oppliger 2002)

Ein Authentifizierungsverfahren bzw. ein System, welches ein solches Verfahren umsetzt, muss selbst informationssicher sein, d. h. es darf durch einen Angreifer im schlimmsten Fall nur durch unverhältnismäßig hohen Aufwand kompromittierbar sein. Diese Anforderung wird im Folgenden als Systemsicherheit bezeichnet.

Zudem darf der Prozess der Authentifizierung die Funktionssicherheit des Geschäftsprozesses, also die Ausübung der fachlichen Aktivitäten durch die personellen Leistungsträger, nicht beeinträchtigen. Dies impliziert vornehmlich Anforderungen bzgl. der Praktikabilität und Nutzbarkeit des Authentifizierungssystems, aber auch hinsichtlich der nutzerseitigen Akzeptanz.

Eine zusätzliche Notwendigkeit, die sich konkret im Kontext von hGP ergibt, ist die strukturelle Verfügbarkeit eines Authentifizierungsdienstes oder verschiedener homogener Authentifizierungsdienste für alle möglichen Prozessteilnehmer innerhalb des relevanten Netzwerkes. Maximale Flexibilität wird hierbei bei der Möglichkeit eines webanwendungsbasierten Zugriffs unterstellt. Flexibilität auf Verhaltensebene erfordert in überbetrieblichen Kooperationen entsprechend Flexibilität auf Strukturebene, d. h. dass je nach Geschäftsvorfall die dynamische Einbindung unterschiedlicher, ex ante potenziell nicht bekannter externer Entitäten möglich sein muss. Steht für eine Entität die Möglichkeit einer adäquaten Authentifizierung nicht zur Verfügung oder kann diese nicht zeitnah hergestellt werden, so wird diese Entität aus struktureller Sicht ausgeschlossen und schränkt so gleichzeitig die Verhaltensflexibilität ein.

Eine weitere, essenzielle Anforderung der Nutzer-Authentifizierung ist die Personenbindung oder Nicht-Transferierbarkeit. Ist diese nicht gegeben, so kann zum einen die Autorisierung umgangen werden (Gefährdung der Schutzziele) und zum anderen ist keine effektive Verfolgung der Ordnungsmäßigkeitsziele möglich.

3.3 Faktorenspezifische Bewertung

3.3.1 Wissensbasierte Authentifizierung

Der Identitätsnachweis durch Wissen basiert prinzipiell auf der Abmachung eines gemeinsamen Geheimnisses zwischen einem Subjekt und der authentifizierenden Instanz. Die Identität eines Subjekts ist somit an dieses Geheimnis geknüpft. Am Gebräuchlichsten sind *statische* Geheimisse, wie sie für Passwort- und PIN[5]-basierte Verfahren verwendet werden. Solche Methoden sind technisch einfach und effizient implementierbar sowie praktikabel und portabel in ihrer Anwendung. Nichtsdestotrotz wird deren Sicherheit stark kritisiert. Die Sicherheit von Passwörtern (bzw. PINs) steigt mit der Zunahme des enthaltenen Informationsgehalts, der sich durch Verlängerung der Zeichenkette sowie der Verwendung von Sonderzeichen etc. erhöhen lässt. Länge und Komplexität des Passworts wirkt sich allerdings wiederum negativ auf die Praktikabilität aus, da das Einprägen und Merken

[5] Personal Identification Number

hierdurch tendenziell erschwert wird. Das Erfordernis unterschiedlicher, technisch sicherer Zeichenketten verstärkt diesen Effekt. Als Konsequenz tendieren Nutzer dazu Passwörter aufzuschreiben oder ein Passwort für unterschiedliche Systemzugänge zu verwenden, wodurch das Risiko eines Kompromittierens zusätzlich erhöht wird und zudem potenziell unbemerkt bleibt. Alternative Verfahren basieren auf sog. *kulturellen* oder *dynamischen* Geheimnissen. Da kulturelle Geheimnisse wie Geburtsdatum oder Sozialversicherungsnummer prinzipiell nicht vertraulich sind, sind darauf aufsetzende Methoden von Natur aus schwach und ungeeignet. Dennoch finden sie aus implementierungs- und praktikabilitätstechnischen Gründen häufig Anwendung in Passwort-Reset Szenarien, z. B. im Rahmen der Verwaltung von persönlichen e-Mail-Konten. Verfahren, die auf dynamischen Geheimnissen, z. B. TANs (Transaction Authentication Numbers) oder Einmalpasswörtern basieren, erreichen zwar potenziell eine höhere Authentifizierungsstärke, bringen aber wesentliche praktische Nachteile mit sich; da das Einprägen durch den Nutzer kaum möglich ist, muss eine meist physikalische Synchronisation und Speicherung stattfinden. (Oppliger 2002; Smith 2002) Dies reduziert die mögliche Strukturflexibilität.

	Nicht-Transferierbarkeit	**Praktikabilität/ Akzeptanz**	**Systemsicherheit**	**Strukturflexibilität**
Statische Geheimnisse	o	oo	oo	ooo
Kulturelle Geheimnisse	o	ooo	o	ooo
Dynamische Geheimnisse	o	oo	ooo	oo

(o = negative, oo = neutrale, ooo = positive Bewertung)

Tabelle 1: Vergleichende Bewertung wissensbasierter Authentifizierungsverfahren

Ein entscheidender Nachteil aller wissensbasierten Methoden, insbesondere aus einem juristischen Blickwinkel, ist die Tatsache, dass Geheimnisse keine Personenbindung aufweisen und somit eine starke Authentifizierung nicht realisierbar ist. Aus diesem Grund herrscht in der Literatur Einigkeit darüber, dass ein rein wissensbasierter Authentifizierungsansatz für viele Anwendungsfälle keine ausreichende Sicherheit bietet (St. Clair et al. 2006). So müssen konsequenterweise andere Authentifizierungsverfahren als Ergänzung oder Ersatz in Betracht gezogen werden (Benatar 2006; Pope und Bartmann 2009; Smith 2002). Tabelle 1 stellt die Ergebnisse einander gegenüber.

3.3.2 Besitzbasierte Authentifizierungsverfahren

Im Rahmen einer besitzbasierten Authentifizierung weist ein Subjekt seine Identität durch den Besitz einer spezifischen Hardwareeinheit (Token) nach. Dies kann beispielsweise eine Smart Card oder ein USB-Token sein. Analog zu wissensbasierten Authentifizierungsverfahren sind hierbei die zum Identitätsnachweis herangezogenen Nutzerattribute nicht an die Person gebunden und können gewollt oder ungewollt an andere Personen weitergegeben werden. Ein weiterer Nachteil liegt in den hohen Kosten für die Herstellung, Personalisierung, Distribution und Wartung der Tokens sowie für die zugehörige Eingangsschnittstelleninfrastruktur. Ist diese Infrastruktur nicht flächendeckend vorhanden, so ist die Strukturflexibilität stark reduziert. Zudem schränken die Maße der Hardwareeinheit potenziell die Portabilität ein. Ein wesentlicher Vorteil ist hingegen, dass eine Kompromittierung eines Tokens leicht erkannt werden kann und in diesem Fall ein einfacher Austausch möglich ist. Nichtsdestotrotz stellen die erforderlichen Aufwände sowie die inhärente Transferierbarkeit entscheidende Nachteile besitzbasierter Authentifizierungsmethoden dar. Die Anwendbarkeit in verteilten Umgebungen ist zudem eingeschränkt. (Benatar 2006; Oppliger 2002; Pope und Bartmann 2009; Smith 2002) Eine Zusammenfassung der Bewertung findet sich in Tabelle 2.

	Nicht-Transferierbarkeit	**Praktikabilität/ Akzeptanz**	**Systemsicherheit**	**Strukturflexibilität**
Besitzbasierte Authentifizierung	o	o	ooo	o

(o = negative, oo = neutrale, ooo = positive Bewertung)

Tabelle 2: Bewertung besitzbasierter Authentifizierung

3.3.3 Biometrische Authentifizierung

3.3.3.1 Grundlagen

Biometrie basiert auf der Messung spezifischer biologischer Charakteristika zur Bestimmung einer Person bzw. der Identität eines Individuums (Jain und Ross 2007). In Anlehnung an Maltoni et al. (2009) wird biometrische Authentifizierung demzufolge im gegebenen Kontext als die automatisierte Identifikation oder Verifikation einer Person anhand differenzierender verhaltensbasierter oder physiologischer Merkmale definiert. Voraussetzung für die Durchführung einer biometrischen Authentifizierung ist ein vorangegangener Enrolment-Prozess. Hierbei werden die entsprechenden Merkmale des Nutzers beim authentifizierenden

System abgegeben, als sogenannter Referenzdatensatz registriert und somit logisch mit der Identität der Person verknüpft. Im Rahmen des Authentifizierungsprozesses wird der registrierte Referenzdatensatz mit der erneut abgegebenen Probe des jeweiligen biometrischen Merkmals verglichen. Die Authentifizierung gilt hierbei als erfolgreich, wenn Probe und Referenzdatensatz gemäß einem zuvor definierten Toleranzwert konsistent zueinander sind. Aufgrund von Variationen in der Beschaffenheit des Merkmals und der Aufnahmebedingungen, sind Referenz und Probe praktisch nie identisch. Es kann lediglich eine Ähnlichkeit bestimmt werden. Der Ergebniswert der Authentifizierung unterliegt somit stets einer statistischen Varianz, womit die Leistungsfähigkeit eines biometrischen Authentifizierungssystems im Wesentlichen anhand von drei empirisch zu ermittelnden Fehlerraten bewertet wird:

- **Falschakzeptanzrate** (engl. False Acceptance Rate, FAR): prozentualer Anteil der fälschlich angenommenen, aber unautorisierten Personen einer Grundgesamtheit
- **Falschrückweisungsrate** (engl. False Rejection Rate, FRR): prozentualer Anteil der fälschlich zurückgewiesenen autorisierten Personen einer Grundgesamtheit
- **Gleichfehlerrate** (engl. Equal Error Rate, EER): Fehlerrate für die gilt: FAR = FRR

Wie in Abbildung 2 dargestellt, hängen diese Fehlerraten unmittelbar mit dem spezifizierten Toleranzwert zusammen. Je höher die geforderte Ähnlichkeit zwischen Referenzdatensatz und Probe, desto niedriger ist das Risiko, eine unautorisierte Person fälschlicherweise positiv zu authentifizieren. Gleichzeitig steigt allerdings die Wahrscheinlichkeit, eine autorisierte Person fälschlich zurückzuweisen. Somit entspricht die Bestimmung der Toleranzschwelle immer der Kompromissfindung zwischen erreichbarer Sicherheit und gewünschtem Komfort und hat sich am jeweiligen Anwendungskontext zu orientieren. Ein allgemeines Maß für die Trennschärfe eines biometrischen Systems ist die ERR. Ein niedrigerer Wert impliziert hierbei eine höhere Leistungsfähigkeit. (Jain und Ross 2007; Mansfield und Wayman 2002)

