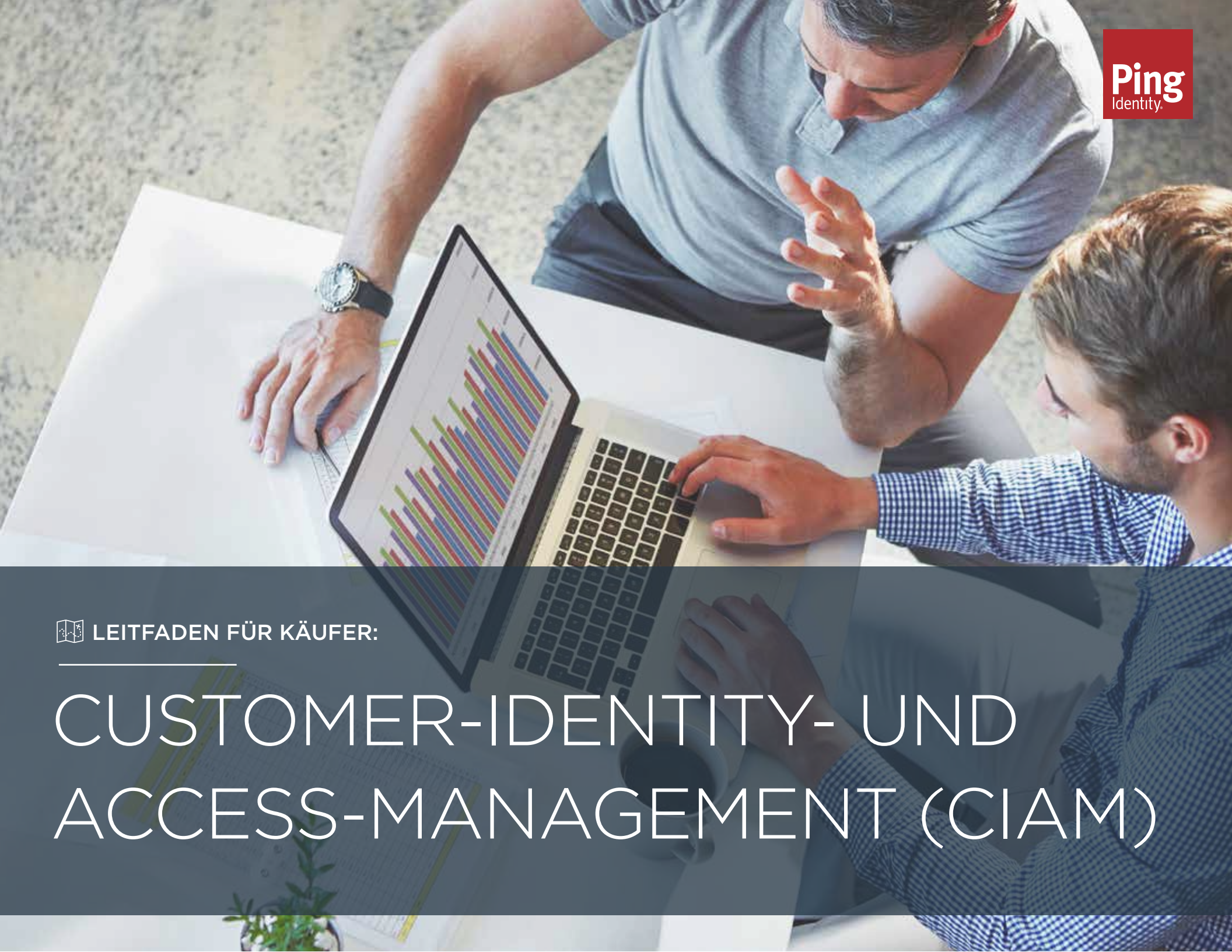


LEITFADEN FÜR KÄUFER:

CUSTOMER-IDENTITY- UND ACCESS-MANAGEMENT (CIAM)

