Introduction to Customer Identity and Access Management

By Ian Glazer

Table of Contents

Abstract

Customer Identity and Access Management (CIAM) refers to the processes and technologies that facilitate secure interactions between individuals and organizations. In particular, this article focuses on those that secure digital interactions. Whether the organization is in the public or private sector, the need to interact digitally is essential in this day and age – regardless of whether those interactions are to transact commercially, access social services, attend an online class, etc. While CIAM shares some concepts and technologies with workforce IAM, the two are sufficiently distinct to warrant further investigation. This article compares and contrasts the two while highlighting the unique challenges and opportunities inherent to CIAM.

Introduction

Customer Identity and Access Management (CIAM) represents one of the most notable opportunities for identity professionals to shine. Through CIAM, identity professionals can help organizations reduce costs and reach new customers. For commercial entities, this means growing both the top and bottom lines. With these wide-ranging opportunities, CIAM is different from workforce IAM. CIAM presents IAM professionals with new challenges, vocabularies, processes, and requirements – all of which serve to ensure that individuals can interact with organizations easily and securely.

Terminology

Many of these terms have been sourced from "Terminology in the IDPro Body of Knowledge."[1]

Term	**Definition**
Authentication	Authentication is the process of proving that the user with a digital identity who is requesting access is the rightful owner of that identity. Depending on the use-case, an 'identity' may represent a human or a non-human entity; may be either individual or organizational; and may be verified in the real world to a varying degree, including not at all.[2]
Authenticator	The means used to confirm the identity of a user, processor, or device, such as a password, a one-time pin, or a smart card.[3]
Authoritative Source	The system of record (SOR) for identity data; an organization may have more than one Authoritative Source of data in their environment.[4]
Authorization	Determining a user's rights to access functionality or resources within a computer application and the level at which that access should be granted. In most cases, an 'authority' defines and grants access, but in some cases, access is granted because of inherent rights (like patient access to their own medical data).[5]
Consent	Permission for something to happen or agreement to do something.[6]
Customer Identity and Access Management (CIAM)	CIAM is the field of IAM that focuses on the Registration, Authentication, and Authorization services for an individual or entity receiving or purchasing services from an organization.
Credentials	In the context of CIAM, credentials are how individuals authenticate themselves to an organization's CIAM system
Credential Stuffing	An attack in which an adversary tests lists of username and password pairs against a given CIAM system.
Identification	Uniquely establish a user of a system or application.

Identifier	An identifier is a means by which a system refers to a record (at the most abstract levels.) In this case, it could mean the string that a person provides that “names” their use account.
Lifecycle	In the context of CIAM, lifecycle refers to the stages that an individual or entity might experience over the course of their relationship with an organization, beginning with the formation of a relationship (such as being hired into an organization or signing up for service) and ending with the severance of that relationship (such as termination or closing an account)
Passwordless	Any means of authenticating a user account that does not require a static stored shared secret. Techniques include one-time passwords and passkeys.
Policy Store	A repository that houses configuration information for the CIAM system and serves as an Authoritative Source for that information. For example, OAuth token Lifecycle policies or Authorization policies.
Preferences	Choices that individuals or entities make in administering the relationship they have with an organization. These choices may include topics of interest or approved communication methods. Often, Preferences are stored with Profile information.
Profile	A collection of attributes about an individual. The individual may provide it directly, or the organization may gather it indirectly.
Progressive Profiling	A technique to reduce customer friction by gathering Profile, preference, and Consent information over time (when needed) rather than all at once.
Registration	The creation of a relationship between an individual and an online system that is initiated by the individual and results in the creation of a user account or Profile.
Workforce IAM	The application of IAM sub-disciplines such as access governance, authentication, and Authorization for employees as opposed to the applications of such disciplines for customers.

Acronyms

ATO	Account Takeover
B2B	Business-to-Business
B2C	Business-to-Consumer
B2B2C	Business-to-Business-to-Consumer
CIAM	Customer Identity and Access Management
CRM	Customer Relationship Management
DAU	Daily Active Users

IAM	Identity and Access Management
IDP	Identity Provider
JML	Joiner, Mover, Leaver (used in Workforce IAM)
MAU	Monthly Active Users
OTP	One-Time Password (or Passcode)

What is CIAM?

Over the last decade, organizations in every industry, sector, and geography have sought to provide services online. Trading under the name "digital transformation" and "digital engagement," organizations have pushed to interact with people through websites, mobile apps, and connected devices to reach new customers, offer more valuable services, and lower service delivery costs. The COVID-19 pandemic further amplified the need for all organizations to have a robust online presence.

But for people to interact with these online services, they need a means to safely and efficiently identify themselves to those services. How organizations offer sign-up and sign-in services is the core of CIAM.

What Does the "C" Stand for?

Digital identity practitioners love abbreviations, but this can cause confusion. The C in CIAM is just such an example. Despite the assertions of Sesame Street's Cookie Monster,[7] C stands for more than just cookie: in this context, it also stands for customer, consumer, or citizen. The typical usage is customer, but that may have inaccurate implications. For example, it may imply that CIAM systems only apply to contexts in which the individual pays for a service from an organization. This is not the case.

