Customer Identity and Access Management

A WSO2 Reference Architecture

Version Q2-2019

Author

- Dakshitha Ratnayake, Enterprise Architect - CTO Office dakshitha@wso2.com

> *This paper will introduce Customer Identity and Access Management (CIAM), which is a subgenre of identity and access management. It 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. This paper will introduce a CIAM reference architecture to address minimal and full-scale CIAM needs with open source WSO2 products, which mainly focus on identity and access management, API management, integration, and streaming analytics.*

1.0 Introduction to Customer Identity and Access Management (CIAM)

1.1 Hyper-connected Customers and Their Security, Privacy, and Experience Requirements

Today's increasingly sophisticated customers now view digital interactions as the primary mechanism for connecting with brands and, therefore, expect significant online interactions to be delivered simply and seamlessly. Transforming the customer experience is at the heart of digital transformation and digital technologies are changing the game of customer interactions with new rules and possibilities that were unimaginable only a few years back. Most enterprises have a large number of customers who access mobile, IoT and other channels in addition to mere web apps, which may or may not reside inside the firewall. As consumers increasingly conduct high-value, sensitive transactions digitally, it is imperative for organizations to protect their businesses from threats to consumer-facing channels especially in the context of financial services, pharmaceutical, and other highly regulated industries.

Collecting, storing, and analyzing consumer data allow enterprises and government organizations to provide better digital experiences for their consumers. This creates additional sales opportunities and increases brand loyalty. Companies that capitalize on customer insights have a competitive advantage over their contenders who do not. As the number of customers, applications, and services continues to grow, the data collected on customers is also increasing rapidly. At the same time, because consumer data is collected from various channels, this data is often found in disparate identity stores, creating inconsistent user experiences and hindering the ability to have a single unified view of these consumers.

Moreover, the customers do expect some control around how firms collect, store, manage, and share their profile data. With the competition only a click away, a company's misuse of customer data, whether deliberate or inadvertent, can significantly damage brand equity.

1.2 CIAM for a Secure and Seamless Customer Experience

Customer Identity and Access Management (CIAM) addresses the above-mentioned requirements of the hyper-connected customer. CIAM is an emerging sub-genre of traditional IAM, which is of vital importance 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.

1.2.1 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.

Traditional IAM solutions do not provide these benefits (as explained in section 1.2.2).

1.2.2 CIAM vs Traditional IAM

CIAM goes beyond traditional IAM, also known as Workforce IAM. Workforce IAM looks inward, where the focus is on business-to-employee (B2E) and business-to-business (B2B) interactions. Some enterprises have a mistaken impression that an IAM solution that's purpose-built for employees is a natural fit for their customer interactions. It is important to note that CIAM transcends traditional IAM especially in analyzing customer behavior, collecting consent for user data usage, and integration into customer relationship management (CRM) systems, connected devices, and marketing automation systems.

The goal of workforce IAM is to reduce the risk and cost associated with on-boarding and off-boarding new employees, partners and suppliers. By contrast, the purpose of CIAM is to help drive revenue growth by leveraging identity data to acquire and retain customers. If the CIAM processes are cumbersome, the experience is poor and the security is weak, customers will naturally reach out to competitors who offer these processes in ways more streamlined or easier to use. The same is not true of employees because employees are required to comply with and conform to their company's systems and technologies. Very few employees leave their employer because business-to-employee (B2E) IAM processes are archaic or hard to use - employees are paid to use an organization's systems. On the other hand, customers will walk away if the user experience is not smooth enough.

