UBISECURE®

Connecting Identity.
Transforming Digital Business.

The Difference Between Internal IAM and Customer IAM

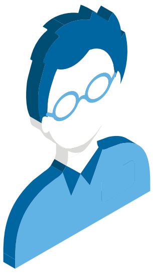
CAN TRADITIONAL IDENTITY AND ACCESS MANAGEMENT (IAM) SOLUTIONS BE USED FOR EXTERNALLY FACING APPLICATIONS?

Contents

Internal (employee) identities or external identities?

Most people dealing with digital identity are familiar with IAM (Identity and Access Management), with its main purpose being control of what employees can & cannot do, and to make sure that the organisation's systems are not accessible to anyone external. CIAM (Customer Identity and Access Management), is all about managing those external identities – be it customers, partners, organisations, contractors, things (think IoT) or even citizens. For a further refresher on what CIAM is before we go any further, **read this blog**.

Therefore, the most obvious difference between IAM and CIAM is this: are you managing internal employee identities (IAM – aka legacy/enterprise/internal IAM) or external customer/consumer identities (CIAM)?

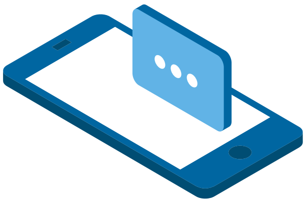


While it may not be immediately clear that this difference would call for drastically different platforms, these groups actually demand very different use cases. So let's dive into the usability differences between IAM and CIAM.

Use Cases

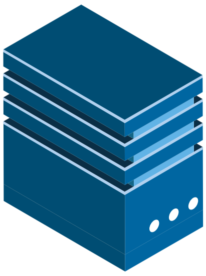
USER EXPERIENCE

The largest functional difference between IAM and CIAM is the user experience.



As a group, employees (usually) do what they are told and use the systems the employers provide for them – and are often trained to do so. The demands on an IAM system in terms of User Experience (UX) are important, but not as critical as in a CIAM system. The fact is that user experience for customers (or 'customer experience') is one of the key success factors in today's digital business. If you deliver a bad experience, your customers will leave unhappy, quickly moving to another service provider and taking their money - your revenue - with them. The same can't be said about employees (typically).

A good example of this is **Single Sign-On** (SSO). In an internal environment (IAM), the aim of SSO is to increase productivity and ease of use by enabling employees to log in to company applications without repeated password entry. For external identities (CIAM), SSO must draw on credentials that customers already possess, like a social login, business ID, Bank ID or digital identity issued by a



mobile network operator. This means that SSO must be offered in combination with federation to activate the benefits - namely increased convenience and enhanced customer experience.

In a typical IAM solution, there is usually only one Identity Provider, but with CIAM you will often have multiple identity providers from social logins to strong authentication, e.g. from financial institutions or government entities.

As you can see, CIAM is a much more diverse solution in terms of user experience.

PLATFORM FLEXIBILITY

Another difference between IAM and CIAM is in how the environments are treated. In an enterprise environment (IAM), changes to the system tend to be slower, and the systems are quite inflexible. It's not commonplace for such systems to constantly keep up with the latest trends and hop on board with every new technology.

This is in stark contrast to customer facing solutions, who do try to update system (like their CIAM) features on a regular basis, as it could be a way to stand out from the competition. Rigid enterprise IAM solutions are not built for these kinds of demands.

CIAM should enable quick changes to be made through simple configuration, rather than laborious and error-prone coding, and at the same time offer a variety of REST APIs that allow you to embed extra CIAM functions into applications.

TECHNOLOGY & SCALABILITY

Most of the basic underlying technologies for both IAM and CIAM are the same, which often leads organisations to believe that it's easy to adopt an enterprise IAM system to meet the demands of Customer IAM. This is because it's common to see the same technology specifications listed, including SAML, OAuth, OpenID Connect, LDAP, SQL, 2-factor authentication, REST API etc. Don't be fooled though – these are the basic, necessary building blocks for both IAM and CIAM, but what differentiates the actual solution is built on top.

Scalability is a big differentiator. There are all sizes of company, from a single person all the way up to a huge multinational organisation. This said, for any-sized company the number of employees rarely matches the potential numbers of consumers. For example, a customer-facing solution might have a million users, but nowhere near that many employees. Therefore, the scalability requirements for IAM and CIAM solutions are hugely different. Using an IAM solution for an external service with a substantial number of users is a recipe for disaster, as an IAM solution is not likely to scale to meet the requirements. This alone should be enough of a reason to not use an IAM solution where a CIAM solution is needed.

IDENTITY AND ACCESS MANAGEMENT – WHO DOES WHAT?

One more difference between IAM and CIAM is in who is managing the identities in the system.

Internal IAM is driven by the Human Resources team and the number of identities doesn’t usually fluctuate rapidly – adding or removing employees is a difference of few hundred per day in even the largest global organisations. Employees and their access credentials, as well as appropriate authorisations, are controlled internally according to position/job description/project memberships. When an employee’s role changes, the HR system and the provisioning engine will see that the information is passed on to the relevant internal systems. Once in a while, the IT admin has to reset a few passwords.

Compare this to an external system, where the number of users (hopefully) grows rapidly and the need to effectively manage these identities is crucial. For a customer-facing service, it is not enough to know who is accessing your online services, but also in which role/capacity they are entering, or which organisation they represent. One of the biggest mistakes an organisation can make when trying to get control over customer identities, is to start managing said identities themselves.