All organizations need CIAM to interact with people who could or do use their services. Such organizations include public sector agencies that deliver on behalf of citizens and residents, universities that empower students and researchers, and non-profits that serve communities and engage with supporters. And yes, this also includes for-profit businesses that sell goods and services.

Why CIAM is Important

CIAM enables organizations to reach more people and offer more valuable services. In widening reach, CIAM provides a way for organizations to expand their total addressable market while reducing service delivery costs. As a result, an effective CIAM program improves both the top line and the bottom line of organizations. These benefits are equally relevant for public sector entities that aim to reach more citizens, deliver more social services, and reduce taxpayer costs. While traditional workforce IAM is an essential cost-center focused on efficiency, security, and compliance requirements, CIAM can be seen as a profit-center.

How CIAM Differs from Workforce IAM

Some readers may be more familiar with the primary goal of workforce IAM to deliver the right access to the right people at the right place and time. To meet this goal, IAM practitioners deploy, for example, automated user provisioning, birthright policies triggered by a small number of central authorities, access request systems, and authorization policies governed by a central Identity Provider (IDP).

CIAM has a different goal. It supports organizational digital engagement efforts to deliver the right experience (in addition to access) to the right people at the right place and time. In collaboration with Chief Information Security Officers, Chief Digital Officers seek to ensure engaging, personalized experiences at every touchpoint during an individual's relationship with a given organization – and doing so securely.[8] With this goal in mind, CIAM professionals deploy different tools, including just-in-time user provisioning, social sign-on, and user registration. This article will continue to draw out further differences and similarities between workforce IAM and CIAM.

B2C vs B2B vs B2B2C

Readers may have seen references to business-to-consumer (B2C)[9] and business-to-business (B2B). In some cases, CIAM focuses primarily on B2C use cases with a secondary focus on B2B. CIAM technology offerings tend to help an organization offer sign-up and sign-in services optimized for an individual to interact with an organization. Secondarily, a CIAM technology offering might also provide B2B service to facilitate trust between two different organizations, enabling employees from one to access services from another. Knowing whether a problem or project relates to a B2C or B2B context significantly impacts the requirements.

There is a third B2* permutation: business-to-business-to-consumer (B2B2C). In this case, a technology service provider offers CIAM capabilities to multiple organizations that use those services to engage with their customers. In B2B2C scenarios, delivering CIAM services with the correct brand experience is critical. This experience consists of everything, from the logos and colors on the screens to the URLs that an end-user would see. Instead of the upstream service provider brand, the customer should always see the brand of the business with whom they have a direct relationship.

(The primary focus of this article is on B2C use cases, though it will highlight some notable differences in B2B use cases. Unless otherwise specified, the reader should assume examples and guidance are oriented towards B2C use cases.)

The Stakeholders and Measurements

Successful digital engagement requires a successful CIAM strategy. Successful digital engagement also requires a very different collection of stakeholders than workforce IAM professionals might be used to. This expanded set of stakeholders has a new vernacular

and a different set of goals from which the CIAM practitioner needs to derive requirements. Furthermore, the varied perspectives of these audience members require practitioners to translate the benefits and value of CIAM to different contexts. The stakeholders in digital engagement include marketing, digital, sales and distribution, product, privacy, legal, and customer service. In addition to these players, CIAM teams will also see a more familiar face: security.

A shared digital engagement mission often includes the following goals:

- **Increase Engagement**: Increase the number of people actively using whatever the organization produces, be they physical, informational, or digital
- **Reduce Friction**: Reduce the number of steps and tasks that stand in the way of an individual getting to use whatever the organization produces
- **Build Loyalty**: Ensure repeat use/engagement through products and customer service

CIAM practitioners partner to conduct this mission against a backdrop of security, appropriate data usage, and operating costs.

The stakeholders sharing this mission use different metrics than workforce IAM practitioners. In digital channels, engagement is often measured by the number of:

- Unique visitors to an organization's site or app
- Page views
- People actively using the products and services within a given time frame, often referred to as "Monthly Active Users" (MAU) or "Daily Active Users" (DAU)
- Unknown visitors converting to either sales or registered accounts, known as "Conversion Rate."

Further to these goals, building loyalty comes with its own set of measures, including customer satisfaction, net promoter score, and customer lifetime value. While CIAM teams might not be directly involved in gathering these metrics, they will certainly hear about it if customer satisfaction dips because of (or is inherently limited by) an onerous login process.

Although people recognize friction when they see it, defining and quantifying it is more difficult. Often, CIAM teams hear statements such as "It's too hard to register for an account" or "It's too many clicks to get to the content." Abandoned account sign-ups, the number of screens or fields to register, failed logins, support calls, and even password reset rates are all indicators of friction. The organization's need to reduce friction in its sign-up and sign-in flows demands a careful, iterative design process that finds (and seeks to eliminate) the places where people get stuck or give up in frustration. To add to the challenge, security and privacy stakeholders often seek to introduce *more* friction to thwart

automated attacks, ensure regulatory compliance, and avoid harmful user choices. The balancing act for stakeholders and the implementation team is not simple.

