
Customer Identity and Access Management – der Generalschlüssel für digitale Märkte

Digitale Transformation ist in aller Munde – und das schon eine ganze Weile. Aus den ersten, einfachen Webshops in den 2000er Jahren hat sich ein komplexes digitales Ökosystem entwickelt. Die Möglichkeiten und Anforderungen haben sich seitdem vervielfacht. Heute geht es nicht mehr alleine darum, traditionelle Prozesse digital nachzubilden.

Immer wichtiger wird stattdessen, neue Produkte und Dienstleistungen weltweit zuverlässig im Markt einführen zu können. Und das in oft sehr engen Zeitfenstern. Bei digitalen Diensten ist Time to Market längst einer der entscheidenden Erfolgsfaktoren. Darüber hinaus bieten digitale Plattformen bisher nicht vorhandene Möglichkeiten zur Erprobung und Umsetzung völlig neuer Geschäftsmodelle. Die Geschwindigkeit und Flexibilität, mit der sie sich implementieren, testen, anpassen und in bestehende Infrastrukturen integrieren lassen, werden zu entscheidenden Wettbewerbsfaktoren.

Im Mittelpunkt dieses Spannungsfeldes stehen die Kunden – oder präziser: die Schnittstellen zu ihnen.

- Wer ist der Kunde?
- Wie lässt sich seine Identität zuverlässig bestätigen?
- Wie lässt sich eine konsistente User Experience – auch über Geräte- und Anwendungsgrenzen hinweg – sicherstellen?

Für die Beantwortung all dieser Fragen ist ein leistungsfähiges Customer Identity and Access Management (CIAM) notwendig. Die damit verbundenen Voraussetzungen, Herausforderungen und Chancen wollen wir in diesem Whitepaper untersuchen.

Kundenbeziehung – alles eine Frage der Identität

Der Gedanke hinter Customer Identity and Access Management ist ein ganz einfacher: Wer ist wer und wer darf was? In der Praxis jedoch bedeutet das nicht weniger, als die Identität des Kunden in all ihren Facetten sicher und zuverlässig abbilden, überprüfen und schützen zu können.

Am Anfang steht dabei die Sicherstellung der Identität: Vom einfachen Passwort über 2-Faktor-Authentifizierung bis hin zur Abfrage biometrischer Merkmale sind dafür verschiedene Verfahren denkbar. Hierzu zählen auch Identifizierungsverfahren der großen Player wie Apple, Facebook oder Amazon.

Im nächsten Schritt geht es darum, das digitale Profil des Kunden zu erstellen und zu verfeinern. Neben den Stammdaten wie Adresse, Geburtsdatum und Kontaktdaten sind vor allem Informationen zu Vorlieben, Interessen, Besitz etc. von großem Wert, um den Kunden näher kennenzulernen und seine Bedürfnisse besser einschätzen zu können. Schließlich lassen sich ihm erst so relevante Angebote zur richtigen Zeit und unter den richtigen Umständen unterbreiten.

Doch Vorsicht: Selbstverständlich sind für diese Profile die entsprechenden Einwilligungen zur Datenverarbeitung seitens des Kunden erforderlich. Denn erst wenn diese vorliegen, lassen sich die Daten rechtskonform für E-Mail-Marketing oder Customer Data Analytics nutzen. Spätestens seit dem Inkrafttreten der europäischen Datenschutz-Grundverordnung (EU-DSGVO) ist daher ein integriertes Consent Management für jede CIAM-Lösung unverzichtbar.

„Die grundlegende Philosophie hinter Service Layers klingt sehr einfach und nachvollziehbar: Anspruchsvolle kundenindividuelle Anforderungen ermöglichen und gleichzeitig einen maximalen Automatisierungsgrad erreichen – vom ersten Deployment bis zum langjährigen Support. Tatsächlich war es bis dahin aber ein langer Weg. Auch mit über zwanzig Jahren IAM-Erfahrung gab es für uns zahlreiche Herausforderungen zu bewältigen. Am Ende aber zählt das Ergebnis. Und mit dem sind wir mehr als zufrieden. Denn mit Service Layers steht jetzt erstmals eine CIAM-Lösung zur Verfügung, in der sich Leistungsfähigkeit angepasster Best-of-Breed-Produkte mit der schnellen, unkomplizierten Bereitstellung von Cloud-Services verbindet.“

Heiko Hütter
Product Owner Platform

Vom Passwort zum Ökosystem – eine kurze Geschichte der Customer Identity

Wer einen Blick zurück auf die historische Entwicklung der Customer Identity wirft, wird darin gleichzeitig die steigenden Anforderungen eines prosperierenden Online-Unternehmens wiedererkennen.