CIAM systems vary from employee IAM systems in the following foundational areas:

	Traditional IAM	**Customer IAM**
Business Objective	Reduce risk and improve efficiency	Attract and retain customers
User Profile	All required information of an employee is acquired when hiring	Customer information is acquired gradually over time (progressive profiling)
Control	Employee identities are centrally managed by the enterprise	The control of identity is shared between the enterprise and the customer (distributed)
Experience	Low priority (unless it detracts from efficiency)	High priority
Personalization	Low priority	High priority
Privacy and User Involvement	Organization-centric policies and procedures	Customer-centric policies and preferences
Scale	100s and 1000s	1000000s
Performance and Reliability	Generally not prioritized	Extremely important

Table 1 - Traditional IAM vs Customer IAM

2.0 CIAM Key Features

ciam key features

Figure 1 - Key Features of CIAM

2.1 User On-boarding - The Start of a Digital Relationship

2.1.1 Registration

Usually, the first step in a CIAM process is user registration. The goal of this phase is 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. Personalized services and deepening the relationship with the digital customer are some benefits of registration in addition to identifying a user. 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.

2.1.1.1 Self-Service Registration

Self-service registration is the most common method for registering online users, allowing them to self-register for a user account and provide their identity data. A self-service registration form usually expects components such as username, password, and one or more data fields. The form should ideally be as minimal as possible and require only the fields necessary to create an account. The type of data collected at registration is dependent on the type of service or information the user is requesting. The organization can collect more data about the user over time, which is referred to as progressive profiling.

2.1.1.2 Social Registration

The need for seamless registration has given rise to the use of social identities in the process, which is known as social registration. Social registration streamlines registration by leveraging a social login such as Facebook, Google, LinkedIn, and Twitter. Users can consent to allowing attributes from their social media account to be filled into the registration form with this approach, greatly reducing typing and simplifying the entire registration process. Users save registration time, and they can log in with their social logins when they return to the website. This approach provides benefits to both the user and the website. That being said, social registration is not sufficient for all use cases such as high-assurance use cases, or with users who don’t use social media.

2.1.1.3 Delegated Administration

Delegated administration is another form of registration. Even though this model is similar to self-registration, in delegated administration, a delegate acts on behalf of the user and manually creates the account for the user. A customer service center or help desk that creates online user accounts on behalf of users are classic examples. The CIAM solution should provide an administrative interface that allows delegates to create, manage and delete user accounts and passwords on behalf of the user. To support this type of model, the CIAM solution must provide a robust authorization framework that controls who can access which user accounts and data.

2.1.2 Account Validation

An individual’s identity and associated identity data elements must be validated before a user account is created. Even in the case where user attributes required for registration are fetched via a third-party identity provider, the last phase of the registration will involve submitting a form by the user. The objective of validation is to verify the information provided, and ensure that users are who they say they are. Levels of validation vary: high-risk account operations will require more sophisticated validation techniques, whereas low-risk account operations may require little to no validation.

CIAM solutions may provide several techniques for validating user accounts and their associated identity data including:

- Format validation - Enforces consistent data entry formats, such as required fields, field length or field type.
- Data validation - Ensures the accuracy of data entered (with or without third-party services). E.g. validate credit card data or a person’s age.
- Completely Automated Public Turing Test to Tell Computers and Humans Apart (CAPTCHA) or Google’s reCAPTCHA - Discerns humans from computers by presenting a user with a task that humans can perform, but computers (hopefully) cannot.

At the same time, additional identity-proofing techniques must be applied for some accounts and transactions. Identity proofing helps organizations validate the authenticity of users. The two most common proofing techniques are as given below:

- Email verification - Verifies the authenticity of the email address by sending an automated email to the user and providing a link that redirects the user back to the website to finish the registration process.
- Dynamic Knowledge-Based Authentication (KBA) - Verifies the user based on facts (secrets) that aren’t widely disclosed, ideally based on previous transactions with the organization. KBA can also include fingerprinting and geolocation analysis among other things.

When onboarding customers, it is also important to think about the usability aspect. There has been much debate about the precedence of security over usability in recent years because finding the right balance has been extremely hard.

2.2 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 comfortable with the organization, i.e. they request more services or perform transactions, they become more willing to share personal data. At that point, the company can prompt for additional identity data. For example, at the time of registration, a user may need to provide only a first name, last name and an email address. If that user then wants to download a white paper, access a digital service or purchase a product, the company may ask for additional identity attributes, such as company name, job title, and contact information.