Authorities, Lifecycles, and Administration

CIAM underpins digital engagement and enables organizations to offer products and services via digital channels as a sole channel or in addition to existing brick-and-mortar channels (e.g., phone or a physical location). This difference in context means that the sources of authoritative information about end-users, the lifecycle of those users, and the methods by which those users are administered differ from workforce sources, cycles, and techniques.

Authoritative Sources

In the workforce context, an IAM system can usually rely on human resource systems or databases to be authoritative about who is an employee, their demographics, and their roles and job responsibilities. In CIAM, no such system is consistently present and reliable. While a customer relationship management (CRM) system might exist and possess customer profile data, it is not definitive. Similarly, an eCommerce system, if present, might maintain shopper profile data that is, again, not definitive. While either might have information about an individual, neither is authoritative: the individual is the authoritative source of information. After an individual creates a user account via the CIAM system, their resulting profile is (ideally) linked to CRM, eCommerce, Customer Support, etc., using one or more unique, verified identifiers such as email, phone number, and account number. [10] One notable exception is the B2B use case in which a CRM system might be considered authoritative (about which individuals work for which organizations).

Lifecycles

The user lifecycle in CIAM may seem different from what the reader is familiar with if they come from a workforce background. In workforce scenarios, the reader might be familiar with the concept of “joiner”, “mover,” “leaver” (JML), which reflects how a new employee joins the organization, changes roles (aka moves) throughout their career, and eventually leaves the organization. Such events are recorded in authoritative sources, like a human resource system.

However, the lifecycle for a customer looks quite different: they register for an account and, ideally (from the organization's perspective), never stop using that account. There is often no event from an HR system equivalent to trigger user account creation, change, or deletion. CIAM and associated authorization systems will often query CRM systems to pull information such as “Is the person a Gold Level member?” to determine access to downstream resources at the precise time the resource is accessed. In this regard, CIAM tends to be a world of just-in-time authentication and authorization instead of admin-time, in which user accounts and associated resource access are set up in advance.[11]

Some readers might ask, "If my existing customers' profiles exist in the CRM, can we use that to automate user account creation and distribute the credentials?" Do not do this. In a post-GDPR world (referring to the European Union's General Data Protection Regulation[12]), such an action will be interpreted as a violation, i.e., signing the individual up for an account without their consent. The individual is in control in B2C CIAM use cases; thus, actions need to be taken just-in-time, not *a priori*.

Administration

The theme of individual control continues into the topic of administration. The individual can and must be able to control and update the information they have provided to the organization, including name and contact information.[13] The data they must be able to control includes their password, if they have one. The organization might also grant workers similar abilities in their customer service organization to help individuals who reach out to contact centers. These capabilities come with significant security risks, and the reader is encouraged to read IDPro's BoK article entitled "Managing Identity in Customer Service Operations."[14]

In B2B use cases, the organization not only needs to provide user accounts and associated access to their business partners but also enable specific people within the partner's organization to manage their own users' access. Known as "Delegated Administration," this capability looks similar to granting different people within the organization the ability to administer users in other parts of the organization.

Profile, Preferences, and Consent

CIAM systems are often used to enable information gathering, including demographic data (such as age and address), contact preferences (if at all), and their approved uses for any data collected. Organizations use this information to personalize experiences, deliver goods and services, as well as use data the individual shares for business purposes.

Profile

A profile is a collection of attributes about the individual. The individual may provide it directly or indirectly, such as in social sign-up and sign-in experiences. This information enables personalized user experiences, such as using an individual's first name on the welcome screen of a mobile app. This personalization can also include providing specialized offers based on, for example, where they live.

The profile can also include information that businesses require for essential processes. For example, the individual might provide their street address so the organization can send physical goods to their home. In some cases, organizations' business processes include evidence that an individual is old enough to use the service itself. For example, an online gambling site may have specific regulatory requirements to verify that an individual is over 18. Alternatively, the organization may be required to gather and verify legal identity information from the individual. For example, a bank must verify an individual's legal

identity to adhere to “Know Your Customer” (KYC) regulations that prevent money laundering and other financial crimes.

Preferences

Commonly, individuals are not interested in every possible product and service an organization offers; similarly, the individual may prefer one contact method over another (e.g., text message vs. email). This kind of choice is captured in the form of preferences. Preferences may include topics of interest related to an organization’s offerings (e.g., sporting goods, elder care, etc.), approved communication channels (e.g., “none” or “email but not text messaging”), and frequency of communication (e.g., monthly emails not daily.) While this information is not strictly required for business processes, it vastly improves the individual’s experience with the organization.

Consent

In response to questionable practices, an increasing number of regulators require that an individual actively and positively chooses to interact or share data with an organization. This proof is referred to as consent. Said differently, an organization often needs to record evidence that the individual asserted that they want to interact with the organization. Organizations often bundle this consent with an acknowledgment that individuals agree to terms of service and conditions of use. The presentation of this choice must be clear: this means visible and accessible as well as understandable. The granularity of consent requirements varies from region to region and industry to industry. The cadence with which an organization must gather consent information may also differ. Organizations often bundle the gathering of consent with an acknowledgment that individuals agree to terms of service and conditions of use. Understanding the consent requirements for any use case or jurisdiction is critical.

