



Evaluierung von CIAM-Anbietern hinsichtlich wichtiger Eigenschaften

Wichtige Funktionen, Definitionen
und Fragen an CIAM-Anbieter



Inhaltsverzeichnis

Wirtschaft und Gesellschaft – acht Digitalisierungstrends und ihre Auswirkungen	3
Warum herkömmliche Systeme nicht mithalten können	5
Systemvielfalt und Silos.....	5
Bestehende IAM-Systeme.....	6
Herkömmliche Cloud-basierte IAM-Lösungen.....	7
Für die Zukunft gerüstet: Enterprise CIAM	8
Worauf es bei der Wahl des richtigen CIAM-Anbieters ankommt	9
Grundlegende CIAM-Funktionen.....	9
Mittlere CIAM-Funktionen.....	12
Erweiterte CIAM-Funktionen.....	23
ForgeRock: Der unangefochtene Marktführer für Enterprise CIAM	30
Weitere Informationen	31

Wirtschaft und Gesellschaft – acht Digitalisierungstrends und ihre Auswirkungen

Acht voneinander nicht zu trennende Digitalisierungstrends transformieren derzeit unsere Wirtschaft und Gesellschaft – und sind ein wichtiger Indikator dafür, welche Anforderungen eine zukunftsfähige CIAM-Plattform (Consumer Identity and Access Management) erfüllen muss. Um in Zeiten der Pandemie und darüber hinaus zu überleben und zu florieren, müssen Unternehmen jedem dieser Trends Rechnung tragen.

1. Disruption: Die Erneuerung der Wirtschaft

Für Unternehmen steht damit viel auf dem Spiel: Sie befinden sich in einer Zeit ökonomischer und geopolitischer Unsicherheit, in der sie darum kämpfen müssen, Kunden zu gewinnen und zu binden, ihre Verluste zu minimieren und ihr Geschäft zukunftssicher zu machen.

2. Partner-Ökosysteme

Im Rahmen ihrer Neuerfindung schließen sich viele Unternehmen digitalen Ökosystemen mit mehreren Partnern an, um das unstillbare Verlangen der Verbraucher nach einem herausragenden Nutzungserlebnis und hohem Komfort zu erfüllen.

3. „Phygitale“ Erlebnisse

Die Verbraucher erwarten ein nahtloses Erlebnis, egal wie und wo sie mit einem Unternehmen interagieren – ob über physische und digitale Kanäle hinweg.

4. Intelligente Geräte und das Internet der Dinge (IoT)

Angesichts der großen Nachfrage nach „phygitalen“ Erlebnissen wird der globale IoT-Verbrauchermarkt voraussichtlich von 97,50 Milliarden US-Dollar im Jahr 2020 auf schätzungsweise 188,34 Milliarden US-Dollar im Jahr 2026 ansteigen.¹ Das Problem: Viele dieser „Dinge“ sind nicht ausreichend geschützt.

5. Cyberkriminalität, Datenschutzverletzungen, Betrug und Übergriffe

Die Zahl der Datenschutzverletzungen, Betrugsfälle, Ransomware-Angriffe sowie Datenübergriffe ist während der letzten Jahre sprunghaft angestiegen und der Höhepunkt scheint noch nicht erreicht.

6. Öffentliche Meinung und Aktivismus

Wir leben in einem Zeitalter des Misstrauens. Die öffentliche Meinung hat sich gewandelt. Verbraucher möchten Kontrolle über ihre persönlichen Daten haben und Unternehmen im Ernstfall zur Verantwortung ziehen können.

7. Datenschutz, Zustimmung und gesetzliche Bestimmungen

Als Antwort auf Forderungen seitens der Bevölkerung haben Regierungen weltweit Gesetze erlassen, um den Umgang mit Daten zu regulieren. Und in kommenden Jahren werden höchstwahrscheinlich weitere folgen.

8. Gen Z, Gen Alpha und das Metaversum

Mit einem Anteil von 32 % an der Weltbevölkerung ist Generation Z heute die zahlenmäßig stärkste Gruppe.² Auf sie folgt Generation Alpha, deren Mitglieder zwar noch keine 12 Jahre alt sind, aber bereits Kaufentscheidungen im Wert von über 500 Milliarden Dollar beeinflussen. Beide Generationen legen größeren Wert auf das Erlebnis als auf die Marke. Zudem werden Gen Z und Gen Alpha in den kommenden Jahren nicht mehr nur im Metaversum spielen, sondern auch dort lernen, arbeiten, einkaufen und investieren.

¹ <https://www.marketdataforecast.com/market-reports/consumer-iot-market>

² <https://nypost.com/2020/01/25/generation-z-is-bigger-than-millennials-and-theyre-out-to-change-the-world/>

Der Ausbau der eigenen Zukunftsfähigkeit ist von entscheidender Bedeutung – insbesondere für den Aufbau eines stabilen Unternehmens, das Volatilität und Disruption frühzeitig erkennen und abfedern kann.³

Gartner

Die acht Digitalisierungstrends dominieren das Geschehen am Markt. Um ihnen zu begegnen, brauchen Unternehmen folgende Fähigkeiten:

- Sie müssen ihre Geschäfts- und IT-Strategien überarbeiten, um jegliche Art der Disruption abzufedern und die Anforderungen der Verbraucher mit maximaler Flexibilität und Zuverlässigkeit zu erfüllen.
- Sie müssen in sicheren digitalen Ökosystemen mit mehreren Partnern vernetzt sein.
- Sie müssen ein sicheres und nahtloses Omnichannel-Kundenerlebnis über physische und digitale Kanäle hinweg bieten.
- Sie müssen das Internet der Dinge sichern und die Beziehungen zwischen Benutzern und Dingen regeln.
- Sie müssen Cyberkriminalität und Betrug erkennen und verhindern.
- Sie müssen sich an die Vorgaben hinsichtlich Datenschutz, Zustimmung und gesetzliche Bestimmungen halten und Vertrauen in ihre Marke aufbauen.
- Sie müssen ihr Geschäft zukunftssicher machen, damit es auch die Anforderungen der nächsten Generationen erfüllen kann.

Diese Fähigkeiten stellen die Unternehmen von heute leider vor große Herausforderungen.

³ Gartner, The C-Suite Guide: Accelerate Digital for Future-Ready Business. Frameworks for composable tech, empowered customers and the future of work, 2021



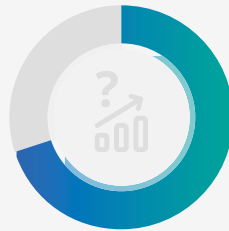
Ausführliche Informationen zu diesen acht Trends lesen Sie in unserem Whitepaper: **Wirtschaft im Wandel - die 8 wichtigsten Digitalisierungstrends und ihre Auswirkungen.**



Warum herkömmliche Systeme nicht mithalten können

Vor dem Hintergrund dieser acht Trends sind Unternehmen bestrebt, ihre Kundenakquise zu beschleunigen und ihr Kundenerlebnis zu optimieren, während sie gleichzeitig die gesetzlichen Bestimmungen einhalten und ihre Kunden sowie das Unternehmen schützen. Dies ist in herkömmlichen IT-Ökosystemen jedoch nur schwer umsetzbar.

70 % der Befragten gaben an, dass disruptives Wachstum ein entscheidender Faktor für den Erfolg ihres Unternehmens sei, aber nur **13 %** waren zuversichtlich, dass ihr Unternehmen dieser strategischen Priorität gerecht wird.⁴



Deloitte.

Daher müssen die verantwortlichen Führungskräfte als ersten Schritt auf dem Weg der Neuerfindung zunächst einmal eine Bestandsaufnahme der aktuell in ihrem Unternehmen genutzten Systeme und Prozesse machen.

⁴ https://www2.deloitte.com/content/dam/insights/articles/6730_TT-Landing-page/DI_2021-Tech-Trends.pdf
⁵ <https://www.forgerock.com/resources/view/108814636/customer-story/bmw-motors-into-the-digital-era-with-forgerock.pdf>

Systemvielfalt und Silos

Um die Identitäten und Daten von Verbrauchern, Partnern und IoT zu erfassen, zu schützen und zu verwalten, nutzen die meisten Unternehmen eine Vielzahl isolierter Systeme in ihren verschiedenen Abteilungen.

BMW nutzte ForgeRock, um 20 verschiedene IAM-Systeme auf einer ForgeRock-Plattform zu konsolidieren. Dadurch konnten erhebliche Kosteneinsparungen sowie eine schnellere Markteinführung, eine bessere Skalierbarkeit und eine höhere Compliance erzielt werden.⁵



Ein Beispiel: Die Marketingabteilung erfasst Kundendaten, wie Standort und Kaufhistorie, in mehreren Softwarelösungen. Gleichzeitig verwaltet die IT-Abteilung die Sicherheit der Abteilungslösungen und der darin erfassten Daten sowie des Unternehmens insgesamt in einem Flickwerk aus separaten Systemen.

Diese Systemvielfalt erzeugt Silos und hat eine ganze Reihe unerwünschter Konsequenzen. So führen diese isolierten Systeme nicht nur zu einer uneinheitlichen und somit häufig fehlerhaften Sicht auf den Kunden, sie erschweren auch die Risikobewertung und erhöhen demzufolge die Gefahr von Gesetzesverstöße. Erschwerend hinzu kommt, dass die Gefahr von Sicherheitsverstößen umso größer ist, je mehr Zugangspunkte es in einem Unternehmen gibt.

Bestehende IAM-Systeme

Aus Kostengründen haben viele Unternehmen versucht, ihre bestehenden IAM-Systeme für die Mitarbeiter so zu modifizieren, dass sie den Trends und Anforderungen Rechnung tragen, anstatt in eine unternehmensweite CIAM-Plattform zu investieren. Die Ergebnisse sind jedoch alles andere als ideal, wie die Disruption im Zuge der Pandemie gezeigt hat.

