



White Paper

The Five Pillars of Customer Identity and Access Management

By **Dakshitha Ratnayake**

Enterprise Architect - CTO Office, WSO2



Table of contents

| | |
|---|----|
| 1. Introduction to Customer Identity and Access Management..... | 4 |
| 1.1 Benefits of CIAM..... | 4 |
| 1.2 Key Features of CIAM..... | 5 |
| 2 The Five Pillars of CIAM..... | 8 |
| 3 The WSO2 Platform for a CIAM Implementation..... | 14 |
| 4 Summary..... | 15 |
| 5 References..... | 17 |



Abstract

Customer Identity and Access Management (CIAM), a subgenre of IAM, enables organizations to scale and ensure secure, seamless digital experiences for their customers, while collecting and managing customer identity data purposefully. Powerful CIAM solutions provide a variety of key features including customer registration, social logins, account verification, self-service account management, consent and preference management, single sign-on (SSO), multi-factor authentication (MFA), and adaptive authentication as well as other nice-to-have features. Such CIAM solutions will operate at extreme scale and performance over different channels of customer interaction, such as web and mobile. This paper will explain the five pillars of CIAM — the core underlying technology required to support the key features of a CIAM solution.

1 Introduction to Customer Identity and Access Management

Customer Identity and Access Management (CIAM) is an emerging sub-genre of traditional IAM, which is vital for a seamless digital customer experience. An effective CIAM system provides more than just access because it enables a relationship between the customer and the organization, and facilitates data sharing on which cross-marketing capabilities and business intelligence activities depend.

1.1 Benefits of CIAM

Enterprises should consider implementing a CIAM solution because it

- ▶ Helps provide a holistic view of the customer, which will enable companies to understand their customers' actions across various access points.
- ▶ Provides a unified customer experience. It enables customer conversion and retention through consistent registration and authentication options at extreme scale and performance, thus allowing a secure and seamless customer experience.
- ▶ Can deliver consolidated reports and analytics around users to drive various sales opportunities. These statistics typically include user demographics, social registration and login data, behavioral data, and revenue activity.
- ▶ Adheres to privacy regulations and improves agility and scalability to support millions of customer identities.
- ▶ Helps to build the bridge between marketing and line of business to deliver offerings that keep customers delighted while delivering actionable data to the business.

1.2 Key Features of CIAM



Figure 1 - Key Features of CIAM

User On-Boarding - The Start of a Digital Relationship

The first step in a CIAM process — user registration — allows to convert anonymous, casual website visitors to known, active, registered users. If the registration is too difficult, the customer will abandon the registration process, which will have a negative impact on the business. It is important that registration must be as user-friendly and simple as possible while collecting valuable customer identity data.

Ideally, organizations must provide users with multiple registration options, such as self-service registration, social registration and delegated administration, where a delegate acts on behalf of the user and manually creates the account for the user. At the same time, an individual's identity must be validated and proven before a user account is created. The objective of validation is to verify the information provided, and ensure that users are who they say they are. CIAM solutions may provide several techniques for validating user accounts, and additional identity-proofing techniques, such as email verification, can be applied for some accounts and transactions. Identity proofing helps organizations to validate the authenticity of users.

Progressive Profiling

Progressive profiling allows an organization to build a comprehensive user profile over time. At the time of registration, a user account is typically an account with only a few attributes. Once the customer is more accustomed with the organization, the company can prompt for additional identity data, such as company name, job title, and contact information.

Single Sign-On

Single Sign-On (SSO) ensures that customers have a consistent login experience with common credentials across all the accessible digital properties of a company. SSO is a commonly sought feature in most IAM implementations today, and a CIAM system should also provide the same by supporting the standard federation protocols, such as SAML, OAuth and OIDC among an organization's websites.

User Profile Management

Customer self-care portals should be provided by CIAM solutions to allow customers and delegated administrators to explicitly define preferences, which should be stored in a unified customer profile to facilitate consistent, personalized experiences across channels.

