Risikobasierte und adaptive Authentifizierung

René Riedel · Norbert Pohlmann

Institut für Internet-Sicherheit – if(is)
Westfälische Hochschule
{riedel | pohlmann}@internet-sicherheit.de

Zusammenfassung

Die aktuellen Verfahren zur Authentifikation im Internet überfordern die digitale Gesellschaft zunehmend. Für immer mehr Dienste muss ein separater Registrierungs- oder Identifikationsprozess durchgeführt werden. Die Praxis zeigt: Sichere Passwörter sind für viele verschiedene Dienste inpraktikabel und hardwarebasierte digitale Identitäten schaffen aufgrund der fehlenden Akzeptanz bisher nur geringfügig Abhilfe. Ein vielversprechender Lösungsansatz für diese Problematik ist die Zentralisierung der Authentifikation durch sogenannte „Identity Provider". Große Unternehmen wie Google, Facebook oder Amazon bieten schon seit längerer Zeit die übergreifende Nutzung der bereits erstellten Konten für die Authentifizierung bei externen Diensten an. Der Vorteil bei diesem Konzept ist, dass potentiell nur noch wenige Identitäten im Internet benötigt werden und somit die Authentifizierung sowohl clientseitig, als auch serverseitig, effektiver gestaltet werden kann. Die bestehenden Konzepte weisen jedoch Probleme hinsichtlich der Skalierbarkeit auf, denn die konkreten Verfahren für die Authentifizierung können in der Regel nicht an den Bedarfsfall gebunden werden. Dieser Artikel knüpft an die fehlende Berücksichtigung der Skalierbarkeit an. Es wird ein High-Level Design eines skalierenden „Identity Providers" vorgestellt, der basierend auf einem berechneten Risikowert eine adaptive Auswahl der verwendeten Verfahren für die Authentifizierung ermöglichen soll. Die technologische Grundlage hierfür bildet ein vierter Faktor, der unteranderem aus „Device Fingerprints", Verhaltensmustern, Netzwerkkennzahlen und Sensordaten besteht.

1 Einführung

Die aktuell gängigsten Verfahren zur *Authentifikation* im Internet sind entweder unsicher oder sicher aber (sehr) komplex in der Handhabung. Als Beispiele hierfür kann die Authentifizierung mittels Passwort als unsicheres oder digitale Identitäten in Verbindung mit einem kostspieligen Kartenlesegerät als aufwändiges Verfahren betrachtet werden. Grundsätzlich bieten die bestehenden Verfahren nur eine grobe Unterscheidung von verschiedenen Sicherheitsniveaus: Für IT-Integratoren entsteht daraus das Problem, dass sie eine „Entweder-oder-Entscheidung" treffen müssen und somit die Verwendung eines bestimmten *Authentifikation*sverfahrens nicht an den Sinn und Zweck einer Anwendung binden können.

Dieser Artikel befasst sich deshalb mit neuen und handhabbaren Methoden zur *Authentifikation* im Internet, bei denen die Art der *Authentifikation* adaptiv an die durchzuführende Aufgabe angepasst wird. Ziel ist es also eine feinere Unterscheidung zwischen verschiedenen Sicherheitsniveaus und Anwendungshintergründen zu schaffen, um die Nutzbarkeit solcher Dienste zu verbessern.

P. Schartner · N. Pohlmann (Hrsg.) · D•A•CH Security 2018 · syssec (2018) 360-371.

Hierfür können beispielsweise bestehende Verfahren in Abhängigkeit von dem benötigten Sicherheitsniveau kombiniert werden, um somit Synergien zu erzielen. Als Ergebnis werden neue *Authentifikation*sverfahren geschaffen und die bestehenden Verfahren gestärkt. Neben den Funktionalitäten der bestehenden Verfahren, werden weitere Parameter für die Durchführung der Authentifizierung herangezogen. Hierbei kann es sich um Verkehrsdaten auf Netzwerkebene, Informationen über die Hard -und Software eines Informationssystems oder Profile über das Verhalten eines Nutzers handeln. Die gesammelten Informationen können für die Bewertung des Sicherheitsniveaus und des Restrisikos verwendet werden.

Damit aus der Kombination der bestehenden *Authentifikation*sverfahren keine weiteren unannehmbaren Komplexitäten entstehen, beschreibt dieser Artikel einen sogenannten *„Auth-Service“*, der in Form eines *„Identity Providers“* die benötigten Funktionalitäten für verschiedene Anwender zur Verfügung stellt.

Die Verwendung des *„Auth-Services“* erfolgt über eine einfache Schnittstelle, die in Form von sogenannten *„Service-Klassen“* realisiert wird: Ein Anwender könnte somit anhand der bereitgestellten *„Service-Klassen“* entscheiden, welches Sicherheitsniveau für seinen konkreten Anwendungshintergrund relevant ist. Eine Bank könnte in diesem Zusammenhang beim *„Auth-Service“* eine stärkere Authentifizierung für die Durchführung einer Transaktion anfordern, als der Betreiber eines Blogs für die Anmeldung auf einer Internetseite.

Basierend auf der ausgewählten Service-Klasse wird vom *„Auth-Service“* entschieden, welche zusätzlichen Parameter für die Authentifizierung herangezogen und welche Kombinationen der bestehenden Authentifikationsverfahren verwendet werden müssen.

Aus diesem Beispiel geht exemplarisch hervor, dass der Vorteil einer risikobasierten und adaptiven Authentifizierung Auswirkungen auf verschiedene Anwendergruppen hat. Für den Endanwender erleichtert sich in erster Linie die Durchführung einer *Authentifikation*. Darüber hinaus wird durch die Verwendung von weiteren Parametern im Hintergrund der Authentifizierung die Sicherheit des Endanwenders erhöht.