Bestehende IAM-Systeme ohne die erforderliche Flexibilität, Erweiterbarkeit oder Skalierbarkeit anpassen zu wollen, ist ein Fehler, den viele Unternehmen begehen ...⁶

ComputerWeekly

Die bestehenden IAM-Systeme wurden für bestimmte Anwendungsfälle der Mitarbeiter entwickelt. Sie sind nicht darauf ausgelegt, Millionen oder gar Milliarden von Kunden-, Partner- und IoT-Identitäten zu sichern und zu verwalten – ganz zu schweigen von deren Daten. Des Weiteren wurde bei den bestehenden IAM-Systemen weder Wert auf nahtlose Omnichannel-Erlebnisse gelegt, noch unterstützen sie die aktuellen gesetzlichen Bestimmungen zum Schutz von Daten, wie die Datenschutz-Grundverordnung (DSGVO), den California Consumer Privacy Act (CCPA) oder das Consumer Data Right (CDR), oder mindern die Gefahr moderner Cyberkriminalität und Betrugsmethoden. Auch erfüllen die bestehenden IAM-Lösungen keine modernen Standards, wodurch sie die heute üblichen

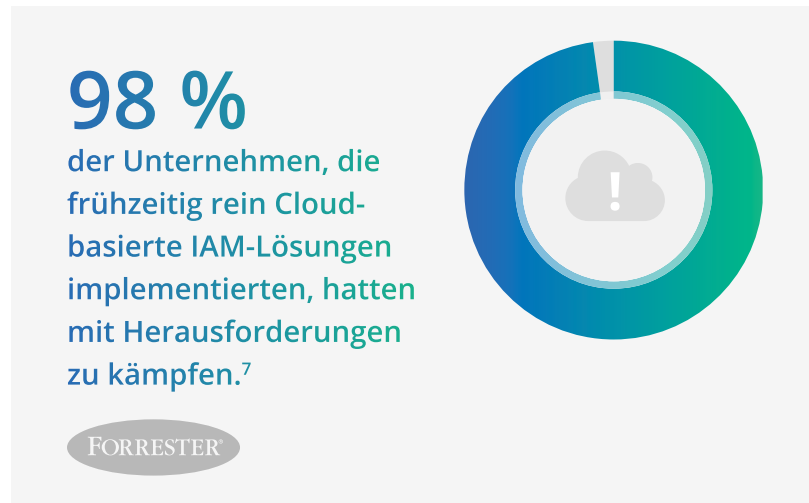


Anwendungsfälle von Verbrauchern, Partnern und IoT mit mittleren bis anspruchsvollen Anforderungen nicht abdecken. Zudem ist es äußerst schwierig und kostspielig, sie aufzurüsten – und dennoch ist ein Upgrade unumgänglich, damit sie die grundlegendsten Anwendungsfälle abdecken, ganz zu schweigen von den acht Trends.

⁶ <https://www.computerweekly.com/news/450429018/Consumer-identity-management-will-benefit-business>

Herkömmliche Cloud-basierte IAM-Lösungen

Um schnell und einfach die benötigte CIAM-Funktionalität zu erhalten, implementierten viele Unternehmen herkömmliche Cloud-basierte IAM-Lösungen. Bei diesen frühen rein Cloud-basierten IAM-Lösungen stand vor allem die Einfachheit für kleine bis mittelständische Unternehmen im Vordergrund und dies ging zu Lasten der Funktionalität und Konfigurierbarkeit, die für große Unternehmen unverzichtbar sind. Diese enge Zielgruppe erlaubte ihnen, schnell Marktanteile bei Unternehmen mit einfachen Anforderungen zu gewinnen.



Große Unternehmen benötigen jedoch mehr Funktionalität, als sie herkömmliche Cloud-basierte IAM-Lösungen bieten können. Dazu gehören Sicherheit und Konfigurierbarkeit auf Unternehmensniveau.

Laut einer Studie von Forrester aus dem Jahr 2021 hatten fast alle Unternehmen (98 %), die bereits früh herkömmliche Cloud-basierte IAM-Lösungen implementierten, mit den folgenden Herausforderungen zu kämpfen:

- Keine Möglichkeit zur Integration mit vorhandenen Geschäftsprozessen
- Keine Möglichkeit zur Verwaltung von Identitäten über die aktuellen Anwendungen und Systeme hinweg
- Kein Überblick über die lokal vorhandenen Systeme und folglich ein unvollständiges Bild der Risiko- und Sicherheitslage

Eine Hürde, mit der nahezu alle von Forrester befragten Unternehmen konfrontiert waren, bestand in der Unfähigkeit, bestehende Prozesse oder Legacy-Lösungen abzubilden oder zu integrieren. Geschäftsprozesse und Identitätsintegrationen sind von Anwendung zu Anwendung sehr unterschiedlich. Sie alle unterstützen unterschiedliche Standards und Protokolle. Dies bringt Komplikationen für jede Cloud-basierte IAM-Lösung mit, die die erforderlichen Standards nicht unterstützt oder nicht die nötige Flexibilität und Erweiterbarkeit bietet, um sie an die geschäftlichen Anforderungen des Unternehmens anzupassen. Einfach ausgedrückt: Diese herkömmlichen Cloud-basierten IAM-Lösungen lassen sich weder in ältere oder moderne Anwendungen nahtlos integrieren noch an die Geschäftsprozesse des Unternehmens anpassen.

⁷ <https://www.forgerock.com/resources/analyst-reports/forrester-study-hybrid-cloud-iam>

Für die Zukunft gerüstet: Enterprise CIAM

Anders als bestehende IAM-Lösungen und herkömmliche Cloud-basierte IAM-Lösungen ist Enterprise CIAM das ideale Fundament für Erneuerung, Sicherheit und Disruption. Führende Unternehmen setzen darauf, um allen acht Digitalisierungstrends zu begegnen und gleichzeitig ihre IT-Ressourcen zu entlasten. Mit einer Enterprise CIAM-Lösung können sie die Kundenakquise beschleunigen, das Kundenerlebnis verbessern und sowohl die Kunden als auch das Unternehmen schützen. Dies gelingt ihnen wie folgt:

- Sie überarbeiten ihre Geschäfts- und IT-Strategien, um jegliche Art der Disruption abzufedern und die Anforderungen der Verbraucher mit maximaler Flexibilität und Zuverlässigkeit zu erfüllen.
- Sie sind in sicheren digitalen Ökosystemen mit mehreren Partnern vernetzt.
- Sie bieten ein sicheres und nahtloses Omnichannel-Kundenerlebnis über physische und digitale Kanäle hinweg.
- Sie sichern das Internet der Dinge und regeln die Beziehungen zwischen Benutzern und Dingen.
- Sie halten sich an die Vorgaben hinsichtlich Datenschutz, Zustimmung und gesetzliche Bestimmungen und bauen Vertrauen in ihre Marke auf.
- Sie erkennen und verhindern Cyberkriminalität und Betrug.
- Sie machen ihr Geschäft zukunftssicher, damit es auch die Anforderungen der nächsten Generationen erfüllen kann.



CIAM trägt maßgeblich dazu bei, dass die digitalen Unternehmen von heute Kunden gewinnen und an sich binden können. Die Kunden wiederum erhalten die nötigen Sicherheits- und Personalisierungsfunktionen, um mit dem Unternehmen zu interagieren und Geschäfte zu machen.⁸

FORRESTER

⁸ <https://www.forrester.com/report/now-tech-customer-identity-and-access-management-ciam-q2-2020/RES160459?objectid=RES160459>

Worauf es bei der Wahl des richtigen CIAM-Anbieters ankommt

Die folgende Tabelle gibt einen Überblick über die wichtigsten Funktionen und Eigenschaften, die CIAM-Anbieter mitbringen sollten. Sie beschreibt, worum es sich bei diesen handelt und warum sie wichtig sind; außerdem enthält sie Fragen, die Sie den Anbietern in der Angebotsphase stellen sollten. Wir unterteilen die Tabelle in „grundlegende“, „mittlere“ und „erweiterte“ CIAM-Funktionen und -Eigenschaften bezogen auf die Komplexität des Anwendungsfalls. Die Anforderungen großer Unternehmen fallen meist in den Bereich der erweiterten CIAM-Funktionen und -Eigenschaften.

Grundlegende CIAM-Funktionen

GRUNDLEGENDE CIAM-FUNKTION	BESCHREIBUNG UND BEDEUTUNG	FRAGEN AN CIAM-ANBIETER
Föderiertes SSO	<p>Mit „föderiertem“ Single Sign-On (SSO) können Benutzer, zum Beispiel Partner, mit nur einem einzigen Konto auf die verschiedenen Web-Standorte und -Anwendungen eines anderen Unternehmens zugreifen, daher auch der Name Single Sign-On. Dies erfordert ein „föderiertes“ Vertrauensverhältnis zwischen den Unternehmen. Föderiertes SSO nutzt offene Standards (z. B. OAuth, WS-Federation, WS-Trust, OpenID Connect oder SAML) und überträgt so Authentifizierungstokens zwischen den Identitäts Providern der Unternehmen.</p> <p>Diese Funktion sorgt für ein erstklassiges Nutzungserlebnis. Sie spricht die Trends Partner-Ökosysteme und Cyberkriminalität an.</p>	<ul style="list-style-type: none"> • Bietet der Anbieter föderiertes Single Sign-On auf Basis offener Standards wie OAuth, WS-Federation, WS-Trust, OIDC oder SAML?
Social Registration und Social Authentication	<p>Social Registration und Social Authentication sind Formen des Single Sign-Ons, mit denen Benutzer sich schnell und einfach mithilfe ihrer Anmeldedaten aus sozialen Netzwerken wie Google oder Facebook registrieren und authentifizieren können.</p> <p>Diese Funktion sorgt für ein erstklassiges Nutzungserlebnis. Sie spricht die Trends Phygitale Erlebnisse, Gen Z und Gen Alpha sowie Cyberkriminalität an.</p>	<ul style="list-style-type: none"> • Ermöglicht der Anbieter Social Registration und Social Authentication? • Welche sozialen Netzwerke deckt er mit seinem Angebot ab? • Wie konfiguriert der Administrator der CIAM-Lösung die Verifizierung der Identität in sozialen Netzwerken?

GRUNDLEGENDE CIAM-FUNKTION	BESCHREIBUNG UND BEDEUTUNG	FRAGEN AN CIAM-ANBIETER
<p>Multi-Faktor-Authentifizierung (MFA)</p>	<p>Die Multi-Faktor-Authentifizierung (MFA) ist eine Methode zur Validierung einer Benutzeridentität mithilfe mehrerer Authentifizierungsmechanismen. Diese beinhalten etwas, das der Benutzer besitzt, etwas, das er weiß, und etwas, das er ist. So wird der Zugang beispielsweise erst dann gewährt, wenn der Benutzer sein Passwort (etwas, das er weiß) eingegeben und es mit einem Zahlencode, der ihm per SMS auf sein Mobiltelefon (etwas, das er besitzt) geschickt wurde, bestätigt hat.</p> <p>Diese Funktion dient dem Schutz der Verbraucher und des Unternehmens. Sie spricht die Trends Cyberkriminalität und Öffentliche Meinung an.</p>	<ul style="list-style-type: none"> • Bietet der Anbieter Multi-Faktor-Authentifizierung? • Welche Authentifizierungsmechanismen werden unterstützt?
<p>Autorisierung</p>	<p>Als Teil der Zugriffskontrolle innerhalb einer digitalen Identitätslösung bestimmt die Autorisierungsfunktion, ob ein Benutzer berechtigt ist, auf bestimmte Ressourcen, beispielsweise eine Webseite, einen Datensatz oder ein Dokument, zuzugreifen.</p> <p>Diese Funktion dient dem Schutz der Verbraucher und des Unternehmens. Sie spricht die Trends Partner-Ökosysteme, Phygitale Erlebnisse, Cyberkriminalität, Öffentliche Meinung sowie Datenschutz, Zustimmung und gesetzliche Bestimmungen an.</p>	<ul style="list-style-type: none"> • Welche Arten der Autorisierung und der Zugriffskontrolle bietet der Anbieter?
<p>Identitätsverzeichnis</p>	<p>Als Teil der Verzeichnisdienste speichert das Identitätsverzeichnis die Attributionsdaten von Identitäten. Dabei sollten die gespeicherten Identitätsdaten sowohl während der Speicherung als auch während der Übertragung verschlüsselt werden. Außerdem empfiehlt sich als Best Practice ein einbettbarer Speicherort, über den Identitätsdaten von Kunden, Geräten und Benutzern problemlos und in Echtzeit über verschiedene Umgebungen hinweg geteilt werden können. Aus Hosting-Perspektive sollten Identitätsverzeichnisse zudem eine hohe Verfügbarkeit, Leistung und Sicherheit bieten, vollständig LDAPv3-fähig sein und sich nahtlos mit jedem Verzeichnis integrieren lassen.</p> <p>Dieses zentrale Identitätsattribut dient dazu, die Trends Erneuerung der Wirtschaft, Partner-Ökosysteme, Phygitale Erlebnisse, IoT, Cyberkriminalität sowie Datenschutz, Zustimmung und gesetzliche Bestimmungen zu erfüllen.</p>	<ul style="list-style-type: none"> • Verschlüsselt das Identitätsverzeichnis Daten sowohl während der Speicherung als auch während der Übertragung? • Bietet die Lösung Teilreplikation und Multi-Master-Replikation? • Wie kann das Identitätsverzeichnis skaliert werden, um Abermillionen von Identitäten, einschließlich Geräten und „Dingen“, zu unterstützen? • Inwieweit ist das Identitätsverzeichnis der Lösung LDAPv3-fähig und wie lässt es sich nahtlos mit jedem Verzeichnis integrieren?

