transmit security

WHITEPAPER

The Divergence of Customer IAM and Workforce IAM

December 2022

IAM or CIAM: The Short Story

Identity and access management (IAM) solutions built for the workforce are simply not designed to meet requirements for customer identity and access management (CIAM). Even if your IAM solution works great for employees, it cannot satisfy customer needs like a CIAM solution that's built from the ground up for customers. The reason is simple: IAM and CIAM are distinctly different.

On the surface, the core building blocks of IAM and CIAM look the same: authentication, authorization and user management. But when companies try to consolidate the two in a single stack, they eventually discover it doesn't work.

One fundamental difference between managing customers and employees? Control. Companies manage and limit the devices employees use. But customers expect the freedom to log in with any device they choose. So if you try to meet customer needs with IAM instead of CIAM, multi-device support becomes your first challenge.

When applied to customer use cases, IAM breaks down — challenged by the sheer volume and variety of customer devices, operating systems, browsers and apps. It's just not built for customers.

Control of devices is merely one example. Many factors invoke major differences in the capabilities needed to serve and secure customers. We'll cover it all.

Executive Summary

In this white paper, you'll learn 8 key differences between IAM and CIAM — unique challenges that dictate different capabilities and design. Customers and employees have vastly different needs in terms of user experience (UX), scalability, support for multiple devices, browsers and channels, integrations, privacy and security.

First, we'll establish why analysts recommend separate workforce and customer identity solutions. Then we'll cover the top CIAM and IAM requirements that are either misaligned or completely incompatible. Throughout the paper, you'll find relevant insights and examples that demonstrate why repurposing IAM for customers is not the best approach.

By the end, you'll know what's needed in a CIAM solution to achieve better outcomes for your customers. You'll fully understand why a purpose-built CIAM solution is the only way to optimize the user experience and fortify security, while delivering what customers require.

Table of Contents

I. Why analysts draw a line between IAM and CIAM 4

II. Serving adjacent markets 4

III. 8 Key Differences Between CIAM and IAM 4

1. User experience 5
2. Scalability and reliability 6
3. Devices 7
4. Channels 7
5. Integrations 8
6. Privacy and data regulations 8
7. Identity verification 9
8. Fraud detection and prevention 9

IV. Only CIAM meets customer needs 10

Why analysts draw a line between IAM and CIAM

Analysts agree that repurposing IAM for customer use cases is a misguided approach based on common but flawed assumptions. A 2022 IDC report describes the outdated practice of using IAM for CIAM as, "an accommodation strategy where workplace identity solutions were being stretched to include consumers." IDC states, "Most [organizations] will replace such band-aid approaches within the next 18-24 months."[1]

The fact that IAM and CIAM serve different needs is not a new revelation. Back in 2020, Forrester wrote, "CIAM is no longer just an extension of general IAM capabilities..."[2] Since then, CIAM has benefited from rapid innovation that's led to stronger security and smoother customer experiences. By contrast, IAM vendors have remained focused on enhancements for employees, placing less emphasis on UX.

Gartner® reinforces this idea of divergent needs. According to a 2022 Gartner report, companies prefer to keep CIAM and IAM separate because doing so, "creates better separation along the lines of business, and each community has unique requirements."[3]

A 2022 IDC report describes the outdated practice of using IAM for CIAM as, "an accommodation strategy where workplace identity solutions were being stretched to include consumers."

Serving adjacent markets

Solving identity management challenges for two distinct user constituencies also requires different IT skillsets. CIAM falls in the realm of account protection, anti-bot, customer onboarding and know your customer (KYC). IAM is supported by privileged access management (PAM), identity governance and administration (IGA), secure remote access and other zero trust solutions for employees. The project teams, roadmaps and desired outcomes will range from divergent to conflicting.

8 Key Differences between IAM and CIAM

1. User Experience
2. Scalability & Reliability
3. Devices
4. Channels
5. Integrations
6. Privacy & Data Regulations
7. Identity Verification
8. Fraud Detection & Prevention

[1] IDC, *"IDC Analyst Connection: Why Passwordless Customer Authentication Should Be a Priority for CISOs,"* Jay Bretzmann, Program Director, Security Products, March 2022.
[2] Forrester, *"The Forrester Wave™: Customer Identity And Access Management, Q4 2020,"* Oct. 8, 2020, Andras Cser, Vice President, Principal Analyst.
[3] Gartner, *"5 Essential Ingredients of a Successful Access Management Strategy,"* ID G00759824, by analyst(s): Michael Kelley, Henrique Teixeira, Abhyuday Data, March 28, 2022.