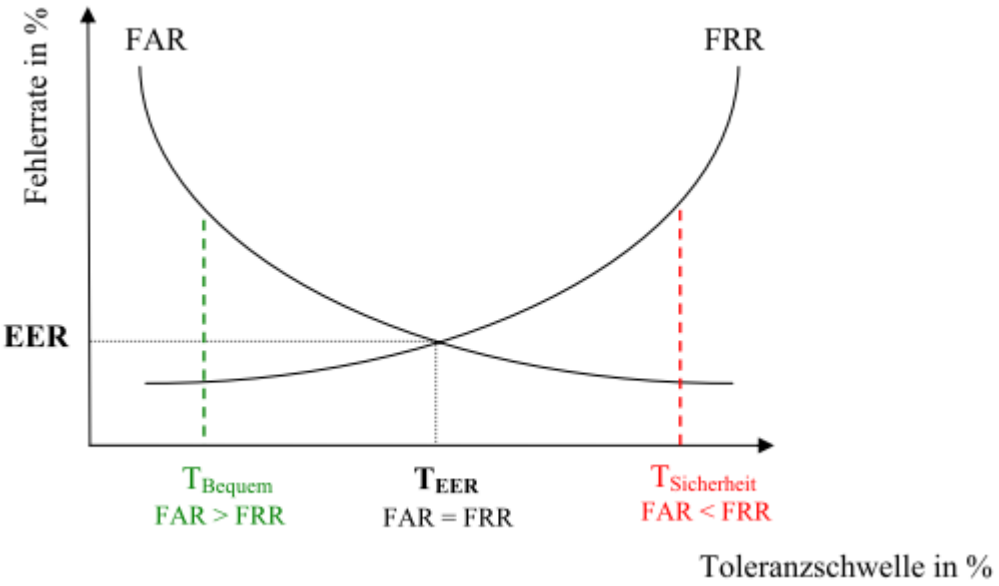

Abbildung 2: Zusammenhang zwischen Toleranzschwelle, FAR, FRR und EER
Quelle: (Breu 2003)

3.3.3.2 Bewertung biometrischer Merkmale

Für die Bewertung der prinzipiellen Eignung biometrischer Merkmale zur Realisierung effektiver Authentifizierungsmethoden werden vier elementare Anforderungen spezifiziert: (z. B. Maltoni et al. 2009)

- **Universalität:** Jedes Subjekt im gegebenen Kontext muss in der Lage sein, das geforderte Merkmal bereitzustellen. Andernfalls kann kein Enrolment stattfinden und eine Authentifizierung muss auf anderem Wege durchgeführt werden.
- **Einzigartigkeit:** Ein Merkmal muss ausreichend differenzierende Informationen enthalten, um ein Subjekt von anderen Subjekten im gegebenen Kontext eindeutig abgrenzen zu können.
- **Dauerhaftigkeit:** Die Korrelation zwischen Referenzdatensatz und Probe muss zeitlich robust sein, was insbesondere bei verhaltensbasierten Merkmalen ein Problem darstellt, da diese potenziell stärkeren Alterungsprozessen unterliegen. Bei hinreichend häufiger Nutzung eines Systems lässt sich diese Problematik jedoch sehr effektiv durch Adaptionsmechanismen adressieren, die dafür sorgen, dass der Referenzdatensatz schrittweise den Änderungen der abgegebenen Proben angepasst wird (Bakdi 2007; Olden 2008).
- **Messbarkeit:** Für eine automatisierte Authentifizierung muss das verwendete Merkmal digitalisierbar sein. Hierfür werden geeignete Hardware-Sensoren verwendet.

	Anforderungen			
Biometrisches Merkmal	**Universalität**	**Einzigartigkeit**	**Dauer-haftigkeit**	**Messbarkeit**
Gesicht	ooo	o	oo	ooo
Fingerabdruck	oo	ooo	ooo	oo
Handgeometrie	oo	oo	oo	ooo
Tippverhalten	oo	oo	o	ooo
Retina	ooo	ooo	oo	o
Unterschrift	o	o	o	ooo
Stimme	oo	o	o	oo
DNA	ooo	ooo	ooo	o
Gangbild	oo	o	o	ooo

(o = negative, oo = neutrale, ooo = positive Bewertung)

Tabelle 3: Bewertung biometrischer Merkmale
Quelle: in Anlehnung an (Olden 2008)

Diesen Anforderungen folgend wird für die methodische Anwendung in Forschung und Praxis eine Vielzahl biometrischer Merkmale herangezogen, die in ihrer Eignung stark variieren. Exemplarisch seien die Erkennung von Iris, Retina, Fingerabdruck, Gesicht, Ohr, Unterschrift, Stimme sowie Tippverhalten genannt (Maltoni et al. 2009; Weber 2008). Eine vergleichende Bewertung ausgewählter biometrischer Merkmale findet sich in Tabelle 3.

3.3.3.3 Allgemeine Bewertung biometrischer Authentifizierungsverfahren

Ein gemeinsames Charakteristikum aller biometrischen Merkmale ist deren inhärente Personenbindung, was sowohl als positive als auch als negative Eigenheit ausgelegt werden kann. Zum einen besteht die Implikation einer potenziellen, verfahrens- bzw. systemspezifischen Datenschutzproblematik (Dotzler 2009), die wiederum zu Akzeptanzproblemen führen kann (Weber 2008). Zum anderen können Merkmale nicht unmittelbar gestohlen oder weitergegeben werden, was die Effektivität der Authentifizierung im Vergleich zu nicht-biometrischen Ansätzen potenziell erhöht, da eine digitale Identität stärker mit einer eindeutigen Person verknüpft wird (Jain und Ross 2007). Eine Schwäche biometrischer Authentifizierungsverfahren in diesem Zusammenhang ist wiederum die Möglichkeit von Replay-Angriffen. Hierunter versteht man Versuche, eine fremde biometrische Probe während des Authentifizierungsprozesses abzufangen, mit der Absicht diese anschließend in unveränderter oder modifizierter Form wieder einzuspielen, um dem authentifizierenden System eine falsche Identität vorzutäuschen. Durch die Implementierung von Mechanismen zur Lebenderkennung können solche Angriffe jedoch effektiv verhindert werden. Das weitere Risiko, dass eine Person von einem Angreifer zur Authentifizierung gezwungen wird (Pfitzmann 2006), bleibt davon jedoch unberührt. Ein weiterer Vorteil der Personenbindung ist die potenzielle Steigerung der Praktikabilität. So muss der Nutzer weder einen Token mit sich führen noch sich ein Passwort einprägen. Diesem Vorteil stehen jedoch mögliche Sensorqualitäts- und, wie bereits erläutert, Akzeptanzproblematiken entgegen (Benantar 2006). (Pope und Bartmann 2009; van Graevenitz 2006; Weber 2008)

	Nicht-Transferierbarkeit	Praktikabilität/ Akzeptanz	Systemsicherheit	Strukturflexibilität
Biometrische Authentifizierung	ooo	~	~	~

(o = negative, oo = neutrale, ooo = positive Bewertung, ~ = variabel)

Tabelle 4: Allgemeine Bewertung biometrischer Authentifizierung

Tabelle 4 liefert eine Zusammenfassung der allgemeinen Bewertung von Biometrie als Faktor für eine Authentifizierung im Kontext hochflexibler Geschäftsprozesse. Für die Bewertungskriterien Praktikabilität/ Akzeptanz, Systemsicherheit und Strukturflexibilität können jedoch keine allgemeingültigen Aussagen getroffen werden, da diese unmittelbar von den individuellen Verfahrens- und Systemspezifika abhängen.

3.4 Zusammenfassung

Zusammenfassend ist Biometrie im Allgemeinen potenziell praktikabler, sicherer und aus rechtlicher Sicht aussagekräftiger als traditionelle, auf Wissen oder Besitz basierende Authentifizierungsmethoden und wird in der Literatur deswegen als Ersatz oder Ergänzung dieser Ansätze diskutiert (Albrecht und Probst 2001; Jain und Ross 2007). Darüber hinaus wird der biometrischen Authentifizierung sogar eine Rolle als Schlüsseltechnologie prognostiziert (van Graevenitz 2006; Weber 2008). Dennoch konnten sich biometrische Authentifizierungsansätze bislang nicht im Geschäftsprozesskontext durchsetzen, was teilweise auf mangelnde Systemreife, aber auch auf inhärente Datenschutzproblematiken zurückzuführen ist (Pfitzmann 2006; van Graevenitz 2006; Weber 2008).

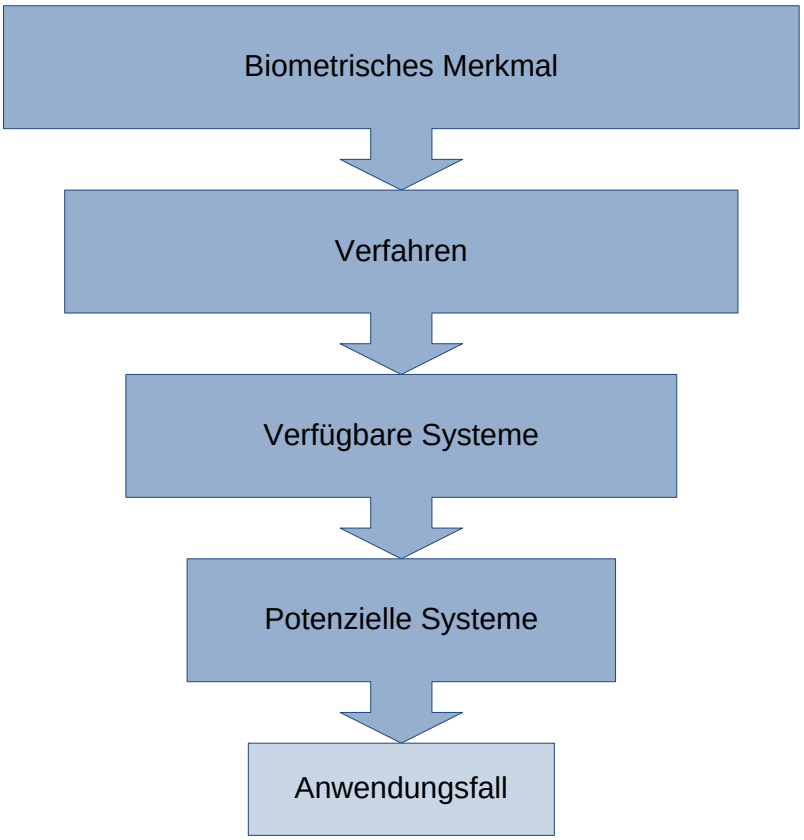

Abbildung 3: Funktionsschichtenmodell biometrischer Systeme
Quelle: in Anlehnung an (Breu 2003)

Wie sich anhand des Funktionsschichtenmodells biometrischer Systeme (Abbildung 3) veranschaulichen lässt, sind unterschiedlichste biometrische Authentifizierungsverfahren bekannt, die jeweils auf spezifischen biometrischen Merkmalen aufbauen und ggf. durch

verfügbare Systeme umgesetzt werden. Für den flexiblen Einsatz im Geschäftsprozesskontext eigenen sich nur wenige potenzielle Systeme. Aus diesem Grund wird im Folgenden in Anlehnung an Pope und Bartmann (2009) eine detailliertere Untersuchung von biometrischen Verfahren vorgenommen, die durch marktreife Systeme im Kontext der logischen Zugriffskontrolle bereits umgesetzt wurden. Die Auswahl beschränkt sich hierbei auf die Erkennung von Fingerabdruck, Stimme und Tippverhalten. Als weitere biometriespezifische Anforderungen werden die Skalierbarkeit des Verfahrens sowie die Datenschutzfreundlichkeit aufgenommen.