GRUNDLEGENDE CIAM-FUNKTION	BESCHREIBUNG UND BEDEUTUNG	FRAGEN AN CIAM-ANBIETER
<p>CIAM-SaaS-Plattform (Software as a Service)</p>	<p>Die Wartung und Aktualisierung von Identitätslösungen stellt ein komplexes und arbeitsintensives Unterfangen dar. Mit einer umfassenden, als SaaS-Lösung bereitgestellten CIAM-Plattform stehen Unternehmen die neuesten Funktionen zur Verfügung, ohne dass sie sich um Dinge wie Hosting, Wartung, Upgrades und vieles mehr Gedanken machen müssen. Anders ausgedrückt: Mit CIAM SaaS können sich die IT-Mitarbeiter im Unternehmen auf andere wichtige Aufgaben konzentrieren, z. B. Innovationen.</p> <p>Sicherheitsbedenken – einschließlich der Weitergabe von Daten und der Datenhoheit – zählen zu den Hauptgründen, warum sich viele große Unternehmen gegen eine vollständig Cloud-basierte CIAM-Plattform entschieden haben. Dies hängt damit zusammen, dass viele SaaS-Anbieter mehrere Kunden (Mandanten) in einer einzigen Instanz bündeln. Dieser überholte Ansatz der Mandantenfähigkeit birgt jedoch ein hohes Risiko, da sich die Handlungen eines Unternehmens auf andere Unternehmen auswirken können. Die ideale CIAM-SaaS-Plattform bietet deshalb eine vollständige Mandantenisolierung, in der Daten und Workloads niemals vermischt werden. Eine solche Mandantenisolierung beseitigt auch die typischen Herausforderungen im Zusammenhang mit der Skalierung und Speicherung sensibler und regulierter Identitätsdaten in der Cloud. CIAM SaaS muss zudem Datenhoheit und Compliance sowie maximale Verfügbarkeit mit individuellen Backups sicherstellen. Darüber hinaus braucht es eine Hochverfügbarkeitsarchitektur mit transparentem Failover, um die strengen SLA-Anforderungen (Service Level Agreement) zu erfüllen, sowie eine mandantenspezifische Sicherung und Wiederherstellung. Auf diese Weise können Unternehmen versehentliche oder böswillige Datenverletzungen schnell und effizient beheben.</p> <p>Dieses Cloud-Architekturmodell ermöglicht es, die Kundenakquise zu beschleunigen, die Kundenerlebnisse zu verbessern und sowohl die Verbraucher als auch das Unternehmen zu schützen. Es spricht die Trends Erneuerung der Wirtschaft, Partner-Ökosysteme, Phygitaler Erlebnisse, Cyberkriminalität, Öffentliche Meinung sowie Datenschutz, Zustimmung und gesetzliche Bestimmungen an.</p>	<ul style="list-style-type: none"> • Bietet die CIAM-SaaS-Lösung vollständige Mandantenisolierung innerhalb einer mandantenfähigen Architektur? • Wie gewährleistet die CIAM-Lösung eine differenzierte Datenhoheit? • Wie gewährleistet der CIAM-Anbieter die Datenresidenz von Identitäts-, Anwendungs- und Sicherungsdaten? • Wie sieht das Verfügbarkeits-SLA des CIAM-Anbieters für die SaaS-Identitätslösung aus? • Inwieweit nutzt der CIAM-SaaS-Anbieter Branchenstandards für die Datensicherheitsarchitektur der Lösung? • Welche Bewertungen, Audits, Prüfungen oder Zertifizierungen durch Dritte wurden für die Identity-Cloud-Lösung durchgeführt?

Mittlere CIAM-Funktionen

MITTLERE CIAM-FUNKTION	BESCHREIBUNG UND BEDEUTUNG	FRAGEN AN CIAM-ANBIETER
<p>Selfservice</p>	<p>„Selfservice“ bedeutet, dass Benutzer die Möglichkeit haben, ihre Konten selbst zu verwalten, ohne dafür das IT-Team im Unternehmen in Anspruch nehmen zu müssen. So können z. B. die Verwaltung von Login-Einstellungen, das Passwort-Management, die Aktualisierung von Kontaktinformationen, Support-Anfragen etc. per Selfservice durchgeführt werden. Das reduziert nicht nur die Support-Kosten, sondern verbessert auch das Benutzererlebnis und die Kundenbeziehung.</p> <p>Diese Funktion sorgt für ein erstklassiges Nutzungserlebnis. Sie spricht die Trends Partner-Ökosysteme, Phygitale Erlebnisse sowie Gen Z und Gen Alpha an.</p>	<ul style="list-style-type: none"> • Welche Selfservice-Funktionen unterstützt der Anbieter und wie? • Wie gestaltet die CIAM-Lösung individuelle und themenspezifische Selfservice-Erlebnisse für unterschiedliche Benutzergruppen?
<p>Sicherer Identitätswechsel</p>	<p>Die Mitarbeiter eines Unternehmens, wie z. B. der Helpdesk, müssen manchmal (im guten Sinne) die Identität eines Benutzers annehmen, um in dessen Namen Maßnahmen durchzuführen. Mit der Funktion zum sicheren Identitätswechsel können Benutzer für einen begrenzten Zeitraum die Kontrolle über ihr Konto an jemand anderen abgeben.</p> <p>Damit dies möglich ist, muss OAuth 2.0 für den Token-Austausch unterstützt werden.</p> <p>Diese Funktion sorgt für ein erstklassiges Nutzungserlebnis und schützt sowohl die Verbraucher als auch das Unternehmen. Sie spricht die Trends Erneuerung der Wirtschaft, Partner-Ökosysteme, Phygitale Erlebnisse, Gen Z und Gen Alpha, Cyberkriminalität, Öffentliche Meinung sowie Datenschutz, Zustimmung und gesetzliche Bestimmungen an.</p>	<ul style="list-style-type: none"> • Unterstützt die CIAM-Lösung den Token-Austausch nach OAuth 2.0 einschließlich CIBA-Berechtigung (Client-initiierte Backchannel-Authentifizierung)? • Wie handhabt der Anbieter die Endbenutzerdelegation und den sicheren Identitätswechsel?

MITTLERE CIAM-FUNKTION	BESCHREIBUNG UND BEDEUTUNG	FRAGEN AN CIAM-ANBIETER
<p>Einheitliche Sicht auf Identitäten</p>	<p>Eine unternehmensweit einheitliche Sicht auf die Identität des Verbrauchers verbessert Sicherheit, Kundenservice, Marketinginitiativen und vieles mehr. Damit CIAM-Plattformen eine solche einheitliche Sicht auf Identitäten unterstützen, müssen sie mit anderen Systemen integrierbar sein und verschiedene separate Kundendaten konsolidieren.</p> <p>Diese Funktion sorgt für ein erstklassiges Nutzungserlebnis und schützt sowohl die Verbraucher als auch das Unternehmen. Sie spricht die Trends Erneuerung der Wirtschaft, Partner-Ökosysteme, Phygitale Erlebnisse, Gen Z und Gen Alpha sowie Cyberkriminalität an.</p>	<ul style="list-style-type: none"> • Wie lässt sich die Lösung mit anderen Systemen integrieren, um separate Identitätsdaten zu konsolidieren und so eine unternehmensweit einheitliche Sicht auf den Kunden zu gewährleisten? • Kann die Lösung eine bidirektionale Synchronisation und Abstimmung von Identitätsattributen zwischen Datenspeichern ermöglichen? • Wie konfiguriert der Administrator der CIAM-Lösung die Migration der Kunden von einer früheren CIAM-Lösung auf die CIAM-Lösung des Anbieters? Wird eine schrittweise Migration unterstützt? • Wie importiert der Administrator der CIAM-Lösung vorhandene Passwort-Hashes?