1. User experience

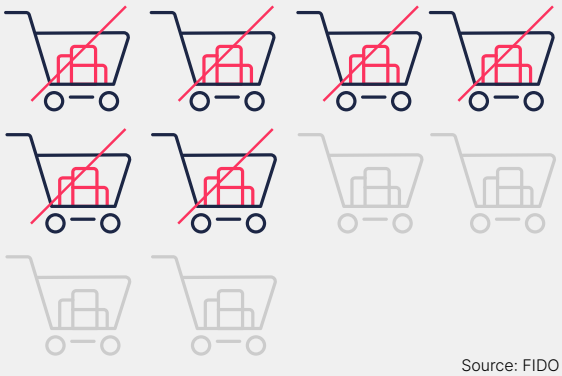
Differences	IAM	CIAM
Users	Built for internal employees and contractors	Designed for customers (B2C or B2B) and partners
User experience (UX)	Prioritizes security over ease of use and convenience	Eliminates the tradeoff between ironclad security and exceptional user experiences

When it comes to user experience, employees and customers have distinctly different expectations. Employees are more tolerant of friction, whereas customers are quick to drop off if it's too difficult or slow. According to FIDO Alliance, up to 60% of consumers have abandoned a transaction because they forgot their password or were asked to set up a new account.

Conversely, giving customers an easy, consistent UX boosts conversion rates. CIAM provides passwordless authentication methods designed for customers to easily register and log into accounts. If there are no passwords to forget, there are few if any lockouts. Plus, modern CIAM can assess a trusted customer with a high level of confidence and remove friction from their path. IAM lacks UX enhancements focused on customers.

60% of consumers

have abandoned a transaction because they forgot their password or were asked to set up a new account.



Source: FIDO Alliance

Branded UX

Workforce IAM is often handled as a third-party experience, "Secured by (insert vendor name here)." This is not acceptable for customers who prefer a consistent brand experience throughout their journey. Customers don't want to feel tossed to another realm. It's unsettling. An API-centric CIAM solution gives developers an easy way to customize the UX to reflect the company's own brand and keep customers in their domain.

More authentication options

Companies can make employees use any authentication method their IAM policy dictates. But customers demand a greater variety of options. They want the freedom to choose whether to log in with a social login, biometrics, magic links or one-time passcodes (OTPs). This also makes enrollment easier for new customers. Businesses that provide a range of authentication options boost customer registrations and retention rates.

Self-service UX

Employees can rely on in-house HR and IT teams to assist with onboarding, account setup and recovery. Customers, however, must be able to enroll and manage their own accounts. Born of necessity to support millions of customers, self-service is a key feature of CIAM. If customers have trouble registering or accessing their accounts, they will drop off or call support. CIAM optimizes the self-service UX to handle most customer needs — from account setup to recovery. IAM is simply not designed for this and certainly not at scale.

2. Scalability and reliability

Differences	IAM	CIAM
Scalability & reliability	Handles hundreds of thousands of employees	Manages up to a billion customers per day

IAM solutions are built to support thousands of employees, whereas CIAM must scale for millions or billions of customers and requests per day. Only a cloud-native CIAM service can handle high traffic volumes with no perceptible latency. On-prem or cloud-migrated IAM solutions will fall short. CIAM must also handle surges in traffic by more than tenfold in less than a minute. It's essential to support traffic bursts on Cyber Monday or after an ad blitz. IAM solutions do not need to account for this.

Performance impacts revenue

Customers won't suffer through delays or downtime. According to Google, when a page load time is delayed by 1 to 3 seconds, bounce rates increase by 32% and by 90% when the page load time takes up to 5 seconds. Companies can't afford sluggish systems or else conversion rates and revenue will decline.

Scalability and reliability are expected, baseline requirements of CIAM. To ensure availability and high performance 24/7, companies need purpose-built cloud-native CIAM services that can expand and contract with natural business fluctuations.

32% increase
in bounce rates when page loads are delayed by 1 to 3 seconds.

90% increase
in bounce rates when page loads are delayed up to 5 seconds.

Source: Google

3. Devices

Differences	IAM	CIAM
Devices	Devices managed by the organization, including personal devices with MDM policies	Any unmanaged devices, including outdated and unsecured devices

We've touched on this briefly. Devices are either part of the managed or unmanaged IT environment. In the internal IAM world, the IT department can use mobile device management (MDM) to impose tight controls on the devices employees use. An enterprise can also mandate software installation and updates on desktops and mobiles.

In the unmanaged consumer realm, there's little to no control over devices or software. A CIAM service must be designed to authenticate customers on any device and build a portfolio of supported devices for each individual. The ideal solution can bind additional devices to an account without asking customers to use passwords. It's the only way to optimize both security and UX.

Regardless of the device, the UX should be smooth and non-disruptive. CIAM is built to support hundreds of user flows, including a customer switching devices. Additionally, CIAM must support all browsers and cross-device types on any OS. This is especially important since each device may have different implementations of open standards such as Fast Identity Online (FIDO).