4 Vergleichende Bewertung biometrischer Verfahren

4.1 Fingerabdruckerkennung

Fingerabdrücke repräsentieren die Haut eines Fingers, welche aus einzigartigen Mustern von Erhöhungen und Vertiefungen besteht (Maltoni et al. 2009). Diese können mit Hilfe verschiedener Arten von Sensoren digitalisiert werden (Breitenstein 2002). Sensoren werden im Allgemeinen anhand des zugrunde liegenden physikalischen Verfahrens klassifiziert (Breitenstein 2002). Der Authentifizierungsprozess basiert auf der Digitalisierung des Fingerabdrucks und dem Abgleich differenzierender Muster (Maltoni et al. 2009). Aufgrund sinkender Preise und Ausmaße sowie verhältnismäßig hoher Reife der Verfahren gewinnen solche zunehmend an Popularität in verschiedensten Anwendungsszenarien (Jain und Ross 2007; van Graevenitz 2006; Weber 2008). Solche kostengünstigen Sensoren verzichten allerdings auf Mechanismen zur Lebenderkennung, was ein Problem darstellen kann. Fingerabdrücke werden oft und unbewusst zurückgelassen. Sobald ein Angreifer in den Besitz eines solchen Abdrucks gelangt, kann er mit wenig Aufwand ein Imitat des Fingers anfertigen und damit das biometrische System auf einfache Weise täuschen (Breitenstein 2002; von Graevenitz 2006). Ein aus Nutzersicht schwerwiegendes Risiko wird durch die Speicherung des Referenzdatensatzes durch den Betreiber impliziert. Datenschutzrechtlich sind Fingerabdrücke bedenklich, da diese Informationen über mögliche genetische Erkrankungen beinhalten (van Graevenitz 2006). Zudem können Fingerabdrücke prinzipiell für kriminalistische Zwecke gegen den Nutzer verwendet werden. Eine Möglichkeit diese Problematik abzuschwächen ist die nutzerseitige Speicherung des Referenzdatensatzes in einer vertrauenswürdigen Umgebung des Nutzers, z. B. einem mobilen Endgerät oder einem Token. Hierdurch sinkt jedoch sowohl die Praktikabilität als auch die Strukturflexibilität der Authentifizierung, da ein Besitzmerkmal mitgeführt werden muss und gleichzeitig die Notwendigkeit einer zusätzlichen physischen Infrastruktur entsteht. Die Praktikabilität und Benutzerfreundlichkeit von Fingerabdruckverfahren ist theoretisch hoch, da der Nutzer den vom System geforderten Finger lediglich auf dem Sensor (bei berührungsbehafteten Methoden) oder in dessen Nähe (bei berührungslosen Methoden) platzieren muss. In der Praxis wird die Authentifizierung jedoch durch qualitätsbedingte Faktoren wie z. B. verschmutzte Sensoroberflächen oder fehlerhaft platzierte Finger erschwert und somit die Benutzerfreundlichkeit reduziert (Behrens und Heumann 2001). Zur Skalierung der Sicherheit

der Authentifizierung bei gegebenem Sensor gibt es prinzipiell zwei Möglichkeiten. Zum einen kann die optische Auflösung des Sensors erhöht werden; allerdings ist der differenzierende Informationsgehalt eines Fingerabdruckes begrenzt. Zum anderen kann die Anzahl der vom System zur Authentifizierung geforderten Finger im Rahmen der verfügbaren Finger erhöht werden. Beide Skalierungsansätze unterliegen offensichtlichen Limitationen.

4.2 Stimmerkennung

Stimmerkennungsverfahren zählen zu den verhaltensbasierten Biometrien und können in Fest- und Freitextverfahren klassifiziert werden. Für Nutzerauthentifizierung im betrieblichen Kontext werden üblicherweise Festtextverfahren verwendet. Hierzu wird ein Nutzer aufgefordert, einen bestimmten Satz über ein Mikrofon nachzusprechen. Anschließend wird die Probe mit den Sprachmustern des zuvor aufgenommenen Referenzdatensatzes verglichen. Hierbei kommen wahlweise schablonenbasierte oder statistische Methoden zum Einsatz. Die Identität eines Nutzers wird sowohl an differenzierenden physiologischen als auch soziolinguistischen Faktoren (z. B. Dialekt, Bildungsniveau) geknüpft. Ein Vorteil des Verfahrens ist prinzipiell dessen einfache Anwendbarkeit. Allerdings hängt die Benutzerfreundlichkeit unmittelbar mit der Erkennungsqualität zusammen, welche wiederum von verschiedenen variablen Faktoren abhängt und somit potenziell starken Schwankungen unterliegt. (Gonzáles-Rodrígues et al. 2007)

Wesentliche Einflussfaktoren umfassen (Gonzáles-Rodrígues et al. 2007):

- Aufnahmebedingungen (Sprachkanal, Sprechumgebung)
- Natürliche Schwankungen der Sprachmerkmale (aufgrund von Alterung, Stimmung oder Krankheit)
- Qualität des Trainings- bzw. Enrolment-Materials

Im unternehmensinternen Einsatz wird die breite Verfügbarkeit einer Telefoninfrastruktur unterstellt, so dass die Einführung stimmerkennungsbasierter Authentifizierungssysteme keine signifikanten Investitionskosten mit sich bringt. Aus diesem Grund finden solche Systeme zunehmend Verbreitung in unternehmensinternen Passwort-Reset-Szenarien. Dennoch implizieren die Ergebnisse einer Studie in einer deutschen Großbank nutzerseitige Akzeptanzprobleme (Pope und Bartmann 2009). Neben den genannten qualitätsinduzierenden Faktoren können weitere akzeptanzmindernde Aspekte identifiziert werden. Diese umfassen die prinzipielle Erkennbarkeit von Erkrankungen sowie das Unbehagen eines Nutzers während des Sprechens Mithörern in einem Mehrpersonenbüro ausgeliefert zu sein oder generell aufgenommen zu werden.

Im mobilen und unternehmensübergreifenden Anwendungskontext sind zudem unterschiedliche Qualitätsniveaus aufgrund potenziell unterschiedlicher Eingabegeräte zu erwarten. Systeme, die auf der Verwendung der gebräuchlichen Festtext-Variante der Spracherkennung basieren, weisen eine wesentliche Verwundbarkeit auf, da Aufnahmen der Sprechproben durch Angreifer (Replay-Angriff) oder den Nutzer selbst (für einen wissentlichen Transfer an andere Nutzer) angefertigt werden können, um diese anschließend

zur Authentifizierung zu nutzen. Da die aufgenommene Probe durch den Sprachkanal und eine Re-Digitalisierung zwangsweise verändert wird, erscheint eine eindeutige Erkennung von wiedereingespielten Proben schwierig. (Gonzáles-Rodrígues et al. 2007) Die Skalierbarkeit eines Spracherkennungssystems ist prinzipiell gegeben, da ein Nutzer aufgefordert werden kann, längere Sätze zu sprechen (Pope und Bartmann 2009). Dies bewirkt eine Senkung der FAR und somit eine Erhöhung der Authentifizierungsstärke.

4.3 Tippverhaltenserkennung

Ebenso wie Spracherkennung lässt sich die Tippverhaltenserkennung als verhaltensbasierte Biometrie mit möglicher Fest- und Freitextvariante klassifizieren. Beide Methoden basieren auf der Analyse spezifischer Muster im Tippverhalten eines Nutzers. Während festtextbasierte Methoden dieses Verhalten für eine konstante Zeichenkette bewerten, verwenden freitext-basierte variable Eingabetexte. Hierbei können Freitextvarianten als flexibilitätsfördernder eingestuft werden, weil eine Authentifizierung potenziell im Hintergrund und ohne störende Unterbrechungen ablaufen kann. Durch eine andauernde und intransparente Auswertung von Nutzereingaben steht diese allerdings im möglichen Konflikt mit Datenschutzvorgaben (Dotzler 2009). Da sowohl Leistungsfähigkeit als auch Benutzerfreundlichkeit von Festtextverfahren höher sind, erscheinen solche als geeigneter für die Anwendung in hGP. (Bakdi 2007)

Viele der verfügbaren Ansätze beschränken sich auf die symmetrische Erkennung des Tastenanschlags, d. h. Geschwindigkeit und Rhythmus des Tippens (Bakdi 2007; Bartmann et al. 2007). Solche Methoden sind anfällig für Fluktuationen im Tippverhalten, wie sie beispielsweise durch Stimmungswechsel oder externe Einflüsse bewirkt werden können (Bartmann et al. 2007). Um die Robustheit zu erhöhen, wurden fortgeschrittene Verfahren entwickelt, deren Erkennungslogik auf komplexen statistischen Modellen beruht (Bartmann et al. 2007). Ein Beispiel hierfür ist das System Psylock, das auf den Arbeiten von Bartmann (2000) basiert. Unter Verwendung einer Standard-Tastatur werden nicht nur Tippgeschwin-digkeit und Rhythmus aufgezeichnet und analysiert, sondern auch statistisch stabilere Merkmale wie Agilität, Kontinuität, typische Fehler, inkohärentes Tippen sowie die Nutzung der Shift-Taste (Bartmann et al. 2007). Zusätzlich verfügt Psylock über einen Adaptions-mechanismus, der den Referenzdatensatz stetig an Änderungen im Tippverhalten eines Nutzers anpasst und somit zusätzlich die Robustheit des Systems erhöht (Bakdi 2007). Die systemische Verwundbarkeit von Psylock wird als niedrig bewertet. Zunächst kann das Tippverhalten vor der eigentlichen Quantifizierung des Merkmals durch den Sensor (d. h. die Tastatur) nicht aufgezeichnet werden. Danach werden mögliche Replay-Angriffe (z. B. mit Hilfe eines Key-Loggers) durch einen integrierten Filter verhindert, der bereits eingespielte Proben, d. h. nicht oder leicht manipulierte Duplikate, effektiv erkennt und abweist.

Ein weiterer Vorteil der Tippverhaltensbiometrie im Allgemeinen und Psylock im Besonderen ist die freie Skalierbarkeit. Da die Sicherheit (bzw. die FAR) direkt mit dem Informationsgehalt der bereitgestellten Probe korreliert, kann die Länge und Komplexität der

herangezogenen Zeichenkette dynamisch dem gewünschtem Sicherheitsniveau angepasst werden (Pope und Bartmann 2009).

Um die Leistungsfähigkeit und Skalierbarkeit zu verdeutlichen, wurden gesammelte Daten mit Ergebnissen der BioPII-Studie verglichen, die 2005 durch das deutsche Bundesamt für Informationssicherheit durchgeführt wurde (Psylock 2009). Das Ergebnis wird durch Abbildung 4 illustriert.