MITTLERE CIAM-FUNKTION	BESCHREIBUNG UND BEDEUTUNG	FRAGEN AN CIAM-ANBIETER
<p>Verfügbarkeit und Skalierbarkeit</p>	<p>Skalierbarkeit, Leistungsfähigkeit und Verfügbarkeit sind entscheidende Faktoren für eine CIAM-Plattform, denn wenn die Identitätsplattform ausfällt, ist auch das Unternehmen betroffen. Deshalb ist es wichtig, einen Plan für ein hohes Aufkommen von Benutzern, Geräten und Dingen, die in einer Datenbank gespeichert werden müssen, sowie für eine unterschiedliche Frequenz und Dauer von zeitgleich ablaufenden Sitzungen zu haben.</p> <p>CIAM-Anbieter sollten also sowohl die Serviceverfügbarkeit als auch die Sitzungsverfügbarkeit gewährleisten können. Die Serviceverfügbarkeit stellt sicher, dass Benutzer selbst dann auf eine Seite zugreifen können, wenn ein Server ausfällt. Die Sitzungsverfügbarkeit hält im Falle eines Serverausfalls die aktuelle Sitzung aufrecht.</p> <p>CIAM-Anbieter sollten zudem eine Vielzahl von Skalierungsszenarien unterstützen, z. B. eine sich stets verändernde Anzahl von Benutzern, Geräten und Dingen (oftmals Millionen), die in einer Datenbank gespeichert werden müssen, sowie die unterschiedliche Frequenz und Dauer von zeitgleich ablaufenden Sitzungen. Darüber hinaus ist es wichtig, Latenzzeiten bei Zugriffsentscheidungen zwischen Microservices zu vermeiden (zunehmender Datenverkehr in/zwischen Rechenzentren) und ein zustandsloses, auf JWT-Sitzungstoken basierendes Protokoll zu unterstützen.</p> <p>Verfügbarkeit und Skalierbarkeit sind dabei nicht nur Teil der CIAM-Plattform selbst, sondern auch des Hostings der Plattform. Einzelheiten zur Cloud finden Sie im Abschnitt zu CIAM-Software-as-a-Service.</p> <p>Diese Funktionen ermöglichen eine schnellere Kundenakquise und ein besseres Kundenerlebnis. Verfügbarkeit und Skalierbarkeit sprechen die Trends Erneuerung der Wirtschaft, Partner-Ökosysteme, Phygitaler Erlebnisse und IoT an.</p>	<p>Was die Evaluierung der CIAM-Plattform selbst und nicht des Hostings betrifft, stellen sich folgende Fragen:</p> <ul style="list-style-type: none"> • Bietet der CIAM-Anbieter ein Performance-Benchmarking für alle Transaktionen pro Abschnitt, inklusive Laden und Synchronisieren von Identitätsdaten? Welche Auswirkungen hat es, wenn eine große Anzahl von IDPs (10, 100 oder 1000) benötigt wird? • Kann die CIAM-Lösung die Identitätsregistrierung, -authentifizierung und -autorisierung um ein Vielfaches skalieren, um auf erwartete Spitzen, wie z. B. während einer großen Veranstaltung, oder auf unvorhersehbare Ereignisse, wie z. B. eine hohe Nachfrage aufgrund von Trends oder Social-Media-Aktivitäten, zu reagieren? • Unterstützt der Identitätsanbieter Sitzungsverfügbarkeit, zustandsabhängige Verfügbarkeit und zustandslose Protokolle? Unterstützt der Anbieter redundante Services, Load Balancing, HA-Implementierungen mit n-facher Multi-Master-Replikation? Kann die Lösung in mandantenfähigen Umgebungen horizontal erweitert werden?

MITTLERE CIAM-FUNKTION	BESCHREIBUNG UND BEDEUTUNG	FRAGEN AN CIAM-ANBIETER
<p>Unterstützung offener Standards</p>	<p>Als „offene Standards“ werden fest etablierte, einheitliche technische Normen bezeichnet, die von Entwicklern genutzt werden. Jeder Standard verfügt dabei über spezifische Fähigkeiten und Funktionen. Die Sicherheit von Identitäten beruht auf den Standards OAuth2, OpenID Connect und SAML. Führende Anbieter digitaler Identitätslösungen gehen jedoch noch weiter und integrieren auch Standards, die zur Unterstützung der aktuellen Digitalisierungstrends erforderlich sind, wie beispielsweise UMA 2.0, womit Benutzer persönliche Daten sicher mit Dritten teilen können. Weitere hochentwickelte Standards sind OAuth 2.0 Proof-of-Possession, der sicherstellt, dass der Benutzer eines Bearer Tokens auch der tatsächliche Inhaber ist, und OAuth2 Device Flow, der für Client-Geräte mit eingeschränkter Benutzeroberfläche entwickelt wurde.</p> <p>Dieses Funktion ermöglicht es, die Kundenakquise zu beschleunigen, die Kundenerlebnisse zu verbessern und sowohl die Verbraucher als auch das Unternehmen zu schützen. Sie spricht die Trends Erneuerung der Wirtschaft, Partner-Ökosysteme, Phygitaler Erlebnisse, Gen Z und Gen Alpha, Cyberkriminalität sowie Datenschutz, Zustimmung und gesetzliche Bestimmungen an.</p>	<ul style="list-style-type: none"> • Unterstützt die CIAM-Lösung sowohl grundlegende als auch erweiterte offene Standards, einschließlich OAuth2, OpenID Connect, SAML, UMA 2.0, OAuth2 Device Flow sowie OAuth 2.0 Proof-of-Possession, FIDO2, WebAuthN und CIBA?
<p>Kontextbasierter Zugriff</p>	<p>Die meisten Identitätslösungen schützen nur bei der ersten Authentifizierung. Um die Authentizität von Benutzern, Geräten, „Dingen“ und Diensten jederzeit sicherzustellen und Risiken im Falle von Anomalien zu minimieren, sollte auch während laufender Sitzungen ein kontextbezogener Zugriff sichergestellt werden.</p> <p>Ein solcher kontextbasierter Zugriff integriert Erkenntnisse in Richtlinien, um nicht nur zum Zeitpunkt des Zugriffs, sondern auch während einer laufenden Sitzung fortlaufend die Risiken zu bewerten und die Ressourcen zu schützen. Dabei kommen präzise Autorisierungsrichtlinien, eine adaptive Risikobewertung, Multi-Faktor-Authentifizierung und Push-Autorisierung zum Einsatz. Diese strengeren Authentifizierungsmechanismen werden jedoch nur im Bedarfsfall eingesetzt, um so für ein ausgeglichenes Verhältnis zwischen Benutzerfreundlichkeit und Systemsicherheit zu sorgen.</p> <p>Diese Funktion sorgt für ein erstklassiges Nutzungserlebnis und schützt sowohl die Verbraucher als auch das Unternehmen. Sie spricht die Trends Erneuerung der Wirtschaft und Cyberkriminalität an.</p>	<ul style="list-style-type: none"> • Nutzt die Lösung während einer Sitzung Authentifizierungs- und Autorisierungsmechanismen für die fortlaufende Risikobewertung, wobei nur im Bedarfsfall strengere Mechanismen zur Evaluierung des Benutzers und des Kontexts zum Tragen kommen?

MITTLERE CIAM-FUNKTION	BESCHREIBUNG UND BEDEUTUNG	FRAGEN AN CIAM-ANBIETER
<p>No-Code-Identitätsorchestrierung</p>	<p>Herkömmliche Authentifizierungs- und Autorisierungsmethoden umfassen Benutzernamen und Passwörter sowie durch Dritte validierte Datenelemente wie beispielsweise Sozialversicherungsnummern und Geburtstage. Bei einem Zero-Trust-Sicherheitsmodell geht man jedoch davon aus, dass auch diese Daten kompromittiert sein könnten. Hinzu kommt, dass die althergebrachten Methoden einem guten Nutzungserlebnis im Wege stehen.</p> <p>Für eine sichere, mühelose User Journey sollte die CIAM-Lösung dem Unternehmen ein Tool zur No-Code-Identitätsorchestrierung zur Verfügung stellen. Dieses No-Code-Tool muss über eine Drag-and-Drop-Benutzeroberfläche verfügen, sodass Administratoren auf einfache Weise Workflows für Schritte im User Journey, wie z. B. Registrierung, Authentifizierung, Autorisierung, Selfservice usw., zusammenstellen und anpassen können. Diese Funktion bedeutet, dass die Benutzer über alle Kanäle und Marken hinweg ein höchst individuelles und personalisiertes Nutzungserlebnis genießen.</p> <p>Die No-Code-Identitätsorchestrierung versetzt Administratoren zudem in die Lage, Authentifizierungs-Workflows zu entwickeln, die den Anmeldeprozesse problemlos konfigurieren, messen und anpassen. Dabei kommen digitale Signale wie geräte-, kontext-, verhaltens- und risikobasierten Faktoren sowie Wahlmöglichkeiten und Analysen zum Einsatz. Administratoren können außerdem vorkonfigurierte Authenticators in kürzester Zeit einsetzen oder auch bestehende Authenticators nutzen und Cybersicherheitslösungen integrieren.</p> <p>Dieses Funktion ermöglicht es, die Kundenakquise zu beschleunigen, die Kundenerlebnisse zu verbessern und sowohl die Verbraucher als auch das Unternehmen zu schützen. Sie spricht die Trends Erneuerung der Wirtschaft, Partner-Ökosysteme, Phygitale Erlebnisse, Gen Z und Gen Alpha sowie Cyberkriminalität an.</p>	<ul style="list-style-type: none"> • Unterstützt die Lösung eine schnelle und einfache Erstellung, Ansicht und Änderung von Registrierungs-, Autorisierungs- und Authentifizierungserlebnissen ohne Programmierung, sondern mittels Drag-and-Drop-Funktion über Workflows und Strukturen? • Wie konfiguriert, misst und verändert die Lösung Authentifizierungsprozesse mithilfe von Faktoren und digitalen Signalen (Kontext, Risiko, Verhalten, Wahlmöglichkeiten und Analysen), um nicht nur das Risiko zu bestimmen, sondern auch das Nutzungserlebnis zu verbessern und die gesammelten Erkenntnisse an nachgelagerte Anwendungen während des Authentifizierungsprozesses weiterzugeben? • Wie ermöglicht die Lösung eine Vorabidentifizierung von digitalen Signalen eines Benutzers, wie z. B. Standort, IP-Adresse, Gerätetyp, Betriebssystem, Browsertyp usw., noch bevor der Benutzername erfasst wird? • Bietet die Lösung Out-of-Band-Authenticators sowie die Möglichkeit, maßgeschneiderte Authenticators zu erstellen? Ermöglicht sie eine schnelle und zentrale Integration mit den Authentifizierungs-, Betrugsermittlungs- und Risikomanagementtools von Drittanbietern? • Bietet die Lösung eine transaktionale Autorisierungsfunktion für risikobehaftete Transaktionen innerhalb einer Sitzung?

MITTLERE CIAM-FUNKTION	BESCHREIBUNG UND BEDEUTUNG	FRAGEN AN CIAM-ANBIETER
<p>Passwortlose Authentifizierung</p>	<p>Durchschnittlich verfügt ein Benutzer über mehr als 90 verschiedene Konten. Diese Menge an Passwörtern kann sich kaum jemand merken. Folglich verwenden auch über 50 % der Benutzer ihre Passwörter mehrfach auf verschiedenen Websites. Zudem basieren viele Passwörter auf persönlichen Daten, was die Konten anfällig für Angriffe macht. Eine Möglichkeit, mit dem Passwortdilemma umzugehen, ist der Einsatz eines Passwort-Management-Systems. Doch einige dieser Dienste sind selbst anfällig für Angriffe.</p> <p>Führende CIAM-Plattformen versetzen Unternehmen in die Lage, sichere und nahtlose Anmeldeprozesse ohne Eingabe von Passwörtern zu gestalten, die sogenannte passwortlose Authentifizierung. Bei einigen CIAM-Lösungen ist sogar die Eingabe von Benutzernamen überflüssig.</p> <p>Die passwortlose Authentifizierung macht den Zugangsdaten-Diebstahl durch Phishing-Angriffe, die Mehrfachverwendung von Passwörtern, Credential Stuffing, Keylogger usw. praktisch unmöglich und verkleinert so die Angriffsfläche des Unternehmens.</p> <p>Diese Funktion sorgt für ein erstklassiges Nutzungserlebnis und schützt sowohl die Verbraucher als auch das Unternehmen. Sie spricht die Trends Erneuerung der Wirtschaft, Partner-Ökosysteme, Phygitale Erlebnisse, Gen Z und Gen Alpha, Cyberkriminalität sowie öffentliche Meinung an.</p>	<ul style="list-style-type: none"> • Wie versetzt die CIAM-Lösung den Administrator in die Lage, eine passwortlose Authentifizierung in den Authentifizierungsprozess des Benutzers zu integrieren? Welche Schritte muss der Administrator ergreifen? • Kann die Lösung zur passwortlosen Authentifizierung des CIAM-Anbieters sowohl für die Erstanmeldung als auch für die fortlaufende Authentifizierung, einschließlich der Transaktionsautorisierung, verwendet werden? • Bietet die CIAM-Lösung eine benutzernamenlose Authentifizierung?