4. Channels

Differences	IAM	CIAM
Channels	Multichannel: corporate network, VPN, web, and mobile apps	Omnichannel: web, mobile apps, kiosks, call centers, stores or branches and smart home devices (IoT)

Employees access work resources from cloud apps, VPNs, corporate networks and portals. IAM usually provides single sign-on (SSO) across all of those channels, whether an 'internal' or cloud-based system. However, SSO is likely to render multichannel experiences in a way that feels fragmented or siloed. IAM solutions make it more difficult for various apps and channels to work together, making it harder to provide a seamless UX.

A disjointed UX may work for employees, but customers expect smooth, consistent omnichannel experiences. CIAM must enable easy access to mobile apps, websites (even incognito mode), brick-and-mortars, call centers and kiosks — with a single, unified customer identity. A customer service agent in the call center, for example, must be able to see the context and identity data of a customer who is calling about their online order. The customer's information must be shared from the website or mobile app to the call center. IAM is not designed to accomplish this.

Customers want easy access to all channels, digital or non-digital. When CIAM is optimized for thousands of user flows, customers can securely and predictably engage with all that a business offers. A streamlined omnichannel experience replaces the physical-to-digital patchwork created by IAM solutions.

5. Integrations

Differences	IAM	CIAM
Identity integrations	One or more Identity providers (IdPs), often in the form of LDAP directories	Many identity providers, including social and decentralized identity (DID) providers
App integrations	Light integration with many apps, typically with SAML, OIDC, SCIM or proprietary protocols	Tight integration with fewer apps, sites, chatbots, and other channels, often via APIs or OIDC and SAML
Integrator role	Identity administrator, focused on SSO and federated identity use cases for workers	App developer, focused on the end-to-end experience of customers and other external users

Most workforce identity solutions suffer from an inconsistent IdP infrastructure that lacks uniform implementation across channels. A contributing factor is that IAM requires more integration points with enterprise systems and legacy identity solutions.

IAM typically needs only light integration with workforce apps. Use cases such as SSO, user provisioning and user lifecycle management rarely require code changes in the supported applications. APIs that enable apps to talk to each other are rarely needed for IAM and are primarily reserved for custom-developed workforce applications.

In comparison, modern CIAM is far more flexible and able to easily integrate with existing or future technologies such as payment solutions, analytics, ecommerce and marketing tools, consumer apps and support portals. The end result is a more consistent UX.

CIAM also enables tighter integration with apps and channels, making life easier for everyone. Developers need APIs or microservices to build those capabilities into their apps or sites. They also need a consolidated CIAM solution to provide unified user management, which in turn improves the user experience — from authentication and authorization to self-service.

6. Privacy and data regulations

Differences	IAM	CIAM
Privacy and control of data	Personal data is managed internally, often by a central department	Personal data is managed via consent and under customer control

Internal employee data can be managed within an organization, while customer data is far more vulnerable. For this reason, securing private customer data is a fundamental CIAM requirement, built into customer identity management by design.

More advanced CIAM solutions deliver out-of-the-box compliance with complex privacy regulations, like the EU's General Data Protection Regulation (GDPR). Data privacy regulations are very detailed, requiring the right tools in place for consumers to provide consent, correct data inaccuracies and opt out with 'the right to be forgotten.'

7. Identity verification

Differences	IAM	CIAM
Identity verification	Hiring and onboarding verification with manual steps	Automated identity proofing and document analysis

When onboarding new employees, identity verification is often carried out manually through internal HR, IT and security teams. External identity verification services (e.g., credit checks, background checks and immigration status) are rarely performed in real time. It may be hours or days before the employee's identity is confirmed and cleared. With slow, manual identity proofing processes, workforce IAM is not built to detect and prevent bad actor account creation, which is a growing threat in the customer space.

Customer onboarding must be quick, if not immediate, to prevent fraudsters from opening fake accounts. Speed is important to legitimate customers too. Real-time, automated processes must establish trust in the user's true identity while minimizing time, effort and friction for your customer.

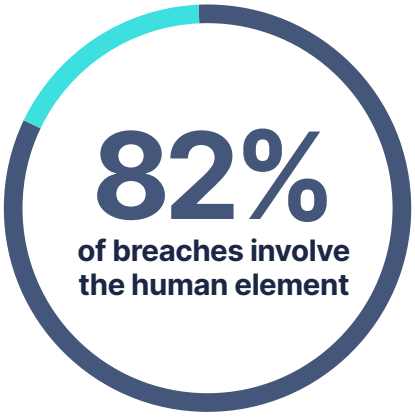
Identity verification built into a scalable, cloud-native CIAM platform is able to process a higher volume of requests rapidly. Robust features like selfies with liveness detection and vision AI for document verification of government-issued IDs are needed to improve accuracy.