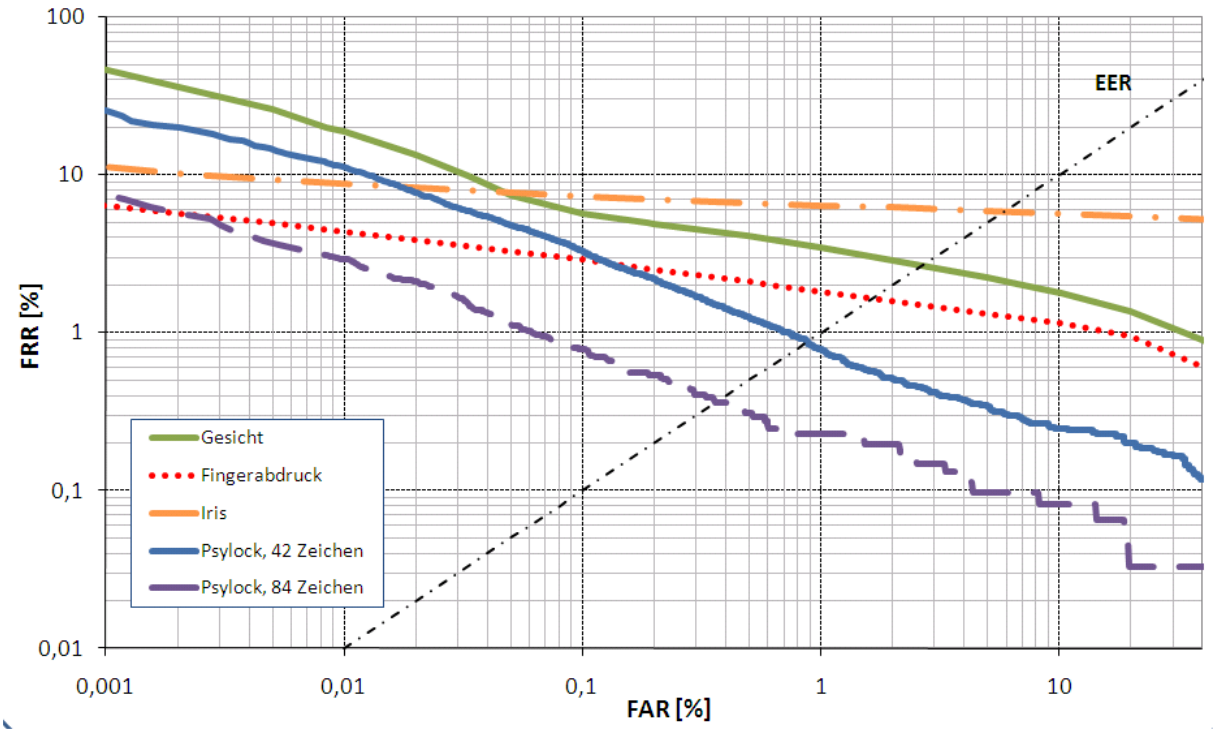

Abbildung 4: Vergleich von Psylock mit Gesichts- Fingerabdruck- und Iriserkennung
Quelle: (Psylock 2009)

Betrachtet man als Arbeitspunkt eine FAR von 0,1%, so erreicht Psylock bei der Verwendung von 42 Zeichen (Festtextvariante) eine FRR vergleichbar zur Fingerabdruckerkennung. Iris- und Gesichtserkennung weisen signifikant schlechtere Werte auf. Für Stimmerkennung liegen dem Autor keine qualifizierten Daten vor. Bei einer Verdoppelung der Eingabetextlänge auf 84 Zeichen zeigt sich eine signifikante Leistungssteigerung von Psylock. So sinkt die FRR von 3,3% auf 0,8%.

Aufgrund der hohen Leistungsfähigkeit und der niedrigen Komplexität des Verfahrens, weist Psylock eine hohe Benutzerfreundlichkeit auf. Im Gegensatz zu anderen Verfahren ist Psylock als datenschutzrechtlich unbedenklich zu bewerten[6] (Dotzler 2009). Aus Organisations- bzw. Betreibersicht zeigt sich vorteilhaft, dass keine zusätzlichen Infrastruktur- bzw. Sensorkomponenten erforderlich sind, da handelsübliche PC- oder Laptop-Tastaturen verwendet werden können. Weil das System faktisch eine reine Softwarelösung

[6] Bezogen auf das deutsche Bundesdatenschutzgesetz, Psylock-Festtextverfahren

darstellt und somit flexibel und skalierbar auch im Rahmen von Webanwendungen eingesetzt werden kann, eignet sich Psylock prinzipiell für eine Nutzer-Authentifizierung in hGP.

4.4 Zusammenfassung

Tabelle 5 fasst das Ergebnis der Untersuchung abschließend zusammen. Die vergleichende Bewertung der ausgewählten Verfahren erfolgt qualitativ anhand der in der Literatur aufgeführten Argumentationen und hat aus diesem Grund nur exemplarischen Charakter.

	Nicht-Transferierbarkeit	Praktikabilität/ Akzeptanz	Systemsicherheit	Strukturflexibilität	Skalierbarkeit	Datenschutzfreundlichkeit
Fingerabdruckerkennung	ooo	oo	oo	o	oo	o
Stimmerkennung	ooo	oo	oo	ooo	ooo	oo
Tippverhaltenserkennung[7]	ooo	ooo	ooo	ooo	ooo	ooo

(o = negative, oo = neutrale, ooo = positive Bewertung)

Tabelle 5: Spezifische Bewertung biometrischer Authentifizierungsverfahren

Die Nicht-Transferierbarkeit ist bei allen Verfahren prinzipiell gegeben, da diese Eigenschaft ein Spezifikum biometrischer Authentifizierung darstellt. Allerdings können Fingerabdrucksensoren sowie Stimmerkennungssysteme verhältnismäßig effektiv auf Systemebene getäuscht werden, auch wenn dies mit dem entsprechenden Aufwand der Merkmalsentwendung verbunden ist. Hinsichtlich der Praktikabilität bzw. nutzerseitigen Akzeptanz werden die Leistungsniveaus der ausgewählten Verfahren als praktisch gleichwertig und ausreichend erachtet. Abzüge gibt es hier bei Stimm- und Fingerabdruckerkennung aufgrund bekannter, sensorbedingter Qualitätsprobleme. Auch nutzerseitig wahrgenommene Datenschutzrisiken reduzieren hier potenziell die Praktikabilität und Akzeptanz in Relation zur Tippverhaltensbiometrie (Weber 2008). Aufgrund der unterstellten Verfügbarkeit von PC-Tastaturen und Telefonen[8] ist die Strukturflexibilität der Stimm- und Tippverhaltensbiometrie gegeben. Alle drei Verfahren sind prinzipiell skalierbar. Während Fingerabdrücke allerdings nur begrenzten Informationsgehalt haben, können

[7] Festtextverfahren

[8] Jeweils wahlweise mobil oder stationär

verhaltensbasierte Biometrien beliebig dimensioniert werden. Das letzte betrachtete Kriterium ist die Datenschutzfreundlichkeit des zugrunde liegenden Merkmals[9]. Hier zeigt sich, dass die Tippverhaltensbiometrie kaum Risiken aufweist, während Fingerabdrücke als datenschutzrechtlich bedenklich einzustufen sind. Stimmerkennung wird neutral bewertet.

Trotz des nur qualitativen Charakters der vergleichenden Bewertung kann konstatiert werden, dass die Tippverhaltensbiometrie prinzipiell eine äußerst geeignete Authentifizierungslösung im Kontext hochflexibler Geschäftsprozesse darstellt. Kein anderer verfügbarer biometrischer Authentifizierungsansatz lässt sich per se effektiver und flexibler in eine bestehende technische Infrastruktur zur Unterstützung von hGP integrieren. Im Gegensatz zu marktreifen Alternativen erfordert die Tippverhaltenserkennung lediglich die Ergänzung um logische, d. h. softwarebasierte Komponenten. Hardwareinduzierte Qualitätsunterschiede bei der Authentifizierung von Nutzern, die geschäftsprozessweit verteilt sind, können so weitestgehend eliminiert werden. So wird der Forderung nach einer sicherheitstechnischen Härtung des hochflexiblen Gesamtprozesses aus der Perspektive der Authentifizierung genügt. Die freie Skalierbarkeit des Verfahrens eröffnet weitere Flexibilitätspotenziale.

5 Biometriebasierte AAI im Kontext hGP

5.1 Authentifizierungs- und Autorisierungsinfrastrukturen

Um im Kontext von hGP organisationsübergreifend den Zugriff auf geschützte Onlineressourcen zur Laufzeit des hGP zu ermöglichen, müssen entsprechende logische Infrastrukturen geschaffen werden, die Sicherheitsdienste für Zugriffskontrolle, Authentifizierung und Autorisierung bereitstellen (Schläger 2008). Solche werden unter dem Begriff Authentifizierungs- und Autorisierungsinfrastrukturen (engl. authentication and authorization infrastructures, AAI) zusammengefasst. Prinzipiell wird unter zentralisierten (z. B. PAPI, MS Cardspace) und föderativen Ansätzen (z. B. Liberty's Identity Federation Framework, Shibboleth, OpenID) unterschieden (Olden 2008; Schläger et al. 2007).

Für eine Betrachtung föderativer Architekturen ist eine Abgrenzung von Service Provider (SP) und Identity Provider (IdP) erforderlich. Während SPs als Anbieter externer Ressourcen bzw. Dienste fungieren, verkörpert ein IdP eine mögliche Heimatorganisation eines spezifischen Nutzers und verwaltet dessen Identität. Eine Organisation kann i. d. R. beide Rollen annehmen. Zusätzliche vertrauensstiftende Rollen sind Attribute Authorities (AAs) und Trusted Third Parties (TTPs). AAs dienen dazu, bereitgestellte Informationen eines IdPs wahlweise zu ergänzen oder zu verifizieren. Eine TTP ist eine Organisation, zu der eine explizite Vertrauensbeziehung besteht und die keine der anderen beschriebenen Rollen einnimmt (z. B. Broker oder Registrierungsdienste). (Hommel 2008)

---

[9] Bewertung auf der Basis des deutschen Bundesdatenschutzgesetzes und (Dotzler 2009)

5.2 Architekturmuster für biometriebasierte AAIs

Der Einsatz des Authentifizierungsfaktors Biometrie in Authentifizierungs- und Autorisierungsinfrastrukturen steigert zwar potenziell die Sicherheit, erhöht aber gleichzeitig die Komplexität der zugrunde liegenden Systemarchitektur, da Spezifika der Biometrie explizit berücksichtigt werden müssen (Olden 2008).

Um diese architekturrelevanten Besonderheiten der Biometrie zu analysieren, betrachtet Olden (2008) einen flexiblen Zwei-Faktor-Authentifizierungsansatz basierend auf Passwort und dem beschriebenen Psylock-System (Tippverhaltensbiometrie). Psylock wurde gewählt, weil es der einzige verfügbare Ansatz ist, der aus Praxissicht eine reine Softwarelösung darstellt, die in Webanwendungen integriert werden kann und mit der ein einheitliches Qualitätsniveau in hGP durchgesetzt werden kann.

Im Rahmen der Untersuchung konnten im Wesentlichen vier Architekturmuster identifiziert werden: (Olden 2008)

(1) Zentrales Single Sign On mit biometrischer Authentifizierung

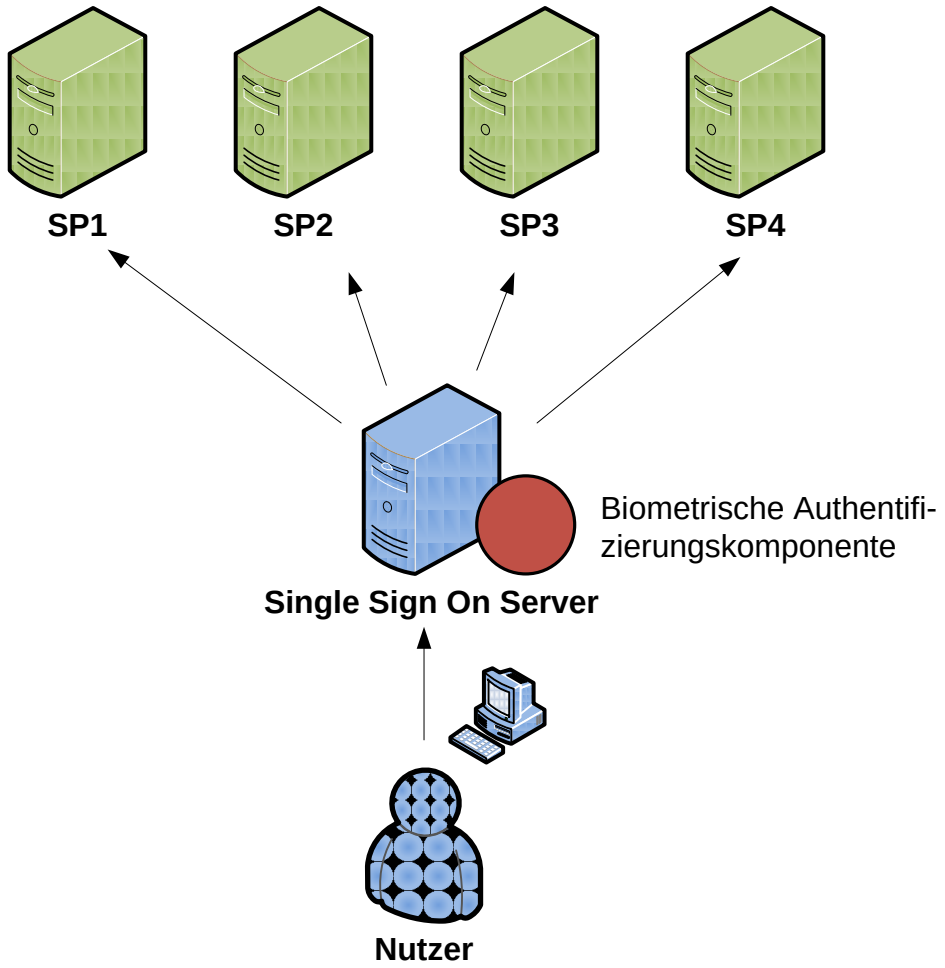

Abbildung 5: Zentrales Single Sign On mit biometrischer Authentifizierung
Quelle: in Anlehnung an (Olden 2008)

Eine Erweiterung einer zentralisierten Single Sign On (SSO) Infrastruktur um biometrische Authentifizierung (Abbildung 5) erfordert minimalen Aufwand, da der zentrale SSO-Server, der als IdP fungiert, lediglich um die biometrische Komponente bzw. die entsprechende Methode ergänzt werden muss.