MITTLERE CIAM-FUNKTION	BESCHREIBUNG UND BEDEUTUNG	FRAGEN AN CIAM-ANBIETER
<p>Betrugsprävention</p>	<p>Zwar kann keine Einzellösung alle Facetten des Online-Betrugs abdecken, doch eine Kombination aus Sicherheitsinfrastruktur und CIAM-Funktionen kann den Zugangsdaten-Diebstahl, unbefugte Zugriffe auf privilegierte Konten und Betrug im Zahlungsverkehr aufdecken.</p> <p>Um die Wahrscheinlichkeit eines Betrugs zu beurteilen, ist der Kontext entscheidend. CIAM-Plattformen sollten Unternehmen in die Lage versetzen, User Journeys zu entwerfen, die Anomalien sowohl vor als auch nach der Benutzerauthentifizierung erkennen. Folgende Signale können auf einen Betrug oder eine Bedrohung hinweisen: Standort des Benutzers, IP-Adresse, Gerätetyp, Betriebssystem, Browsertyp, Benutzerprofilattribute, Geräte-Cookie, letzte Anmeldung, Anfrage-Header, Tageszeit, Gerätefingerabdruck und ob das Gerät jailbroken oder gerootet ist. Weitere Signale nach der Authentifizierung sind die Anzahl der Authentifizierungsversuche, die Tageszeit und die Entfernung zum Computer des Benutzers und dessen MFA-Faktor.</p> <p>CIAM-Lösungen können auch mit Technologien von Drittanbietern integriert werden, um das Risiko und die Kosten eines Betrugs weiter zu verringern.</p> <p>Diese Funktion dient dem Schutz der Verbraucher und des Unternehmens. Sie spricht die Trends Cyberkriminalität und Öffentliche Meinung an.</p>	<ul style="list-style-type: none"> • Wie verknüpft die CIAM-Lösung Betrugs- und Bedrohungssignale, um einer Sitzung Kontext zu verleihen, bevor sich ein Benutzer authentifiziert? • Wie erfasst und speichert die Lösung nach der Authentifizierung zusätzliche Signale, um nachgelagerte Anwendungen zu informieren? • Kann die CIAM-Lösung einen Google reCAPTCHA-Knoten in den Registrierungsprozess einbinden, um eine Benutzereingabe zu erzwingen und automatisierte/Bot-Angriffe zu reduzieren? • Wie ermöglicht die CIAM-Lösung eine Step-up-Authentifizierung und Transaktionsautorisierung für Transaktionen, die außerhalb des normalen Geräte-, Standort- oder Verhaltenskontexts eines Benutzers stattfinden? • Bewertet die CIAM-Lösung Benutzersitzungen als hoch-, mittel- oder niedriggradig verdächtig und leitet Benutzer mit hohem Risiko an eine Honeypot-Version des gewünschten Ziels weiter?

MITTLERE CIAM-FUNKTION	BESCHREIBUNG UND BEDEUTUNG	FRAGEN AN CIAM-ANBIETER
<p>Analyse von Anmeldeversuchen und Entscheidungslogik</p>	<p>Datengestützte Erkenntnisse bilden die Grundlage für eine kontinuierliche Verbesserung und optimale Sicherheit der Customer Journey. Als Teil der Identitätsorchestrierung bietet User Login Analytics Kennzahlen und Timer für die Analyse von Benutzerinteraktionen und Geräten über Kanäle und Geschäftseinheiten hinweg. CIAM-Plattformen sollten deshalb die Performance von Betrugsmanagement- und Analyse-Tools Dritter, die den Anmeldeprozess beeinflussen, überwachen können. Sie sollten es Administratoren zudem ermöglichen, die Customer Journey mit kontext- und verhaltensbezogenen Analysen zu optimieren, die untersuchen, welche Geräte und Browser genutzt werden, wo ein Login stattfindet, wie lang der Anmeldeprozess im Durchschnitt dauert und vieles mehr. Aus den gewonnenen Erkenntnisse können Unternehmen Zusammenhänge auf Basis der Login-Methode ableiten und dadurch die Kundenakzeptanz erhöhen.</p> <p>Dieses Funktion ermöglicht es, die Kundenakquise zu beschleunigen, die Kundenerlebnisse zu verbessern und sowohl die Verbraucher als auch das Unternehmen zu schützen. Sie spricht die Trends Erneuerung der Wirtschaft, Partner-Ökosysteme, Phygitale Erlebnisse sowie Gen Z und Gen Alpha an.</p>	<ul style="list-style-type: none"> • Analysiert die Lösung Zusammenhänge zwischen Login-Szenarien und möglicherweise vermehrten Kaufabbrüchen? • Untersucht die Lösung die Durchschnittsdauer für Interaktionen mit Betrugsmanagementsystemen? • Überwacht die Lösung die Auswirkung von Service Level Agreements auf Login-Szenarien? • Erkennt die Lösung, ob eine kürzere Login-Dauer die Zahl der Helpdesk-Anrufe reduziert?
<p>Progressive Profiling</p>	<p>Anstatt Ihre Benutzer zu bitten, umfangreiche Anmeldeformulare auszufüllen, können Sie das Progressive Profiling implementieren. Dies ist eine Methode, mit der Benutzerinformationen bei jeder Interaktion mit Ihrem System, Ihrer Webseite oder Ihrer Anwendung erfasst werden. So können Sie beispielsweise bei der ersten Anmeldung lediglich den Namen, die E-Mail-Adresse und das Passwort eines Benutzers abfragen. Zu einem späteren Zeitpunkt erfragen Sie dann vielleicht den Namen des Unternehmens und den Titel des Benutzers</p> <p>Diese Funktion ermöglicht eine schnellere Kundenakquise und ein besseres Kundenerlebnis. Sie spricht die Trends Phygitale Erlebnisse sowie Gen Z und Gen Alpha an.</p>	<ul style="list-style-type: none"> • Unterstützt die Lösung Progressive Profiling im Rahmen der Customer Journey und des Kundenlebenszyklus? • Wie konfiguriert der Administrator der CIAM-Lösung das Progressive Profiling? • Wie konfiguriert der Administrator der CIAM-Lösung Berichte zur Unterstützung von A/B-Tests (z. B. wie verbessert sich die Abbruchrate bei einer Änderung der Anmeldeseiten)? • Wie konfiguriert der Administrator der CIAM-Lösung den Support für Konten im Anfangsstadium (nicht authentifizierte, nicht registrierte Benutzer)?

MITTLERE CIAM-FUNKTION	BESCHREIBUNG UND BEDEUTUNG	FRAGEN AN CIAM-ANBIETER
Geschäftssystemintegration	<p>CIAM-Plattformen stellen einen wichtigen Bestandteil des Lösungsökosystems dar, in dem Kundenidentitäten gespeichert und Daten erfasst bzw. analysiert werden. Dieses Ökosystem umfasst Systeme für Identity and Access Management (IAM), Mobile Device Management (MDM) und Customer Relationship Management (CRM) sowie Marketing-Automatisierungssoftware. Leider führt die Vielzahl der Lösungen innerhalb eines Ökosystems oftmals zu einer fragmentierten Sicht auf den Kunden. CIAM-Plattformen sollten deshalb in der Lage sein, diese Systeme zu integrieren und zu verbinden, um eine unternehmensweit einheitliche Sicht auf den Kunden zu ermöglichen. Diese aggregierten Daten liefern zudem eine wesentlich robustere Datenbasis für Kundeninteraktionen. So können beispielsweise Standortdaten des Sicherheitssystems für ein besser auf den Kunden zugeschnittenes Marketing genutzt werden.</p> <p>Diese Funktion ermöglicht eine schnellere Kundenakquise und ein besseres Kundenerlebnis. Sie spricht die Trends Erneuerung der Wirtschaft, Partner-Ökosysteme, Phygitale Erlebnisse sowie Gen Z und Gen Alpha an.</p>	<ul style="list-style-type: none"> • Lässt sich die Lösung problemlos mit anderen Systemen integrieren und konsolidiert sie separate Identitätsdaten, um eine unternehmensweit einheitliche Sicht auf den Kunden zu schaffen und dadurch die Personalisierung und das Omnichannel-Erlebnis zu verbessern? • Wie konfiguriert der Administrator der CIAM-Lösung diese für die Integration mit einer CRM-Lösung (z. B. Salesforce)?
Privacy by Design und Zustimmungsmechanismen	<p>Datenschutzbestimmungen wie die DSGVO schreiben vor, dass Benutzer die Kontrolle über ihre personenbezogenen Daten erhalten müssen. Dies schließt Datenschutz, Sicherheit und Benutzereinstellungen mit ein. Für die Einhaltung globaler und regionaler Bestimmungen und Gesetze ist es deshalb unerlässlich, dass CIAM-Plattformen „Privacy by Design“, also integrierte Datenschutzfunktionen, sowie Zustimmungsmechanismen auf Basis des UMA 2.0-Standards enthalten und sich problemlos mit anderen Softwareprogrammen zur Einhaltung gesetzlicher Bestimmungen integrieren lassen. Derartige Mechanismen stellen Benutzer mit präzisen Kontrollmöglichkeiten für die Freigabe und Auditierung von Daten zu ihrer Person, ihren Geräten und verbundenen Dingen aus. Die Benutzeroberfläche für die Datenschutz- und Kontrollmechanismen sollte zudem intuitiv und benutzerfreundlich sein.</p> <p>Diese Funktion sorgt für ein erstklassiges Nutzungserlebnis und schützt sowohl die Verbraucher als auch das Unternehmen. Sie spricht die Trends Öffentliche Meinung sowie Datenschutz, Zustimmung und gesetzliche Bestimmungen an.</p>	<ul style="list-style-type: none"> • Beinhaltet die Lösung auf dem UMA 2.0-Standard basierende Datenschutz- und Zustimmungsmechanismen? • Wie stattet die Lösung Benutzer mit präzisen Kontrollmöglichkeiten für die Freigabe und Auditierung von Daten zu ihrer Person, ihren Geräten und verbundenen Dingen aus? • Wie unterstützt die Lösung das Recht auf Löschung („Recht auf Vergessenwerden“), das in Bestimmungen wie der DSGVO vorgeschrieben ist? • Wie konfiguriert der Administrator der CIAM-Lösung mehrere Versionen von Zustimmungsdokumenten und sorgt dafür, dass die Kunden diesen Versionen zustimmen?