MARKT IM UMBRUCH

Was die Anforderungen an die Verwaltung von Kundenidentitäten betrifft, hat in den letzten Jahren ein tief greifender Wandel stattgefunden. Dieser Wandel ist nicht zuletzt auf Analysten zurückzuführen, die ab 2015 damit begannen, Customer-Identity- und Access-Management (CIAM) als eigenen Bereich mit eigenen Anforderungen zu definieren. Verstärkt wird diese Entwicklung durch ein immer anspruchsvolleres Wettbewerbsumfeld, bei dem das Kundenerlebnis der Trumpf im Kampf um Marktanteile ist.

Heutige Kunden sind stark vernetzt und verteilen ihre Aktivitäten auf neue Art und Weise über unterschiedliche Kanäle hinweg. Daher muss jeder Interaktionspunkt ein konsistentes Kundenerlebnis bieten, sicher sein und alle Vorgaben hinsichtlich Datenschutz und Verbrauchereinwilligung einhalten.

CIAM-Business-Treiber erstrecken sich über unterschiedliche Teams – angefangen beim Geschäftsbereich über das Marketing bis hin zu Technik und IT-Sicherheit. Dabei sind die Anforderungen ebenso unterschiedlich, wie die Abteilungen selbst. Um die passende CIAM-Lösung zu finden, müssen die Teams funktionsübergreifend zusammenarbeiten und darauf achten, dass sie sich für eine umfassende CIAM-Plattform mit vielfältigen Funktionen entscheiden.

CUSTOMER-IDENTITY- UND ACCESS-MANAGEMENT (CIAM)

Seit einiger Zeit wachsen sowohl das Angebot als auch die Qualität spezialisierter CIAM-Lösungen enorm. Die Branche hat viel dazugelernt: Man hat erkannt, dass es nicht ausreicht, das Kunden-Identitätsmanagement einfach nur als Erweiterung in bestehende Enterprise-Identity-Lösungen einzubinden. CIAM unterscheidet sich fundamental von Mitarbeiter-IAM:

1. **Business-Treiber** – Zu den wichtigsten Mitarbeiter-IAM-Business-Treibern zählen Risikominimierung und Effizienzoptimierung, während es bei den CIAM-Business-Treibern vor allem um Kundenbindung und Umsatzsteigerung geht.
2. **Skalierbarkeit** – Große Unternehmen haben häufig Tausende von Mitarbeitern, aber selbst mittelgroße Kundenimplementierungen können bereits Millionen von Kunden und Milliarden von Attributen umfassen.
3. **Registrierung** – Die Zugangsdaten von Mitarbeitern werden bereitgestellt, wobei dieser Prozess von der Personalabteilung gesteuert wird. Kunden dagegen registrieren sich selbst.
4. **Datenschutz** – Anders als bei Mitarbeitern gelten für Kunden äußerst strenge Datenschutzvorgaben wie die DSGVO. Verstöße gegen diese Bestimmungen können der Marke schaden, das Vertrauen der Kunden aufs Spiel setzen und zu hohen Geldstrafen führen.
5. **Anforderungen an die Servicequalität** – Die Anforderungen an die Servicequalität sind oft schon für Mitarbeiter hoch, doch für Kunden gelten besonders strikte Vorgaben, deren Einhaltung sogar noch wichtiger ist als bei Mitarbeitern. Kunden tolerieren keine Verzögerungen und Ausfälle. Mitarbeiter dagegen haben keine andere Wahl.