Progressive Profiling

The aggregate of profile, preferences, and consent data can be considerable. Organizations are not advised to gather all this information at any one moment, like when the individual signs up for a new account or attempts to checkout during an e-commerce transaction. Doing that would ask the individual to fill out too many fields and screens. It puts too many hoops between them and the goal they set out to achieve. In e-commerce scenarios, too much friction can lead to dropouts when individuals give up and move on to a competitive offering. In the CIAM world, friction is akin to inefficiency in workforce user provisioning: it is the enemy.

To combat this enemy, organizations can employ a technique by which they ask for profile, preference, and consent information over time and not all at once. They can ask for information, such as shipping address, at the time they need it instead of when the individual first arrives at the website or service. Known as “Progressive Profiling,” this technique reduces friction by spreading it out across interactions and over a longer period.

Profile Versus Credential

It is essential to keep clear in one's head the relationship and separation between a profile and a credential. Where a profile is a collection of attributes related to an individual, the credential is the means by which the individual identifies themselves to the website or app with a certain degree of certainty. In its simplest and most basic form, a credential is a username and password combination. On the other hand, a profile can have a very rich data structure composed of many attributes of different types. Because the purpose of these resources differs, the techniques needed to manage and protect them are different. At the highest levels, profile data is within the domain of data management and privacy professionals and their tools, while credentials are squarely in the domain of identity and security practitioners and their associated tools.

This distinction leads to a critical question about ownership within the organization. In this context, do not think of ownership with a legal mindset: we are not discussing ownership like one discusses owning a candy bar. In this context, ownership is a conversation about who, within an organization, is responsible for gathering, managing, protecting, and making use of this data. Although a CIAM technology stack may be able to obtain and store profile data, it does not mean that a) the identity team owns the profile or b) that the profile is the only form or representation of a customer within the organization. Consider that organizations will have many "pictures" of a given customer in systems such as the CIAM, customer support, marketing, and operational systems. Profile data is legion within organizations.

Why dwell here? Previously, this article discussed the various teams involved in a digital engagement program. These teams will claim, with good reason, that they own the customer profile and are thus responsible for gathering and managing it. They are not wrong in this regard, and their requirements, as foreign feeling to identity teams as they may feel, are just as valid as security or regulatory requirements with which an identity team may be more familiar. Partnership here is a must: calories spent debating ownership are better applied to building better experiences for the individual.

In the case of credentials, however, these fit in the CIAM domain and are the subject of the next section.

Credentials

Where profiles are information shared by individuals to help organizations personalize their experience, credentials are how those individuals make themselves known to an organization. Said differently, credentials are how individuals authenticate themselves to an organization's CIAM system and, thus, the entire digital landscape. Generally speaking, there are two parts to a credential:

- An identifier
- An authentication mechanism

Identifier

As the name implies, identifiers are the "name" an individual uses to tell an organization's CIAM, "I am HappyCustomer01@my.mail." More often than not, email addresses and phone numbers are used as identifiers. Using them has a side benefit: it cuts down on the information an individual has to provide as a part of their profile. Because organizations want to communicate with the individual, they often ask for their preferred email address or phone number. Using email and phone as identifiers allows them to serve double duty as both an identifier and a communication channel. Importantly, the identifier is the username in the classic username and password combination.

While seemingly straightforward, identifiers and the handling thereof can be far more complicated than expected. It is strongly recommended that the reader reviews the IDPro Body of Knowledge article "Identifiers and Usernames."[15]

Authentication Mechanisms

Having provided a valid identifier, the individual is prompted to authenticate. The most well-known and entrenched are passwords, but others exist. Increasingly, these alternatives to passwords are becoming popular.

Passwords and One-Time Passwords

The most familiar authentication mechanism is the password. Passwords are shared secrets, meaning that both the individual and the CIAM system maintain the secret to verify that the individual is who they claim to be.

Passwords are the somewhat unfortunate bedrock upon which authentication has built its castle. Refer to the IDPro Body of Knowledge "Authentication and Authorization" for more on authentication.[16] Read the National Institute of Standards Special Publication 800-63B, section 5.1, to receive guidance on good practices for password composition and treatment.[17]

Because individuals' memories are fallible, organizations need to provide means for individuals to prove they are who they claim to be and then set a new password. Known as either account recovery or password reset, these processes are often overlooked and become attack vectors for adversaries. Neglecting these processes leads to difficult user experiences, constrains account protection, and increases customer support interactions. Failing to protect password reset processes can lead to account take-overs in which an adversary exploits a weak password reset process, sets a new password known to them rather than the account owner, and takes control of the account and its associated resources (e.g., emails, photos, files, social media accounts, bank accounts, etc.). Readers

should review the IDPro Body of Knowledge article "Account Recovery" for more information.[18] Additionally, it is strongly recommended that identity professionals spend time at the *beginning* of a CIAM project considering their account recovery processes across all channels (web, mobile, phone, etc) through which their organization will interact with individuals.