(2) Föderierte AAI mit zentraler biometrischer Authentifizierungskomponente

Wie in Abbildung 6 dargestellt, ist dieses Architekturmuster eine Kombination aus einer föderierten AAI und einem zentralen SSO-Server. Die verschiedenen IdPs teilen sich föderationsweit eine zentrale biometrische Authentifizierungskomponente. Verwaltet ein Nutzer mehrere (nicht-biometrische) IdPs, kann dies zu Problemen führen, da unterschiedliche digitale Identitäten mit einer zentralen biometrischen Identität assoziiert werden müssten. Zudem entsteht ein „single point of failure“, der die Verfügbarkeit der Authentifizierung gefährdet.

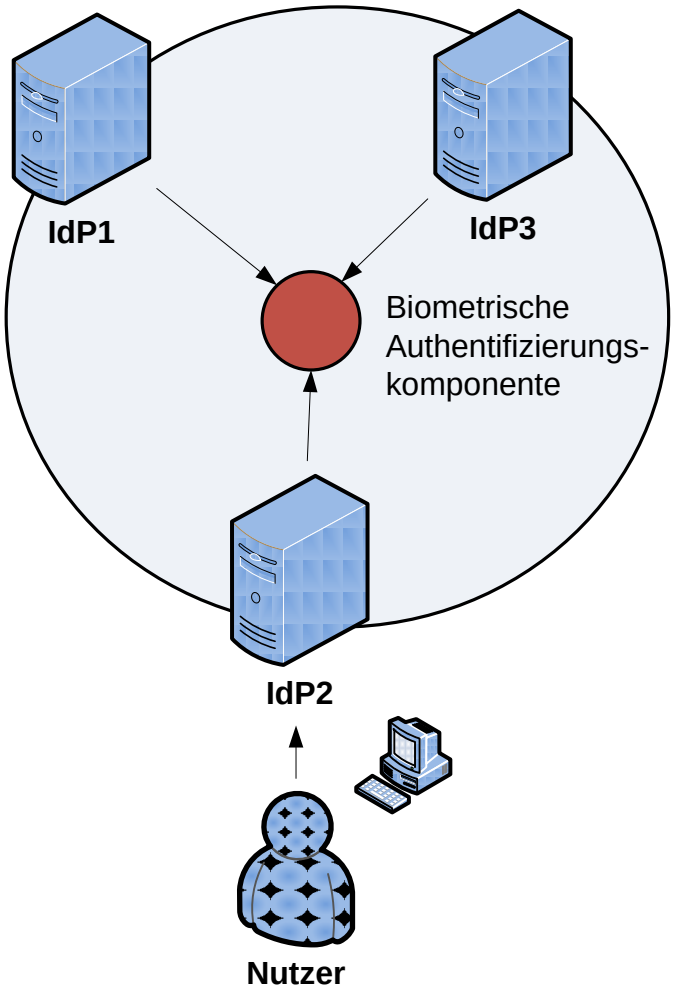

Abbildung 6: Föderierte AAI mit zentraler biometrischer Authentifizierungskomponente
Quelle: in Anlehnung an (Olden 2008)

(3) Föderierte AAI mit dezentraler biometrischer Authentifizierungskomponente

Dieses Architekturmuster unterstellt, dass jeder einzelne IdP eine eigene integrierte biometrische Authentifizierungskomponente ausführt (Abbildung 7). Dies ermöglicht zwar maximale Flexibilität seitens des Nutzers, da er nicht auf einen IdP angewiesen ist, der seine biometrische Identität autonom verwaltet, impliziert aber gleichzeitig auch maximale Herausforderungen bzgl. Qualität und Sicherheit, die mit der systemseitigen Verteilung der biometrischen Komponenten verbunden sind.

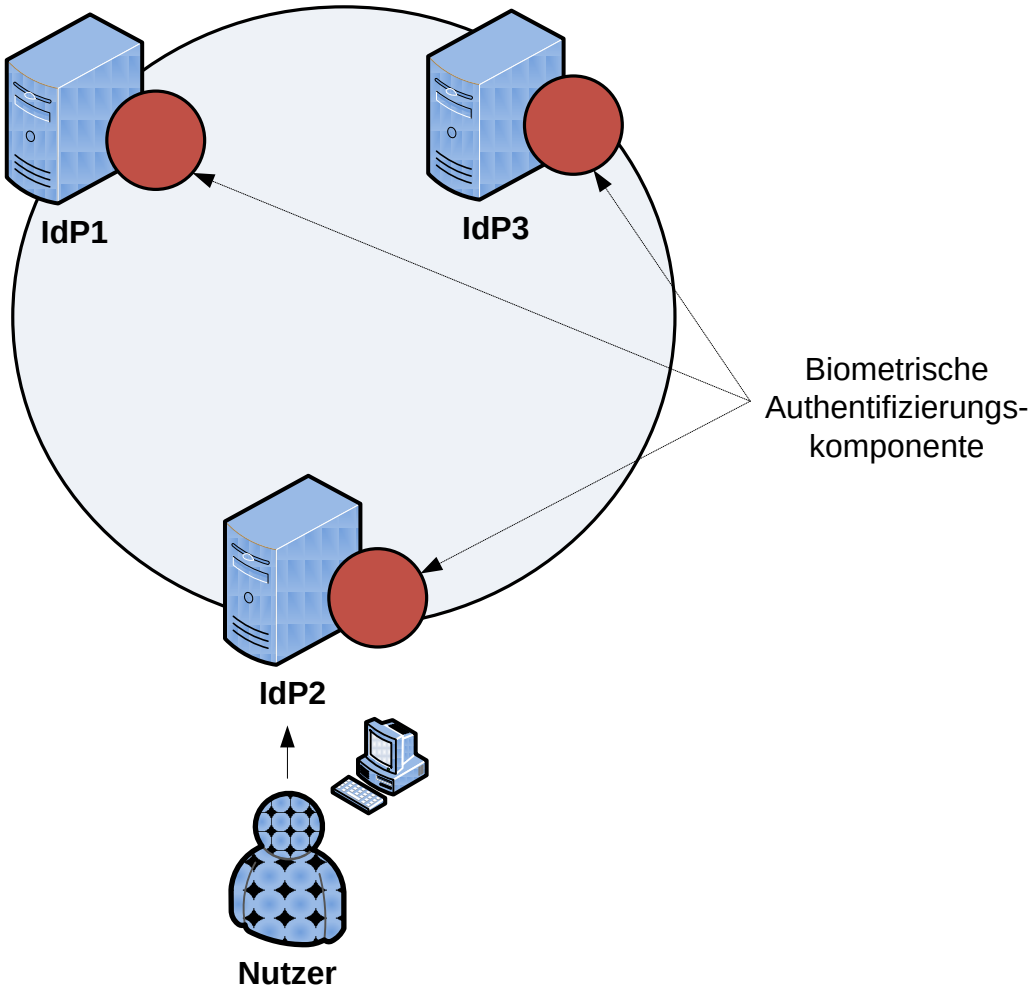

Abbildung 7: Föderierte AAI mit geteilter, dezentraler biometrischer Authentifizierungs-komponente
Quelle: in Anlehnung an (Olden 2008)

(4) AAI mit nutzerseitig gespeicherter biometrische Authentifizierungskomponente

Spezifisch für dieses Architekturmuster ist die nutzerseitige Speicherung der biometrischen Authentifizierungskomponente. Somit hat der Nutzer zwar idealerweise vollkommende Kontrolle über seine biometrische Daten; diese müssen allerdings in einer vertrauenswürdigen Hardwareumgebung mitgeführt werden, womit ein wesentlicher Vorteil der Biometrie verloren geht.

Zusätzlich sind weitere Kombinationen aus verschiedenen Architekturmustern denkbar. Die Erkenntnisse der atomaren Architekturmuster müssen in solchen Fällen entsprechend zusammengeführt werden (Olden 2008).

5.3 Probleme biometriebasierter AAIs

Zur Untersuchung und Systematisierung biometriespezifischer Herausforderungen beim Architekturentwurf wählt Olden (2008) den Ansatz der föderierten AAI mit dezentraler Authentifizierungskomponente (Abbildung 7). Die Untersuchungsfelder adressieren konkret den verteilten Charakter des betrachteten Architekturmusters und werden im Folgenden detailliert betrachtet. (Olden 2008)

5.3.1 Alterung biometrischer Daten

Biometriespezifische Aspekte, die beim Architekturentwurf zu berücksichtigen sind, umfassen insbesondere die Alterung biometrischer Merkmale. Vor allem bei verhaltensbasierten Biometrien muss dieser Prozess durch geeignete Adaptionsmechanismen kompensiert werden. Diese sorgen analog zur biologischen Alterung des Merkmals für eine technische Alterung des Referenzdatensatzes, sodass die Diskrepanz zwischen Merkmalsausprägung und der digitalen Repräsentation zur keiner fälschlichen Ablehnung des Nutzers führt. Dies erfordert allerdings die regelmäßige Zurverfügungstellung aktueller biometrischer Proben. Geht man von einer Verteilung der biometrischen Komponenten und somit der Verteilung der Referenzdatensätze auf verschiedene IdPs aus, wird unterstellt, dass sich der Nutzer bei diesen in unterschiedlichen Abständen authentisiert. Abbildung 8 zeigt beispielhaft, wie sich ein Nutzer zunächst an einem Identity Provider (IdP1), dem verhältnismäßig aktuelle Tippproben vorliegen, erfolgreich authentisiert (Schritt 1). Später versucht er sich an einem weiteren IdP der Föderation (IdP2) zu authentisieren. Jedoch liegen hier nur alten Daten vor, so dass eine fälschliche Rückweisung des Nutzers wahrscheinlicher wird. Kann föderationsweit keine effektive Adaption gewährleistet werden, so entstehen zwangsläufig Qualitätsunterschiede zwischen den IdPs. (Olden 2008)