In ihrer einfachsten Form sollten CIAM-Lösungen Funktionen für die drei wichtigsten Aspekte der Kundeninteraktionen mit Ihrer Marke bereitstellen:

1. **Zugang** – Unternehmen müssen Kunden anhand von Authentifizierungs- und Registrierungsfunktionen einen sicheren Zugriff auf ihre digitalen Ressourcen bieten können. Diese Funktionen sollten über alle Kanäle hinweg konsistent sein und Features wie Social Login enthalten, die den Ablauf optimieren.
2. **Erkennung** – Unternehmen müssen in der Lage sein, ihre Kunden nach der Authentifizierung zu erkennen, egal, über welchen Kanal oder welche App sie sich angemeldet haben. Dazu gehört es auch, Kunden den richtigen Zugriff auf die richtigen Inhalte mit einem einheitlichen Profil für alle Anwendungen bereitzustellen, um das Kundenerlebnis über alle Kanäle hinweg zu personalisieren.
3. **Schutz** – Unternehmen müssen ihre Kunden vor Datenlecks schützen und Kundendaten zuverlässig verwalten. Dies beinhaltet die Implementierung sicherer Authentifizierungs- und Registrierungs-Best Practices, inklusive kontextbezogener Multifaktor-Authentifizierung (MFA), Schutz der API-/Anwendungsebene mit Zugriffskontrolle und Sitzungsmanagement sowie Schutz der Kundendaten mithilfe von Data-Access-Governance, Datenverschlüsselung in jedem Zustand, etc.

Unternehmen müssen in der Lage sein, diese fundamentalen CIAM-Funktionalitäten mit einer leistungsstarken Lösung zu erfüllen, die auch extremen Skalierungsanforderungen gewachsen ist.

DEFINITION DER GESCHÄFTLICHEN ZIELE

Wenn Sie Ihre geschäftlichen Ziele schon im Vorfeld klar definieren, können Sie das Angebot gezielt eingrenzen und dafür sorgen, dass Sie sich auf die passenden Lösungen konzentrieren. Die wichtigsten Gründe, warum Unternehmen CIAM-Lösungen benötigen:

1. **Digitale Transformation** – Unternehmen entscheiden sich immer öfter für Digital-Business-Initiativen, um die Interaktion von Kunden mit ihrer Marke zu verändern. CIAM ermöglicht sichere, konsistente Kundenerlebnisse über mehrere Kanäle hinweg und kann Unternehmen dabei unterstützen, die Art und Weise zu verändern, wie sie ihr digitales Geschäft abwickeln.
2. **Zunehmende Sicherheitsbedrohungen** – Datenlecks passieren immer häufiger und nehmen von Mal zu Mal größere Ausmaße an. Daher steht Breach Prevention ganz oben auf der Agenda der IT- und Sicherheitsteams. CIAM-Lösungen mit speziell auf Kundenidentitäten ausgerichteter End-to-End-Sicherheit können das Risiko von Datenlecks drastisch reduzieren.
3. **Einhaltung von Datenschutzvorgaben** – Aufgrund der strengen Vorgaben, die je nach Region, Branche, Unternehmen und sogar von Person zu Person variieren können, erscheint die Einhaltung kundenbezogener Datenschutzvorgaben sehr schwierig. Neben zentralisierten Governance-Regeln für den Datenzugriff bieten CIAM-Lösungen weitere Funktionen, um die Einhaltung von Richtlinien zur Einwilligung des Kunden zur Weitergabe persönlicher Daten, zu regionalen Datenspeichern und zu anderen Datenschutzvorgaben sicherzustellen.
4. **Entwicklung und Bereitstellung mobiler Anwendungen** – Die Einführung einer neuen Anwendung dient oft als Impulsgeber für ein konsistentes, kanalübergreifendes Kundenerlebnis. Dies kann es Unternehmen erleichtern, die grundlegenden Voraussetzungen zu schaffen und Skalierbarkeit, Performance, Sicherheit, Single Sign-on, Social Login und andere CIAM-Funktionen einzuführen.

Wir haben hier die gängigsten Business-Treiber aufgeführt. Es kann jedoch noch weitere geben, die Skalierbarkeit, Performance, Sicherheit sowie andere CIAM-Funktionen erfordern – z. B. Fusionen und Übernahmen, die Einführung des Internets der Dinge (IoT), etc.