Authentication

Authentication beyond the scope of username and password, through mechanisms such as social login, multi-factor authentication (MFA), and adaptive authentication (risk-based authentication) is a requirement for an increasing number of CIAM use cases. Social login allows a user to access a third-party application without having to go through a new registration process, and the third-party IdP, such as Facebook, Twitter, LinkedIn or Google, authenticates the user and allows the CIAM system to capture the user's identity attributes. MFA confirms a user's identity and ensures only the right people get access by providing a variety of factors to choose from, ranging from asking a security question to capturing and confirming biometric data to using physical authentication keys, codes or One-Time Passwords (OTPs). Adaptive authentication is the evaluation of runtime environmental parameters, user behavioral analytics, and fraud/threat intelligence to match the appropriate authentication mechanism to the level of business risk or as required by regulations.

Fraud Detection

A CIAM system must be able to consume fraud information for the purpose of evaluation by a risk or fraud detection engine to choose the right authentication mechanisms and permit or deny access, or transaction completion.

Consent and Privacy Management

Organizations must follow the rules and regulations pertaining to gathering user data enforced by governments and different industrial bodies. Therefore, CIAM solutions must provide centralized data access governance policies, facilities within the user interface to allow consumers to provide granular user-centric preferences so they can decide how the firm uses their data, and other capabilities to ensure that regional data storage and other privacy mandates are met.

Omni-channel Support

Today's customers interact with online services through various channels, such as laptops, smartphones, kiosks, gaming consoles, and personal digital assistants. CIAM solutions should be optimized for cross-channel user experiences. The role of CIAM in an omni-channel environment ranges from authenticating the customer through multiple channels to managing the customer preferences through those same channels to build a unified customer profile.

2 The Five Pillars of CIAM

The key features of CIAM that were discussed above are only the visible portion of the CIAM realm. To ensure a seamless customer experience, a CIAM solution must be based and built upon the following five factors. They will be referred to as the five pillars of CIAM.

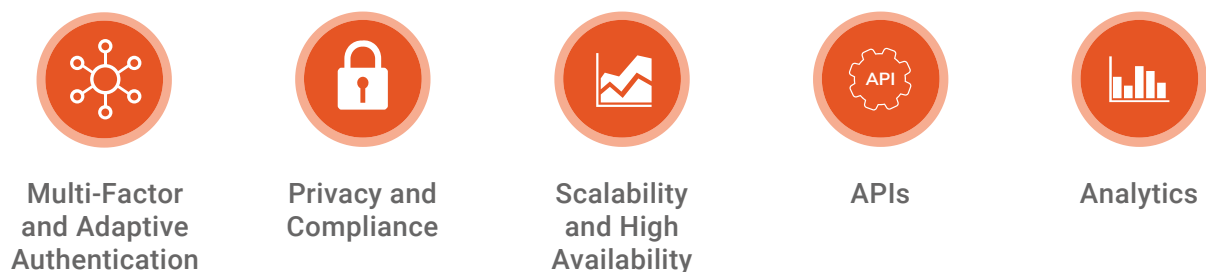


Figure 2 - The Five Pillars of CIAM

Multi-Factor and Adaptive Authentication

Good security must underpin all CIAM initiatives and is key to protecting consumers' information and to maintaining their trust. It is imperative for organizations to protect their businesses from threats to consumer-facing channels as consumers increasingly conduct high-value, sensitive transactions digitally. Therefore, organizations must focus on increasing the sophistication of their customer user authentication processes in a way that provides an acceptable user experience. Due to this reason, support for MFA and adaptive access is increasingly important.

Consumer MFA is now being adopted more broadly outside financial services because consumers across industries have become more sensitized to protecting their personal data. Today's security threats require much more robust protection measures especially for high-risk or high-reward transactions, such as a purchase or payment. Strong authentication or MFA confirms a user's identity and ensures only the right people get access by adding an additional layer to the authentication process to enhance the security of applications and services. MFA provides a variety of factors to choose from, ranging from asking a security question to capturing and confirming biometric data to using physical authentication keys, codes or One-Time Passwords (OTPs) over SMS/email or Time-based One-time Password (TOTP) (Google Authenticator).