Für den IT-Integrator entsteht der Vorteil, dass er keine „Entweder-oder-Entscheidungen“ bei der Auswahl der benötigten Authentifikationsverfahren treffen muss, sondern vielmehr auf ein breites Spektrum an verschiedenen Schutzniveaus zugreifen kann. Ihm wird somit durch den *„Auth-Service*“ und der damit verbundenen adaptiven Authentifizierung ein flexibles und interoperables Werkzeug für einen zentralen Bestandteil von IT-Systemen zur Verfügung gestellt.

Im weiteren Verlauf dieser Arbeit werden die folgenden Ergebnisse vorgestellt:

- Es wird eine Definition der Begriffe „adaptiv“ und „risikobasiert“ vorgenommen
- Basierend auf den technischen und rechtlichen Rahmenbedingungen wird das tatsächliche Potential der risikobasierten und adaptiven Authentifizierung identifiziert
- Kritische Protokollabläufe des „Identity Lifecycle Managements“ werden im Kontext dieser Arbeit analysiert
- Es wird ein High-Level Design eines risikobasierten und adaptiven „Identity Providers“ als mögliches Referenzsystem vorgestellt

2 Begriffsbestimmung

Für den weiteren Verlauf dieses Artikels gelten die nachfolgenden Definitionen für die aufgelisteten Begriffe:

- **ID-Verifikation:** Dem Anwendungsfall entsprechende Überprüfung der angegebenen Eigenschaften einer Identität und Verbindung der überprüften Eigenschaften mit einem digitalen Merkmal im Rahmen der erstmaligen Registrierung einer digitalen Identität.
- **Authentifikation:** Erbringen eines Nachweises zu der Übereinstimmung von behaupteter und tatsächlicher Identität.
- **Adaptiv:** Eine Authentifizierung ist adaptiv, falls die Auswahl der benötigten Verfahren zur *ID-Verifikation* und *Authentifikation* nicht pauschal im Vorfeld für eine bestimmte Menge an Anwendungsfällen festgelegt wird, sondern auf Basis von Eingabeparametern E dynamisch zur Laufzeit für eine unbestimmte Menge ermittelt wird.
- **Risikobasiert:** Eine Authentifizierung ist risikobasiert, falls das gelernte Verhalten einer Person X mit den Eingabeparametern eines zukünftigen Request R abgeglichen wird und die Wahrscheinlichkeit $\mathrm{P}(\mathrm{A})\ mit\ A \coloneqq X\ hat\ R\ erstellt$ als Maß für die Authentizität von R verwendet wird.
- **Risikobasiert ∘ Adaptiv:** Die risikobasierte und adaptive Authentifizierung verwendet die Wahrscheinlichkeit P als Eingabeparameter E für die dynamische Ermittlung der benötigten Verfahren zur *ID-Verifikation* und *Authentifikation*. Die Sicherheitsanforderungen an die auszuwählenden Verfahren sind proportional zur Gegenwahrscheinlich von P, also $P(\bar{A})\ mit\ \bar{A} = X\ hat\ R\ nicht\ erstellt$.

3 Abgrenzung zu bestehenden Technologien

Die konkreten Anwendungsszenarien eines risikobasierten und adaptiven „Identity Providers“ und der damit verbundene Mehrwert im Vergleich zu den bestehenden Anbietern hängt sowohl von technischen, als auch von rechtlichen Rahmenbedingungen ab. Diese Abhängigkeiten werden in den nachfolgenden Unterkapiteln genauer beschrieben. Im Vergleich zu den verwandten Arbeiten wird das Potential der risikobasierten und adaptiven Authentifizierung genauer dargestellt.

3.1 Technische Rahmenbedingungen

Zu den technischen Rahmenbedingungen gehören die verschiedenen Faktoren, die bei der Bestätigung einer Identität grundsätzlich zum Einsatz kommen können. Eine Liste der verschiedenen Faktoren und konkrete Beispiele sind in Tabelle 1 aufgeführt (vgl. mit [1]). Im Internet werden aktuell die drei Faktoren: *Wissen*, *Besitz* und *Inhärenz* (einzeln oder in Kombination) verwendet. Die Kombination von zwei oder mehr Faktoren wird in diesem Kontext als *„Multi-Faktor-Authentifizierung“* (MFA) bezeichnet und bereits von den meisten *„Service Providern“* im Internet als zusätzliche Sicherheitsmaßnahme angeboten. Die Aktivierung der zusätzlichen Sicherheitsmaßnahme hat aktuell zur Folge, dass der Nutzer pauschal bei jeder Anfrage oder Transaktion die zusätzlichen Faktoren aktiv bestätigen muss. Aus Gründen der Effizienz (z.B. hohe Anschaffungskosten für externe Lesegeräte oder eine geringe Nutzbarkeit) hat sich im Internet der Spezialfall der MFA mit lediglich zwei Faktoren – die *„Zwei-Faktor-Authentifizierung“* (2FA) - durchgesetzt.

Tab. 1: Faktoren für die „Multi-Faktor-Authentifizierung“

Faktor	Beispiele
Wissen	Benutzername, Kundennummer, Geburtsort, Geburtsdatum, PIN, Passwort
Besitz	Kryptographische Schlüssel, Hard- und Software Token, Sicherheitsmodule, Smartcards
Inhärenz	Unterschrift, Fingerabdruck, Stimme, Tippverhalten, Mausbewegungen
Verhalten	Vergangene Transaktionen, verwendete Geräte, Besuchte Orte, verwendete Softwareversionen, Aktivitäten in sozialen Medien, Timing

Den Problemen der MFA kann mit einer adaptiven Komponente und dem Verhalten eines Nutzers als vierter Faktor entgegengewirkt werden. Durch die Auswertung von anfallenden Hintergrundinformationen bei der Verwendung eines Services und der Erstellung von Verhaltensmustern, kann ein Gefahrenwert berechnet werden, auf dessen Basis adaptiv die Anzahl der benötigten Faktoren für die Authentifizierung bestimmt werden kann.