TOP 3 BEST PRACTICES FÜR DIE CIAM-IMPLEMENTIERUNG

1. **Auf Balance zwischen Kundenerlebnis und Sicherheit achten** – Hierfür ist eine enge Zusammenarbeit zwischen Geschäftsbereich/Marketing und IT-/Infosec-Teams erforderlich. Diese Zusammenarbeit gewährleistet, dass die Anforderungen an das Sicherheitsteam und die vom Geschäftsbereich definierten Usability-Standards erfüllt werden.
2. **Voraussetzungen für Skalierbarkeit schaffen** – Konzentrieren Sie sich nicht nur auf die Gesamtzahl der Benutzer, sondern auf unerwartete Szenarien mit Spitzenlasten. Ausfälle während Spitzenzeiten können äußerst teuer werden. Achten Sie darauf, dass die von Ihnen favorisierte Lösung sowohl vom Preis als auch von der Geschwindigkeit her für Verbraucher ausgelegt ist (nicht mehr als 1 Sekunde Antwortzeit für Verbraucher-Apps).
3. **Für Multichannel planen** – Egal, ob Sie es Multichannel nennen oder nicht – Ihre Kunden interagieren mit Ihrem Unternehmen schon jetzt über viele Kanäle hinweg. Machen Sie sich vorab schon Gedanken, wie Ihre CIAM-Lösung Kunden die Nutzung unterschiedlicher Kanäle erleichtern und Konsistenz gewährleisten kann.

STOLPERSTEINE, DIE ES ZU VERMEIDEN GILT

1. Teillösungen (z. B. MFA, aber keine Sicherheit auf der Datenebene, SSO, aber kein einheitliches Profil)
2. Komplexer, inkohärenter Software-Stack, um CIAM-Anforderungen zu erfüllen
3. DIY-Projekte, die auf den ersten Blick einfach erscheinen, aber am Ende mehr Zeit und Geld kosten, wenn man Sicherheit, Datenschutz, Authentifizierung und die lange Liste der damit verbundenen Best Practices berücksichtigt

KRITERIEN ZUR AUSWAHL DES RICHTIGEN CIAM-ANBIETERS

- Erfahrung und Referenzen
- Finanzielle Durchführbarkeit und Marktstabilität
- Umfang der Services/Vollständigkeit der Lösung
  - Erfahrung mit der Implementierung von Identity Management-Lösungen
  - Erfahrung mit Managed Services
- Bewährte Implementierungen mit extremer Skalierbarkeit und Performance
- End-to-End-Sicherheit, die Authentifizierungs-, Anwendungs-/API- und Datenebenen umfasst
- Standardbasierte Lösungen, die erweiterbar und zukunftssicher sind
- Möglichkeit, in beliebiger Umgebung zu implementieren (lokal, Cloud, hybrid)

CHECKLISTE

FUNKTIONALE ASPEKTE

Authentifizierungsebene – Anforderungen

EVALUIERUNGSKRITERIEN	WICHTIG
Stellt der Anbieter Federated-SSO-Funktionen bereit?	Federated SSO sorgt für ein konsistentes Anmeldeerlebnis – d. h. Kunden können mit den gleichen Anmeldedaten über sämtliche digitale Ressourcen hinweg auf die gewünschten Inhalte und Seiten zugreifen.
Umfasst die Lösung des Anbieters Social Login?	Wenn Sie Ihren Kunden erlauben, bestehende Identitäten (z. B. Facebook oder Google) für die Authentifizierung gegenüber Ihrer Marke zu nutzen, können Sie das Benutzererlebnis bei der Registrierung und Authentifizierung optimieren.
Unterstützt der Anbieter Selfservice-Funktionen für die Kontoverwaltung?	Nach der Registrierung brauchen Kunden Selfservice-Funktionen, um ihre Daten zu verwalten, hinzuzufügen, zu aktualisieren oder zu löschen.
Implementiert der Anbieter Registrierungs-Best Practices, wie Accountwiederherstellung und zentral verwaltete Passwortregeln?	CIAM-Anbieter sollten Best Practices wie Passwortzurücksetzung und zentralisierte Passwortregeln für zusätzliche Sicherheit implementieren.
Unterstützt der Anbieter risikobasierte, kontextbezogene MFA?	Benutzer um die Bereitstellung eines zweiten Authentifizierungsfaktors (z. B. SMS oder Biometrie) zu bitten, ist keine Patentlösung. Der Einsatz von Zweitfaktoren muss risikobasiert erfolgen und den Kontext des Benutzergeräts, sowie den geografischen Standort oder die Transaktionsart berücksichtigen.

