transmit security

IAM vs. CIAM

Why You Need a Purpose-Built CIAM Solution for Your Customers

With digital transformation exploding, security and customer experience has had to evolve in order to meet the needs and requirements of demanding customers. In an era increasingly characterized by competition, your customers have the power of choice. As customer experience and security have become critical factors for competitive differentiation, the need for a dedicated Customer Identity and Access Management (CIAM) service has become a strategic imperative.

	IAM	CIAM
User	Internal employees	External facing customers or partners

It's a common misconception that traditional IAM, which was built to support internal workforces, can be repurposed to serve customers. As we explain the very different needs of customers vs. employees, we'll explain why the restricted capabilities of IAM solutions will not suffice to serve and secure your customers.

CIAM solutions have been built to specifically handle the requirements for customer authentication, scalability, privacy and data regulations, the user experience, as well as integration. Whereas IAM solutions were created to support internal workforces, ensuring corporate security, employee productivity and to streamline access to work applications. Therefore, trying to bend traditional IAM solutions for your customers simply won't work.

The 6 Key Differences Between IAM and CIAM:

1. **User experience**
2. **Scalability**
3. **Devices**
4. **Channels**
5. **Integrations**
6. **Privacy and data regulations**

1. User experience

Difference	IAM	CIAM
User experience	Prioritizes security over user experience	Values balance between security and customer experience

The end users for IAM or CIAM solutions are distinctly different and therefore require a different user experience. An IAM solution won't serve your customers as it was built with a focus on security and control with much less focus on end-user experience and usability.

Customer-focused authentication services need to be designed to provide a balance between customer experience and security. Customers today demand easy and quick passwordless login experiences. If met with layers of friction that make them jump through hoops to access their own accounts — they will abandon the transaction altogether causing high customer churn rates and loss of business.

2. Scalability

Difference	IAM	CIAM
Scalability	10s to 100,000 of users	100s of millions of users

CIAM solutions must have the ability to seamlessly accommodate tens of millions of customers, if needed, without any decrease in response time or availability. IAM solutions were created for internal teams where there is a certain level of control over a finite amount of workers employed by the organization and therefore lacks the ability to scale to the extent that's needed for customers. Any business should (hopefully) be growing their customer base, which means you need a purpose-built CIAM solution that has the ability to scale with your business and meet all requirements.

3. Devices

Difference	IAM	CIAM
Devices	Through organizational-owned and managed devices	Through any device

In the internal IAM world, the IT department can impose tight control around all the user devices used in a very specific environment. In the CIAM world, there is no such control over any of the devices that a client may choose to use. A customer-focused authentication service should allow for authentication based on identity, which allows organizations to build up a portfolio of devices for a given, identified customer. The end client experience should be seamless and non-disruptive, regardless of the device/s being used.

4. Channels

Difference	IAM	CIAM
Channels	Access from a single corporate network or VPN	Access from any channel (Web, mobile, incognito browsers and offline channels)

Employees access internal work apps from fixed channels in order to carry out their specific job function. Whereas customers are typically accessing via public-facing channels to transact, make purchases, gain access to services and systems via different endpoints. A CIAM solution enables customers to be properly authenticated in order to securely and reliably engage with a business across any channel (web, mobile, incognito browsers or offline channels like call centers or kiosks) ensuring a consistent cross-channel experience.

5. Integrations

Difference	IAM	CIAM
Integrations	Static Identity provider (IdP) internal to the organization	Many decentralized identity providers

IAM solutions have a static IdP infrastructure that is typically inconsistent and not uniformly implemented across all channels. Purpose-built customer authentication services are designed to be flexible and integrate with any existing tools and technology an organization relies on such as marketing tools, payment solutions, internal IAM and more.

6. Privacy and data regulations

Difference	IAM	CIAM
Privacy and data regulations	Personal data managed internally	Personal data managed according to regulations

Given the two different sets of end users in IAM and CIAM solutions, data is managed and stored differently in each case. While internal data can be managed with an organization, customer data is subject to stringent privacy and data protection regulations. Customer-focused authentication services are built to ensure that the personal data of customers is protected and stored according to global regulations.

Summary

While it may seem like an easy fix to repurpose an existing IAM solution for your customers, it's clear that customers have a different set of needs and requirements compared to employees which is why an IAM service can't be used in place of a purpose-built CIAM service.

By implementing a passwordless customer authentication service, businesses can put an end to the age-old dilemma of security vs. customer experience. Businesses can now optimize both: effortless experiences and secure authentication. If done well, CIAM solutions provide strong and seamless identity experiences and are flexible to integrate with traditional IAM solutions, marketing tools, payment solutions and more.

Transmit Security's BindID is the only passwordless customer authentication service that allows customers to effortlessly access all channels with no passwords — anywhere. As the first app-less customer authentication service, BindID creates a frictionless identity experience without the need for complex changes at the web and application levels. Integration is flexible with existing IdPs and takes days while deployment can begin with as little as one developer ensuring your business reaps the benefits and value of BindID quickly.

Ready to implement the future of authentication?

Learn more about BindID today!

transmit security