3.2 Rechtliche Rahmenbedingungen

Dem Innovationspotential der risikobasierten und adaptiven Authentifizierung stehen rechtliche Rahmenbedingungen und technische Umsetzungsempfehlungen gegenüber. Stellvertretend hierfür können die verschiedenen Definitionen der sogenannten „Level of Assurance“ (LoA) betrachtet werden. Hierbei handelt es sich grundsätzlich um eine Klassifizierung von Sicherheitsanforderungen an die verschiedenen Verfahren im Umfeld von digitalen Identitäten, also beispielsweise Anforderungen an kryptographische Protokolle, zu verwendende Faktoren oder Token. Eine genauere Betrachtung der einzelnen LoA ist nur innerhalb von bestimmten Domänen möglich. Im Rahmen dieses Artikels werden die folgenden zwei Domänen betrachtet, die im Mittelpunkt des in Kapitel 5 vorgestellten High-Level Designs stehen:

- **D1:** Sicherheitsanforderungen an die *ID-Verifikation*
- **D2:** Sicherheitsanforderungen an die *Authentifikation*

Stellvertretend für **D1** kann in der europäischen Union die „eIDAS-Verordnung“ betrachtet werden. Innerhalb einer Durchführungsverordnung [2] werden feingranular Anforderungen an die *ID-Verifikation* definiert. Es wird eine Unterteilung in die folgenden drei verschiedene LoA vorgenommen: „niedrig“, „substantiell“, „hoch“. Diese Einteilung ist in der „eIDAS-Verordnung“ ebenfalls für **D2** vorgesehen. Im Gegensatz zu **D1** sind die Anforderungen an **D2** aber nur geringfügig berücksichtig worden. Aus diesem Grund werden für **D2** im weiteren Verlauf die Anforderungen des „National Institute of Standards and Technology“ (NIST) [3] betrachtet. In den Anforderungen des NIST wird eine Unterteilung von „Level 1“ bis „Level 4“ (mit steigendem Sicherheitsniveau) vorgenommen. Die Anforderungen des NIST konzentrieren sich überwiegend auf **D2**, sodass eine alleinige Betrachtung dieser Anforderungen im Kontext dieses Artikels nicht ausreichend ist.

Weitere LoA-Definitionen von anderen Institutionen und deren Zusammenhänge sind in [4] dargestellt. Eine vergleichbare Differenzierung der betrachteten Domänen wird in [5] vorgenommen.

3.3 Potential

Die unterschiedlichen LoA-Domänen und deren Definitionen haben direkt zur Folge, dass eine Verknüpfung ohne weiteres nicht möglich ist. Die Übergänge der verschiedenen LoA von **D1** und **D2** können jedoch hergeleitet werden, indem die Konzepte der bereits bestehenden oder angekündigten „Identity Provider" im Internet miteinander verglichen werden. Eine Einordnung der „Identity Provider" und deren Potential mit Blick auf die risikobasierte und adaptive Authentifizierung ist in Abbildung 1 dargestellt. Drei der eingeordneten „Identity Provider" sind noch nicht weit verbreitet oder im Einsatz. Eine kurze Erläuterung zu diesen Anbietern ist nachfolgend aufgeführt:

- **Verimi:** Einer der ersten „Identity Provider", der das Verfahren „Mobile Connect" in sein Portfolio aufgenommen hat. Mit Unterstützung der Telekommunikationsunternehmen „Telekom", „Telefónica", „Vodafone", soll eine Authentifizierung über das Mobilfunknetz, also mittels Mobilfunknummer und Smartphone, realisiert werden.
- **YES:** Ein von der Sparkasse konzipiertes Single-Sign-On-System. Zukünftig soll ein interoperabler Login-Dienst angeboten werden, der eine Anmeldung bei externen *„Service Providern"* mit den Zugangsdaten zu einem Bankkonto ermöglicht.
- **SkIDentity:** Dieser Service bietet Funktionalitäten für die einfache Verwendung der eID-Funktion des Personalausweises, insbesondere im Bereich von mobilen Geräten, an.

Die Abbildung zeigt, dass die Login-Dienste von Amazon, Google, Facebook und LinkedIn zum aktuellen Zeitpunkt nicht konform mit den Anforderungen aus der LoA-Domäne **D1** sind. Die Konzepte und anvisierten Ziele der Dienste von „Verimi", „YES" und „SkiDentity" sind bereits konform mit **D1** oder weisen aufgrund ihrer *ID-Verifikation* ein hohes Potential für eine zukünftige Zertifizierung auf. Als Beispiel hierfür kann die *ID-Verifikation* bei der Erstellung von Bankkonten („YES") und beim Kauf einer SIM-Karte („Mobile Connect" über „Verimi") betrachtet werden.