FUNKTIONALE ASPEKTE

Anwendungs-/API-Ebene – Anforderungen

EVALUIERUNGSKRITERIEN	WICHTIG
Kann der Anbieter eine fein abgestimmte Zugriffskontrolle für Anwendungen und APIs bereitstellen?	Es ist wichtig, dass Unternehmen die Zugriffskontrolle für bestimmte URLs und APIs zentral verwalten können. Anbieter sollten auch zentralisierte kontextbezogene Zugriffskontrollregeln bereitstellen.
Stellt der Anbieter Funktionen für die Verwaltung von Kundenpräferenzen zur Verfügung?	Unternehmen müssen Kunden die Möglichkeit geben, Präferenzen explizit zu definieren. Diese sollten in einem einheitlichen Kundenprofil gespeichert werden, um konsistente, personalisierte Erlebnisse über unterschiedliche Kanäle hinweg zu erleichtern.
Unterstützt der Anbieter Sitzungsmanagement und Single Logout?	Unternehmen, die mehrere Kanäle und Anwendungen bereitstellen, müssen Single Logout für alle Anwendungen anbieten können, um die Sicherheit und den Komfort für ihre Kunden zu verbessern.

FUNKTIONALE ASPEKTE

Datenebene – Anforderungen

EVALUIERUNGSKRITERIEN	WICHTIG
Stellt der Anbieter eine sichere, skalierbare Verzeichnislösung bereit?	Bei der Speicherung von Kundenidentitäts- und Profildaten sind Sicherheit, Skalierbarkeit und Performance gleichermaßen wichtig. Achten Sie darauf, dass Anbieter ein sicheres Verzeichnis bereitstellen, das Millionen von Identitäten und Milliarden von Attributen speichern kann. Vergewissern Sie sich, dass der Anbieter anhand von Kundenreferenzen einen Nachweis für die von Ihnen benötigte Skalierbarkeit vorlegen kann.
Kann das Verzeichnis des Anbieters unstrukturierte Daten speichern?	Die Daten, die Sie über Ihre Kunden sammeln möchten, könnten vielfältige und unstrukturierte Informationen enthalten, wie beispielsweise Browser Fingerprints. Es ist wichtig, dass Sie diese Daten unkompliziert in Ihrem Kundenverzeichnis speichern können.