Externally, outsourced & tiered management makes much more sense.
It enables an organisation to attach (authorise) access privileges to their customers, or even to authorise access to an individual to represent a company, saving a lot of time and effort – and therefore money.

PRIVACY, TRUST & DATA REGULATION

Companies want to own their employee identities, at least to some extent. The concept of Bring Your Own Identity (BYOI/BYO-ID) might change this to some degree, but still the ownership of access privileges (roles, authorisations) should remain in the control of the company, not the user, for internal identities.

For external identities, trust and users feeling in control of their data is much more important, particularly in light of certain regulations (such as GDPR). CIAM can provide crucial transparency and the possibility for the end customer to manage, erase and export/transport their own data, providing the much-needed trust element.

Likewise, an online service provider should be able to trust the identities coming from the customer domain, and trust that any delegated access privileges are properly maintained within the customer organisation.

Internal IAM solutions are built around the idea that the company owns and operates the data of a user, in a customer-facing environment it should be the other way around and this again is reflected in the technical features of a good CIAM platform.

IAM and CIAM also have a difference emphasis on compliance. The driver internally is to comply to the organisation security policy, which should consider local regulations. Compliance to local regulations typically means that sometimes it might be necessary to enforce stronger authentication to grant access to sensitive information, and maybe use a credential which has a security level prescribed by the local legislation/regulation (e.g. NIST, eIDAS or PSD2). The biggest compliance obligation, especially in the EU area, comes from the General Data Protection Regulation (GDPR). Customer IAM solutions are therefore contrastingly designed to help organisations in areas such as consent management and management of user data.

REVENUE

The final difference is quite a simple one - does the solution bring revenue or at least save support costs? Internal IAM, with the emphasis on employees, isn’t intended to bring revenue to the company; it’s about internal operational efficiency and control. CIAM solutions concentrate on external users who generate revenue for your company. The first thing any business needs is to know their customers, in any digital process. The second is to create new digital processes that will improve customer experience and satisfaction, thus increasing revenue or creating completely new revenue streams through new digital services.

Conclusions

In summary, internal IAM is driven by the IT department, and their need to improve security and reduce admin costs. It is not designed to boost customer experience or convenience. It's also not designed to increase conversion and the creation of new digital business processes. It's about corporate control and providing internal employees necessary usability and access when using internal systems. It supports up to thousands of users.

CIAM, on the other hand, is driven by the business, embracing a diverse set of requirements. It's about empowering the customer and increasing trust. The goal is to grow existing business and to create new opportunities by forming business ecosystems with customers, subcontractors, partners and other stakeholders.

The underlying technology for both IAM and CIAM can be similar, but what differentiates the two will be the functionality built on top of those basic building blocks.

To find out more about how CIAM could work for your organisation, see **Ubisecure CIAM** - a proven, flexible Identity Platform to help you create secure, seamless, & trusted digital experiences for your customers.

The Difference Between IAM & CIAM

Customer Identity and Access Management

Identity and Access Management

External users (consumers, customers, partners, contractors, things, citizens)	MANAGE IDENTITIES FOR:	Internal users (employees)
Key driver to business success and differentiation	USER EXPERIENCE	Needs to meet a minimum standard – employees should have training
Normally several	IDENTITY PROVIDERS	Normally one
Needs to keep up technology trends and remain flexible	PLATFORM FLEXIBILITY	Often quite rigid, doesn't need new add-ons very often
Significantly more users than IAM, must be able to scale at a higher rate	SCALABILITY	Predictable number of users, typically significantly fewer employees than customers
Requires outsourced & tiered management	IDENTITIES MANAGED BY:	HR/IT – can be relatively manual
The external user should be in control of their own data	PRIVACY, TRUST & DATA REGULATION	The organisation owns and operates the data of a user
May bring in revenue through new digital services, or at least saved support costs	REVENUE	Not designed to bring in revenue

About Ubisecure

Ubisecure is a pioneering European b2b and b2c Customer Identity & Access Management (CIAM) software provider and cloud identity services enabler dedicated to helping its customers realise the true potential of digital business. Ubisecure provides a powerful Identity Platform to connect customer digital identities with customer-facing SaaS and enterprise applications in the cloud and on-premise. The platform consists of productised CIAM middleware and API tooling to help connect and enrich strong identity profiles; manage identity usage, authorisation and progressive authentication policies; secure and consolidate identity, privacy and consent data; and streamline identity based workflows and decision delegations. Uniquely, Ubisecure's Identity Platform connects digital services and Identity Providers, such as social networks, mobile networks, banks and governments, to allow Service Providers to use rich, verified identities to create frictionless login, registration and customer engagement while improving privacy and consent around personal data sharing to meet requirements such as GDPR and PSD2.

Ubisecure is accredited by the Global Legal Entity Identifier Foundation (GLEIF) to issue Legal Entity Identifiers (LEI) under its RapidLEI brand, a cloud-based service that automates the LEI lifecycle to deliver LEIs quickly and easily. The company has offices in London and Finland.

UBISECURE®

www.ubisecure.com
sales@ubisecure.com

UBISECURE UK
The Granary, Hermitage Court
Hermitage Lane, Maidstone
Kent, ME16 9NT, UK

UBISECURE FINLAND
Vaisalantie 2
FI- Espoo, 02130
Finland

UBISECURE SWEDEN
Blekholmstorget 30 F
111 64 Stockholm
Sweden

UBISECURE DACH
Franz-Joseph-Str. 11
80801 Munich
Germany