Sometimes consumer-facing organizations try to avoid requiring a second authentication factor because it involves friction. Consumers rarely find second-factor options usable; so, when an organization is deciding on appropriate measures for MFA, they must carefully consider usability aspects in addition to security. Consequently, organizations may allow users to choose whether they want to go through additional steps to increase security.

Beyond MFA, adaptive authentication is context-aware access that considers not only standard authentication factors, such as a username and a password, but also additional context-based attributes. These additional context elements can include dynamic identifiers such as the user's device or location. So, the CIAM solution must consider the user's device context, the resource they're attempting to access, the type of transaction they're performing, or other contextual factors in order to determine the second to nth authentication factors. Adaptive authentication is also known as risk-based authentication.

Privacy and Compliance

Privacy and compliance capabilities are foundational and CIAM initiatives should focus on protecting the individual. Privacy standards and best practices continue to evolve in terms of both formal regulations and consumer expectations. CIAM teams must adhere to an increasing number of consumer protection laws and regulations. For example, the EU General Data Protection Regulation (GDPR), which came into effect in May 2018 in the EU, is top of mind for organizations based in the EU or those that collect and hold data on people in the EU. GDPR primarily focuses on the protection of personal data and individual rights by giving control of their personal data to individuals. The regulation has catalyzed many countries to come up with their own privacy regulations. Multi-national organizations must worry about privacy regulations of each and every country they do business with and use a CIAM solution sophisticated enough to ensure adherence to international privacy and data retention regulations.

An organization should clearly specify why user data is collected and must declare the purpose of data usage. Also, the control of personally identifiable information must be given to the end user. Users must be able to give consent at the time of registration, during a progressive profiling flow, as well as manage consent from the user profile. To do that, a CIAM solution must provide self-service portals for users to manage their consents. For example, users should be able to opt into data sharing between domains and to change their mind. Moreover, once registered, the user should be able to edit or delete the connection to social providers, and if a connection to a social provider is deleted, all shared attributes should also be removed. Therefore, the self-care portals can be effectively used to review and withdraw consents by customers and also be used to keep their profiles up to date. When the self-care portal provides means to enforce data protection standards for personal information, application developers can be relieved to delegate such aspects to a CIAM solution.

Furthermore, the CIAM solution must also support data retention laws that require organizations to purge user data when a user deletes identity attributes or an entire user account.

Scalability and High Availability

Today's customers expect services and apps to always be available. While a workforce IAM system may expect thousands of users, a CIAM solution must be able to handle millions of users across mobile and web channels with no perceived performance degradation and with a common user experience across these channels. Customers won't tolerate lags and outages, whereas employees have little choice. The CIAM system must be able to accommodate large volumes of users and spikes in registrations and access requests while maintaining a high level of performance.

There are two traditional ways to handle scaling - horizontal and vertical scaling.

- ▶ Vertical Scaling - Adding more computational and/or memory power to the underlying hardware of the systems.
- ▶ Horizontal Scaling - Adding more replicas of the system to the deployment.

To decide on the computational power or number of instances of the solution, it is important to consider the load. In most cases, there is a considerable difference between the average and peak loads, where the peak load could even be a twofold (or higher) increase in the average load. This is because there may be circumstances where hundreds of thousands of users are using the service within a short period of time. It is important to stress that a CIAM system would only experience such a peak load only for a relatively brief period of time. For example, this could be for a few hours in a couple of days in a single month. Because it is a waste of resources and money to keep the CIAM infrastructure running continuously to handle the maximum load, the best option is to adopt autoscaling methods. Autoscaling makes a system scale automatically based on certain load parameters. Such a model will ensure that the system will spin up adequate servers to address the increasing load and shut down the redundant servers when the load goes down. Mature container technologies such as Docker and Kubernetes have enabled systems in production to be autoscaled seamlessly.

CIAM systems must also provide failover and redundancy mechanisms to ensure that the system is always available. Furthermore, they must maintain the highest levels of performance and responsiveness because today's customers do not have the patience to wait for latent services and therefore must offer millisecond response times.

