CIAM vs. IAM: Why Traditional IAM Should Not Be Used for Customers

Understanding the Differences Between CIAM and IAM

Digital identity is at the center of every company's digital transformation. The value of the customer profile data that are linked to customer identities has grown dramatically and is now a crucial success factor for many companies. It forms the foundation for analyzing, understanding, and predicting consumer behavior and customer journeys – from first contact to purchase decisions and long-term brand loyalty.

It is a common misconception that the technology required for customer identity and access management (CIAM) is the same for traditional identity access management (IAM). Traditional IAM solutions – also called enterprise, employee, or workforce IAM – are the IT systems that ensure that only the workforce or known business partners of a company can access the corporate network and its resources.

Traditional IAM is typically well established, leading some companies to make the misguided assumption that "because we have this technology in-house already, it cannot be that hard to extend it to our customers." At the root of this approach is a drastic underestimation of the differences between workforce IAM and customer IAM, and the complexity of managing customer identities for a business's public-facing digital properties. CIAM has disparate – and far more challenging – requirements than workforce IAM; as a result, repurposing workforce IAM solutions can be a problematic approach.

A traditional IAM cannot provide insights into who the users are, the actions they take, or what influences their digital behavior.

Repurposing Traditional IAM for CIAM Is Not the Answer

As traditional IAM is designed to facilitate employee access to internal systems, it cannot provide insights into who a user is. In fact, identity is assumed, and advanced data (like the actions users take, and what influences their journey and behavior within the digital sphere) cannot be tracked. But businesses require these types of data insights to understand their customers and compete in the digital market space.

Furthermore, at many of the largest corporations, traditional IAM systems might be charged with administering up to tens of thousands of employee identities. But high-volume brands must handle tens — or even hundreds — of *millions* of customer accounts simultaneously. And modern consumers expect zero friction; an identity solution needs to scale "out" as well as "up" to meet this workload with little to no perceptible latency.

A recent Akamai study found that a two-second delay in web page load time increases bounce rates by 103%, and 53% of mobile site visitors will abandon a page that takes longer than three seconds to load.[1] So if your identity management system fails — or slows because it cannot handle the load — your conversion rates and revenue will likely suffer. Ironically, load peaks and increased customer traffic are typically caused by successful campaigns, meaning that a sluggish identity management system is actively working against deliberate and hard-fought business efforts.

> *A sluggish identity management system actively works against deliberate and hard-fought business efforts.*

Dedicated CIAM platforms like the Akamai Identity Cloud are architected to provide companies with maximum value from customer profile data. Such solutions enable seamless and frictionless customer experiences so that tasks like login, authentication, or preference management do not impede activity. Additionally, CIAM technologies address the critical need to secure personal data across public networks, as well as enable global businesses to comply with varied and frequently changing privacy regulations.

The following table outlines the primary differences between traditional IAM and CIAM — and their applications.

Traditional IAM	Customer IAM
Manage **employee identity** within a corporation.	Manage **customer identity** on digital, customer-facing, multichannel sites (web, mobile, IoT).
Users are **registered by their company,** with key profile data filled in by HR or IT.	Users **register themselves** and generate their own user-specific data.
Authentication against internal **directory services.**	Authentication against **public services** like OpenID and social media, as well as directory services and external credential verification services.
Users are known and captive: employees, contractors, partners. **Identity may be assumed.**	Users are **unknown** (until registration) and may create multiple and fake accounts. **Identity cannot be assumed.**
Workforce users are **more tolerant** of latency and poor performance because they often **do not have an alternative.**	Customers and prospects have **very low tolerance** for poor performance and have **many attractive alternatives.**
Scalable from **10s to 100,000s of users,** one identity each.	Scalable up to **100s of millions of users** with up to billions of consumer identities.
Traditional identity provider (IdP) is typically **one central internal IT system.**	**Many decentralized identity providers:** social login through Facebook, Google, LinkedIn, etc., as well as traditional login.
Many heterogeneous IT systems, on a **closed, corporate network.**	Many heterogeneous IT systems, **on public networks (Internet).**
Employee profile data collected for **administrative and operational purposes.**	Customer profile data collected for **highly critical business purposes** (transactions, marketing, personalization, analytics, and business intelligence).
Integration with **HR and ERP systems.**	Integration with a **broad landscape** of **marketing and sales automation** technology, **analytics systems,** and **security and compliance** solutions.
Management of personal data and user privacy/ preferences/consent happens only within a tightly **controlled, homogenous corporate environment.**	Handling of personal data subject to a **broad variety of privacy and data protection regulations** that require enabling users to view, modify, and revoke preference and consent settings.

Read "Build vs. Buy? A Guide for Customer Identity and Access Management" to learn more about CIAM solutions, or visit akamai.com/identitycloud to learn more about how Akamai's CIAM enables you to provide trusted digital experiences to your end users.

SOURCE

1) https://www.akamai.com/us/en/about/news/press/2017-press/akamai-releases-spring-2017-state-of-online-retail-performance-report.jsp

Akamai

Akamai secures and delivers digital experiences for the world's largest companies. Akamai's intelligent edge platform surrounds everything, from the enterprise to the cloud, so customers and their businesses can be fast, smart, and secure. Top brands globally rely on Akamai to help them realize competitive advantage through agile solutions that extend the power of their multi-cloud architectures. Akamai keeps decisions, apps, and experiences closer to users than anyone – and attacks and threats far away. Akamai's portfolio of edge security, web and mobile performance, enterprise access, and video delivery solutions is supported by unmatched customer service, analytics, and 24/7/365 monitoring. To learn why the world's top brands trust Akamai, visit www.akamai.com, blogs.akamai.com, or @Akamai on Twitter. You can find our global contact information at www.akamai.com/locations. Published 04/19.