Durch die Bereitstellung einer 2FA können alle aufgeführten Dienste mindestens in „Level 3" von **D2** eingeordnet werden. Die Roadmap von „Verimi" sieht eine zukünftige Umsetzung von „Level 4" vor. Durch die Integration der eID-Funktion des Personalausweises ist „SkiDentity" in „Level 4" einzustufen. Da Bankkonten potentiell durch Hardware Token oder Sicherheitsmodule abgesichert werden können, erreicht „YES" konzeptionell ebenfalls „Level 4" von **D2.**

Die Einordnung der Token und Protokolle ist gemäß der NIST-Richtlinie erfolgt (vgl. mit [4]). Das Anwendungspotential der risikobasierten und adaptiven Authentifizierung ergibt sich aus der Möglichkeit, dass die Token und Protokolle aus den höheren LoAs, ebenfalls in den darunterliegenden LoAs verwendet werden dürfen. Hieraus können Synergien durch neue Kombinationen erzielt werden. Zusätzlich ist durch die Verwendung des „Verhaltens" als zusätzlicher Faktor bei der Authentifizierung eine Stärkung der einzelnen Sicherheitsmechanismen denkbar. Einen besonderen Anwendungsfall stellt in diesem Zusammenhang die Authentifizierung in Level 1 von **D2** dar. In diesem Level muss prinzipiell keiner der klassischen Faktoren zum Einsatz kommen. Die fehlende Sicherheit kann durch die Verwendung des „Verhaltens" kompensiert werden und so beispielsweise eine Transaktion auch in Level 1 authentifiziert werden. So ist es beispielsweise denkbar, dass bei der Überweisung von geringen Geldbeträgen eine Authentifizierung in Level 1 durchgeführt und bei höheren Geldbeträgen eine Kombination der Verfahren aus höheren Leveln verwendet wird.

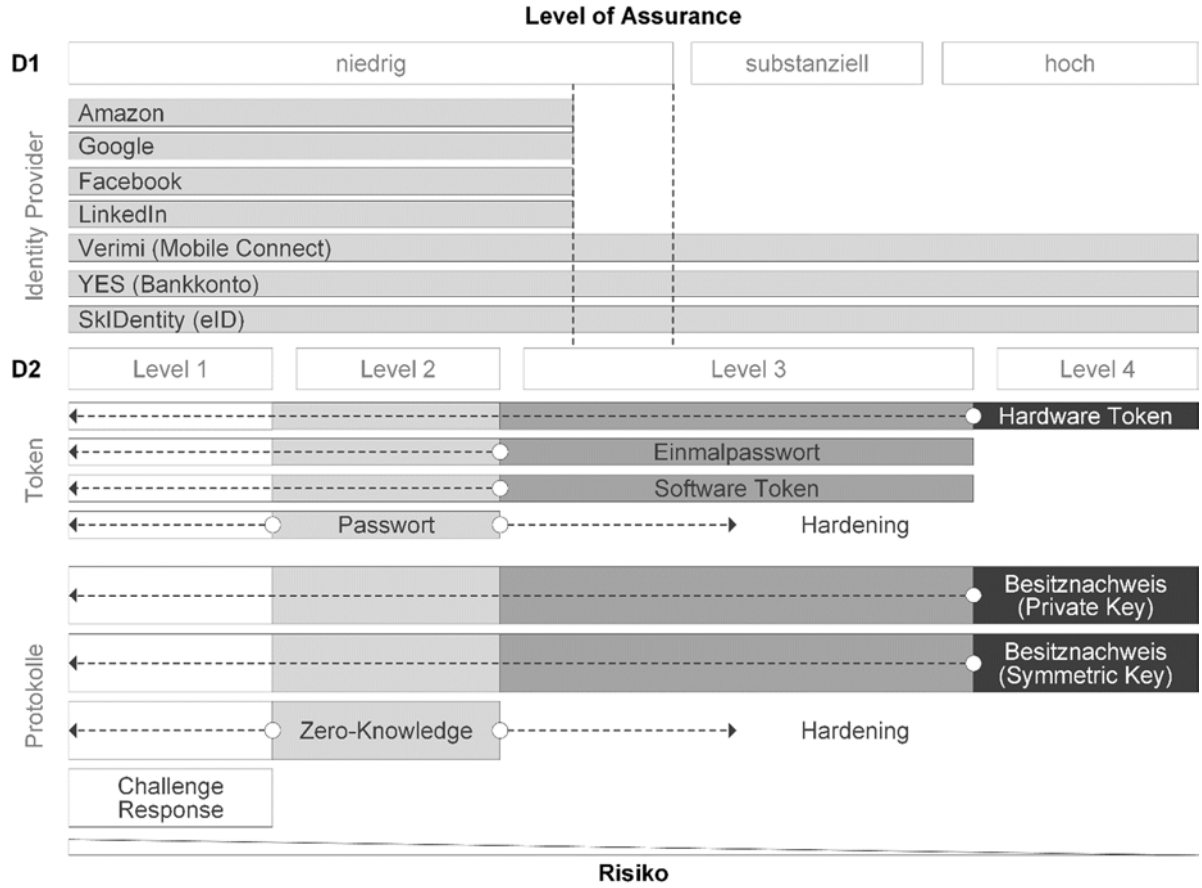

Abb. 1: Potential der risikobasierten und adaptiven Authentifizierung

3.4 Bestimmung eines Risikolevels

Aus der Definition der Sicherheitsanforderungen in der LoA Domäne **D2** können ebenfalls Anforderungen für die Bewertung eines berechneten Risikolevels abgeleitet werden. Hierfür muss die prognostizierte Wahrscheinlichkeit für einen Fehler bei der Authentifizierung in Abhängigkeit von der Auswirkung dieses Fehlers gesetzt werden. Werden beide Eigenschaften in die Kategorien „Low“, „Moderate“ und „High“ eingeteilt, ergeben sich die in Tabelle 2 dargestellten Risikostufen (vgl. mit [5]). Die adaptiven Entscheidungen müssen sich an der dargestellten Verteilung der Risikostufen orientieren.