Am Anfang der Evolution stand die Überprüfung der Kundenidentität mittels Passwort. Es genügte, dass der Kunde sich online in einen Webshop einloggen und vielleicht einen kleinen personalisierten Bereich nutzen konnte. Mehr war nicht nötig.

Bald aber stiegen die Anforderungen. Um bei breiter aufgestellten Angeboten einen einheitlichen, komfortablen Zugang zu ermöglichen, wurde Single Sign-on in den 2000er Jahren ein großes Thema. Dabei zeigte sich rasch, dass die Bewegungs- und Aktionsdaten des Kunden einen großen Mehrwert darstellen. Der nächste Schritt lautete daher konsequent Datenintegration ins CRM-System. Was ursprünglich einmal als einfache Passwort-Tabelle begonnen hatte, schloss nun bereits eine Vielfalt von nachgelagerten Systemen ein.

Aus dieser Situation entstand rasch der Wunsch nach einem 360-Grad-Blick auf den Kunden. Mit zunehmender Anzahl an Berührungspunkten des Kunden (Website, Smartphone-App, Serviceberater beim Händler vor Ort, Telefon-Hotline, etc.) wurde ein einheitlicher, durchgängiger Service immer wichtiger. Schließlich erwartet der Kunde zu Recht, dass alle beteiligten Abteilungen oder Dienste stets auf dem aktuellen Stand in Bezug auf seine Daten und Aktionen sind.

Aus diesem Stadium haben sich mittlerweile regelrechte Ökosysteme entwickelt. Die Auswertung der anfallenden Daten zur Verbesserung des eigenen Angebots und zur Unterbreitung von relevanteren Angeboten sind die entscheidenden Geschäftsfaktoren. Das Kundenverhalten in allen Kanälen und Systemen, die Nutzung all seiner Werkzeuge und Endgeräte generieren heute Unmengen an Daten und damit Erkenntnisse für künftige Geschäftsoptionen. Schon jetzt ist absehbar, dass mit dem Internet of Things dieses Ökosystem beinahe ins Unermessliche wachsen wird. Amazon zeigt schon heute, wie aus einem Buchhändler ein Videoanbieter (dank Fire Stick), eine persönliche Bücherei (dank Kindle) und ein universeller Butler (dank Alexa) wird. Die

Kundenidentität ist dabei in all diese Geräte integriert. Customer Data Analytics ermöglicht es, all diese Daten aus unterschiedlichsten Quellen zusammenzufassen, auszuwerten, die Customer Journey jedes Kunden besser zu verstehen und in der Folge ein noch besseres Interaktions-Erlebnis zu schaffen.

Die Reise geht weiter in Richtung Open API. Unternehmen wollen sich nach außen öffnen, um ihre eigene Plattform anzubieten und in Applikationen anderer integriert zu werden. Das Ziel ist es, ständig im Kontakt mit dem Kunden zu sein. Für APIs und für den Zugriff von außen nach innen sind zwei Dinge absolut erforderlich. Das eine ist die Kundenidentität. Es muss klar sein, in welchem Benutzerkontext der Zugriff auf die APIs und Daten erfolgt. Das andere ist der Datenschutz und das bereits erwähnte Consent Management, um den Zugriff immer nur dann zu gewähren, wenn der Kunde seine Identität nachgewiesen und in die jeweilige Verarbeitung seiner Daten eingewilligt hat.

Datenschutz – Wichtig für Anbieter und Kunden

Selbstverständlich war eine sichere Handhabung der Kundendaten schon immer ein zentraler Bestandteil von CIAM-Lösungen. Zunehmende Sensitivität seitens der Nutzer und strengere gesetzliche Auflagen wie die EU-DSGVO erfordern zusätzliche Anstrengungen. Für international agierende Unternehmen ist es daher entscheidend, eine entsprechend skalierbare/adaptierbare Lösung zu haben, die sich nach Bedarf leicht und ohne großen Aufwand an neue oder unterschiedliche gesetzliche Vorschriften anpassen lässt.