2.3 Single Sign-on

Single Sign-on (SSO) ensures that customers have a consistent login experience with common credentials across digital properties. SSO is a commonly sought feature of 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 amongst an organization’s websites. The CIAM system can also include proprietary connectors for internally hosted applications and SaaS applications, such as CRM systems and marketing automation systems, to enable a one-time sign-on experience. Undoubtedly, SSO is an absolute must in a CIAM system when a company offers multiple portals to perform business functions.

2.4 User Profile Management

Once registered, customers need self-service capabilities to manage, add, update, or delete their own data. 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. The self-care portal is the one-stop shop to

- View or update a profile
- Manage consents given to third-party applications
- Reset a password
- Manage credentials
- Manage preferences
- Configure account recovery options
- View concurrent login sessions and activity logs
- Request for data export
- Associate social logins and more

2.5 Authentication

Authentication beyond the scope of username and password is a requirement for an increasing number of CIAM use cases.

2.5.1 Social Login

Social login is a key success factor in CIAM and a good CIAM system should support login with multiple social identity providers to facilitate easy customer acquisition. Social login provides federated sign-on that enables users to use an existing digital identity issued by a trusted third-party identity provider (IdP). This allows a user to access a third-party application without having to go through a new registration process, and the third-party IdP authenticates the user and allows the CIAM system to capture the user’s identity attributes.

Social login has become increasingly popular in recent years because users complain of registration fatigue after being forced yet again to register to complete a transaction. Traditional IAM systems do not encourage social login. Notably, social login is treated as a high-risk factor as the enterprise has no control over how the user credentials are stored and managed by a third party identity provider. The same risk factor exists in CIAM but it is a compromise between convenience and security. Also, the line of business plays a key part to negotiate on whether to use social login or not. For example, financial institutes do not even consider integrating social login due to obvious security and privacy concerns.

2.5.2 Multi-factor Authentication (Strong Authentication)

When systems nowadays contain so much confidential and personally identifiable information, it becomes clear that passwords alone are not enough. 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 Multi-factor Authentication (MFA) confirms a user's identity and ensures only the right people get access by adding an additional layer to the authentication process. 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).

Strong authentication is encouraged in both CIAM and workforce IAM. Workforce IAM systems rely on hardware tokens for MFA, while a large scale CIAM system uses soft tokens like One-time Password (OTP) over SMS/Email or Time-based One-time Password (TOTP) (Google Authenticator). Both Google and LinkedIn use FIDO U2F internally for employee authentication. Almost all consumer mobile applications produced by vendors in financial, retail and airline domains now support login with Touch ID.

2.5.3 Adaptive Authentication (Risk-based Authentication)

Second authentication factors (e.g. OTP over SMS, biometrics) must be adaptive or risk-based. That is, 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.

Risk-based 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. It is a non-static authentication system, which takes into account the profile of the agent requesting access to the system to determine the risk profile associated with that transaction. The risk profile is then used to determine the complexity of the challenge. Based on the risk factors, the system will decide on whether to use SMS OTP or use Knowledge-based Authentication (KBA). To determine the risk of the transaction, the authenticating system may use a risk engine, which takes into consideration the geographical location where the transaction initiated, the frequency, and the value of the transaction among other criteria.

2.6 Fraud Detection

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

Identity analytics can be used to identify a returning user and generate a risk score based on the device, IP address, geolocation or user behavior. In other words, known bad domains, compromised credentials, accounts suspected of fraud, fraud patterns and botnet behavior, will be fed into the fraud detection engine during a transaction. Based on the anomaly detection algorithms or rules defined in the engine, the CIAM system will respond to the fraudulent events by blocking the transactions, locking the customer accounts and generating alerts to the responsible parties.

For example, if a customer logs into their account from the USA first and then from China within a span of one hour, it is considered a fraud event with a high fraud score. For another example, if a customer accesses online services between 9 PM to 11 PM GMT 90% of the time, and then if the same user credentials are used to access the system between 2 AM to 3 AM GMT, then that too is considered to be a fraud event with a medium fraud score.