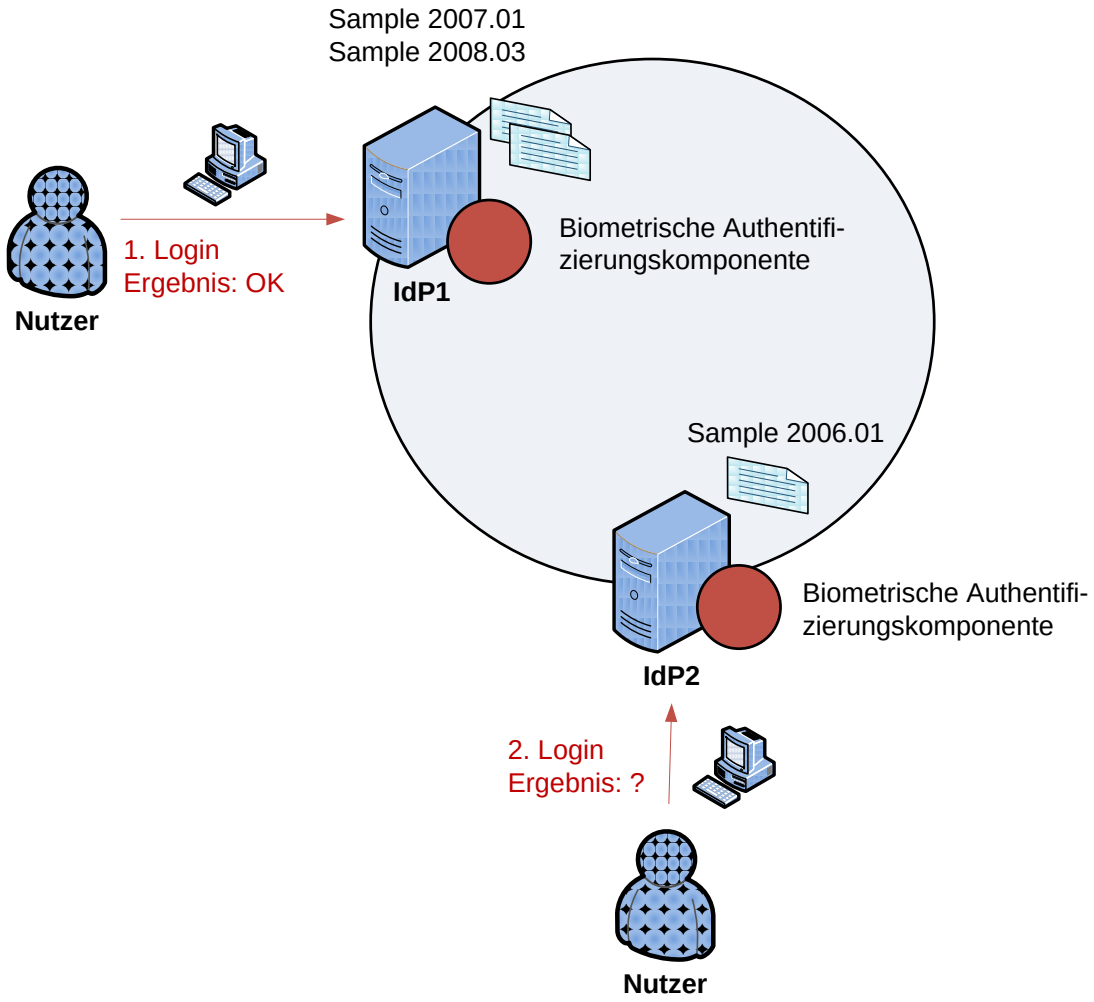

Abbildung 8: Alterung in biometriebasierten AAIs
Quelle: in Anlehnung an (Olden 2008)

5.3.2 Systemsicherheit

Ein inhärentes Sicherheitsproblem biometrischer Authentifizierungsverfahren sind Replay-Angriffe. Speziell die Offenheit eines Netzwerkes, wie sie im Rahmen der Hochflexibilität gefordert wird, erhöht die Verwundbarkeit gegenüber Angreifern. Aufgrund der Sensorstandardisierung im Kontext der Tippverhaltensbiometrie und der Möglichkeit der Verwendung von Key-Loggern muss das Risiko von Replay-Angriffen als zentrales Sicherheitsrisiko angesehen werden.

Während in zentralisierten Architekturen Replay-Filter einen effektiven Schutz bieten können, kann dieser in der untersuchten föderativen Umgebung per se nicht gewährleistet werden (Olden 2008). Das in Abbildung 9 skizzierte Szenario soll dies verdeutlichen.

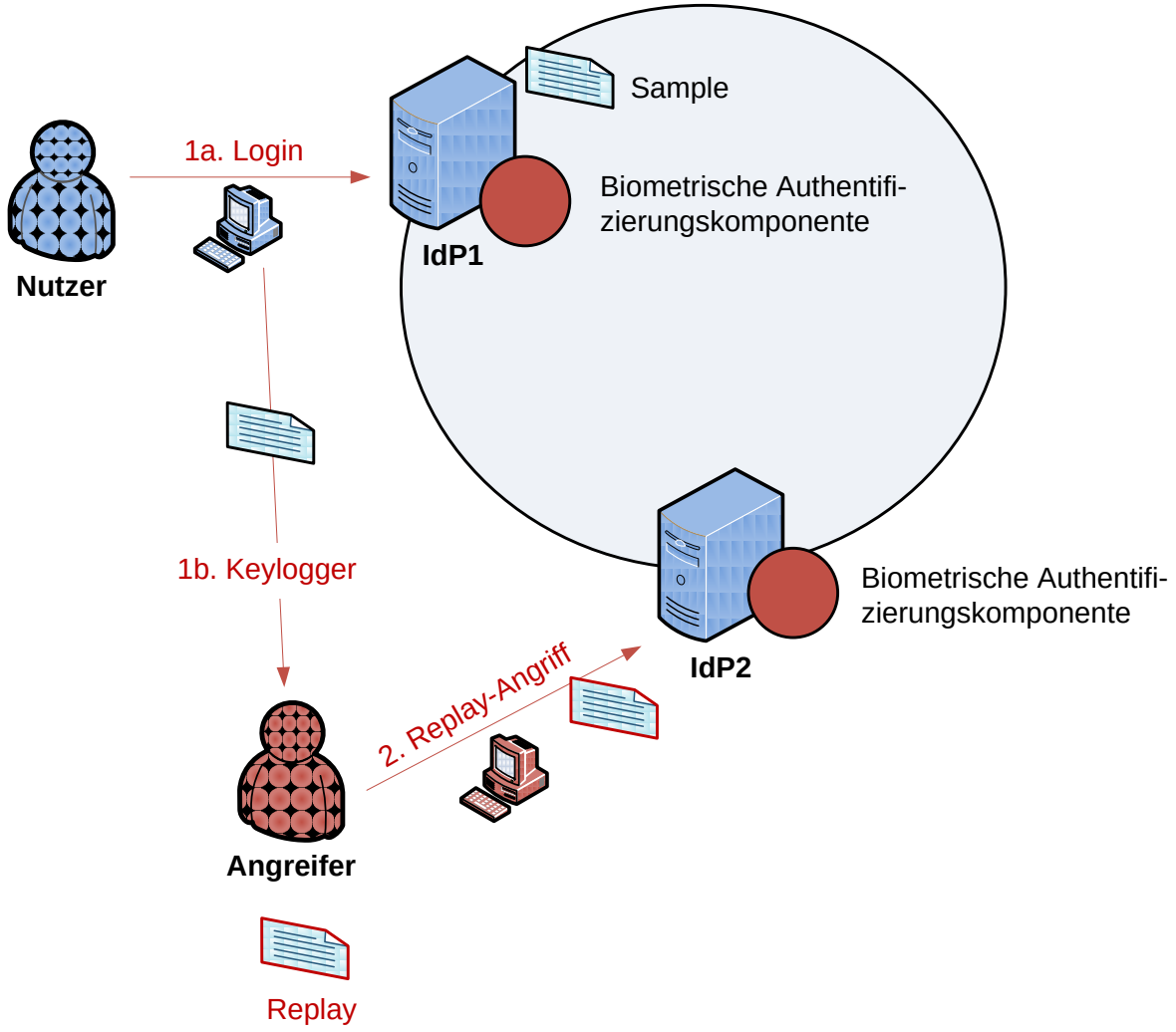

Abbildung 9: Replay-Angriff in biometriebasierten AAIs
Quelle: (Olden 2008)

Ein Nutzer authentisiert sich gegenüber IdP1 unter Verwendung von Passwort und Tippverhaltensbiometrie (Schritt 1). Ein Angreifer kann sowohl das Passwort als auch die Tippprobe mit einem Key-Logger abgreifen, um diese anschließend wiedereinzuspielen und sich somit als genannte Nutzer zu authentisieren (Schritt 2). IdP1 würde die Tippverhaltensprobe im Original oder in abgeänderter Form als Wiedereinspielung erkennen und abweisen. Verwendet der Angreifer allerdings im *Circle of Trust* den alternativen IdP2 (Schritt 3), so wird der Angriff nicht als solcher erkannt und ist erfolgreich durchgeführt. (Olden 2008)

5.3.3 Qualitätsaspekte

Die Qualität der Ergebnisse einer Biometrie hängen unmittelbar vom Sensor ab, der die biometrischen Daten während der eigentlichen Authentifizierung und des vorgelagerten Enrolments erfasst. In Föderationen müssen von allen beteiligten IdPs vergleichbare Qualitätsstandards gefordert werden. (Olden 2008)

Dies erfordert zum einen die Möglichkeit, qualitätsrelevante Attributinformationen zwischen den IdPs auszutauschen. Zum anderen muss festgelegt werden, wie mit unterschiedlichen Qualitätsniveaus, die durch Verwendung unterschiedlicher Profile für PC-Tastatur und Laptoptastatur begründet sein können, umgegangen wird. (Olden 2008)

5.4 Lösungsansätze

Um die beschriebenen Probleme innerhalb einer föderierten AAI mit dezentraler Authentifizierungskomponente zu lösen, beschreibt Olden (2008) zwei Lösungsansätze, die im Folgenden beschrieben werden. Technische Grundlage bildet in beiden Fällen das OpenID-Protokoll. Gründe hierfür sind insbesondere die Benutzerfreundlichkeit, Reife und Verbreitung des Protokolls im Kontext des Nutzer-zentrierten Identitätsmanagements (Olden 2008).

5.4.1 Synchronisierung der biometrischen Daten

Unter Synchroniserung wird in diesem Zusammenhang die wechselseitige Aktualisierung der biometrischen Datensätze im Sinne einer Datenintegration verstanden. Diese kann wahlweise auf Datenbank- oder Anwendungsebene des Circles of Trust erfolgen. Eine effektive Synchronisierung erfordert zwischen den beteiligten IdPs ein gemeinsames syntaktisches sowie semantisches Verständnis der biometrischen Daten und der Kommunikationsprotokolle. Zudem müssen die IdPs während des Aktualisierungsprozesses gleichzeitig online sein. Aus diesen Gründen eignet sich dieser Ansatz nur in geschlossenen Netzwerken. (Olden 2008)

5.4.2 Entfernte Authentifizierung

Nachdem jeder Nutzer bzgl. eines Merkmals nur eine biometrische Identität besitzt, liegt die Unterstellung nahe, dass nur ein IdP innerhalb der Föderation diese biometrische Identität kennen und verwalten sollte. Diese eine Identität bei einem „Heimat“-IdP reicht theoretisch aus, um föderationsweit auf alle Ressourcen zugreifen zu können. (Olden 2008) Dies entspricht dem Grundgedanken eines föderierten Identitätsmanagements (engl. Federated Identity Management, FIM) (Hommel 2008).

Nach dem von Olden (2008) weiterentwickelten Konzept wird ein Nutzer, der sich bei einem IdP authentisieren möchte, der nicht sein „Heimat“-Provider ist, logisch zu diesem umgeleitet und dort authentifiziert.