Customer Identity als Motor von Geschäftsprozessen

Der kurze Abriss zeigt bereits, dass Customer Identity bzw. das damit zusammenhängende Customer Data Management immer mehr Funktionen abdeckt und damit ein zentraler Erfolgsfaktor aller digitalen Geschäftsprozesse ist. Auf dem Weg zur bestmöglichen Umsetzung sind jedoch einige Stolpersteine zu beachten. Projektübergreifend stechen dabei vor allem die folgenden Anforderungen hervor:

- kurze Time to Market
- reibungslose internationale Rollouts
- verlässliche Verfügbarkeit
- flexible Unterstützung von Mergers & Acquisitions
- Umsetzung neuer Geschäftsmodelle
- und natürlich: kalkulierbare Kosten

Nicht jede dieser Anforderungen muss für jedes Unternehmen sofort relevant sein. Wenn man aber die grundlegende Bedeutung einer CIAM-Lösung für die digitale Strategie bedenkt, sind Unternehmen gut beraten, bei der Wahl einer passenden Lösung die eigenen Anforderungen langfristigen zu betrachten.

Zwei Wege zum Ziel?

Für die Umsetzung der vorgenannten Anforderungen in ein modernes, leistungsfähiges Customer Data Management werden zahlreiche Lösungen angeboten. Dabei lassen sich traditionell zwei unterschiedliche Ansätze ausmachen.

Der Produktansatz

Eine ganze Reihe von Produktherstellern bieten teils äußerst leistungsfähige Customer Identity und Access Management Lösungen an. Diese werden meist von Systemintegratoren an die Bedürfnisse des Kunden angepasst. Auf diese Weise lässt sich eine bestmögliche Integration in die vorhandene IT-Landschaft gewährleisten. Dabei können aber beträchtliche Zeit-, Kosten- und Schulungsaufwände entstehen. Ähnliches gilt für den Wartungsaufwand. Die hohe mögliche Individualisierung dieser Lösungen birgt zudem die Gefahr, künftige Upgrades aufgrund komplexer Abhängigkeiten nicht durchführen zu können.

Cloud-Services

Auf der anderen Seite bieten Cloud-Dienstleister verschiedene Identity-as-a-Service-Lösungen (IDaaS) an. Ähnlich wie bei Microsoft Office 365, Google Docs oder Dropbox stehen diese Dienste ausschließlich online zur Verfügung. Da es sich um weitgehend standardisierte Lösungen handelt und keine große Anpassung nötig ist, lassen sich CIAM-Projekte damit schnell umsetzen und eine kurze Time to Market realisieren.

Der Trend zeigt deutlich in Richtung Identity as a Service. Eine Gartner-Studie* geht davon aus, dass sich der Anteil von IDaaS-Lösungen bis 2022 von heute 50 % auf dann über 80 % ansteigen wird. Dennoch fürchten viele Unternehmen, sich mit einer cloud-basierten Lösung abhängig vom jeweiligen Anbieter zu machen und die Kontrolle über essentielle Geschäftsprozesse aufgeben zu müssen. Auch die Integration physischer Touchpoints und die derzeit unbefriedigende, aber immer wichtiger werdende Integration von IoT-Geräten bereitet vielen Entscheidern Kopfzerbrechen.

Die Vereinigung zweier Welten: Führende Produkte, optimaler Service

Beide vorgestellten Ansätze sind gute Lösungen für eng umrissene Szenarien. Der Produktansatz etwa bietet sich für Unternehmen mit komplexen Anforderungen, die die Hoheit über die Lösung und die darin gespeicherten Daten behalten wollen. IDaaS andererseits eignet sich für all jene, die eine schnelle, standardisierte Umsetzung ohne große Individualisierung wünschen.

Die meisten Unternehmen dürften jedoch zwischen diesen beiden Extremen liegen. Mit den vorliegenden Lösungen mussten sie bisher zwangsläufig an der einen oder anderen Stelle Abstriche machen.

Ein Ausweg aus diesem Dilemma bietet die Synthese der beiden Ansätze: Man nehme ein fertiges Produkt von einem der Marktführer und adaptiere und konfiguriere es so, dass es als Service angeboten werden kann.