MITTLERE CIAM-FUNKTION	BESCHREIBUNG UND BEDEUTUNG	FRAGEN AN CIAM-ANBIETER
Datenresidenz	<p>Datenresidenz und Datenhoheit sind verwandte Konzepte, bei denen es darum geht, wo Daten rechtmäßig gespeichert werden und wer unabhängig vom jeweiligen Speicherort die rechtliche Autorität über die Daten ausübt. Das Konzept der Datenresidenz besagt im Allgemeinen, dass die personenbezogenen Daten eines Bürgers nur innerhalb des Landes gespeichert und verarbeitet werden dürfen, in dem sie erhoben wurden.</p> <p>Um die Einhaltung der DSGVO und der darin vorgeschriebenen Datenresidenz zu gewährleisten, sollten CIAM-Anbieter eine datenschutzgerechte Speicherung und Teilreplikation personenbezogener Daten ermöglichen. Dies erlaubt die im Hinblick auf die jeweilige Gerichtsbarkeit unterschiedliche, kontextspezifische Verarbeitung von Benutzerdaten.</p> <p>Diese Funktion dient dem Schutz der Verbraucher und des Unternehmens. Sie spricht die Trends Öffentliche Meinung sowie Datenschutz, Zustimmung und gesetzliche Bestimmungen an.</p>	<ul style="list-style-type: none"> • Unterstützt die Lösung Datenresidenz? • Wie konfiguriert der Administrator der CIAM-Lösung die Datenresidenz für verschiedene geografische Regionen (d. h. Speicherung der Daten in den richtigen Regionen, Wahrung des Datenschutzes auf globaler Ebene)?
API-First-Ansatz	<p>Der API-First-Ansatz ist eine entwicklerorientierte Methode für die Lösungsentwicklung, bei der ein Anbieter zunächst die API erstellt und erst im nächsten Schritt die entsprechende Plattform aufbaut. Dies vereinfacht maßgeblich die Prozesse für externe Entwickler und Unternehmen. Anbieter digitaler Identitätslösungen sollten diesen API-First-Ansatz nutzen und zunächst ein gemeinsames REST-API-Framework für die gesamte Plattform schaffen. So wird ein einheitliches Verfahren für den Abruf aller Identitätsservices bereitgestellt, was die Benutzerfreundlichkeit, Skalierbarkeit und Flexibilität erhöht. Gleichzeitig entsteht ein einfacher und sicherer Weg, um Identitätslösungen auf alle erforderlichen Bereiche zu erweitern, z. B. auf soziale Netzwerke, Mobilanwendungen, Cloud und IoT.</p> <p>Dieses Modell ermöglicht eine schnellere Kundenakquise und ein besseres Kundenerlebnis. Es spricht die Trends Erneuerung der Wirtschaft, Partner-Ökosysteme, Phygitaler Erlebnisse und IoT an.</p>	<ul style="list-style-type: none"> • Nutzt der Anbieter den API-First-Ansatz, um so ein gemeinsames REST-API-Framework für die gesamte Plattform zu erstellen? • Wie stellt die CIAM-Lösung eine einzige, einheitliche Methode zum Aufrufen eines beliebigen Identitätsdienstes bereit?

MITTLERE CIAM-FUNKTION	BESCHREIBUNG UND BEDEUTUNG	FRAGEN AN CIAM-ANBIETER
<p>Ein starkes Partnernetzwerk</p>	<p>Starke CIAM-Lösungen, die für die acht aktuellen und für künftige Digitalisierungstrends gerüstet sind, zeichnen sich vor allem dadurch aus, dass sie reibungslos mit einer Vielzahl weiterer Technologien, Softwarelösungen und Branchenführern zusammenarbeiten, um so den individuellen Zielen von Unternehmen gerecht zu werden. Daher sollten CIAM-Anbieter über ein starkes und breit aufgestelltes Netzwerk anerkannter Beratungs-, Technologie- und Integrationspartner verfügen. Dieses Ökosystem umfasst vorzugsweise vorgefertigte, gründlich getestete und stets aktuelle Integrationen, die sofort und auf einfache Weise einsetzbar sind.</p> <p>Diese Eigenschaft ermöglicht es, die Kundenakquise zu beschleunigen, die Kundenerlebnisse zu verbessern und sowohl die Verbraucher als auch das Unternehmen zu schützen. Sie spricht die Trends Erneuerung der Wirtschaft, Partner-Ökosysteme, Phygitaler Erlebnisse, Gen Z und Gen Alpha, Cyberkriminalität sowie Datenschutz, Zustimmung und gesetzliche Bestimmungen an.</p>	<ul style="list-style-type: none"> • Verfügt der Anbieter über ein starkes Netzwerk anerkannter Beratungs-, Technologie- und Integrationspartner? • Wie viele der Partnerintegrationen sind vorgefertigt, gründlich getestet und stets aktuell? • Sind die Partnerintegrationen ohne zusätzliche Kosten in der CIAM-Plattform enthalten?

Erweiterte CIAM-Funktionen

ERWEITERTE CIAM-FUNKTION	BESCHREIBUNG UND BEDEUTUNG	FRAGEN AN CIAM-ANBIETER
<p>Flexibilität der Benutzeroberfläche</p>	<p>Die Elemente der Benutzeroberfläche (UI), zum Beispiel für Anmeldefelder, Profelseiten, Schnittstellen zum Zurücksetzen des Passworts usw., sind ein wichtiger Faktor der CIAM-Strategie, da sie die Benutzerfreundlichkeit als Teil eines hervorragenden digitalen Erlebnisses fördern. Die Benutzeroberfläche von CIAM-Plattformen sollte sich zudem in die übergreifende UI-Strategie eines Unternehmens einfügen. Dabei ist es völlig normal, dass sich solche Strategien weiterentwickeln.</p> <p>Dieses Attribut ermöglicht eine schnellere Kundenakquise und ein besseres Kundenerlebnis. Es spricht die Trends Erneuerung der Wirtschaft, Phygitale Erlebnisse sowie Gen Z und Gen Alpha an.</p>	<ul style="list-style-type: none"> • Erlaubt die CIAM-Lösung Unternehmen die Erstellung einer maßgeschneiderten Benutzeroberfläche, d. h. die Möglichkeit, REST-APIs aufzurufen? • Inwiefern nutzt die CIAM-Lösung SDKs, um Identitäten einfacher einzubetten? • Bietet die CIAM-Plattform flexible gehostete UI-Optionen?
<p>Multi-Brand / Omni-Channel / Cross-Channel (UI-Design)</p>	<p>Jeder Benutzer ist einzigartig und muss entsprechend behandelt werden. Ein Unternehmen mit mehreren Marken oder Kanälen (z. B. Filialen) muss in der Lage sein, jeden einzelnen Benutzer zu erkennen und ihm ein personalisiertes Erlebnis zu bieten, indem es ihn zu dem entsprechend gebrandeten Zugangsbereich weiterleitet. Darüber hinaus muss es Unternehmen möglich sein, innerhalb von Ökosystemen mit mehreren Partnern verschiedene Geschäftseinheiten oder Benutzergruppen in ihrer Identitätshierarchie unabhängig und getrennt voneinander verwalten. Dazu müssen sie möglicherweise einige Berechtigungen auf Partner übertragen, um ihre Endkunden besser verwalten zu können (B2B2C).</p> <p>Eine CIAM-Lösung sollte folglich UI-Designs für mehrere Marken beinhalten, die es Unternehmen ermöglichen, spezifische User Journeys zu kreieren, die die Benutzer mit dem entsprechenden Kanal oder der entsprechenden Marke zusammenbringen. Außerdem sollte die Lösung hierarchische Ebenen von Benutzern und delegierten Administratoren unterstützen.</p> <p>Diese Funktion ermöglicht eine schnellere Kundenakquise und ein besseres Kundenerlebnis. Sie spricht die Trends Erneuerung der Wirtschaft, Partner-Ökosysteme, Phygitale Erlebnisse sowie Gen Z und Gen Alpha an.</p>	<ul style="list-style-type: none"> • Wie passt die CIAM-Lösung die Designs der Benutzeroberfläche für Endbenutzer an? • Kann die CIAM-Lösung auf der Grundlage einer Spracheingabe dynamisch ein Design auswählen? • Kann die CIAM-Lösung das Unternehmen erkennen, dem der Benutzer angehört, und dann eine thematisch auf das Unternehmen abgestimmte Oberfläche anzeigen? • Kann die CIAM-Lösung erkennen, dass der Benutzer eine Sehschwäche hat, und auf ein kontrastreiches Design umschalten?

ERWEITERTE CIAM-FUNKTION	BESCHREIBUNG UND BEDEUTUNG	FRAGEN AN CIAM-ANBIETER
<p>Hierarchisches, markenübergreifendes und komplexes Unternehmensdesign</p>	<p>Die meisten Unternehmen verfügen über eine Hierarchie von Abteilungen oder Geschäftsbereichen (Lines of Business, LOB) entsprechend ihren Bedürfnissen und ihrer Geschäftsstruktur (z. B. mehrere Marken). Diese Hierarchien geben Aufschluss darüber, wie sie die Verwaltung und die Zugriffsrechte an Benutzer innerhalb des Unternehmens vergeben.</p> <p>Mit der Funktion für ein hierarchisches, markenübergreifendes und komplexes Unternehmensdesign können Unternehmen flexibel individuelle Identitäts- und Zugriffsmanagementkonfigurationen für unterschiedliche Zielgruppen einrichten, z. B. Passwortrichtlinien und Zugriffsberechtigungen. Dies geschieht durch die Möglichkeit, hierarchische Benutzerebenen und delegierte Administratoren zu erstellen, sodass Unternehmen separate Benutzergruppen entsprechend ihren Geschäftsanforderungen einrichten und verwalten können.</p> <p>Bei Bedarf können Hierarchien auch in andere Hierarchien eingebettet werden. Jeder Hierarchie werden Inhaber und Administratoren zugewiesen, die die detaillierten Zugriffs- und Autorisierungsberechtigungen der Benutzer innerhalb ihrer Ebene verwalten. Ein Administrator eines Unternehmens hat möglicherweise vollen Zugriff auf die Benutzer in diesem Unternehmen, aber keinen Zugriff auf die Benutzer eines Schwesterunternehmens. So kann jeder Administrator in der Hierarchie die Änderungen vornehmen, die er benötigt, um die Anforderungen der Benutzer an Sicherheit, Benutzerfreundlichkeit und Komfort zu erfüllen.</p> <p>Dieser Ansatz spart Unternehmen viel Zeit und Kosten, da sie mehrere Identitätsarten in einem einzigen System konsolidieren können.</p> <p>Diese Funktion ermöglicht es, die Kundenakquise zu beschleunigen, die Kundenerlebnisse zu verbessern und sowohl die Verbraucher als auch das Unternehmen zu schützen. Sie spricht die Trends Erneuerung der Wirtschaft, Partner-Ökosysteme und Cybersicherheit an.</p>	<ul style="list-style-type: none"> • Wie unterstützt die CIAM-Lösung eindeutige Identitäts- und Zugriffsmanagementkonfigurationen für verschiedene Hierarchien oder Geschäftsbereiche (LOBs)? • Wie kann der Administrator der CIAM-Lösung diese so einrichten, dass sie mehrere Marken oder Online-Angebote desselben übergeordneten Kundenunternehmens unterstützt? Demonstration der Kontoverknüpfung. • Wie erstellt der Administrator der CIAM-Lösung ein neues Unternehmen zwecks Mandantenfähigkeit (dies ist in der Regel eine Voraussetzung, wenn ein MSSP oder ein sehr großes Unternehmen die CIAM-Lösung nutzt und sicherstellen muss, dass bestimmte Administratoren nur für bestimmte Kunden oder interne Unternehmen Administratorrechte haben)?