Shared secrets are not the only game in town. Increasingly, organizations are opting for one-time passwords (OTP). These are shared secrets with a limited lifespan and, as the name implies, can only be used once. Common examples of one-time passwords include sending a code to a mobile phone or email address. OTPs can have a better user experience; they do not require the individual to remember or store a password, and operating systems and browsers perform better at automatically filling in OTPs when they detect them. However, these benefits can be outweighed by the risks of phishing and interception. One thing to note, at this time, OTPs are often considered part of the larger "passwordless" authentication world: this is both confusing and inaccurate.[19]

Passwordless

Passwords and OTPs are not the only methods that a CIAM team can choose to deploy. Increasingly, technology providers are offering truly passwordless offerings. These offerings generally rely on a combination of public key infrastructure (shielded from the user), trusted computing mechanisms for storing those keys, and a dedicated app or browser or operating system-provided user experience to strongly assert that the individual is who they claim to be. From the individual's perspective, they either provide a biometric (such as TouchID or FaceID Apple-centric environments) or interact with a mobile app protected by biometrics or PIN. These interactions "unlock" access to the site or service.

The interest and popularity of passwordless approaches are partially fueled by the acknowledgment that passwords are poor solutions for individuals and organizations. More recently, the industry is adopting the WebAuthn standard (and associated standards). WebAuthn is a standard overseen by the W3C,[20] and its implementations can be found in most modern mainstream browsers and operating systems. Most recently, agreements on how the cryptographic material needed to power WebAuthn-based passwordless authentication can be synchronized between devices and browsers to facilitate an "enroll once, use anywhere" end-user experience, known as passkeys, have driven even more excitement and interest.

Challenges still exist with passwordless approaches, including how an organization should trust an individual they have never seen before and how an individual can get back to their user account in case of a lost device. Additionally, passwordless approaches often require modern smartphones or computers, which are unavailable to many. But that said,

passwordless approaches, especially those that are standards-based, represent a path from passwords to something materially stronger with an improved user experience.

Social Login

IAM professionals may choose to augment their password and passwordless sign-on offerings with social sign-up and sign-on. In this case, an individual identifies themselves to the organization by first authenticating to another service, such as a social network or email provider. In this case, the organization doesn't hold any secrets (e.g., passwords) from the user but instead records that the associate user account needs to be authenticated by the external identity provider (the social network, email provider, etc.) Organizations can not only use a social credential to authenticate an individual but also use the information that the external identity provider provides to create or pre-populate a profile for the individual; this is social sign-up.

While social sign-up can be very appealing, it does come with some downsides. It is inherently exclusive in providing a different kind of login experience to people who are members of a specific social network. While claiming hundreds of millions of members, offering a specific social network may not feel that exclusive; individuals will likely have strong preferences. This means that organizations often offer login via multiple social networks and email providers. In turn, this leads to the NASCAR problem in which a site's login page starts to resemble a NASCAR car festooned with different logos. Leaving the NASCAR problem aside, even having one social credential option means the organization is putting another organization's brand on theirs. These choices, to some, can be polarizing at the worst and off-putting. There is an inherent assumption that the external identity provider can protect secrets and offer recovery options that are superior to what the organization can do itself. That is often a reasonable assumption, but it is worth considering before deploying such offerings.

Some organizations may require higher assurance about individuals for regulatory or business process reasons. Such organizations can deploy a user experience similar to social login – one that relies on an external identity provider and is presented as a set of choices on sign-up and sign-in screens. The key difference is that the external identity provider is a government or financial sector service. This topic area is robust and requires a more advanced examination in a future Body of Knowledge article.

Functions and Components

Functions

At their core, CIAM systems perform at least user registration and authentication. User registration allows an individual to create an account and establish a credential. It may also include collecting profile, consent, and preference data. User authentication validates the credential the individual provides when they access the organization's apps and services. It is important to note that CIAM systems usually do not trigger a user provisioning process

after establishing a new user credential. However, this may be more common in utilities or B2B and B2B2C scenarios. This stands in stark contrast to more traditional workforce IAM scenarios in which the detection of a new employee in an HR system often triggers user provisioning workflows. CIAM more often relies on the just-in-time (JIT) creation of user accounts brokers by single sign-on during run-time instead of user provisioning at admin-time.

Additionally, CIAM systems often provide two more capabilities: single sign-on and OAuth token management. The single sign-on capabilities offer individuals a seamless experience as they navigate across the different websites and services an organization provides. For example, this ensures that when the individual logs into the eCommerce site to purchase something, they can access the customer support site without logging in again. The OAuth token management capabilities are used to issue OAuth tokens to the individual and their apps. These tokens are used to access APIs that the organization provides. The individual may not be aware that they have been issued tokens and are using them in many interactions with the organization's goods and services, but identity professionals and their security peers need to be aware of this – if only to take steps if an individual's app or device is compromised. In this case, revoking the issued token(s) will prevent further access to the compromised app.

Finally, the CIAM system may provide some form of orchestration service. This service can build the user experience the individual sees as they register and integrate third-party services into user experience flows. Such integrations can further enhance the individual's experience, perform progressive profiling, or even add higher assurance that the individual is who they claim to be.

Components

While different technology suppliers' specific architectures and components' names will vary, they generally share the same notional architecture.