5.5 Implikationen für hGP

Im betrieblichen Kontext werden digitalen Nutzeridentitäten von den jeweiligen Heimatorganisationen verwaltet. Eine redundante Datenhaltung erhöht das Risiko von Inkonsistenzen. Zudem ist die Verteilung von Benutzeridentitäten an andere Organisationen aufgrund des inhärenten Personenbezugs mit Datenschutzproblematiken behaftet. (Hommel 2008)

Den Ergebnissen von Olden (2008) folgend ist die Existenz einer einzigen biometrischen Identität pro Nutzer als zielführend einzustufen. Konsequenterweise verbleiben somit zwei mögliche atomare AAI-Architekturmuster sowie verschiedene Mischformen:

(1) Föderative AAI mit Verwaltung der biometrischen Komponente durch die Heimatorganisation des Nutzers
(2) Zentralisierter Ansatz mit einem zentralen, föderationsweit akzeptierten biometrischen Authentifizierungsdienst („Biometric Authentication as a Service“, BioAaaS)

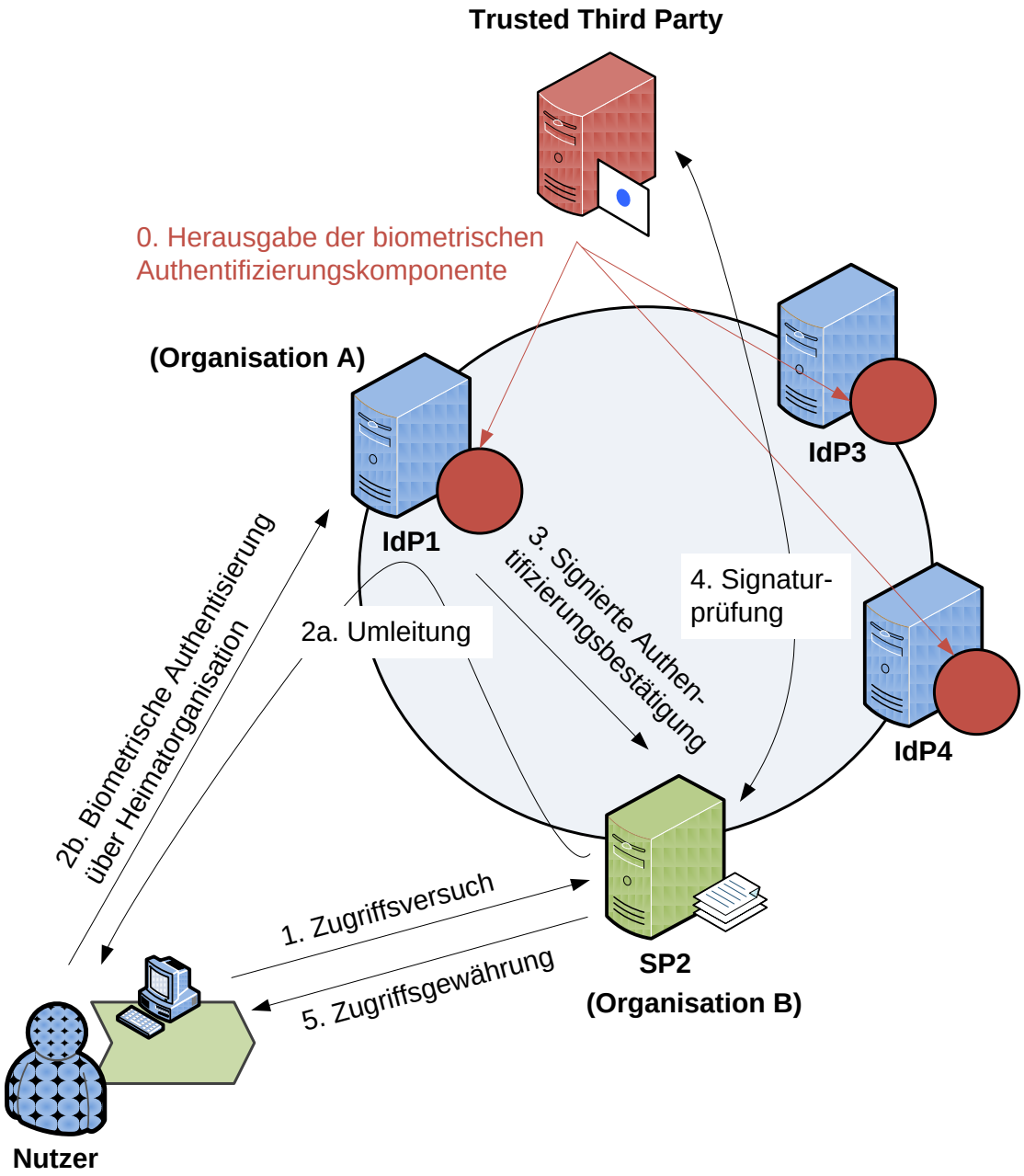

Abbildung 10: Föderative biometriebasierte AAI im Kontext von hGP

Im ersten Fall, der durch Abbildung 10 beschrieben wird, möchte ein Nutzer auf Ressourcen von Organisation B (in der Rolle eines SP) zugreifen (Schritt 1). Hierzu wird er zunächst zu seiner Heimatorganisation (Organisation A in der Rolle IdP1) voll- oder teilautomatisch umgeleitet, die autonom eine biometrische Authentifizierung des Nutzers vornimmt (Schritt 2). IdP1 erstellt eine Bestätigung und sendet diese an SP2 (Schritt 3). Um die Integrität der Vertrauenskette sicherzustellen bzw. organisationsübergreifend ein einheitliches Qualitätsniveau der Authentifizierung zu etablieren, muss die biometrische Authentifizierungskomponente zentral spezifizierten Richtlinien folgen und deren Einhaltung zur Laufzeit transparent und glaubhaft darlegen können. Dies wird durch eine asymmetrische Signaturschlüsselinfrastruktur realisierbar. Zentrale Rolle spielt hierbei eine Trusted Third Party, die eine Signaturkontrolle ermöglicht und im beschriebenen Szenario durch den Herausgeber der biometrischen Authentifizierungskomponente übernommen wird. Wird die Komponente für jede implementierte Authentifizierungsmethode (z. B. zur Unterscheidung von Psylock Festtextverfahren mit 42 und 84 Zeichen) mit einem privaten Signaturschlüssel ausgestattet, so kann die Authentifizierungsbestätigung entsprechend signiert und die verwendete Methode und deren Qualität vertrauenswürdig an mögliche SPs kommuniziert werden. Die Spezifikation einer praktikablen Gültigkeitsdauer vorausgesetzt, lässt sich hierdurch ein organisations- bzw. SP-übergreifendes SSO realisieren. Nach der Prüfung der Authentifizierungsbestätigung und der Signatur (Schritt 4) fällt SP2 anhand der vorliegenden Autorisierungsinformationen eine Zugriffsentscheidung, die im positiven Fall dem authentifizierten Nutzer den gewünschten Zugriff gewährt (Schritt 5).

Der zweite Fall erfordert einen vertrauenswürdigen zentralen biometrischen Authentifizierungsdienst, der föderationsweit verfügbar ist und akzeptiert wird (Abbildung 11). Möchte ein Nutzer auf eine externe Ressource eines SPs zugreifen (Schritt 1), wird dieser zunächst zu diesem Dienst umgeleitet und dort authentifiziert (Schritt 2). Die zentral ausgestellte Authentifizierungsbestätigung (Schritt 3) wird vom SP akzeptiert und der Nutzer erhält den gewünschten Zugriff (Schritt 4). Dieses Szenario abstrahiert allerdings von der Beschaffung zusätzlicher Nutzerattribute, die für die Zugriffskontrollentscheidung des SPs möglicherweise benötigt werden. Dies kann z. B. die funktionale Rolle des Benutzers in seiner Heimatorganisation sein. Möglichkeiten zur transparenten Einbindung des Heimat-IdPs bleiben der zukünftigen Forschung vorbehalten. Bei der Umsetzung des BioAaaS sind zudem Aspekte der Datenschutzfreundlichkeit und der Verfügbarkeit explizit zu untersuchen und zu berücksichtigen, da sie vom Autor als wesentliche Erfolgs- bzw. Akzeptanzfaktoren eines solchen Dienstes erachtet werden.