FUNKTIONALE ASPEKTE

Datenebene – Anforderungen

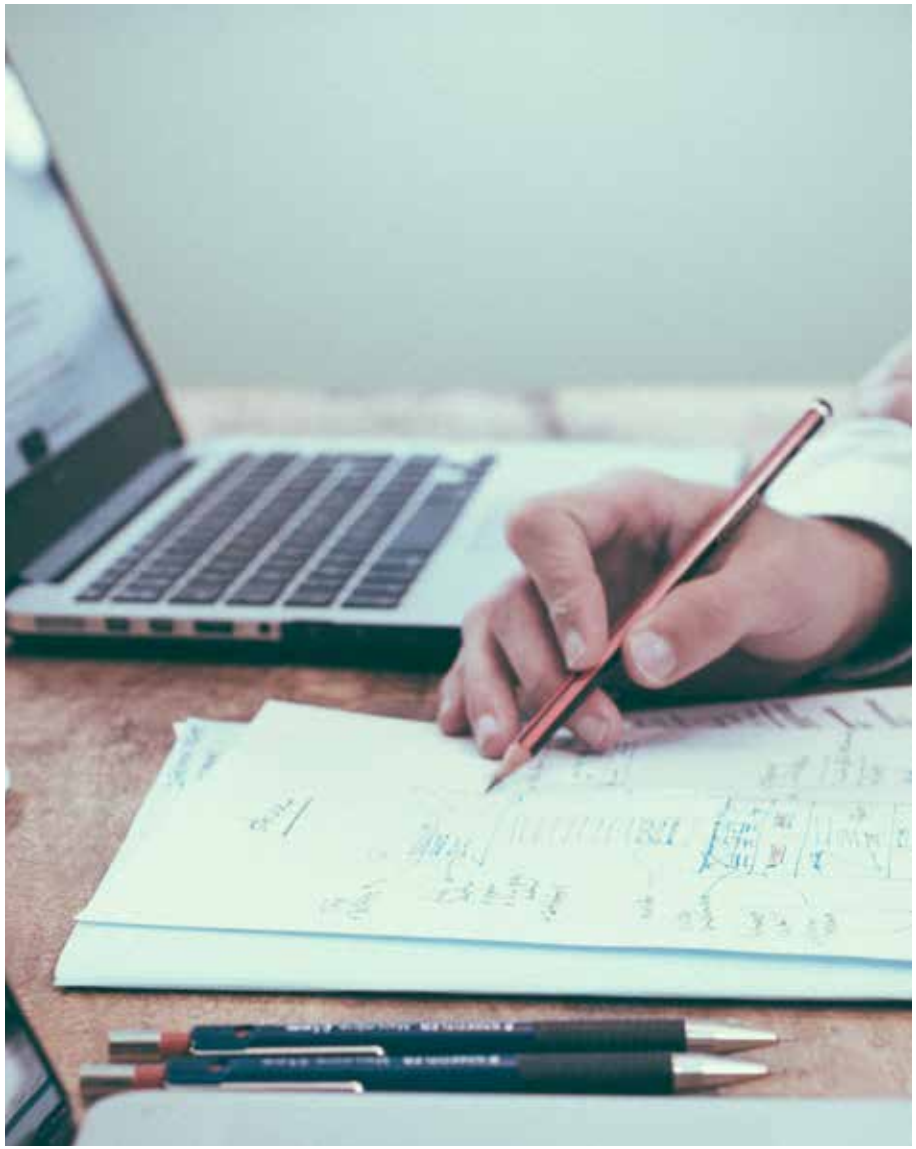
EVALUIERUNGSKRITERIEN	WICHTIG
Kann auf das Verzeichnis des Anbieters via REST-APIs zugegriffen werden?	Die in einem Verzeichnis abgelegten Kunden- und Profildaten müssen mit entwicklerfreundlichen REST-APIs zugänglich sein, damit sie über bestehende Apps leicht abrufbar sind und neue Apps schnell auf dem Markt eingeführt werden können.
Stellt der Anbieter Funktionen zur bidirektionalen Datensynchronisation in Echtzeit zur Verfügung?	Eine bidirektionale Datensynchronisierung in Echtzeit kann bei der Erstellung eines einheitlichen Kundenprofils (in einem CIAM-Verzeichnis) aus unterschiedlichen Identitätsdatensilos behilflich sein, selbst, wenn andere Identitäts-Repositorys gepflegt werden müssen. Sie kann auch risikofreie Datenmigrationen in ein einheitliches Kundenverzeichnis mit null Ausfallzeiten unterstützen.
Unterstützt der Anbieter fein abgestimmte Data-Access-Governance, um Datenschutzvorgaben einzuhalten?	Datenschutzvorgaben sind vielfältig und die entsprechenden Anforderungen unterscheiden sich von Person zu Person. CIAM-Lösungen müssen über zentral verwaltete Datenschutzrichtlinien verfügen, bei denen eine Kundeneinwilligung erforderlich und die Datenweitergabe auf Attributebene an sämtliche interne und externe Anwendungen geregelt ist.
Verschlüsselt der Anbieter Daten in jedem Zustand und implementiert andere Best Practices, um Sicherheit auf Datenebene zu gewährleisten?	Werden Kundendaten gehackt, kann das katastrophale Folgen für die Reputation einer Marke haben. Daher ist es wichtig, die Kundendaten in jedem Zustand zu verschlüsseln – im ruhenden Zustand sowie während der Übertragung und Verwendung – und andere Best Practices wie aktive und passive Warnmeldungen sowie manipulationssichere Anmeldung zu implementieren.