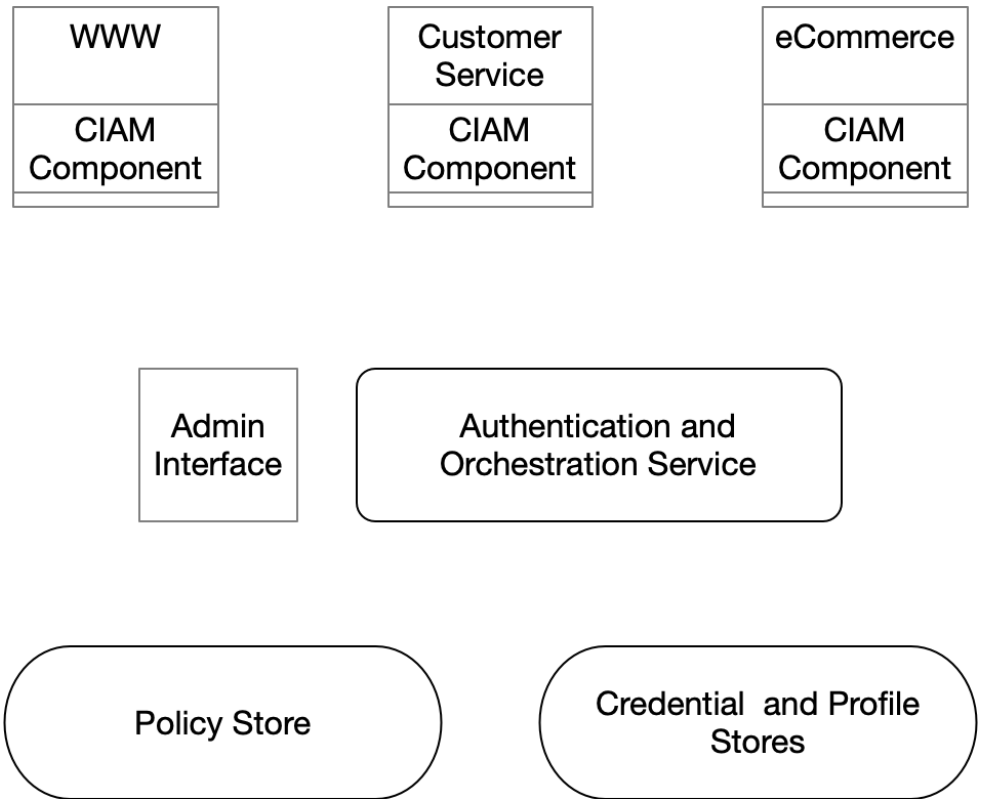

Figure 1: Components of CIAM Architecture

Credential and Profile Stores

At a minimum, a CIAM system provides a credential store or integrates with an existing one. This store is where user accounts are maintained and shared secrets, if any, are housed. The implementation of the credential store can range from a relational database to an LDAP directory to a NoSQL database and beyond.

The CIAM system may have a profile store that could contain profile, preference, and consent data. Profile storage, however, is not a strict requirement. Consider that organizations often centralize this kind of information in a customer data platform or marketing automation system. In such cases, the CIAM system will have the minimum amount of information needed for personalization and communication (e.g., a verified email address used to facilitate password resets) while the rest of the profile information is stored elsewhere.

Policy Store and Admin Interface

This repository houses configuration information for the CIAM system and serves as an authoritative source of that information. Such information could include single sign-on configurations, OAuth token lifecycle policies, and user registration workflow definitions. It

might also house authorization policies that govern which resources an individual can access. The artifacts in this repository are managed by the Admin Interface or via changes to configuration files. The Admin Interface, if provided, presents a user experience where identity professionals can configure and manage the CIAM system.

Authentication and Orchestration Service

This service can serve multiple roles. At a minimum, it authenticates credentials. It can also manage the user's session and broker single sign-on. It may act as an OAuth authorization service. Lastly, it can act as an orchestration service. In this final context, it relies on policies in the policy store to determine, for example, what information must be gathered from an individual as they register, when to present an additional authentication challenge (often mediated by a third-party risk modeling service), or the steps required to reset a password.

CIAM Component

In each of the example websites in the above figure, the reader will notice the CIAM Component. This is an optional component that can help broker user registration and authentication. Often a piece of JavaScript, web component, or library, this piece of the puzzle can securely interact with the authentication and orchestration service. Often, in cases where this component is not present, the individual is redirected to a user experience that the authentication service provides to register and authenticate; they are then redirected to the site or app where they started.

Constraints and Challenges

Like other domains within the digital identity industry, CIAM comes with its own unique set of hills to climb. What follows is not an exhaustive list, and readers have likely discovered others.

Risks of Being on the Internet

CIAM systems, by their very nature, are on the public internet. After all, that's where an organization's customers are. It may go without saying that the internet is a space fraught with adversaries and risks, but it is especially important to say it about the identity systems of the internet. Every major touchpoint in a customer journey is susceptible to attack, especially sign-up, password reset, and login. Three kinds of attacks to be aware of are:

- Fraudulent Registration
- Credential Stuffing (aka cred stuffing)
- Account Takeover (ATO)

Fraudulent Account Registration

In this attack, the adversary (including bots) registers a new user account in the CIAM system using either bogus or stolen personal information. Their motivations vary from wanting to fill forums and chat groups with spam and malware links to harvesting new

customer discount codes. Mitigations to these attacks can include anti-fraud systems for detection and reCAPTCHA-type puzzles, although the latter have been shown to be less effective than in years past.