2.7 Consent and Privacy Management

As organizations grow, more and more customer identity data is collected to make more personalized and context-based decisions. Many consumers have become more sensitive to privacy issues with the recent stream of high-profile identity breaches. Organizations operating in multiple jurisdictions are most likely to need to comply with various privacy regulations. Therefore, customer consent and privacy management is a top priority for most organizations.

Organizations must follow the rules and regulations pertaining to gathering user data enforced by governments and different industrial bodies. There are now many strict privacy regulations that vary by region, industry, company and even from person to person, and complying with these regulations is critical because violations can lead to brand damage, lost customer trust, and whopping fines. Therefore, CIAM solutions must provide centralized data access governance policies, facilities within the UI to allow consumers to provide granular user-centric preferences, and other capabilities to ensure that regional data storage and other privacy mandates are met.

2.8 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 a CIAM in an omnichannel environment ranges from authenticating the customer through multiple channels to managing the customer preferences through those same channels to build a unified customer profile. For instance, subscribers of news magazines can choose either the print version, the digital version or both, and the digital subscription is available through the web, a smartphone or tablet. If a customer uses the magazine's mobile app to highlight some content, the same text should remain highlighted when the user views the same content on the web. This is a seamless experience.

The channels available to a user will vary from organization to organization and from service to service. Furthermore, to provide a better overall customer experience, the current trend is to provide better integration between online and physical shopping experiences. For instance, retail giants see that the future of the industry won't be black or white in choosing either online or in-store, it will be multi-channel. The bottom line is, companies in many verticals are looking to deliver a better, seamless customer experience through multiple channels and it is imperative to have a CIAM system to enable the smooth omnichannel experience.

3.0 CIAM - A WSO2 Reference Architecture

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, e-commerce platforms and more. CIAM requirements evolve over time with new business requirements. Therefore, organizations need an agile, event-driven consumer IAM platform that can flex to meet both new business opportunities and challenges.

WSO2 is the only vendor, which provides an open source (with no vendor lock-in), agile integration platform for CIAM. WSO2 Identity Server along with the WSO2 Integration Agile Platform provides out-of-the-box features to address common CIAM patterns and also extension points to extend its feature set to address unique customer needs. This section will address some key CIAM requirements via a set of commonly-implemented architecture patterns with the WSO2 Identity Server as well as the rest of the WSO2 components.

3.1 Centralized Security and Administration

centralized security

Figure 2 - Centralized Security and Administration (with Adaptive Authentication and Analytics)

At a basic level, a company should leverage a centralized CIAM system to secure customer identity and profile data from authentication by supporting the relevant identity standards, such as SAML, OAuth, OIDC and System for Cross-domain Identity Management (SCIM). They should also provide unified login (SSO) across all of their digital properties, i.e. websites and other applications. Social login capabilities can also be introduced at this point. Inbound, outbound and just-in-time (JIT) user provisioning can be used to manage information about users on multiple systems and applications. Moreover, identity provisioning features can be used to propagate user identities across different SaaS providers. Multiple instances of the CIAM system should be deployed to allow low-latency, high-performance access to identity and profile data from many millions of customers.

As a next step, the company should enable convenient self-service registration, account management, and account recovery features. They must also create a unified view of the customer from disparate identity repositories that is accessible to all applications. Thereafter, secure and fully customizable MFA that balances security and convenience for customers can be introduced.

Needless to say, the CIAM solution must enforce centralized policies and fine-grained data access governance that can be used to enforce customer consent and adhere to applicable regulations at all times.

Subsequently, to support adaptive authentication and analytics, the CIAM system can be integrated with risk engines and analytics systems. CIAM analytics helps an organization understand who its customers are and how to drive more revenue via online customer interactions. With adaptive authentication, different authentication flows can be determined based on contextual parameters and the risk involved. To determine the risk of a transaction, the authenticating system can use a risk engine, which takes into consideration the geographical location where the transaction was initiated, the frequency, and the value of the transaction among other criteria.

