CIAM?

Customer Identity and Access Management enables organizations to securely capture and manage all sources and forms of customer identity and profile data to provide a seamless digital experience to customers online. WSO2 Identity Server helps you to build agile and extensible CIAM solutions to provide secure and seamless customer experiences that leads to loyalty and increased retention

Must-haves of a CIAM platform

Extensibility | Scalability and Usability | Security | Privacy and compliance

Why opt for CIAM with WSO2

- Fully open source
- Support of a complete integration platform including WSO2 API manager and WSO2 Enterprise Integrator
- All products also come with extension points to extend its feature set to address unique needs
- Highly scalable managing 100mn+ identities
- API-driven and cloud native
- Built on top of open standards including SAML, OAuth, OpenID connect

Requirement	What it means	What WSO2 offers	
Self Registration	Support for self-service registration, social registration and call-center facilitated registration	Account Verification	WSO2 Identity Server can connect to external sources for verification during the registration flow. Based on the external source, a connector can be built. For example, there are customer who are connecting to Salesforce during the use registration for verification
		Registration Flow	Supported out of the box
		Device Registration	Can be implemented via product extensions to connect to 3rd party MDM solutions
Progressive profiling	Support for progressive profiling endpoints as well as out-of-the-box (OOTB) templates	Progressive Profiling	While onboarding a service provider, the required user attributes can be specified during the login flow. If a user lacks any of those attributes, WSO2 Identity Server will prompt the user to enter those during the login flow itself
Single sign-on (SSO) and provisioning	Support for third-party identity providers, support for various approaches to automate provisioning and social identity integration	Single Sign-On (SSO)	WSO2 Identity Server supports SAML 2.0, OpenID Connect and WS-Federation for Single Sign On. Further the identity bridging capabilities in Identity Server lets you transform identity tokesn between multiple heterogeneous federation protocols as well as federated account linking. Users are also able to view, manage (or terminate) their session as preferred. WSO2 also provides SLO including cross protocol single log out to faciliate logging out across heteregenous protocols.
		Federation and Social logins	WSO2 Identity Server provides out of the box support for integrating with multiple social identity providers: Facebook, Google, Apple, Twitter, Yahoo, LinkedIn, Yammer, GitHub, Instagram, Foursquare and many more

Requirement	What it means	What WSO2 offers	
Continuous adaptive risk and trust assessment (CARTA)	Support for different types of adaptive access, multi-factor authentication (MFA) and various approaches to identity validationa	Multi-Factor Authentication	WSO2 Identity Server supports a comprehensive set of authenticators for MFA, including SMS OTP, certificates, biometrics (connectors by Veridium and Knomi), FIDO, RSASecurID, CASQUE, OTP via email, IWA, Google authenticatior (TOTP), mepin and Duo Security Biometrics and Mobiles Biometrics are supported via connecting to biometric service providers through connectors Full list can be found here: store.wso2.com/store/assets/isconnector/list
		Passwordless	Identity Server supports passwordless authentication with FIDO2
		Adaptive Authentication	Supported out of the box - based on user attributes, environment attributes, risk score and other contextual parameters. Includes Brute force protection which is supported out of the box - both the registration flow and login flow There is no additional cost for features and everything is included with the standard subscription mentioned above
		Breached password detection	Can be implemented via product extensions.
Privacy and consent management	Support for consent, preference, and audit capabilities	Consent Management	"At the moment product worries about capturing user concent during the sign up and the login processes. The consent captured is corresponding to the Identity Provider - not related to 3rd party applications. In the future we plan to bring in managing consent with respect to 3rd party applications as well The users can view the consent they have given via the user portal - and have the ability change or revoke. Also the product supports Consent Receipts standard by the Kantara Initiative. WSO2 Identity Server also supports anonymization requests for privacy compliance through its privacy toolkit
		Profile Management	The user portal comes with the Identity Server, lets users manage their profiles. Also - the same functionality is exposed via an API, so can be integrated with 3rd part applications
		Link multiple properties, tenants and domains	By default a user belongs to single tenant. Within a tenant, we can achieve further seperation with multiple identity stores, where each identity store is bound to a domain name. We have many customers who have extended the product to support more complex relation-ships - for example, a user belongs to multiple tenants - and plays different roles under different tenants
		Preference Management	WSO2 Identity Server can be integrated with 3rd party consent and preference management vendors: Consent Systems, Didomi, KnowNow Information, Tealium, TrustArc, etc
		User pseudonimization or anonymization	WSO2 Identity Server provides a privacy toolkit containing a simple command line tool, which can be used with any supported WSO2 product. It will anonymize all related metadata in product databases (excluding user stores), log files and analytics data by removing references to deleted user identities
Marketing, CRM and Sales Integration	Support for integration with CRM and marketing tools	Identity Server connector store	WSO2 Identity Server provides a vast ecosystem with connectors to various marketing applications. This includes: Wordpress, Salesforce, Mailchimp, Dropbox and more
Reporting and analytics	Allows to track user activity, local and service provider login requests and suspicious login attempts	Identity Analytics	Monitor anomalous login patterns, fraud detection

Other Requirements	
Role Based Acess Control	Supported out of the box
Support for REST APIs	Supported out of the box
User Managed Access (UMA 2.0)	Supported out of the box
Security Compliance	Product is complaint with HIPAA, PIC-DSS, SOC. These are mostly deployment specific certifications - and we have customers who have gone through that process and certified
Custom Login Form	Supported out of the box
Omnichannel User Experience	All the functionality of the Identity Server is exposed via APIs and the ominichannel experience can be built on top of that