okta

Decoding Customer IAM (CIAM) vs. IAM

Okta Inc.
301 Brannan Street, Suite 300
San Francisco, CA 94107

info@okta.com
1-888-722-7871

Decoding Customer IAM (CIAM) vs. IAM

The world of Identity and Access Management (IAM) is rarely controversial. But today, there is a battle brewing in how we—as an industry—talk about customer-facing use cases for IAM. Many are starting to refer to this as Customer IAM or Consumer IAM, both abbreviated as CIAM.

CIAM does have some unique requirements. But that does not mean that you must use a product that only focuses on CIAM. Okta's approach is to offer a broad IAM cloud service with a strong foundational platform and functionality that enables CIAM use cases—we believe ultimately a better long-term choice.

First off, what is IAM or CIAM?

If you're new to identity management software, here's a quick primer. Wikipedia says it is "the security and business discipline that 'enables the right individuals to access the right resources at the right times and for the right reasons.'" That is broad, and can cover almost everything in computing and IT.

For most apps, this looks like a database table that stores profiles and passwords. It might also have some permissions data. For more complex applications, or large scale deployments, packaged IAM software might be used that adds security and has pre-built frameworks to manage much more complex authorization, potentially across many applications.

Generally, IAM software can do this for many different use cases. Whether users are employees, and the authorization is based on a role in the organization, or the users are customers and authorization is based on loyalty membership status. The latter scenario gets us into the world of Customer IAM, or CIAM.

What's similar between CIAM and IAM?

In a nutshell, the answer is security, scalability, and high availability.

While it is certainly true that not all IAM solutions can handle the requirements for customer-facing (a.k.a. B2C) use cases, the core functional building blocks and protocols of IAM remain the same across areas like authentication, authorization, directory services and lifecycle management. A vendor that leverages a set of core IAM platform capabilities—such as OpenID Connect and OAuth support—across employee, contractor, partner, customer and consumer use cases can gain much more leverage than a vendor that is building proprietary technology to only serve one use case. Ultimately, that leverage leads to greater innovation and long-term success in the market—a long-term partner for your app development projects. You want to build on a foundation that is going to be around for the long haul.

IAM systems hold the keys to the kingdom, therefore regardless of the use case, the security of an IAM product is of paramount importance. The same security controls around an authentication or federation service apply regardless if the use case is employees federating to Office 365, customers federating to a support portal, or consumers federating between multiple hotel web properties of a large hospitality enterprise such as MGM Resorts International. Compromised employee accounts lead to hacking of internal systems, and compromised consumer accounts generally mean required public disclosure and a very bad PR day, even if you aren't publicly listed.

With scalability, we start getting into areas where specialized CIAM vendors may claim there are unique requirements. It’s true in a way. If you compare a specialized CIAM cloud service to a legacy on-prem IAM product, then yeah, your CIAM service must be able to handle a single customer with 10s of millions of identities. Many legacy on-prem products, or even general Identity-as-a-Service (IDaaS) products were not architected for that kind of scale. However, an IDaaS that serves all use cases and has thousands of customers with hundreds of millions of monthly authentications can easily scale to handle a new customer with millions of users. The argument here that CIAM is different becomes a moot point when your vendor is already running a multi-tenant cloud service as massive scale.

Finally, high availability is critical for all use cases. If your IAM is down, you can’t do business. Lost productivity of employees is enormous but your eCommerce site going down means lost revenue. Again, a modern cloud service with extreme redundancy delivers the high availability needed for all use cases.

So, then what’s the difference between CIAM and IAM?

Employee IAM systems are typically used to access internal services, and may include a user portal. The user base for CIAM services are generally website visitors or mobile app visitors. They expect to log into a website, and not go through a third party IAM vendor portal. To do that, CIAM products basically need to be developer driven and easy to use. If the CIAM provider doesn’t make it simple for a developer to register, login, and manage user accounts for their applications, they need to find a new provider. The IAM service needs to have a REST API that is granular enough to access all this functionality programmatically and provide modern developer tools, including SDKs for several programming languages and embeddable widgets.

CIAM requires more flexibility in authentication depending on the use case, from B2B customer federation to social authentication, to native authentication and even passwordless authentication. A modern IAM cloud service that is always at the cutting edge of authentication technology and protocols will have an advantage here and will have this full range of options available. With social auth, linking and unlinking of a social profile to a user’s core profile are important to consumer use cases in particular. A lot of the time, developers will want to customize the behavior of this social data, and the IAM system will need to have the flexibility to perform various user profile operations programmatically.

The authorization model for CIAM can be simpler than IT use cases. Customer roles are often more limited than the wide array of roles found internally within a large enterprise. In this area, an IAM system that has a robust enough authorization capability to handle enterprise scenarios can certainly handle CIAM authorization requirements so long as things like group memberships and user attributes can be modified programmatically.

Managing customer identities does require additional diligence for compliance with regulations, such as the EU General Data Protection Regulation (GDPR) which governs user privacy. For consumer-facing apps, this means having the right checkboxes in place for end user consent. But, the underlying IAM requirement is that it must securely maintain user data. This is a fundamental security requirement of paramount importance to all IAM use cases. The important decision here is to prioritize a platform that has the best underlying security. Handling checkboxes is easy enough to do in your code, and something you probably need to customize anyhow.

What about marketing analytics?

Some CIAM vendors started building their services at a time when the world of digital transformation was just getting started. They may have been visionaries, but their initial focus was more on tracking user behavior and enabling marketing analytics. Those are important requirements, but the market for those products has matured, and there are now plenty of options for marketing analytics for a CMO to choose from.

At the same time, IAM technology has not been standing still. New protocols like OpenID Connect and OAuth are enabling a modern app architecture (mobile or single page app that calls backend REST APIs) and microservices (server to server communication via API). Developers building these modern applications need an IAM platform that can secure their applications using these modern protocols. A modern IAM service is more likely to support all of these scenarios than specialized CIAM products that have a more marketing-oriented focus.

The big picture for enterprise IT

As you can see, within the world of B2C use cases for IAM, there are plenty of reasons why a market-leading IDaaS like Okta is really the best choice. Okta provides modern IAM functionality and is built from the ground up for the security, scalability and high availability requirements of customer use cases.

But the worlds of digital business and enterprise IT are not exclusively B2C. There are many shades of gray in use cases and requirements. Okta sees customers across this wide spectrum, from consumer apps, to B2B customer apps, to B2B partner collaboration, to supply chain integration, to support portals, to internal apps being built for remote workforce productivity, to seamless integration across customer-facing eCommerce sites, to connecting employees to SaaS apps, to providing lifetime access for alumni to university resources, to quickly enabling secure eCommerce and finally to helping organizations monetize their data and build a business on the API Economy.

We see CIOs, CDOs, CTOs and CMOs leading all types of organizations across this spectrum of use cases. And, the best way to handle this varied landscape is by bringing on an IAM partner that can handle this scope of breadth. Any other choice is extremely limiting to future innovation.

Read more about Consumer Identity Management for the CMO, CISO and CIO here:
https://www.okta.com/resources/whitepaper-consumer-identity-management-for-the-cmo-ciso-and-cio/