3.1.1 Centralized Security and Administration with WSO2 Identity Server

centralized security with WSO2

Figure 3 - Centralized CIAM Capabilities with WSO2 Identity Server and WSO2 Stream Processor

WSO2 Identity Server is a uniquely flexible, open source IAM product, which allows enterprises to perform single sign-on/sign-out, identity federation, strong authentication, identity administration, account management, identity provisioning, fine-grained access control, API security, and identity analytics, which include monitoring, reporting, and auditing. It also provides a wide array of ready-to-use connectors that can be used to connect with third-party systems to build tailor-made systems to meet business needs.

By default, the WSO2 Identity Server can connect to JDBC, LDAP or Active Directory user stores and supports username/password based authentication, as well as role-based or attribute-based access control. Multi-option and multi-factor authentication, as well as adaptive authentication, can be enabled in WSO2 Identity Server to define how users should be authenticated to various applications. It allows configuring multi-step authentication where the authentication chain can contain different authenticators at each step. For example, a developer can configure username/password authentication as the first factor and then FIDO authentication as the second factor. WSO2 Identity Server accepts email/SMS OTP, FIDO U2F, Google Authenticator, JWTs, Microsoft Authenticator, Mobile Connect, RSA SecurID, social logins, and x.509 certificates. WSO2 Identity Server provides connectors for Veridium Biometrics and Aware Knomi for mobile biometrics, while a few others are in progress. Such configurations are straightforward in WSO2 Identity Server as they are easily configurable through UI wizards.

SSO is one of the key features of WSO2 Identity Server that enables users to provide their credentials once and obtain access to multiple applications. The users are not prompted for their credentials when accessing each application until their session is terminated. Additionally, the user can access all these applications without having to log in to each and every one of them individually. WSO2 Identity Server supports SSO via SAML2, OpenID Connect, and WS-Federation Passive. Moreover, SSO can be coupled with Identity Federation, which involves configuring a third-party identity provider as the federated authenticator for user login to an application. When federation is coupled with SSO, the user can log in to one application using the credentials of the federated authenticator, and simultaneously be authenticated to other connected applications without having to provide credentials again. Identity provisioning features of the WSO2 Identity Server can be used to propagate user identities across different user stores belonging to different applications. It supports SCIM and Service Provisioning Markup Language (SPML) for this purpose.

WSO2 Identity Server’s self-service portal for end users provides a means to manage the user profile or the user account, add security questions, revoke/update the password, manage the OpenID profile, and view identity providers, user login sessions, pending approvals, and associated accounts.

Furthermore, WSO2 Identity Server provides a comprehensive consent management solution that can be used to manage consents, where consumers have the ability to view, edit, export, and delete their profile data. Its consent management module provides RESTful consent APIs to manage consent remotely; a consent portal for users to review, modify, and revoke given consents; and admin portal support for organizations to define and manage consents. It also has support for the Kantara consent receipt specification.

With social login capabilities, customer profiles can be created from and customers can be authenticated through third-party identity providers. The user can either complete the entire registration form provided by the application or let the application import the existing identity profile data from Facebook, LinkedIn or Google. If the user opts to sign up via their preferred social network, the application will redirect the user to the given social network. Furthermore, whenever the user wants to log in to the application, they will be redirected to the preferred social site, which will perform the authentication and return a secure token to be used with the application.

WSO2 Identity Server can be integrated with risk engines and external systems to perform adaptive authentication. For this purpose, WSO2 Stream Processor, a lightweight stream processing platform that understands streaming SQL queries in order to capture, analyze, process and act on events in real time, is configured as the default risk engine. It can collect events, analyze them in real time, identify patterns, map their impacts, and communicate the results within milliseconds. It can process device fingerprints and history, geo-location, geo-velocity, user attributes, and perform behavioral analysis. Also, third-party intelligence can be imported. WSO2 Identity Server’s adaptive authentication implementation comes with a rich script-based policy language, allowing to write powerful authentication scripts in a script editor to enforce new policies easily. Static elements such as user roles, user attributes, user stores, and dynamic elements such as user tendencies defined on device usage, IP range, and geo-velocity can be taken into consideration when implementing policies for adaptive authentication.