Credential Stuffing

In this attack, an adversary tests whether lists of username and password pairs work in a given CIAM system. Often, adversaries acquire credentials (e.g., they may purchase them on the dark web) and test whether those credentials work at different online services. Their value on the black market is determined by the types of services those usernames and passwords can access. In many cases, the adversary is not interested in abusing an organization's service itself; instead, they are testing to see if the credentials work with your service so that they can sell it at a higher price. The reason why credential stuffing is even a thing is because people have a habit of reusing passwords. Mitigations to these attacks include specialized credential stuffing detection technology (often closely aligned with bot management and protection) and enforced multi-factor authentication (MFA).

It is important to note that credential stuffing differs from brute force attacks. In the brute force attack, the adversary is interested in testing whether an array of passwords works with a specific username. Brute force attacks can be mitigated in a variety of ways, including failed login throttling, in which multiple failed logins for the same user trigger either a slowdown in the number of times the user is allowed to log in or even a cooldown period during which all logins for the user are blocked. Credential stuffing cannot be mitigated with these measures because a CIAM system will only see one failed login per username/password pair.

Account Takeover

In this attack, an adversary possesses the means to act like the genuine authenticated user. The adversary may have the user's password (e.g., via a phishing campaign). The adversary might have found a weakness in the password reset process and forced a password change on a genuine user's account. Regardless of the means, the outcomes are the same: the adversary is in control of the user account – and may very quickly take steps to block the user from regaining access (such as changing the phone number). From that point forward, all means of nefarious actions can happen. Early detection is important but not sufficient to mitigate account recovery. Please refer to the IDPro Body of Knowledge article "Account Recovery" for more information.

Migrating CIAM Systems

Today, most organizations have an existing CIAM system. It might be tightly bound to an eCommerce platform or collaboration platform. If the organization has decided to modernize or replace its CIAM, then it is likely that IAM team members will be confronted with a migration. While migrating usernames is reasonably straightforward, migrating

passwords is not. Two significant challenges are exporting passwords from the old system and getting them into the new one.

Exporting passwords presents significant challenges. It is important to note, for the avoidance of doubt, this article assumes that the word "password," in the context of secure storage, means a password hash: systems should never store passwords in their recoverable plain text form. If exports are allowed, further data must be exported, including those comprising the security features known as "salt" and "pepper."[21] With all three, taking extensive protective measures during migration is essential since they represent "loaded weapons."[22]

Importing passwords requires not only the appropriate "salt" and "pepper" data but also the hashing scheme used by the previous system. Some CIAM solutions have specific features that support this process, but not all do.

Not all systems allow password exports at all. When organizations cannot migrate passwords, then at least two choices exist. Choice one involves telling the users to reset their passwords. This is not a great choice – it will certainly invite the attention of a grumpy Chief Digital Officer or other stakeholder(s). Choice two involves keeping the old CIAM alive and using it as a "dumb" credential store. When the user arrives and attempts to log in, the new CIAM tests the provided username and password against the old CIAM repository. If the credentials are good, the new CIAM records the password and marks the user as migrated. This approach is more complicated to deploy and requires that the old CIAM stays operational for a much longer period of time than the team might hope for (or want to pay for).[23]

Budget and Ownership

As discussed in the "The Team and Measurements" section, there are multiple stakeholders at the CIAM table. Besides bringing a diverse set of requirements and language, they bring their own teams and stakeholders, their motivators, their priorities, and their opinions. Who funds, operates, enhances, and is responsible for a CIAM stack can become a difficult set of questions to answer. It is not unusual to have the Chief Digital Officer take responsibility for the CIAM experience, a large percentage of the requirements, and funding. Partnered with them is the Security team, who have other requirements and are responsible for monitoring and incident response. The Identity team might be part of either organization or a separate Information Technology team. Regardless, expect that upper management will need to establish clear lines of demarcation between the various interested parties and, furthermore, to ensure there is a clear set of priorities that aligns the collective.

Topics for Future Investigation

This Body of Knowledge article is meant to be an introduction to Customer Identity and Access Management. The topic is both broad and deep: exploring the entire landscape is beyond the scope of an introductory article. The following is an incomplete list of what could and should be explored in the future:

- Incident response playbooks and documenting who to call when customers cannot register or log in
- Identity verification and proofing's role in CIAM
- High availability architectures for CIAM
- The use of fraud prevention tools to protect sign-up and sign-in
- Use of government- or financial services-issued credentials
- Emergent trends in credentials, including verified credentials
- Cross-channel or "omnichannel" CIAM

Conclusion

CIAM represents one of the biggest opportunities for identity professionals to demonstrate the value of their work. Through CIAM, identity professionals can help organizations reach new customers and grow the top and bottom lines. In this way, it is different from workforce IAM. These differences invite stakeholders from new parts of the organization – new partners, like Brand, Marketing, and Digital. Each new stakeholder brings their own set of requirements, languages, and business objectives. CIAM is, fundamentally, an internet-facing set of identity services that brings unique risks to model and mitigate. For more experienced identity professionals, CIAM may represent a fresh opportunity to reinvigorate their passion for digital identity. For newer members of the identity profession, it represents an exciting opportunity to have a meaningful positive impact on their organizations.