Tab. 2: Sicherheitsanforderungen in Abhängigkeit von möglichen Risikostufen

		Auswirkung		
		Low	Moderate	High
WK	Low	Level 1	Level 2	Level 3
	Moderate	Level 2	Level 3	Level 3-4
	High	Level 3	Level 3-4	Level 4

4 Identity Lifecycle Management

Die Zentralisierung der Authentifizierung und die damit verbundene Reduzierung der Menge an digitalen Identitäten im Internet sorgt dafür, dass die verbleibenden Identitäten besonders schützenswert sind. Aus diesem Grund haben die bestehenden und zukünftigen „Identity Provider" eine besondere Sorgfaltspflicht für die Schaffung eines hohen Maßes an IT-Sicherheit in jeder Phase des „Identity Lifecycle Managements". Nur bei Berücksichtigung der Sorgfaltspflichten kann sich im Internet ein Vertrauensdienst etablieren, der den wachsenden Anforderungen an die Authentifizierung gerecht wird. Fehler in der Vergangenheit haben bereits gezeigt, dass Implementierungsfehler zu unberechtigten Zugriffen auf Identitäten geführt haben, wie im weiteren Verlauf dieses Kapitels beschrieben wird.

Die besonders kritischen Protokollabläufe werden nachfolgend anhand des in Abbildung 2 dargestellten „Identity Lifecycles" betrachtet. Für die Darstellung der sicherheitsrelevanten Protokollüberschneidungen wurden die vier (englisch benannten) Phasen „Creation", „Authorization", „Management" und „Authentication" aus [6] adaptiert.

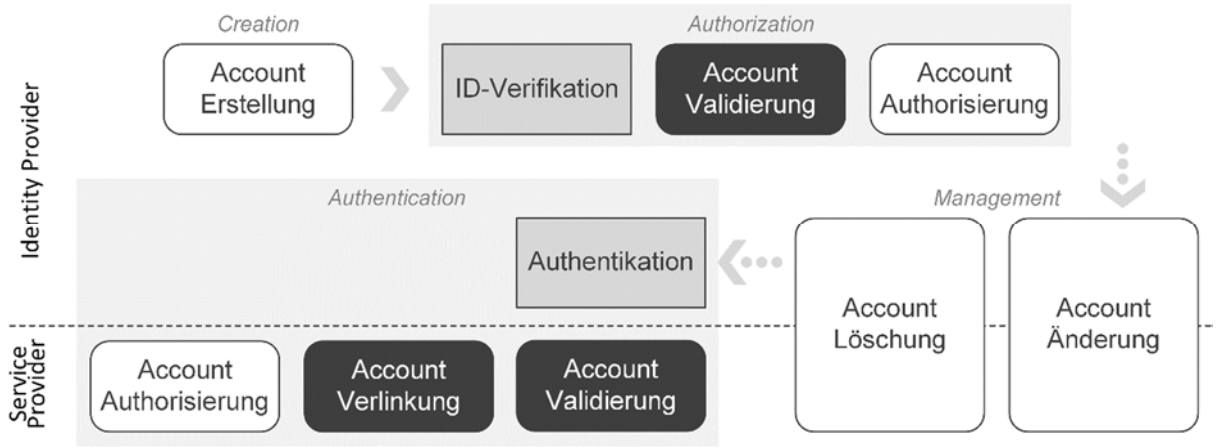

Abb. 2: Sicherheitsrelevante Protokollüberschneidungen im „Identity Lifecycle"

Zu der Validierung eines Accounts auf Seiten der „Identity Provider" gehört in erster Linie die Registrierung, Verifizierung und Aktivierung der zu verwendenden Faktoren für die Authentifizierung, also beispielsweise die korrekte Registrierung und der Besitznachweis von kryptographischen Schlüsseln, Sicherheitsmodulen, Token oder einer E-Mail-Adresse. Insbesondere bei der risikobasierten und adaptiven Authentifizierung ist der Validierungsprozess von besonderer Bedeutung, da verschiedene Kombinationen von Faktoren zum Einsatz kommen können. Durch eine unvollständige Validierung können sich Angreifer durch „Spoofen" eines Faktors unberechtigten Zugriff verschaffen, indem sie beispielsweise ein Account mit der E-Mail Adresse eines Opfers bei einem „Identity Provider" erstellen. Ohne eine Verifizierung der E-Mail Adresse ist eine Anmeldung bei „Service Providern" denkbar, sollte dort die entsprechende E-Mail Adresse bereits hinterlegt sein [7].

Nach der *Authentifikation* mit dem Login-Dienst eines „Identity Providers" sind die „Service Provider" ebenfalls in der Verantwortung eine Validierung durchzuführen. Hierzu gehört beispielsweise der Abgleich mit der eigenen Datenbasis zu bereits hinterlegten Accounts und deren festgelegten Autorisierungen, sowie die Überprüfung der erteilten Zugriffstoken durch den „Identity Provider".

Bei der erstmaligen Anmeldung mit einem externen Login-Dienst, muss eine Verlinkung mit der bestehenden Datenbasis erfolgen oder einer neuer Eintrag erstellt werden. Bei der Validierung und Verlinkung ist besonders zu beachten, dass eine Anmeldung mit verschiedenen Login-Diensten potentiell möglich ist. In diesem Fall muss eine genaue Überprüfung der persönlichen Informationen zu einem Account durchgeführt werden, damit sichergestellt werden kann, dass die verschiedenen digitalen Identitäten im Besitz der gleichen Person sind [7].

5 High-Level Design des Auth-Services

Unter Berücksichtigung der vorherigen Ergebnisse ist in Abbildung 3 das High-Level Design eines risikobasierten und adaptiven „Auth-Services“ dargestellt. Die einzelnen Bestandteile, sowie deren Aufgaben und Zusammenhänge sind in Tabelle 3 beschrieben. Ein Verweis auf die Ergebnisse der vorherigen Kapitel ist in der Beschreibung der jeweiligen Komponente enthalten.