For analytics, the WSO2 Identity Analytics server, which is built-in but runs as a separate process, can be used to generate identity and marketing analytics. The analytics server can be used to perform the following tasks:

- Monitoring and analysis
    - Login events and session monitoring

    - Logged in users/sessions
    - Manually terminated user sessions
    - Admin-forced password reset
- Real-time security alerting for suspicious login activities and abnormal sessions
- Auditing of privileged operations using distributed auditing system (XDAS)
- Built-in collection and monitoring of standard access and performance statistics
- Key system metrics monitoring and management using JMX MBeans

3.2 Customer Data Unification for Digital Transformation

A well-designed CIAM solution will enable customers to suitably connect to an organization’s cross-channel digital offerings. At the same time, such a solution will also provide a single view of the customer, and in order to achieve a single view, organizations must aggregate data from multiple sources because customer identity data is often distributed across many different locations, such as the user profile, multiple account records, third-party databases, and CRM and retail systems.

Digital transformation allows the consumer to achieve self-service by providing direct access to integrated systems to provide a unified user experience across all channels. It will also facilitate new ways of engaging customers and delivering value. Pre-built connectors to other systems as well as integration tools facilitate this. As mentioned previously, 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.

CIAM reference architecture

Figure 4 - A Reference Architecture for a Complete CIAM Solution

3.2.1 A WSO2 CIAM Reference Architecture for Digital Transformation

CIAM reference architecture

Figure 5 - A WSO2 Reference Architecture for a Complete CIAM Solution

The two key WSO2 products that enable enterprise digital transformation are WSO2 API Manager and WSO2 Enterprise Integrator.

WSO2 API Manager is an open source API management solution which provides an API gateway and support for API creation, publication, lifecycle management, versioning, monetization, governance, security, rate limiting and analytics using proven WSO2 technology. It provides web interfaces for development teams to deploy and monitor APIs, and for consumers to subscribe to, discover and consume APIs through a user-friendly storefront. WSO2 API Manager consists of several components: API Gateway, Key Manager, Traffic Manager, Publisher Portal, Developer Portal (Store) and Analytics. Depending on the use case and traffic volumes, these components can be deployed in a single runtime or as separate runtimes. APIs can be directly exposed to client applications via the WSO2 API Manager Gateway, and the Key Manager is responsible for securing API access by issuing and validating all security tokens. WSO2 API Manager provides other API management capabilities such as documentation, service discovery via the store and analytics for the exposed APIs. The WSO2 API Analytics profile is deployed as a separate runtime.

The ESB profile in the WSO2 Enterprise Integrator acts as an Enterprise Service Bus (ESB) and provides its fundamental services through an event-driven and standards-based messaging engine (the bus). This enables enterprises to integrate existing systems, legacy systems and APIs in a centralized way. The integration services or APIs responsible for performing integration tasks will be deployed in the ESB and these endpoints will be exposed to the client applications through the API gateway where they will be secured, throttled, and monitored.

As shown in the architecture above, WSO2 Enterprise Integrator will connect all the data stores, CRM systems, marketing solutions, e-commerce platforms, Content Management Systems (CMS), data management platforms and other systems by transforming data seamlessly across different formats and transports to create a unified experience for the end customer. Leveraging existing APIs of these applications to create new APIs to expose data in different or aggregated formats, and connecting to legacy applications via adapters and exposing their data in standard formats via APIs are the major tasks performed by an ESB in a CIAM system.

The management of all integration APIs of the ESB, as well as the existing exposable APIs, are handled by WSO2 API Manager's Gateway, which will centrally route all the API calls initiated from the customer-facing applications to the back-end applications. The gateway can either connect with WSO2 Identity Server or its own Key Manager to check the validity of security tokens, subscriptions and API invocations. When WSO2 Identity Server and WSO2 API Manager coexist in a deployment, the recommended practice is to allow WSO2 Identity Server to behave as WSO2 API Manager's token server instead of the API manager's own Key Manager. This is because the Key Manager is a stripped-down version of WSO2 Identity Server, where the latter can perform all the tasks required by WSO2 API Manager pertaining to token generation and validation.