FUNKTIONALE ASPEKTE

Plattform – Anforderungen

EVALUIERUNGSKRITERIEN	WICHTIG
Basiert die Plattform des Anbieters auf offenen Standards?	Es ist wichtig, dass CIAM-Plattformen offene Standards wie SAML, SCIM, OAuth2 und OpenID Connect verwenden. So lässt sich die CIAM-Lösung erweitern und vielseitig einsetzen.
Gewährleistet der Anbieter eine hohe End-to-End-Sicherheit auf jeder Ebene?	CIAM-Anbieter müssen während der Authentifizierung ein Höchstmaß an Sicherheit bieten – sowohl auf der Anwendungs-/API- als auch auf der Datenebene.
Kommt der Anbieter mit extrem umfangreichen Datenmengen und Performance-Anforderungen zurecht und verfügt er über Referenzen für vergleichbare Projekte?	Anbieter müssen in der Lage sein, Millionen gespeicherter Identitäten und Milliarden Attribute zu bewältigen, auch in Spitzenzeiten mit Hunderttausenden gleichzeitiger Benutzer. Sie müssen erfolgreich realisierte Projekte mit 99,99999 % Verfügbarkeit und einer Latenz von nur wenigen Millisekunden nachweisen können.
Stellt der Anbieter personalisierbare Referenzanwendungen und vorgefertigte Weboberflächen bereit?	In den meisten Fällen möchten Unternehmen Benutzeroberflächen umfassend personalisieren. Dabei bieten Anbieter mit vorgefertigten Ressourcen und Benutzeroberflächen schnellere Markteinführungszeiten für neue Anwendungen.

ANBIETER-EVALUIERUNG UND -AUSWAHL



Nachdem Sie all Ihre Anforderungen definiert haben, sollten Sie Ihre Daten in eine passende Form bringen, um das Abschneiden der einzelnen Anbieter auf einfache Weise zu evaluieren. Dafür eignet sich eine Sheets- oder Excel-Tabelle. Erstellen Sie am besten eine Reihe für jedes Ihrer Auswahlkriterien und ordnen Sie diese wie oben nach den wichtigsten Anforderungen.

Fügen Sie anschießend für jeden Anbieter, den Sie evaluieren möchten, eine Spalte hinzu. Bewerten Sie anhand von Punkten, wie gut die einzelnen Anbieter Ihre Kriterien erfüllen:

0 = erfüllt die Anforderung nicht
1 = erfüllt die Anforderung nur sehr eingeschränkt
2 = erfüllt die Anforderung teilweise
3 = erfüllt oder übertrifft die Anforderung

Mit diesem System können Sie jeden Anbieter mit 0–3 Punkte für jedes Ihrer Kriterien bewerten. Zählen Sie anschließend die Punkte der einzelnen Anbieter zusammen. Der Anbieter mit der höchsten Punktzahl ist auch der Anbieter, der Ihre Anforderungen am besten erfüllt.

#3061(rev) | 9.17 | v002