To fulfill these requirements, multiple instances of a CIAM solution can be deployed in a single data center and that entire deployment can be replicated in geographically distributed data centers to ensure high availability. The CIAM deployment will thus become multi-regional. Active data centers will serve active traffic. The disaster recovery (DR) data centers will be on standby mode to serve the traffic which is deviated to them in case of an outage in the active data center(s). At the same time, a multi-regional deployment ensures that the data is as close as possible to where the customers reside or where the data is being used, which addresses the need for high performance and responsiveness. Additionally, an enterprise should have on-premise, cloud or hybrid options when it comes to the deployment of the CIAM solution.

APIs

Digital transformation is enabled through the integration of a multitude of applications and services. A CIAM system is not an all-in-one solution and its ability to function in a larger ecosystem, where it can appropriately share information with a variety of systems, is what makes it powerful. The key enabler for integration is APIs, and a CIAM solution should provide means to integrate with such applications via APIs. APIs are increasingly available in CIAM solutions to allow third-party applications to perform identity analytics, marketing analytics, security integration, provisioning/deprovisioning, consent auditing, and more. Furthermore, a CIAM solution's customer and profile data within a directory need to be accessible through developer-friendly REST APIs so that this data can be accessed by existing apps and therefore speed time-to-market for new apps.

To facilitate digital transformation in an enterprise, a CIAM system should have the ability to support integration with the following types of systems:

- ▶ Data stores/ directory services.
- ▶ Customer Relationship Management (CRM) systems, e.g. Salesforce, Sugar CRM, Microsoft Dynamics, and NetSuite CRM.
- ▶ Marketing solutions, e.g. Dataxu, Appboy, MailChimp, Google Analytics, Salesforce, and Pardot.
- ▶ E-commerce platforms, e.g. Shopify, Magento, and Oracle Micros.
- ▶ Fraud detection systems/ identity proofing solutions/ risk engines.
- ▶ Content Management Systems (CMS), e.g. Microsoft SharePoint, Drupal, WordPress, Joomla, and DotNetNuke.
- ▶ Data management platforms, e.g. Blueconic, DoubleClick, Lotame, and Krux.

CIAM offerings are still evolving, and as such, some custom development is usually required. Therefore, APIs in a CIAM system can also allow organizations to customize the functionality of the implementation as well as the look and feel of the user interface. Many organizations will want to use the APIs of a CIAM solution to customize the last mile of the user experience.

Ultimately when exposing these APIs of the CIAM solution to the rest of the world, securing them is also another important aspect to consider. When protecting these APIs, the best practice is to have end-user authentication handled by a separate IAM system that integrates with an API gateway. Usually, an organization would choose CIAM and API gateway tools that are known to interoperate.

Analytics

One of the key objectives of CIAM is to drive revenue growth by leveraging identity data to acquire and retain customers. By transforming data about user activities into information, companies can make informed decisions about the business as well as perform marketing campaigns and provide special offers. Analytics can be built upon the integrated data silos to build a unified user profile. There are three ways of analyzing identity data:

- ▶ **Batch analysis** - Generating insight by processing large amounts of stored data. This large dataset can also be used to develop better threat analytics, which can be used to identify threats and recognize customers when they return.
- ▶ **Real-time analysis** - Generating insight by processing real-time data to strengthen the security of the system by integrating with fraud detection systems and risk engines. Attributes collected as inputs to risk-based authentication (such as location, device type and time of day) can also be used, with appropriate permission, for better targeting and customer service.
- ▶ **Predictive analysis** - Analyzing existing data using machine learning algorithms to predict future events, which helps to make informed decisions regarding customers and services for the future.

Furthermore, a CIAM system should have the ability to generate and customize reports on user actions, as well as representing aggregated activity on enterprise or CxO dashboards in real-time. The audience of the CxO dashboard are the corporate executives, who are keen on tracking the revenue growth from multiple angles.

