NextGen Scientific Publication
American International Journal of Computer Science and Technology

Volume 7 Issue 5, Pg. No. 128- 132, AIJCST-V7I5P111, 2025
https://doi.org/10.63282/3117-5481/AIJCST-V7I5P111

Original Article

Designing Hybrid Identity: Workforce and Customer Access at Scale

***Yuga Sai Kiran Reddy Sudini**

Director of Engineering and operations at Public Partnerships LLC, USA.

Abstract:

The rapid adoption of cloud services, remote work, distributed applications, and digital customer platforms has transformed enterprise identity management into a critical component of modern security architecture. Organizations increasingly need to manage distinct identity populations, including internal workforce users and external customers, while maintaining consistent security, scalability, governance, and user experience. This paper presents a hybrid identity architecture that integrates on-premises Active Directory with Microsoft Entra ID for workforce identity management and Azure AD B2C for customer identity and access management. The proposed approach establishes a unified identity strategy while maintaining appropriate separation between workforce and customer identity domains. The architecture incorporates identity synchronization, authentication, authorization, single sign-on, multifactor authentication, conditional access, identity lifecycle management, and policy-based access controls to support secure access across enterprise applications and digital services. For workforce users, integration between Active Directory and Entra ID enables centralized identity management and controlled access to cloud and on-premises resources. For external users, Azure AD B2C provides a scalable CIAM capability supporting customer registration, authentication, profile management, and application access. The framework demonstrates how hybrid identity architectures can improve security, operational efficiency, scalability, and identity governance across heterogeneous environments. The proposed strategy provides a practical foundation for enterprises seeking to modernize identity services while supporting both workforce productivity and secure customer engagement.

Keywords:

Hybrid Identity, Identity and Access Management, Microsoft Entra ID, Active Directory, Azure Ad B2C, Customer Identity and Access Management, Workforce Identity, Authentication, Authorization, Single Sign-on, Multifactor Authentication, Conditional Access, Identity Governance, Cloud Security.

Article History:

Received: 07.08.2025

Revised: 08.09.2025

Accepted: 19.09.2025

Published: 26.09.2025

1. Two Populations, Two Identity Systems

Workforce identity and customer identity are often conflated, but they have fundamentally different requirements. Workforce identity governs employees and internal systems: it is rooted in the organization's directory, optimized for administrative control, and concerned with governing access to internal applications and resources. Customer identity governs the far larger and less controlled population of external users: it must scale to very high volumes, tolerate that users manage their own accounts, defend against abuse and fraud, and deliver a smooth self-service experience to people who are not employees and cannot be centrally administered.

Designing a complete identity strategy means addressing both well, with the right technology for each, while maintaining a consistent security philosophy across them. The two halves are complementary: workforce identity secures the people who build and operate the platform, and customer identity secures the people the platform serves.

2. Workforce Identity: Bridging Active Directory and Entra ID

Most established enterprises do not get to start fresh with a pure cloud identity model. They have years of investment in on-premises Active Directory — the system that governs access to file shares, legacy applications, and domain-joined machines. At the same time, the future is in the cloud, where Entra ID governs access to modern SaaS and cloud-native applications. Hybrid identity is the discipline of making these two worlds function as one, so that a workforce user has a single identity that works seamlessly across both.

The cornerstone of the hybrid model is synchronization between on-premises Active Directory and Entra ID, so that identities exist consistently in both. Users continue to be managed in the on-premises directory the organization already operates, and those identities are projected into the cloud where they govern access to cloud resources. This gives users one identity rather than two, and gives administrators one authoritative source rather than divergent copies to reconcile. I treated the health of that synchronization as a first-class operational concern — monitored and alerted on like any critical service — because a synchronization process that fails silently produces confusing, hard-to-diagnose access problems.

A central design decision in any hybrid deployment is how authentication actually happens — where credentials are validated and how trust flows between environments. I weighed the trade-offs explicitly: the degree to which authentication should depend on on-premises infrastructure, the resilience implications if that infrastructure is unavailable, and the security characteristics of each option. The guiding aim was a model that was both secure and resilient, avoiding a design in which a single on-premises failure could prevent users from authenticating to critical cloud services.