Infrastructure as Code

Das Problem ist bekannt: Wenn eine umfangreiche Software im eigenen Rechenzentrum installiert wird, ist dies in der Regel ein sehr langwieriger Vorgang. Vor zwanzig, dreißig Jahren musste erst einmal Hardware eingekauft werden. Später wurden virtuelle Maschinen bestellt und das Sizing musste geklärt werden. Alleine die Ermittlung des Bedarfs und die anschließende Beschaffung brachten einen hohen Planungsbedarf mit sich.

Mit dem Ansatz „Infrastructure as Code“ ändert sich dies grundlegend. Denn dabei werden die Infrastruktur-Anforderungen in den entsprechenden Plattform-Code programmiert, so dass die Infrastruktur mit Cloud Infrastrukturen – etwa Amazon AWS, Microsoft Azure, oder Google Cloud Platform – automatisch bereitgestellt werden kann.

Configuration as a Code

Der zweite wichtige Schritt ist es, die Konfiguration vom Produkt zu trennen und ebenfalls als Code abzulegen. Ist sie erst einmal eindeutig definiert, kann die Konfiguration wie jeder andere Programmcode behandelt werden. In einer Versionsverwaltung lassen sich eindeutige Releases festlegen und Vergleiche zu Vorversionen ziehen.



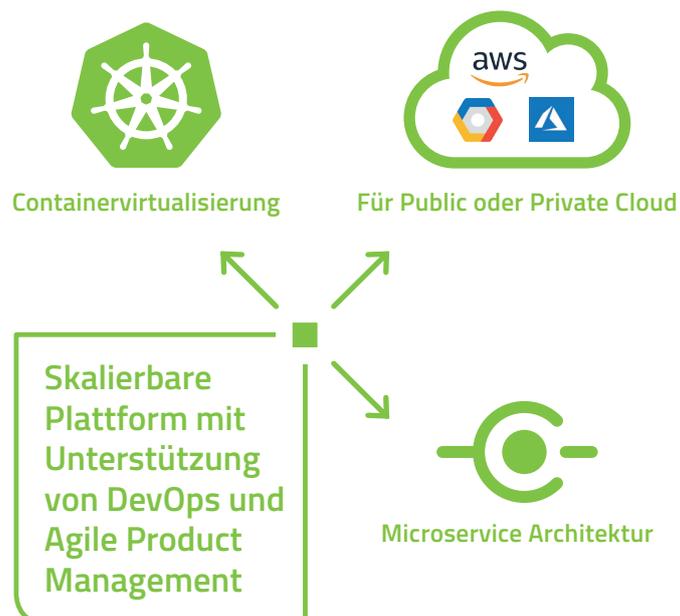
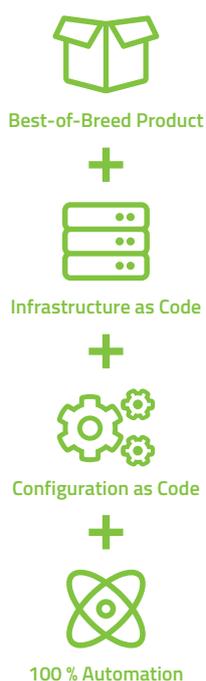
* Gregg Kreizman: „Magic Quadrant for Access Management, Worldwide“, 18. Juni 2018

Das Ergebnis ist eine enorme Qualitätssteigerung und die Gewissheit, jedes Code Artefakt jederzeit wiederverwenden zu können. Auf diese Weise wird digitalisiert, was früher aufwendig per Hand zu erledigen war. Beide Bausteine zusammen, Infrastructure as a Code und Configuration as Code, stellen so letztendlich die Digitalisierung des bisherigen Produktgeschäftes dar.

Wenn man nun noch die Build- und Deployment-Prozesse vollständig automatisiert, ist man schon am Ziel: Quasi auf Knopfdruck lässt sich nun ein Produkt aufsetzen, die benötigte Infrastruktur in einer Cloud bereitstellen und das Produkt entsprechend konfigurieren. Alle für den Produktionsbetrieb benötigten Artefakte lassen sich komfortabel definieren. Automatische Backups oder Monitoring-Funktionen sind ebenso einfach eingerichtet wie etwa Firewalls, Zertifikate und Load-Balancer.