ERWEITERTE CIAM-FUNKTION	BESCHREIBUNG UND BEDEUTUNG	FRAGEN AN CIAM-ANBIETER
<p>Zero-Trust-Sicherheit</p>	<p>Das Zero-Trust-Sicherheitsmodell basiert auf der Annahme, dass kein Netzwerk, Individuum, „Ding“ oder Gerät vertrauenswürdig ist.</p> <p>Fragt eine Einheit eine bestimmte Aktion an, muss die CIAM-Plattform entscheiden können, ob diese dazu berechtigt ist und ob ihre Identität mit einem dem Risiko der angefragten Aktion entsprechenden Maß an Sicherheit belegt werden kann.</p> <p>Im Rahmen eines Zero-Trust-Sicherheitsmodells muss jede Aktion ordnungsgemäß authentifiziert und autorisiert werden. Für die Authentifizierungs- und Autorisierungsentscheidungen werden kontextbezogene Informationen genutzt. Sie erfolgen risikobasiert statt binär und berücksichtigen dabei eine Vielzahl von Informationen.</p> <p>Diese Funktion sorgt für ein erstklassiges Nutzungserlebnis und schützt sowohl die Verbraucher als auch das Unternehmen. Sie spricht die Trends Erneuerung der Wirtschaft, Partner-Ökosysteme und Cyberkriminalität an.</p>	<ul style="list-style-type: none"> • Folgt die Lösung einem Zero-Trust-Sicherheits- und CARTA-Modell für eine risiko- und/oder wertebasierten Authentifizierung (adaptive Authentifizierung)? • Wie ermöglicht sie es, für Personen, Geräte, Dinge und Anwendungen Zugangsdaten mit unterschiedlichem Sicherheitsniveau zu verwenden und diese anhand eines umfassenden Identitätsverzeichnis zu authentifizieren? • Wie konfiguriert der Administrator der CIAM-Lösung die Risikobewertung anhand von Attributen für Geräte mit hohem Risiko (einschließlich, aber nicht beschränkt auf Jailbreaking, Malware, Emulatoren, deaktiviertes JavaScript, gestohlene Cookies aus einer anderen Sitzung)? • Wie konfiguriert der Administrator der CIAM-Lösung die Risikobewertungen zur Umsetzung der Authentifizierungsrichtlinien (z. B. Kunde meldet sich aus einem unseriösen Land an, Kunde meldet sich von einem neuen Gerät an, Kundenanmeldungen zeigen unglaubliche Reisen usw.)? Welche Arten von eigenen und fremden Bedrohungsdaten (böartige IP-Adressen usw.) sind in der CIAM-Lösung verfügbar? • Wie konfiguriert der Administrator der CIAM-Lösung den Schutz der Kunden vor Credential-Stuffing- und Passwort-Spraying-Angriffen?

ERWEITERTE CIAM-FUNKTION	BESCHREIBUNG UND BEDEUTUNG	FRAGEN AN CIAM-ANBIETER
<p>Dedizierte Zugriffsrechte mit PoLP (Principle of Least Privilege)</p>	<p>Das System ermöglicht das Principle of Least Privilege, also das Prinzip der geringsten Privilegien. Das bedeutet, dass jeweils nur der für einen bestimmten Zweck unbedingt erforderliche Zugriff gewährt wird. So haben Kunden beispielsweise nur Zugriff auf die Informationen und Ressourcen, die einem bestimmten und berechtigten Zweck dienen.</p> <p>Ein erster Schritt hin zu dieser Art der präzisen Autorisierung liegt in der Entwicklung eines Mechanismus zur starken Typisierung von Anwendungen, API-Endpunkten und anderen geschützten Ressourcen. Dieser muss dann an verteilten Gateways, die im gesamten Identitätsökosystem für die Durchsetzung von Richtlinien sorgen, mit Echtzeitkontext gekoppelt werden. Auch Mechanismen für präzise, umsetzbare Regeln, die für Autorisierungsentscheidungen genutzt werden können, sollten eingesetzt werden.</p> <p>Diese Funktion dient dem Schutz der Verbraucher und des Unternehmens. Sie spricht die Trends Erneuerung der Wirtschaft, Partner-Ökosysteme und Cyberkriminalität an.</p>	<ul style="list-style-type: none"> • Wie ermöglicht die Lösung, dass durch das „Principle of Least Privilege“ nur der für einen bestimmten Zweck unbedingt erforderlichen Zugriff gewährt wird? • Wie kann die CIAM-Lösung verschiedenen Benutzergruppen auf der Grundlage ihrer Unternehmensstruktur (Standort, Berichtshierarchie, Geschäftsbereiche) Bereiche zuweisen?
<p>Aggregation von Daten zu Personen, Dingen und ihrer Beziehung zueinander</p>	<p>Um sichere, personalisierte Omnichannel-Erlebnisse zu schaffen, müssen CIAM-Anbieter den Unternehmen die Möglichkeit geben, Beziehungsdaten von Personen und ihren „IoT-Dingen“ zu sammeln und so eine einheitliche und umfassende Sicht auf ihre Kunden zu erhalten. Dazu müssen mehrere technische Voraussetzungen erfüllt sein, darunter ein gemeinsames Kundendatenmodell, die Vernetzung einer Vielzahl von Datenquellen, eine einfache Synchronisierungs- und Abstimmungslogik sowie ein adäquater Zugang zu Kundendaten.</p> <p>Diese Funktion sorgt für ein erstklassiges Nutzungserlebnis und schützt sowohl die Verbraucher als auch das Unternehmen. Sie spricht die Trends Erneuerung der Wirtschaft, Partner-Ökosysteme, Phygitaler Erlebnisse, IoT, Gen Z und Gen Alpha sowie Cyberkriminalität an.</p>	<ul style="list-style-type: none"> • Unterstützt die Lösung die detaillierte Modellierung von Beziehungen zwischen Identitäten (Eltern, Kinder, Freunde, IoT usw.) und damit das Identitätsmanagement innerhalb dieser Beziehungen?

ERWEITERTE CIAM-FUNKTION	BESCHREIBUNG UND BEDEUTUNG	FRAGEN AN CIAM-ANBIETER
Edge-Sicherheit	<p>Wie bereits ausgeführt, sind die meisten „Dinge“ im IoT nicht sicher. „Identity at the Edge“ schützt Geräte sowie die von ihnen erfassten Daten mithilfe eines Edge Controllers und eines Identity Message Brokers.</p> <p>Der Edge Controller schützt IoT-Identitäten sowie die damit verbundenen Anmeldedaten und sorgt so dafür, dass sie über eine Vielzahl verschiedener Ökosysteme hinweg vertrauenswürdig und nutzbar bleiben. Auf diese Weise können Man-in-the-Middle- und andere Angriffe verhindert werden.</p> <p>Viele IoT-Dinge nutzen unsichere Protokolle wie beispielsweise MQTT, um sich zu identifizieren und Informationen auszutauschen. Der Identity Message Broker schützt diese Protokolle, indem er sie in HTTPS übersetzt und so die Authentifizierung und Autorisierung entsprechender Geräte und Daten ermöglicht.</p> <p>Diese Funktion sorgt für ein erstklassiges Nutzungserlebnis und schützt sowohl die Verbraucher als auch das Unternehmen. Sie spricht die Trends Erneuerung der Wirtschaft, Phygitale Erlebnisse, IoT und Cyberkriminalität an.</p>	<ul style="list-style-type: none"> • Nutzt die Lösung einen Edge Controller, um IoT-Identitäten sowie die damit verbundenen Anmeldedaten zu schützen, und sorgt sie so dafür, dass diese über einer Vielzahl verschiedener Ökosysteme hinweg vertrauenswürdig und nutzbar bleiben und Man-in-the-Middle- und andere Angriffe verhindert werden? • Verwendet die Lösung Message Broker, um IoT-Protokolle, wie z. B. MQTT, in das sichere HTTPS-Protokoll zu übertragen, sodass eine Authentifizierung und Autorisierung des IoT-Geräts und der Daten möglich ist?
Unterstützung von Altanwendungen	<p>Die meisten Unternehmen verfügen über eine große Anzahl von Altsystemen und -anwendungen. Viele davon speichern Kunden- und Anmeldedaten, verfügen jedoch nicht oder nur begrenzt über integrierte Funktionen für Benutzerregistrierung, Authentifizierung, Autorisierung oder Föderation. Daher ist es wichtig, dass CIAM-Plattformen auch die Vernetzung oder Erweiterung von Altsystemen und -anwendungen mit modernen Identitätssystemen unterstützen. Dies geschieht über ein sogenanntes Identity Gateway, das es bestehenden und neuen Systemen und Anwendungen erlaubt, nahtlos und sicher miteinander zu kommunizieren.</p> <p>Diese Funktion sorgt für ein erstklassiges Nutzungserlebnis. Sie spricht den Trend Erneuerung der Wirtschaft an.</p>	<ul style="list-style-type: none"> • Verfügt die Lösung über ein Identity Gateway und somit über die Möglichkeit einer Vernetzung bzw. Erweiterung von Altsystemen und -anwendungen? • Wie lässt sich das Identity Gateway des CIAM-Anbieters in bestehende Anwendungen integrieren, die nicht für die Zusammenarbeit mit Zugriffsmanagement- oder Single-Sign-On-Lösungen (SSO) ausgelegt sind? • Wie ermöglicht das Identity Gateway des CIAM-Anbieters die sichere Integration von alten und neuen Anwendungen?