Tab. 3: Bestandteile des High-Level Designs eines *Auth-Service*s und deren Aufgaben

Symbol	Aufgabe
	Es existieren aktuell viele unabhängige Verfahren für die *ID-Verifikation* und *Authentifikation*. Ziel ist es durch einen zentralen *„Auth-Service“* möglichst viele Synergien zwischen den einzelnen Verfahren zu erzielen. Das Potential hierfür wurde in Kapitel 3.3 beschrieben.
	Die bestehenden Verfahren und *Kennzahlen* weisen unterschiedliche Eigenschaften bezüglich der Sicherheit und Verwendbarkeit auf. Diese Eigenschaften müssen für eine automatisierte Auswertung modelliert werden. Hierbei müssen die beschriebenen Möglichkeiten und Einschränkungen aus Kapitel 3.3 und Kapitel 3.4 berücksichtigt werden.
	Für den flexiblen Einsatz des *„Auth-Services“* müssen die realen Anwendungsszenarien mit mathematischen Modellen beschrieben werden, damit anschließend eine adaptive Entscheidung auf Basis von maschinellem Lernen und mit Hilfe von Verfahren der Künstlichen Intelligenz erfolgen kann. Für die Berechnung eines Risikolevels, muss das Verhalten der Nutzer im Vorfeld trainiert werden. Das trainierte Verhalten kann für die Auswahl der benötigten Verfahren zur *ID-Verifikation* und *Authentifikation* (siehe Kapitel 2) oder als Eingabewert für „Fraud Prevention Systeme“ verwendet werden.
	Mit Hilfe von *„Service Klassen“* können Akteure die Sicherheitsanforderungen für die Berechnung eines Risikolevels und der adaptiven Entscheidung konfigurieren. Hierbei geht es vor allem um die Definition von Grenzwerten, bei deren Überschreitung zwingend ein höheres Sicherheitsniveau benötigt wird. Als Grundlage hierfür kann die Verteilung in Kapitel 3.4 verwendet werden.
	Der *„Auth-Service“* soll sowohl Informationen von den Akteuren entgegen nehmen, als auch Ergebnisse und aggregierte Informationen nach außen tragen. Hierbei handelt es sich beispielsweise um Warnungen bei verdächtigen Transaktionen oder um Daten, die in externen *Fraud Prevention Systemen* verwendet werden können. Darüber hinaus benötigen die Endanwender eine Schnittstelle, um Änderungen an der hinterlegten digitalen Identität durchführen zu können, wie beispielsweise das Zurückziehen einer erteilten Berechtigung für die Anmeldung bei einem „Service Provider“, für die Festlegung von Zugriffsrechten auf die Eigenschaften der digitalen Identität (siehe Phase „Management“ in Kapitel 4) oder zum Hinzufügen von zusätzlichen Faktoren (siehe Kapitel 3.1).

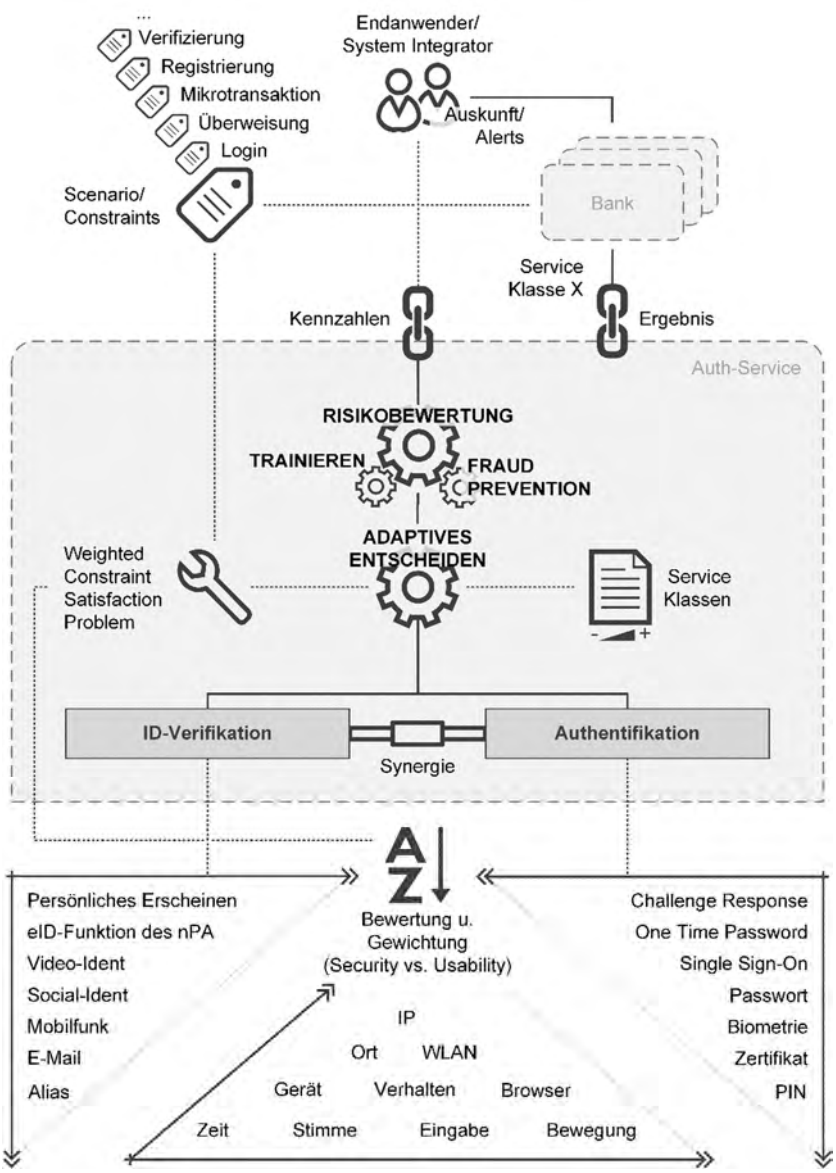

Abb. 3: Konzeptionelle Darstellung der risikobasierten und adaptiven Authentifizierung