However, in this consolidated CIAM system, it is recommended to deploy a separate WSO2 API Key Manager as well as WSO2 Identity Server if there is a requirement to expose APIs of the identity server to consuming applications. In that case, the API manager's Key Manager will solely secure APIs of the identity server and the rest of the APIs. Meanwhile, WSO2 Identity Server will take care of the rest of the identity and access management aspects such as identity federation, social login, single sign-on, identity bridging, adaptive and strong authentication, account management and identity provisioning. It will also publish identity events to the WSO2 Identity Analytics Server and leverage the WSO2 Stream Processor as a risk engine. With over 50 connectors available, WSO2 Identity Server can communicate with various identity providers and applications to perform social login, federated authentication and outbound user provisioning.

The Developer Portal/Store component of WSO2 API Manager is a web application, which provides a collaborative interface for API publishers to host and advertise their APIs and for API consumers to self register, discover, evaluate, subscribe to and use secured APIs.

The Customer Portal of WSO2 Identity Server for end users provides a means to manage the user profile or the user account, add security questions, revoke/update the password, manage OpenID profile, and view identity providers, consents, user login sessions, pending approvals, and associated accounts.

WSO2 API Manager provides a Traffic Manager which helps to regulate API traffic, make APIs and applications available to consumers at different service levels, and secure APIs against attacks. The Traffic Manager features a dynamic throttling engine to process throttling policies in real-time including rate limiting of API requests.

The Analytics component of WSO2 API Manager provides reports, statistics and graphs on the APIs deployed. Alerts can be configured to monitor these APIs and detect unusual activity, manage locations via geolocation statistics and carry out a detailed analysis of the logs.

4.0 Summary

CIAM drives revenue growth by leveraging identity data to acquire and retain customers. CIAM systems are designed to provision, authenticate, authorize, collect and store information about consumers from across many domains.

CIAM differs from traditional or workforce IAM in many ways. User experience is as important as privacy and security. Customer on-boarding, single-sign-on, progressive profiling, social integrations, strong and adaptive authentication, self-service, omnichannel support, fraud detection, analytics, and scalability are the key areas any CIAM implementation should be concerned about. CIAM systems generally feature weak password-based authentication, but also support social logins and other stronger authentication methods. Information collected about consumers can be used for many different purposes, such as authorization to resources, for analysis to support marketing campaigns, or fraud detection initiatives. Moreover, CIAM systems must be able to manage many millions of identities, and process potentially billions of logins and other transactions per day.

WSO2 provides a compelling platform to build a comprehensive CIAM solution with its IAM, 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.

Identity data is the new gold, and CIAM is a mainstream business capability that will further empower developers as a way to continuously adapt to new customer and business needs.

5.0 References

[1] Prabath Siriwardena - Customer IAM (CIAM) - Turning Identity Data Into Gold!
https://medium.facilelogin.com/customer-iam-ciam-turning-identity-data-into-gold-3dcfc93f0073

[2] Mary Ruddy - Top 5 Trends in CIAM Solution Design (Gartner Report, March 2018)

[3] Mary Ruddy - Key Features for Customer Identity and Access Management (Gartner Report,

February 2019)

[4] Merritt Maxim and Andras Cser - Market Overview: Customer Identity And Access Management (CIAM) Solutions (Forrester Report, August 2015)

[5] John Tolbert - CIAM Platforms (Kuppingercole Report, December 2018)

[6] WSO2 Identity Server https://wso2.com/identity-and-access-management/

[7] WSO2 API Manager https://wso2.com/api-management/

[8] WSO2 Enterprise Integrator https://wso2.com/integration/

[9] WSO2 Stream Processor https://wso2.com/analytics-and-stream-processing/

[10] A Guide to WSO2 Identity Server https://wso2.com/whitepapers/a-guide-to-wso2-identity-server/

[11] The Forrester Wave™: API Management Solutions, Q4 2018 https://wso2.com/resources/analyst-reports/the-forrester-wave-api-management-solutions-q4-2018/