8. Fraud detection and prevention

Differences	IAM	CIAM
Fraud detection and prevention	Security monitoring backed by physical security, internal controls, and segregation of duties	Passwordless authentication and fraud detection tailored to the customer journey, supported by continuous risk and trust assessments

Consumers tend to exhibit more careless behavior when it comes to passwords and are more susceptible to social engineering. According to the 2022 Verizon Data Breach Investigations Report, 82% of breaches involve the human element.

The report states, "A social attack gets the actor in the door, which emphasizes the importance of having a strong security awareness program." The problem with this solution is that training is only viable for employees, not customers.



Source: Verizon

True passwordless authentication

To protect against the growing problem of ATO fraud, companies need proactive security. The first step is to start eliminating the greatest risk: usernames and passwords. Only the most cutting-edge CIAM solution is able to remove customer passwords completely — from registration and logins to account recovery. Most organizations will migrate to true passwordless authentication gradually and can do this with a solution that offers a full range of passwordless options, including biometrics, magic links, SMS OTPs and social logins.

IAM solutions that offer passwordless options are not designed to extend password-free authentication to millions of customers on unmanaged devices. Even most 'passwordless' CIAM solutions don't offer true passwordless authentication. Your first hint is when a customer chooses to authenticate with a fingerprint or facial biometric and is then asked to create a password during enrollment.

Real-time risk and trust assessments

To address increasingly complex digital identity fraud, analysts recommend context-aware security that provides continuous adaptive trust (CAT). Real-time risk and trust assessments are needed to detect attackers invading accounts anywhere in the identity lifecycle — not just at login.

Traditional IAM solutions are not built for this. Only the most advanced CIAM services offer continuous trust profiling to identify and challenge account fraud in real time throughout the customer journey. When context-aware security makes access decisions at runtime, the UX also improves. If CIAM establishes a high level of trust, it can remove friction for a trusted customer by extending their session or reducing the need for MFA. The goal is better UX and stronger security.

Identity orchestration

Orchestration requires intelligent machine learning to evaluate the data, score the level of risk or trust and dynamically respond to activity anywhere in the user session. A powerful orchestration engine is essential to identify and mitigate risk signals the instant they appear.

CIAM solutions require embedded orchestration to automate thousands of customer identity journeys and track risk attributes across all customer-facing channels and the wide range of consumer devices. Orchestration that's built-in is much easier for developers to use.

By contrast, workforce IAM solutions support fewer users, devices and journeys — fewer variables and scenarios. There's just no need for such a powerful embedded orchestration engine.

Unified user management

Identity silos, fragmented user profiles and poor visibility weaken your security posture. For customers, a centralized identity store must be able to prevent account duplication and automatically link accounts across channels, devices and providers. Security policies must be flexible and extensible to handle all customer use cases. Only CIAM can provide the robust controls needed for all scenarios in an unmanaged customer environment. IAM is not made for this.

Only CIAM meets customer needs

Trying to bend workforce IAM solutions to meet customer demands simply doesn't work. IAM's limitations make it difficult to differentiate and keep pace with competitors who gain the advantages of modern CIAM solutions.

Companies that leverage cloud-native CIAM services benefit from continuous innovation designed to optimize CX, fortify security and cater to evolving customer needs. Purpose-built CIAM makes it easier to manage identities, authenticate customers, respond to risk, elevate trust and remove friction on the fly.

Customers expect extra functionality that employees don't. They demand smooth omnichannel experiences, self-service, privacy management, a consistent, easy UX and the freedom to use any device. Cloud-native CIAM delivers it all at scale. CIAM offerings built with developer-friendly APIs and SDKs speed time-to-market and make it easier to adapt.

Most importantly, a CIAM platform that is able to completely eliminate passwords significantly increases your security posture and streamlines the user journey. Passwordless MFA supported by modern CIAM services gives customers the option to register, log in and recover their accounts without ever using passwords. Gain the synergies and strengths of a complete CIAM platform.

Achieve 8 CIAM requirements:

1. Smooth customer experiences
2. Endless scalability and reliability
3. Support for all devices
4. True omnichannel journeys
5. Easy, future-proof integrations
6. Privacy compliance
7. Identity verification
8. Proactive fraud prevention and security

Transmit Security CIAM Platform:

- Passwordless & MFA
- Authorization & User Management
- Account Protection
- Identity Verification
- Embedded Orchestration

About Transmit Security

Transmit Security gives businesses modern tools to deliver secure and trusted end-to-end identity journeys. The Transmit Security CIAM Platform is security-first, developer-friendly and modern to provide customers with smooth experiences and prevent fraud across all channels and devices. Transmit Security serves many of the world's largest banks, insurers, retailers and other leading brands, collectively responsible for more than $2 trillion in annual commerce. For more information, please visit www.transmitsecurity.com.