ERWEITERTE CIAM-FUNKTION	BESCHREIBUNG UND BEDEUTUNG	FRAGEN AN CIAM-ANBIETER
<p>DevOps-fähige Architektur und Microservices</p>	<p>Mithilfe von DevOps können Softwareentwicklung und -bereitstellung in einem fortlaufenden Zyklus erfolgen, wodurch Unternehmen Entwicklungszeiten verkürzen und neue Funktionen schneller einführen können. CIAM-Anbieter sollten eine DevOps-fähige Architektur bereitstellen, mit der sich DevOps-Tools wie beispielsweise die Automatisierung und Orchestrierung von Push-Button-Bereitstellungen oder kontinuierlichen Bereitstellungen vollumfänglich nutzen lassen. Sie sollten zudem Docker Images und Container für eine zügige Automatisierung (Rapid Automation) nutzen sowie über eine intelligente Architektur verfügen, die Konfiguration und Binaries trennt, um so die Versionskontrolle von DevOps-Artefakten wirksam nutzen zu können. Darüber hinaus sollten Anbieter digitaler Identitätslösungen Befehlszeilentools für eine Remote-Konfiguration bereitstellen.</p> <p>Microservices sind ein weiteres wichtiges Element in der Entwicklung. Hierbei liegt der Fokus auf der Entwicklung und Bereitstellung von Anwendungen als Gruppen aus modularen, kombinierbaren Services innerhalb einer Anwendung. Der Vorteil dieser Mikroservices liegt in der Möglichkeit, einen einzelnen Service zu modifizieren, ohne die anderen dadurch zu beeinträchtigen.</p> <p>Diese Funktionen ermöglichen eine schnellere Kundenakquise und ein besseres Kundenerlebnis. Sie sprechen den Trend Erneuerung der Wirtschaft an.</p>	<ul style="list-style-type: none"> • Wie unterstützt die Lösung moderne DevOps-Bereitstellungsansätze mit Containerisierungs- und Orchestrierungstechnologien wie Docker und Kubernetes? • Wie sichert die CIAM-Lösung Microservices? • Wie lässt sich die CIAM-Lösung horizontal und vertikal skalieren?
<p>Serverlose Architekturmuster</p>	<p>Wie unter dem Punkt „Verfügbarkeit und Skalierbarkeit“ bereits ausgeführt, müssen Unternehmen auf eine Vielzahl von Skalierungsszenarien vorbereitet sein, beispielsweise auf Millionen zeitgleicher Online-Sitzungen. Um dies auf rentable Weise zu ermöglichen, unterstützen führende Anbieter digitaler Identitätslösungen serverlose Architekturmuster.</p> <p>Mit einer serverlosen Architektur können Server bedarfsgerecht zu- oder abgeschaltet und die Leasing-Konditionen der Rechenzentren sowohl auf die genutzte Speicherkapazität als auch auf die Nutzungsdauer zugeschnitten werden. So müssen Entwickler keine unnötig große Anzahl von Servern verwalten, die möglicherweise nur periodisch zu Spitzenzeiten benötigt werden.</p> <p>Diese Funktion ermöglicht Kosteneinsparungen und spricht den Trend Erneuerung der Wirtschaft an.</p>	<ul style="list-style-type: none"> • Unterstützt die Lösung serverlose Architekturmuster? • Unterstützt die Lösung dreistufige Webanwendungsmuster (REST, GraphQL), ETL-Muster (Extract, Transform, Load; z. B. FanOut), Big-Data-Muster (z. B. MapReduce) und Automatisierungs- und Bereitstellungsmuster (z. B. CI/CD)?

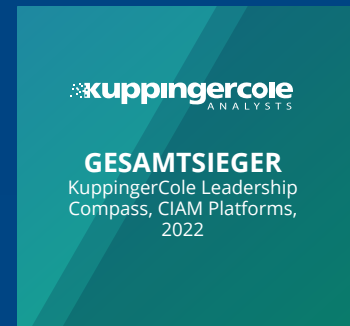
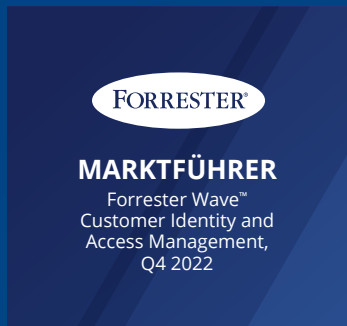
ERWEITERTE CIAM-FUNKTION	BESCHREIBUNG UND BEDEUTUNG	FRAGEN AN CIAM-ANBIETER
Multi-Cloud und Hybrid-Cloud	<p>Multi-Cloud-Umgebungen haben sich aufgrund ihrer großen Flexibilität, Verfügbarkeit und Skalierbarkeit zu einem echten Trend entwickelt. Dank ihnen können Unternehmen eine Anbieterabhängigkeit vermeiden, Markteinführungszeiten verkürzen, die Komplexität reduzieren und sowohl Zeit als auch Kosten sparen.</p> <p>Hybrid-Umgebungen umfassen sowohl On-Premise- als auch Cloud-Umgebungen. Cloud-Umgebungen ermöglichen eine bessere Skalierbarkeit, wohingegen On-Premise-Umgebungen für eine größere Datensicherheit sorgen. Der Vorteil von Hybrid-Umgebungen liegt in ihrer Flexibilität, jede Art von Bereitstellung überall und zu jeder Zeit zu ermöglichen.</p> <p>CIAM-Plattformen sollten flexible Nutzungsoptionen anbieten, die auch Multi-Cloud- und Hybrid-Cloud-Bereitstellungen umfassen.</p> <p>Diese Nutzungsoptionen unterstützen den Trend Erneuerung der Wirtschaft.</p>	<ul style="list-style-type: none"> • Wie kann die Lösung in jeder Cloud-Umgebung bereitgestellt werden, einschließlich Multi-Cloud, Bring-Your-Own-Cloud oder Hybrid-Cloud? • Beinhaltet sie eine hochverfügbare und produktionsreife Konfiguration? • Wie ist die Lösung des CIAM-Anbieters lizenziert, um ein Hybrid-Cloud-Modell zu unterstützen?
Systemaudits und -analysen	<p>Systemaudits und -analysen sind unternehmenskritische Funktionen. CIAM-Plattformen müssen in der Lage sein, Audits für Systemsicherheit, Fehlerbehebung, Nutzungsanalysen und Compliance durchzuführen. Darüber hinaus sollten sie eine Vielzahl von Überwachungs- und Protokollierungsfunktionen unterstützen. Auditprotokolle müssen operative Informationen über Ereignisse innerhalb einer Bereitstellung erfassen, um so nicht nur Prozesse und Sicherheitsdaten zu protokollieren, sondern auch Authentifizierungsmechanismen, Systemzugriffe, Benutzer- und Administratoraktivitäten, Fehlermeldungen und Konfigurationsänderungen. Digitale Identitätsplattformen sollten zudem Audit- und Analysemöglichkeiten für die Systeme zur Verfügung stellen, mit denen sie zusammenarbeiten, beispielsweise Partnersysteme.</p> <p>Diese Funktion dient dem Schutz der Verbraucher und des Unternehmens. Sie spricht die Trends Erneuerung der Wirtschaft, Partner-Ökosysteme, IoT, Cyberkriminalität sowie Datenschutz, Zustimmung und gesetzliche Bestimmungen an.</p>	<ul style="list-style-type: none"> • Kann die Lösung Audits für Systemsicherheit, Fehlerbehebung, Nutzungsanalysen und Compliance durchzuführen? • Unterstützt die Lösung eine Vielzahl von Überwachungs- und Protokollierungsfunktionen?

ForgeRock: Der unangefochtene Marktführer für Enterprise CIAM

Als unangefochtener CIAM-Marktführer hilft ForgeRock Unternehmen wie Ihrem, die acht Digitalisierungstrends erfolgreich aufzugreifen, um schneller Kunden zu gewinnen, das Kundenerlebnis zu verbessern und sowohl die Kunden als auch Ihr Unternehmen zu schützen. Optimieren Sie Ihre Geschäftsabläufe mit ForgeRock und der branchenweit einzigen KI-basierten All-in-One-Plattform der Unternehmensklasse für alle Identitäten und jede Cloud.

„Im April 2020 haben wir BBC Bitesize eingeführt, eine Webseite, die Eltern und Schülern kostenlose Videos, Anleitungen, Aktivitäten und Ratespiele nach Themen und Klassenstufe sortiert anbietet. Das Relaunch hat nur wenige Wochen gedauert, und bereits am Einführungstag wurde der Service ohne Ausfall von drei Millionen Menschen genutzt.“

Matt Gres, Director of Platform



Internationale Konzerne vertrauen auf ForgeRock Enterprise CIAM, um Wachstum und Umsatz zu steigern. Werden Sie Mitglied der ForgeRock-Community und profitieren Sie von der Unterstützung Ihrer einzigartigen Initiativen, um nicht nur die Trends von heute, sondern auch die von morgen zu bedienen.

„Wir bei Philips haben es uns zur Aufgabe gemacht, das Leben der Menschen zu verbessern und sie zu befähigen, besser für sich und andere zu sorgen. Dank ForgeRock können wir innovative Technologien für Datenfreigabe- und Zustimmungsprozesse in unsere digitale HealthSuite-Plattform integrieren und so das Vertrauen von Verbrauchern und Patienten stärken.“

Jeroen Tas,
Chief Innovation and Strategy
Officer

PHILIPS

Weitere Informationen

Mehr zu ForgeRock und CIAM

- ➔ **Lesen Sie**, wie HSBC sichere, personalisierte Nutzungserlebnisse für mehr als 30 Millionen Kunden in 36 Ländern bereitstellt.
- ➔ **Schauen Sie** sich das Webinar von ForgeRock und Deloitte an: *Four Technologies for Designing Captivating Digital CIAM Journeys (Vier Technologien für die Gestaltung überzeugender digitaler CIAM-Erlebnisse)*
- ➔ **Kontaktieren Sie** unseren Vertrieb, um ein Gespräch und eine Demo zu vereinbaren..

„Jetzt ist es an der Zeit, in die Cloud zu migrieren, KI zu nutzen und die Vorteile von Infrastruktur der nächsten Generation zu erschließen; die Architektur, die Unternehmen heute aufbauen, bestimmt ihre Zukunft.“⁹

accenture

⁹ https://www.accenture.com/us-en/insights/technology/_acnmedia/Thought-Leadership-Assets/PDF-3/Accenture-Tech-Vision-2021-Full-Report.pdf

Informationen von unabhängigen Dritten

Sehen Sie sich die Punktplatzierung an und lesen Sie in diesen Analystenberichten, warum ForgeRock der Enterprise CIAM-Marktführer ist:

- ➔ **The Forrester Wave™**: Customer Identity and Access Management, Q4 2022
 - ➔ **Gartner®** Critical Capabilities for Access Management, 2022
 - ➔ **KuppingerCole Leadership Compass**: CIAM Platforms, 2022
-
- ➔ Schulung und Beratung zu CIAM-Markt und -Technologie erhalten Sie bei **The Cyber Hut**.

Über ForgeRock

ForgeRock®, (NYSE: FORG) ist ein weltweit führender Anbieter im Bereich digitale Identität. Das Unternehmen liefert moderne und umfassende Identity und Access Management-Lösungen für Verbraucher, Mitarbeiter und Dinge und bietet so einen einfachen und sicheren Zugang zur vernetzten Welt. Mit ForgeRock orchestrieren, verwalten und sichern mehr als 1.300 globale Unternehmen den gesamten Lebenszyklus von Identitäten, angefangen bei dynamischen Zugriffskontrollen, Governance und APIs bis hin zur Speicherung autoritativer Daten – verwendbar in jeder Cloud- oder Hybridumgebung. Das Unternehmen mit Hauptsitz in San Francisco, Kalifornien, unterhält Niederlassungen auf der ganzen Welt. Für weiterführende Information und kostenlose Downloads besuchen Sie gerne unsere Website www.forgerock.com.



Folgen Sie uns



Copyright © 2022 ForgeRock. Alle Rechte vorbehalten.