Konkrete Umsetzungen in der Praxis: Service Layers

Für professionelles, enterprise-fähiges Identity und Access Management wurde dieser Ansatz erstmals von iC Consult mit der Plattform Service Layers umgesetzt. Als Basis dienen Best-of-Breed IAM-Produkte von Marktführern wie ForgeRock oder Ping Identity. Das Unternehmen mit Hauptsitz in München ist seit langem strategischer Partner aller bedeutenden Hersteller und daher bestens mit den Möglichkeiten der einzelnen Produkte vertraut. Besonderes Augenmerk legte man auf größtmögliche Flexibilität bei der Implementierung. Dazu gehört es auch, mögliche Abhängigkeiten von Cloud-Anbietern erst gar nicht entstehen zu lassen. Deshalb wird bei Service Layers alles über Kubernetes in Container betrieben. Anschließend kann in einer gemagten Kubernetes-Umgebung agil gearbeitet werden. Wer lieber die Kontrolle im eigenen Rechenzentrum behalten will, kann dies tun. Statt in einer Public Cloud lässt sich die gesamte Umgebung problemlos auch in einer Private Cloud betreiben.



Die Microservice-basierte Architektur erlaubt es, alle Features in einzelne Microservices zu trennen. Das Produkt lässt sich also ohne Abhängigkeiten auf andere Bestandteile erweitern und schafft damit ideale Voraussetzungen für DevOps und ein agiles Produktmanagement. Produkte können so sehr schnell, in rasch aufeinanderfolgenden kleinen Schritten aufgebaut werden. Neue Features können in kürzester Zeit eingeführt und erprobt werden. A/B-Tests lassen sich in parallelen Instanzen unkompliziert und kostengünstig durchführen.



Time to Market

Damit schafft die Plattform ideale Voraussetzungen, um mit vertretbarem Aufwand neue Marktnischen zu besetzen. Anstatt bei jeder Markteinführung quasi von Null anfangen zu müssen, lassen sich bereits bewährte Konfigurationen klonen und mit geringen Anpassungen an den Start bringen. Die Time to Market reduziert sich dank der vollautomatischen Einrichtung auf einen Bruchteil der bisherigen Zeit. Für Anbieter neuartiger Dienstleistungen ist dies der entscheidende Vorsprung, um sich noch vor den ersten Nachahmern als Marke im Bewusstsein der Kunden zu verankern.



Internationale Rollouts

Damit internationale Rollouts gelingen, müssen marktspezifische Anforderungen sowie regulatorische und gesetzliche Vorgaben berücksichtigt werden. Der damit verbundene Aufwand verursacht nicht nur erhebliche Kosten, sondern bringt oft zusätzliche Unsicherheiten bezüglich des Zusammenspiels der verschiedenen Systeme mit sich. Mit dem vorgestellten Ansatz entfallen diese Schwierigkeiten. Falls geographische oder gesetzliche Gegebenheiten eine Instanz vor Ort erfordern, ist diese in kürzester Zeit eingerichtet. Es genügt, ein Duplikat der Produktionsumgebung in einem geeigneten Rechenzentrum oder bei einem lokalen Cloud-Anbieter aufzuspielen. Die Deployment- und Setup-Zeiten liegen dabei im Minutenbereich.



Weltweit verfügbar auch in China und Russland Q4'19

Hinzu kommt, dass Service Layers ab dem vierten Quartal 2019 mit eigenen Hosting Standorten in China und Russland verfügbar ist. Kunden müssen sich nicht länger mit lokalen Hosting-Fragen auseinandersetzen, sondern können sich ganz auf ihr Kerngeschäft konzentrieren. Darüber hinaus garantiert ein dediziertes Hosting kurze Server-Latenzen bei gleichzeitiger 24/7-Verfügbarkeit von Support und Service.

Auch marktspezifische Anpassungen sind dank der Versionierung kein Problem mehr: einfach einen Branch ziehen und die Entwicklungslinie teilen. Trotz aller markt- oder kundenspezifischen Anpassungen bleibt das Basisprodukt dasselbe. Das reduziert nicht nur den Entwicklungsaufwand, sondern steigert gleichzeitig auch die Prozesssicherheit. Denn die Grundlage jedes neuen Branches ist eine bereits erprobte und getestete Version. Und das wiederum wirkt sich unmittelbar auf die Verlässlichkeit aus.