6 Fazit

Der Erfolg eines „Identity Providers“ hängt von verschiedenen Faktoren, wie z.B. der Erfüllung von Sorgfaltspflichten, einer starken Authentifizierung oder von der Skalierbarkeit mit neuen Anwendungsfällen und Verfahren zur *ID-Verifikation* und *Authentifikation* ab. Die bereits etablierten „Identity Provider“, wie z.B. „Google“, „Facebook“ oder „Amazon“, werden bezüglich dieser Eigenschaften zukünftig in einem starken Wettbewerb mit potenten Teilnehmern, wie z.B. den Mobilfunkunternehmen oder den Banken stehen.

Banken verfügen seit langer Zeit über eine große Menge an bereits registrierten und verifizierten Kunden, die unteranderem für die Durchführung von Online-Banking Transaktionen im Internet authentifiziert werden müssen.

Das daraus resultierende „Know-How“ und die gesellschaftliche Relevanz machen Banken zu einer idealen „Trusted Party“ für Login-Dienste im Internet. Das angekündigte „Single-Sign-On“-System der Sparkasse verspricht somit ein großes Erfolgspotential. In Bezug auf die risikobasierte und adaptive Authentifizierung wird sich erst in der Zukunft zeigen, ob die Vertrauensvorteile und Konzepte der Sparkasse gegen die große Kompetenz von „Google“, „Facebook“ und „Amazon“ im Bereich der Verhaltensanalyse (also des vierten Faktors) ankommen. Gleiches gilt ebenfalls für die Login-Dienste von „Verimi“ und „SkIDentity“.

Eine wesentliche Richtungsänderung bei der Konzipierung von zukünftigen Geschäftsmodellen und den damit verbundenen Informationssystemen, wird den Banken durch die EU-Richtlinie *„Payment Service Directive 2“ (PSD2)* [8] aufgezwungen. Diese Richtlinie fordert ganz allgemein ein höheres Sicherheitsniveau bei Online-Banking Diensten. Im Speziellen fordert sie eine stärkere Kundenauthentifizierung. An dieser Stelle können die Mechanismen der adaptiven und risikobasierten Authentifizierung anknüpfen. Es wurde in Kapitel 3 gezeigt, dass unteranderem durch die Verwendung eines vierten Faktors grundsätzlich ein höheres Schutzniveau bei der Authentifizierung erzielt werden kann. Darüber hinaus können die ausgewerteten Kennzahlen des „Auth-Services“ ebenfalls als Eingabe für „Fraud Prevention Systeme“ verwendet werden, um beispielsweise potentiell ungewollte Transaktionen zu identifizieren, eine Risikobewertung zu ermöglichen, um anschließend ggf. die Ausführung zu verhindern. Sollte es dennoch zu ungewollten Transaktionen kommen, können die Kennzahlen des „Auth-Services“ auch für die Forensik herangezogen werden, da Sie genauen Aufschluss über die Rahmenbedingungen der Transaktion liefern können.

7 Verwandte Arbeiten

Risikobasierte und adaptive Authentifizierung: Für die zusätzliche Absicherung von potentiell unsicheren Verfahren zur *Authentifikation*, wird in der Praxis ein zweiter Faktor, wie z.B. Token Generatoren oder die Versendung von Transaktionsnummern über einen „Out-of-band“-Kanal verwendet. Die Verwendung von mehr als zwei Faktoren kann die Sicherheit bei der Authentifizierung auf Kosten der Verwendbarkeit erhöhen. Für die effektive Verwendung von mehr als zwei Faktoren sollte eine adaptive Komponente hinzugefügt werden, damit die einzelnen Faktoren nur im Bedarfsfall abgerufen werden und somit die Verwendbarkeit des Systems nicht pauschal geringer ist. Ein entsprechendes System auf Basis des OpenID-Frameworks wird in der Arbeit von Shah et al. [9] vorgestellt. Im Gegensatz zu diesem Artikel wird der Fokus in [9] auf „Identity Federations“ gelegt. Bei diesem Konzept sind die Bestandteile einer Identität über mehrere unabhängige „Identity Provider“ verteilt. In [10], [11], [12] und [3] werden ähnliche Systeme mit adaptiven Komponenten für die Authentifizierung vorgestellt, die sich im Gegensatz zu diesem Artikel jedoch nur auf mobile Endgeräte beziehen.

Device Fingerprinting: Während der Durchführung einer Authentifizierung sollen anfallende Hintergrundinformationen auf allen Ebenen des TCP/IP-Referenzmodells verwendet werden, damit ein Fingerabdruck zu dem verwendeten Endgerät erstellt werden kann. Der ermittelte Fingerabdruck soll anschließend als starkes Indiz in die Berechnung des Risikolevels mit einfließen. Die Effektivität der Fingerabdrücke zu einem Endgerät wurde in den Arbeiten von Vastel et al.[14], Yamada et al. [15] und Eckersley [16] für Hintergrundinformationen auf der Anwendungsebene gezeigt.