The CxO dashboard, which talks to multiple data sources, will focus on building insights around the following key performance indicators:

- ▶ Growth of customers/leads over time.
- ▶ Active customers/leads over time.
- ▶ Customers/leads by geography.
- ▶ Conversion rate - the rate at which prospects are converted to registered customers.
- ▶ Frequently used business functions by customers/leads.
- ▶ The conversion rate of existing customers to online customers over time.
- ▶ Customers/leads by age (inactivity) and by region.
- ▶ Customers/leads access patterns by the channel (web/mobile).

3 The WSO2 Platform for a CIAM Implementation

CIAM capabilities are, in fact, not rendered by a single product. These capabilities are more often than not provided via an integrated solution, usually integrating an IAM system, a data analytics solution, customer data platforms, data management platforms, identity proofing systems, and e-commerce platforms among others. CIAM requirements evolve over time with new business requirements. Therefore, organizations need an agile, event-driven CIAM platform that can flex to meet both new business opportunities and challenges.

WSO2 is the only vendor that provides an open source (with no vendor lock-in), integration agile platform for CIAM. [WSO2 Identity Server](#) along with [WSO2 API Manager](#), [WSO2 Enterprise Integrator](#) and [WSO2 Stream Processor](#) provide out-of-the-box features to underpin the five pillars of CIAM and implement common CIAM features and patterns. These products also come with extension points to extend its feature set to address unique customer needs.

For more information on how WSO2 products can be used to implement an effective CIAM solution underpinning the five pillars of CIAM, read the white paper on [CIAM - A WSO2 Reference Architecture](#).

4 Summary

CIAM is a mainstream business capability that will further empower developers as a way to continuously adapt to new customer and business needs. When architecting a CIAM system, an organization must not neglect the five pillars of multi-factor and adaptive authentication, privacy and compliance, scalability and high availability, APIs, and analytics. Without a strong focus on these pillars, building a CIAM system that delivers on the hyper-connected customer expectations and requirements will be challenging. Incorporating these pillars into a CIAM system, that is, ensuring that the CIAM system inherently provides these capabilities or has means to support them through integrating with other systems, will help to deliver the required functionality of a highly effective, powerful and stable CIAM system.

WSO2 provides a compelling platform to build a comprehensive CIAM solution with its identity and access management, API management, integration, and streaming analytics capabilities. By delivering functionality on a cloud-native, open source platform, WSO2 facilitates agility for the development and deployment of such a CIAM solution. To learn more visit wso2.com/solutions/ciam/.



About WSO2

WSO2 is the world's #1 open source integration vendor, helping digital-driven organizations become integration agile. Customers choose us for our broad integrated platform, our approach to open source, and agile transformation methodology. The company's hybrid platform for developing, reusing, running and managing integrations prevents lock-in through open source software that runs on-premises or in the cloud. Today, hundreds of leading brands and thousands of global projects execute 6 trillion transactions annually using WSO2 integration technologies. Visit <https://wso2.com> to learn more.

5 References

- [1] Prabath Siriwardena - Customer IAM (CIAM) - Turning Identity Data Into Gold! - medium.facilelogin.com/customer-iam-ciam-turning-identity-data-into-gold-3dcfc93f0073?gi=606ba67c3f67
- [2] Dakshitha Ratnayake - CIAM - A WSO2 Reference Architecture - wso2.com/whitepapers/customer-identity-and-access-management-a-wso2-reference-architecture
- [3] Mary Ruddy - Top 5 Trends in CIAM Solution Design (Gartner Report, March 2018)
- [4] Mary Ruddy - Key Features for Customer Identity and Access Management (Gartner Report, February 2019)
- [5] Merritt Maxim and Andras Cser - Market Overview: Customer Identity And Access Management (CIAM) Solutions (Forrester Report, August 2015)
- [6] John Tolbert - CIAM Platforms (Kuppingercole Report, December 2018) - www.kuppingercole.com/report/lc79059
- [7] WSO2 Identity Server - wso2.com/identity-and-access-management
- [8] WSO2 API Manager - wso2.com/api-management
- [9] WSO2 Enterprise Integrator - wso2.com/integration
- [10] WSO2 Stream Processor - wso2.com/analytics-and-stream-processing
- [11] A Guide to WSO2 Identity Server - wso2.com/whitepapers/a-guide-to-wso2-identity-server