Customer Identity and Access Management (CIAM) has emerged as a priority for organizations pursuing digital business initiatives that support both customers and IoT devices. IT Architects evaluating CIAM solutions are seeking out reference architectures and design patterns that have a track record of delivering digital business success.

UnboundID has compiled this introduction to CIAM Reference Architectures based on experience implementing high performing, web scale customer identity management platforms for some of the largest and most demanding companies in retail, financial services, telecom, cable/media, healthcare, and high tech. This experience spans more than 1.6 billion total identities under management using the UnboundID Platform.

The reference architecture and supporting Q&A on the following pages represent a first step. Contact UnboundID for additional resources toward a future-proofed CIAM implementation for large enterprise.
CIAM Reference Architecture

Customers

Drive personalized customer experiences and multi-channel customer engagement

Data Consumers

Campaign Management
Fulfillment Service
Loyalty Programs

Govern access to customer data with centralized policies.

Analytics Consumers

3rd Party Analytics Tools

View multi-channel customer engagement trends and metrics.

Operational Consumers

3rd Party Ops Monitoring Tools

Provide visibility into the operational performance of your CIAM infrastructure.

Social Identity Providers

Social login features

Partners

Share customer data with partners

Identity Verification

Identity proofing services

3rd Party DMP

Behavioral/tracking data

API Gateway

Data Sources

Marketing Automation
CRM
Point of Sales
Master Data Management

Leverage comprehensive customer profiles with bi-directional data sync across disparate data sources.

Leverage comprehensive customer profiles with bi-directional data sync across disparate data sources.

UnboundID.com
Frequently Asked Questions

What problem does this CIAM architecture solve? What will it accomplish?

Organizations are pursuing customer-facing digital business initiatives that span multiple engagement channels, such as mobile, web, IoT devices and more. Providing a personalized customer experience that is also consistent across multiple channels requires a customer identity management solution at the center. Customer experience is becoming a competitive differentiator in many industries, and a best practice CIAM implementation can be a key factor for digital business success.

Can my existing workforce IAM system be repurposed to support Customer Identity and Access Management?

In the vast majority of use cases, the answer is “no”, as echoed by prominent analysts including Gartner and Forrester:

“Consumer IAM differs significantly from traditional workforce IAM in scale and function.”

“Due to the difference between employee and customer IAM requirements, IT pros must evaluate specialized CIAM solutions.”

Why is a purpose-built CIAM solution different?

CIAM platforms are designed for different requirements and objectives relative to workforce IAM solutions. CIAM platforms are designed to balance user convenience and security so organizations can effectively attract and retain customers. Workforce IAM systems essentially deal with a captive audience. CIAM platforms leverage rich customer profiles to drive personalized customer experiences, and provide a wide range of self-service customer features to manage preferences, privacy, and data sharing consent. Workforce IAM systems primarily handle credentials and have limited self-service features. CIAM platforms must operate at extreme scale up to 100’s of millions of customers and deliver high performance or customer experience is sacrificed. Workforce IAM systems deal with thousands of users and don’t suffer from customer defections if system performance is sub-optimal.
What unique business functionality is provided through CIAM?

There are several dozen distinct features of a CIAM solution relative to workforce IAM systems. A subset of the most prominent features are listed below. Contact UnboundID for a complete list and a RFP template you can repurpose:

- **Identity Proofing**: A method to verify identities with one or more third-parties before an organization issues customer credentials.
- **Multi-Factor Authentication**: Grant access to resources only after the user successfully provides multiple forms of identity evidence, such as username/password and a code sent via text message.
- **Customer Registration**: Create a new customer account via an application, device or support rep.
- **Single Sign-On**: Enable a single username and password to access multiple systems.
- **Self-Service Account Management**: Enable customers to add/remove/modify their account details.
- **Data Privacy Management**: Allow customers to specify their privacy choices and consent to share personal data.
- **Opt-in/Out Management**: Allows customers to elect to receive communications based on topic, delivery method, and frequency for a more personalized interaction.
- **Social Login**: Offer added convenience by leveraging existing login credentials from third-party identity providers instead of creating new ones.
- **Delegated Account Management**: Enable account access rights can be delegated to others, such as customer service representatives.
- **Personalization and Preference Management**: Capture detailed preference information from customers and manage how this information is shared and used.

Preparing for Future Customer IAM Requirements?

CIAM is just around the corner for many organizations, and your transition to CIAM may be closer than you think. Beyond this introduction to CIAM reference architectures, UnboundID has several additional resources that can assist you on your journey:

1. Get the **CIAM Maturity Model** white paper
2. **Request a Demo** to explore CIAM use cases and scenarios