Die genannten Arbeiten befassen sich mit der Erstellung von Fingerabdrücken auf Basis von Hintergrundinformationen, die bei der Benutzung eines Browsers anfallen. Hierzu werden in

den genannten Arbeiten zahlreiche innovative Datenquellen verwendet, wie z.B. die Displaygröße, die installierten Schriftarten und Plugins, sowie die Leistungsfähigkeit der Grafikkarte oder CPU.

Die Ergebnisse der Arbeiten zeigen, dass die geplante Verwendung von Fingerabdrücken zu einem Endgerät erfolgsversprechend ist. In [16] wurde beispielsweise gezeigt, dass 83,6% der analysierten Nutzer eindeutig anhand des betrachteten Fingerabdrucks identifiziert werden konnten.

Verhaltensmuster: Neben der Verwendung von Fingerabdrücken zu den verwendeten Endgeräten, soll eine Art Fingerabdruck zu der Verhaltensweise eines Nutzers erstellt und analysiert werden. Das beschriebene High-Level Design in diesem Artikel orientiert sich dabei an den Arbeiten von Traore et al. [17]. Die Autoren haben gezeigt, dass eine Person im Internet mit hoher Wahrscheinlichkeit anhand der getätigten Mausbewegung und Tastatureingabe identifiziert werden kann. In ihrer Arbeit haben die Autoren ein System entwickelt, dass eine „Equal Error Rate“ von 8,21% aufweist. In [1] wurden gezeigt, dass die Identität eines Internetnutzers basierend auf der Interaktion in sozialen Medien verifiziert werden kann. In einer Studie wurden Beiträge von Nutzern einer sozialen Plattform ausgewertet und deren Interessen klassifiziert. Die *Authentifikation* eines Nutzers erfolgt in [1] mit Hilfe von Fragestellungen zu den klassifizierten Interessengruppen des Nutzers. Die Sicherheit des vorgestellten Ansatzes in [1] beruht auf der Annahme, dass Verhaltensmuster, menschliche Interaktionen oder soziale Faktoren eines Internetnutzers nur schwer nachgestellt werden können.

Literatur

[1] W. Anani, A. Ouda: The importance of human dynamics in the future user authentication, in IEEE 30th Canadian Conference on Electrical and Computer Engineering (CCECE), Windsor, ON, Canada, 2017.

[2] Europäische Kommission: EUR-Lex - 32015R1502 - EN - EUR-Lex,2015. https:// eur-lex.europa.eu/legal-content/DE/TXT/?uri= CELEX:32015R1502. Zugriff Juni 2018.

[3] National Institute of Standards and Technology: Electronic Authentication Guideline, NIST Special Publication (SP) 800-63-2, 2013. https://nvlpubs.nist.gov/ nistpubs/ specialpublications/nist.sp.800-63-2.pdf. Zugriff 2 April 2018.

[4] T. Born, M. Peyrard: Levels of Assurance, TU Darmstadt, 2014. https://www.cdc. informatik. tu-darmstadt.de/fileadmin/user_upload/Group_ CDC/ Documents/Lehre/ SS13/ Seminar/CPS/cps2014_submission_1.pdf. Zugriff Juni 2018.

[5] A. Nenadic, N. Zhang, L. Yao: Levels of Authentication Assurance: an Investigation, in 3rd International Symposium on Information Assurance and Security, 2007.

[6] U. Hinz: Digital Identities in the Peer-to-Peer Shareconomy - Establishing Trust in Online Networks, TU Berlin, 2014.[7]O. Peles, R. Hay: SpoofedMe-Intruding Accounts using Social Login Providers A Social Login Impersonation Attack, 2014.

[8] Europäisches Parlament, Rat der Europäischen Union: EUR-Lex - 32015L2366 - EN, 2015.

[9] Y. Shah, V. Choyi, L. Subramanian: Multi-factor Authentication as a Service, in 3rd IEEE International Conference on Mobile Cloud Computing, Services, and Engineering, San Francisco, CA, USA, 2015.

[10] A. Chakraborty, S. Munshi und A. Kundu, An Adaptive Server Side Software Authentication Framework Based on User's Activity Pattern, in 2nd International Conference on Emerging Applications of Information Technology, Kolkata, India, 2011.

[11] RSA, RSA Adaptive Authentication, 2014. https://www.rsa.com/content/dam/rsa/PDF/rsa.adaptive.auth.so.2014.pdf. Zugriff Februar 2018.

[12] C. C. Rocha, J. C. D. Lima, M. A. R. Dantas, I. Augustin: A2BeST: An adaptive authentication service based on mobile user's behavior and spatio-temporal context, in IEEE Symposium on Computers and Communications (ISCC), Kerkyra, Greece, 2011.

[13] E. Shi, Y. Niu, M. Jakobsson, R. Chow: Implicit authentication through learning user behavior, in 13th International Conference on Information Security, Boca Raton, FL, USA, 2011.

[14] A. Vastel, P. Laperdrix, W. Rudametkin, R. Rouvoy: FP-STALKER: Tracking Browser Fingerprint Evolutions, in 39th IEEE Symposium on Security and Privacy, San Francisco, United States, 2018.

[15] T. Yamada, T. Saito, K. Takasu, N. Takei: Robust Identification of Browser Fingerprint Comparison Using Edit Distance, in 10th International Conference on Broadband and Wireless Computing, Communication and Applications (BWCCA), Krakow, Poland, 2015.

[16] P. Eckersley: How Unique Is Your Browser?, in Privacy Enhancing Technologies Symposium (PETS 2010), Springer Lecture Notes in Computer Science, Berlin, Germany, 2010.

[17] I. Traore, I. Woungang, M. S. Obaidat, Y. Nakkabi, I. Lai: Combining Mouse and Keystroke Dynamics Biometrics for Risk-Based Authentication in Web Environments, in Fourth International Conference on Digital Home, Guangzhou, China, 2012.