Verlässliche Verfügbarkeit bemisst sich nicht alleine nach der Up-Time. Im nie ganz auszuschließenden Störfall kommt es vor allem auf eine schnelle und zuverlässige Wiederherstellung des Systems an. Service Layers garantiert dies durch das exakte Klonen einer vom Kunden geprüften und abgenommenen Systemversion. Manuelle Änderungen sind nicht erforderlich. Schwer zu lokalisierende Fehler können sich nicht einschleichen. Unerwartete Ausfälle führen damit nicht länger zu kostspieligen Ausfallzeiten, sondern lassen sich binnen weniger Minuten beheben.



Mergers & Acquisitions

Mergers & Acquisitions stellen ebenso wie De-Merger für die IT eine große Herausforderung dar. Müssen doch unterschiedliche zusammengeführt bzw. wieder getrennt werden. Und das, ohne bestehende Prozesse im Hauptunternehmen zu gefährden.

Der Ansatz von Service Layers sichert die Konsistenz der jeweiligen Kundendaten. Anstatt die Kundendaten-Managementprozesse des übernommenen Unternehmens direkt zu integrieren, werden sie in ein dupliziertes System eingespielt. Sobald die Anfangsschwierigkeiten überwunden sind, werden die Daten dann in das eigene System migriert. Da beide Systeme identisch sind, ist die Migration ohne großen Aufwand machbar.



Neue Geschäfts-
modelle

Die Entwicklung neuer Geschäftsmodelle steht heute unter hohem Zeitdruck. Neue Ideen müssen entwickelt, getestet und bei Erfolg rasch implementiert werden. Gleichzeitig müssen bestehende Prozesse zuverlässig weiterlaufen. Die Einrichtung als separate Instanz ermöglicht beides. Mit den sofort nutzbaren Produktionsumgebungen steht allen, die an neuen Geschäftsmodellen arbeiten, eine digitale Spielwiese zur Verfügung. Das geplante Produktionssystem lässt sich dort samt aller Prozesse ausführlich testen. Die wertvollen Nutzungsdaten bleiben außen vor und können so nicht korrumpiert werden. Hat sich der neue Ansatz bewährt, kann er in wenigen Minuten in das Hauptsystem übernommen werden – oder alternativ auch verkauft werden. Denn mit der vollständig digitalisierten Produktkette lassen sich neue Geschäftsmodelle auch als eigenständige Lösung anbieten.



Kosten

Auch wenn sich alle bisher genannten Anforderungen vollständig umsetzen lassen, entscheiden letzten Endes die Kosten, ob die Maßnahme auch wirtschaftlich sinnvoll ist. Gefragt ist Funktionalität, nicht Infrastruktur. Durch die Codifizierung von Infrastruktur und Konfiguration sowie die Implementierung hochgradig standardisierter und automatisierter Prozesse senkt Service Layers die Betriebskosten nachhaltig.

Ausblick – Bereit für die CIAM-Trends von morgen

Unterm Strich erweist sich der vorgestellte As-a-Code-Ansatz als ein revolutionäres, gleichermaßen flexibles wie mächtiges Konzept für CIAM-Lösungen. Die Möglichkeit, digitale Geschäftsmodelle schnell und sicher zu kreieren, testen, betreiben, splitten und wieder zusammenzuführen und sogar als fertige Ware zu verkaufen, machen diesen Ansatz zu einem Game Changer.

CIAM wird weiter an Bedeutung gewinnen und sich auf immer mehr Geschäftsprozesse auswirken. Die Skalierbarkeit und Erweiterbarkeit der heute eingesetzten Lösungen beeinflusst damit direkt die künftige Wettbewerbsfähigkeit. Unternehmen mit leistungsstarken, aber schwerfälligen On-Premise-Systemen werden ihr eigenes „Sauriersterben“ erleben, wenn der Bedarf an zusätzlicher Flexibilität eine kritische Schwelle überschreitet. Die nächste Evolutionsstufe gehört jenen Identity as a Service Lösungen, deren Infrastruktur als Code vorliegt und sich so künftigen Anforderungen mit minimalem Aufwand anpassen lässt.

Mehr über Service Layers finden Sie unter www.servicelayers.com