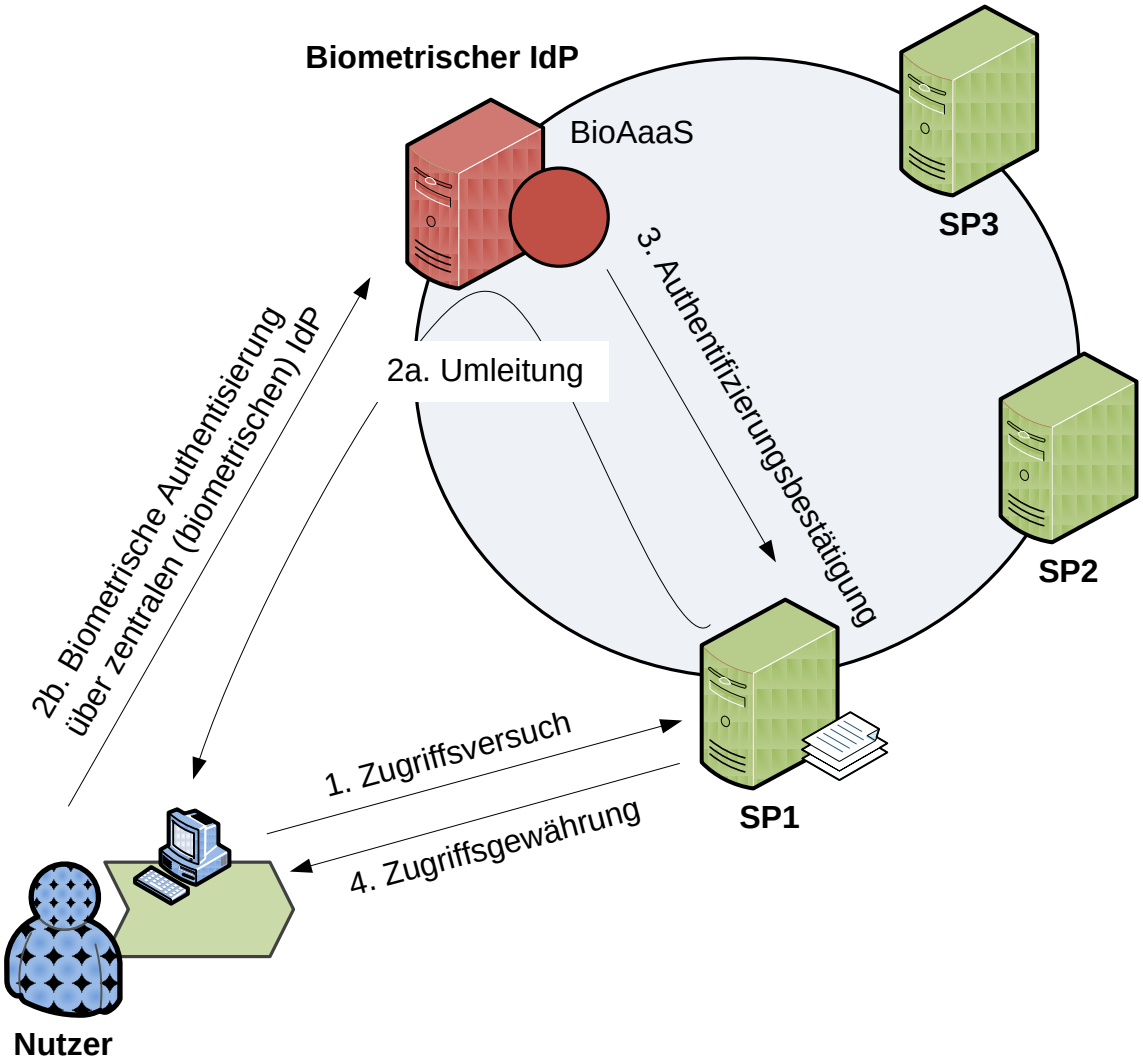

Abbildung 11: Biometric Authentication as a Service

6 Fazit

6.1 Zusammenfassung

Gegenstand dieses Arbeitsberichtes war die Untersuchung von Möglichkeiten zur sicherheitstechnischen Härtung von hochflexiblen Geschäftsprozessen (hGP) durch geeignete Authentifizierungsdienste. Da die Sicherheit des Gesamtprozesses unmittelbar von der Verwundbarkeit des schwächsten Glieds in der Vertrauenskette abhängt, muss prozessweit eine einheitliche Authentifizierungsqualität gewährleistet werden können. Passwortbasierte Verfahren sind hierzu völlig ungeeignet. Aufgrund individueller Passwort-Richtlinien sowie unkontrollierbarer Freiräume in deren Auslegung entstehen zwangsläufig unterschiedliche Qualitätsniveaus. Alternative Token-basierte Methoden schränken die Wertschöpfungsstrukturflexibilität ein, da sie eine vorliegende physische Infrastruktur voraussetzen. Zudem können beide Ansätze keine personenbindende Authentifizierung garantieren. Biometrische Verfahren schaffen hier potenziell Abhilfe. Als ideale Lösung im Kontext von hGP konnte die Tippverhaltensbiometrie identifiziert werden. Für die organisationsübergreifende Anwendung

müssen allerdings geeignete logische Infrastrukturen geschaffen werden. Hierzu wurden verschiedene Architekturmuster für Authentifizierungs- und Autorisierungsinfrastrukturen (AAI) hinsichtlich der Integrierbarkeit biometrischer Authentifizierungskomponenten untersucht. Spezifische Aspekte der Merkmalsalterung, Sensorqualität und Sicherheit (Replay-Angriffe) konnten bei der nutzerzentrierten Verteilung biometrischer Profile als wesentliche Herausforderungen ermittelt werden. Zudem wurden zwei Lösungswege auf der Basis des OpenID-Protokolls konzipiert. Für den Kontext hGP empfiehlt sich ein Ansatz, in dem ein Nutzer innerhalb einer Föderation bzgl. eines spezifischen Merkmals nur eine biometrische Identität besitzt. Auf der Basis dieser Untersuchungsergebnisse wurden zwei AAI-Architekturmuster zur sicherheitstechnischen Härtung von hGP mittels Tippverhaltensbiometrie vorgestellt.

6.2 Zukünftige Forschungsarbeiten

Mögliche Stoßrichtungen für zukünftige Forschungsarbeiten sind:

(1) Die prototypische Implementierung einer föderativen biometriebasierten AAI mit geeigneter Attribut- und Signaturschlüsselinfrastruktur für hGP.
(2) Die prototypische Entwicklung eines datenschutzfreundlichen zentralen biometrischen Authentifizierungsdienstes (BioAaaS) für hGP.
(3) Die Flexibilisierung der Authentifizierung durch dynamische Skalierung der Authentifizierungsstärke zur Laufzeit eines hGP gemäß situativer ggf. modellhaft spezifizierter Authentifizierungsanforderungen.
(4) Evaluierung der Architekturen im Umfeld von hGP anhand von Praxisbeispielen.

Literaturverzeichnis

Albrecht A, Probst T (2001) Bedeutung der politischen und rechtlichen Rahmenbedingungen für biometrische Identifikationssysteme. In: Behrens et al. (Hrsg) Biometrische Identifikation: Grundlagen, Verfahren, Perspektiven, Vieweg, Wiesbaden, S. 27-54

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

Bartmann D (2000) Benutzerauthentisierung durch Analyse des Tippverhaltens mit Hilfe einer Kombination aus statistischen und neuronalen Verfahren, Dissertation, München

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

Behrens M, Heumann B (2001) Fingerbilderkennung. In: Behrens et al. (Hrsg) Biometrische Identifikation: Grundlagen, Verfahren, Perspektiven, Vieweg, Wiesbaden, S. 81-104

Benatar, M. (2006). Access Control Systems. Security, Identity Management and Trust Models, Springer, New York

Breitenstein M (2002) Überblick über biometrische Verfahren. In: Nolde et al. (Hrsg) Biometrische Verfahren. Körpermerkmale als Passwort. Grundlagen, Sicherheit und Einsatzgebiete biometrischer Identifikation, Deutscher Wirtschaftsdienst, Köln. S. 35-82

Breu M (2003) Evaluation des biometrischen Tipperkennungsverfahrens PSYLock im Kontext automatisierter Authentisierungsverfahren, Dissertation, Regensburg

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

Dotzler F (2009) Psylock Password Reset und Datenschutz, Psylock, Regensburg

Eckert C (2009) IT-Sicherheit. Konzepte, Verfahren, Protokolle, 6. Aufl. Oldenbourg, München

Ghattas J, Soffer P (2009) Evaluation of inter-organizational business process solutions. A conceptual model-based approach. In: Information Systems Frontiers, 1(3), S. 273-291

Gonzáles-Rodrígues J, Toledano DT, Ortega-Garcia J (2007) In: Jain et al. (Hrsg) Handbook of Biometrics, Springer, New York, S. 151-170

Hafner M, Breu R (2009) Security Engineering for Service-Oriented Architectures, Springer, Berlin

Hocke S (2004) Flexibilitätsmanagement in der Logistik. Systemtheoretische Fundierung und Simulation logistischer Gestaltungsparameter, Lang, Frankfurt

Hommel W (2008) Architektur– und Werkzeugkonzepte für föderiertes Identitäts–Management, Dissertation, München

Jain AK, Ross A (2007) Introduction to Biometrics. In: Jain et al. (Hrsg) Handbook of Biometrics Springer, New York, S. 1-22

Kronschnabl S (2008) IT-Security Governance, Dissertation, Regensburg

Kupsch F (2006) Framework zur dezentralen Integration systemübergreifender Geschäftsprozesse, Eul, Köln

Lehner F (1995) Grundfragen und Positionierung der Wirtschaftsinformatik. In: Lehner F, Hildebrand K, Maier R (Hrsg) Wirtschaftsinformatik. Theoretische Grundlagen, Hanser, München, S. 1–72

Lotz V, Pigout E, Fischer PM, Kossmann D, Massacci F, Pretschner A (2008) Towards Systematic Achievement of Compliance in Service-Orientied Architectures. The MASTER Approach. In: Wirtschaftsinformatik 50(5), S. 383-391

Maltoni D, Maio D, Jain AK, Prabhakar S (2009) Handbook of Fingerprint Recognition, 2. Aufl. Springer, London

Mansfield AJ, Wayman JL (2002) Best Practices in Testing and Reporting Performance of Biometric Devices, Version 2.01. http://www.cesg.gov.uk/policy_technologies/biometrics/media/bestpractice.pdf. Abruf am 2009-09-14

Masak D (2006) IT-Alignment. IT-Architektur und Organisation, Springer, Berlin

Moormann J, Schmidt G (2007) IT in der Finanzbranche. Management und Methoden, Springer, Berlin

Österle H, Winter R (2003) Business Engineering. In: Österle H, Winter R (Hrsg): Business Engineering. Auf dem Weg zum Unternehmen des Informationszeitalters, 2. Aufl. Springer, Berlin, S. 4-10

Olden M (2008) Biometric Authentication and Authorization Infrastructures, Dissertation, Regensburg

Oppliger R (2002) Internet and Intranet Security, 2. Auf. Artech House, Boston

Pfitzmann A (2006) Biometrie. wie einsetzen und wie keinesfalls? In: Informatik Spektrum 29(5), S. 353-356

Piller FT (2000) Mass customization. Ein wettbewerbsstrategisches Konzept im Informationszeitalter, Gabler, Wiesbaden

Pope JA, Bartmann D (2009). Securing On-Line Transactions with Biometric Methods. In: International Journal of Electronic Marketing and Retailing 2(5), o. S.

Psylock (2009) Vergleich von Psylock und BioPII (intern), Psylock GmbH, Regensburg

Pütz C, Wagner D, Ferstl OK, Sinz EJ (2009) Geschäftsprozesse in Medizinischen Versorgungszentren und ihre Flexibilitätsanforderungen. Ein fallstudienbasiertes Szenario, Forflex, Bamberg

Reiser H (2008) Ein Framework für föderiertes Sicherheitsmanagement, Dissertation, München

Schläger C, Nowey T (2006) Towards a Risk Management Perspective on AAIs. In: Fischer-Hübner et al. (Hrsg) LNCS 4083, Springer, Heidelberg, S. 41-50

Schläger C, Priebe T, Liewald M, Pernul G (2007) Enabling Attribute-bsed Aces Control in Authentication and Authorisation Infrastructures, BLED 2007 Proceedings. Paper 3

Schläger C (2008) Attribute-based Infrastructures for Authentication and Authorization, EUL, Lohmar

Schmelzer HJ, Sesselmann W (2008) Geschäftsprozessmanagement in der Praxis, 8. Aufl. Hanser, München

Shirey R (2000) RFC 2828 - Internet Security Glossary. http://www.ietf.org/rfc/rfc2828.txt. Abruf am 2006-02-06

Sinz EJ (1999) Konstruktion von Informationssystemen. In: Rechenberg P, Pomberger G (Hrsg) Informatik-Handbuch, 2. Aufl. Hanser, München 1999, o. S.

Smith RE (2002) Authentication. From Passwords to Public Keys, Addison-Wesley, Amsterdam

St. Clair L, Johansen L, Enck W, Pirretti M, Traynor P, Patrick-Jaeger T (2006) Password Exhaustion. Predicting the End of Password Usefulness. In: Bagchi A, Atluri V (Hrsg) LNCS 432, Springer, Heidelberg, S. 37-55

Von Graevenitz G (2006) Erfolgskriterien und Absatzchancen biometrischer Identifikationssysteme, LIT, Berlin

Weber M (2008) Akzeptanz biometrischer Authentifizierungssysteme, Dissertation, Mannheim

Prof. Dr. Dieter Bartmann
Universität Regensburg
Universitätstraße 31
93053 Regensburg
Tel.: +49 941/943-1881
Fax: +49 941/943-1871
E-Mail: dieter.bartmann@forflex.de

Prof. Dr. Freimut Bodendorf
Universität Erlangen-Nürnberg
Lange Gasse 20
90403 Nürnberg
Tel.: +49 911/5302-450
Fax: +49 911/5302-379
E-Mail: freimut.bodendorf@forflex.de

Prof. Dr. Otto K. Ferstl
Universität Bamberg
Feldkirchenstraße 21
96045 Bamberg
Tel.: +49 951/863-2679
Fax: +49 951/863-2710
E-Mail: otto.ferstl@forflex.de

Prof. Dr. Elmar J. Sinz
Universität Bamberg
Feldkirchenstraße 21
96045 Bamberg
Tel.: +49 951/863-2512
Fax: +49 951/863-2513
E-Mail: elmar.sinz@forflex.de

Geschäftsführung forFLEX
Dipl.-Wirtsch.Inf. Corinna Pütz
Universität Bamberg
Feldkirchenstraße 21
96045 Bamberg

Tel.: +49 951/863-2777
Fax: +49 951/863-5777
E-Mail: corinna.puetz@forflex.de
Internet: http://www.forflex.de