Author

Ian Glazer

Ian Glazer is the founder and president of Weave Identity – an advisory services firm. Prior to founding Weave, Ian was the Senior Vice President for Identity Product Management at Salesforce. His responsibilities include leading the product management team, product strategy, and identity standards work. Earlier in his career, Ian was a research vice president and agenda manager on the Identity and Privacy Strategies team at Gartner, where he oversaw the entire team's research. He is a Board Emeritus and the co-founder of IDPro and works to deliver more services and value to the IDPro membership, raise funds for the organization, and help identity management professionals learn from one another. During his career in the identity industry, he has co-authored a patent on federated user provisioning, co-authored and contributed to user provisioning specifications, and is a noted blogger, speaker, and photographer of his socks.

---

[1] Flanagan (Editor), H., (2022) "Terminology in the IDPro Body of Knowledge", *IDPro Body of Knowledge* 1(11). doi: https://doi.org/10.55621/idpro.41

[2] Epping, M. & Morowczynski, M., (2021) "Authentication and Authorization (v2)", *IDPro Body of Knowledge* 1(10). doi: https://doi.org/10.55621/idpro.78

[3] Ibid

[4] Glazer, I. & Robinson, L. & Hamlin, M., (2022) "User Provisioning in the Enterprise", *IDPro Body of Knowledge* 1(8). doi: https://doi.org/10.55621/idpro.84

[5] Koot, A., (2020) "Introduction to Access Control (v4)", *IDPro Body of Knowledge* 1(10). doi: https://doi.org/10.55621/idpro.42

[6] Nelson, C., (2020) "Introduction to Privacy and Compliance for Consumers (v3)", *IDPro Body of Knowledge* 1(10). doi: https://doi.org/10.55621/idpro.44

[7] Sesame Street (2009) "Sesame Street: Cookie Monster Sings C is For Cookie" https://www.youtube.com/watch?v=Ye8mB6VsUHw

[8] McKinsey and Company "Enhancing customer experience in the digital age" https://www.mckinsey.com/capabilities/growth-marketing-and-sales/our-insights/enhancing-customer-experience-in-the-digital-age

[9] Yes, C in B2C stands for consumer and that only adds to the confusion on what the C stands for in CIAM. The writer of this article doesn't create the terms of art, just relays them.
[10] Cameron, A. & Grewe, O., (2022) "An Overview of the Digital Identity Lifecycle (v2)", *IDPro Body of Knowledge* 1(7). doi: https://doi.org/10.55621/idpro.31
[11] For more on admin-time versus runtime-time patterns, see: Bago (Editor), E. & Glazer, I., (2021) "Introduction to Identity - Part 1: Admin-time (v2)", *IDPro Body of Knowledge* 1(5). doi: https://doi.org/10.55621/idpro.27
[12] See, for example: Hindle, A., (2020) "Impact of GDPR on Identity and Access Management", *IDPro Body of Knowledge* 1(1). doi: https://doi.org/10.55621/idpro.24
[13] Ibid.
[14] Crow, A. & Rowan, J. P., (2021) "Managing Identity in Customer Service Operations", *IDPro Body of Knowledge* 1(4). doi: https://doi.org/10.55621/idpro.65
[15] Glazer, I., (2020) "Identifiers and Usernames", *IDPro Body of Knowledge* 1(1). doi: https://doi.org/10.55621/idpro.16
[16] Epping, M. & Morowczynski, M., (2021) "Authentication and Authorization (v2)", *IDPro Body of Knowledge* 1(10). doi: https://doi.org/10.55621/idpro.78
[17] Grassi, Paul, James Fenton, Elaine Newton, Ray Perlner, Andrew Regenscheid, William Burr, and Justin Richer. "Digital Identity Guidelines Federation and Assertions: Authentication and Lifecycle Management." Sectino 5.1, National Institute of Standards and Technology, U.S. Department of Commerce, June 2017. https://doi.org/10.6028/NIST.SP.800-63b.
[18] Saxe, D. H., (2021) "Account Recovery (v2)", *IDPro Body of Knowledge* 1(8). doi: https://doi.org/10.55621/idpro.64
[19] Again, the writer of this article doesn't create the terms of art but relays them with no small amount of cynicism.
[20] Hodges, J., Jones, J.C., Jones, M.B., Kumar, .A., and Lundberg, E. (2021) "Web Authentication: An API for accessing Public Key Credentials Level 2" W3C https://www.w3.org/TR/webauthn-2/
[21] Salt and Pepper reference
[22] Spacey, J. (2023) "Cryptography: Salt vs Pepper" Simplicable (Accessed on October 19, 2023) https://simplicable.com/IT/salt-vs-pepper
[23] If you didn't like passwords before, going through a CIAM migration will absolutely make you loathe them for certain.