3. Securing the Workforce Identity Fabric

A unified identity is powerful, which is exactly why it must be rigorously protected. Several controls were central to the design:

- **Multi-factor authentication:** requiring more than a password dramatically reduces the risk of credential compromise, which remains among the most common attack vectors in the enterprise.
- **Conditional access:** access decisions that account for context — user, device, location, and risk signals — so that policy adapts to circumstances rather than being uniformly permissive.
- **Least-privilege access:** users and systems receive only the access they genuinely need, limiting the damage any single compromised identity can do.
- **Monitoring and auditing:** visibility into authentication events and access patterns so that anomalies can be detected and investigated, and so that access to sensitive systems is fully accountable.

In a HIPAA-regulated environment, these are not merely good practices; they are part of demonstrating appropriate safeguards over access to protected health information. The identity system is often the first thing an auditor examines, because it is where the question of who can reach protected data is answered.

4. Customer Identity: A B2C Solution Built for Scale and Trust

Serving over a million external users demands an identity system designed for that population specifically. I built the customer identity and access management solution on Azure AD B2C, using custom policies to orchestrate the full range of user journeys — sign-up, sign-in, password reset, profile management, and multi-factor authentication — while integrating with the backend services that verify and provision accounts. The design below shows the solution end to end.

An identifier-first sign-in resolves account state and routes users into the appropriate journey — existing credential validation, migrated-user onboarding, or new-user sign-up — before an authorization step (group membership and adaptive throttling), step-up MFA, and token issuance. Supporting services provide user/CIN verification, account creation, MFA channels, and the throttling configuration store.

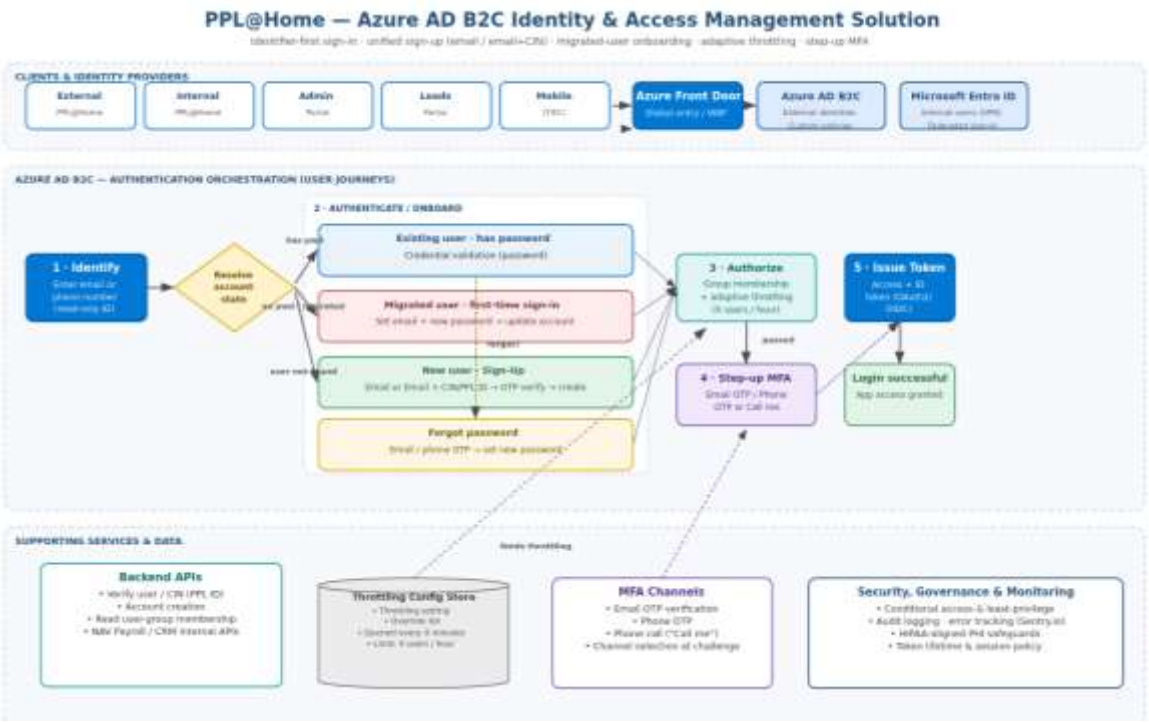

Figure 1. Azure AD B2C Identity and Access Management Solution

Several deliberate design choices in this solution are worth drawing out, because each addresses a real challenge of operating customer identity at scale.

5. Identifier-First Sign-In and Account-State Resolution

Rather than presenting users with a rigid form and hoping they fit it, the journey begins by identifying the user with a single read-only identifier — their email or phone number — and then resolving the state of that account. This identifier-first pattern lets the system route each user into exactly the right journey: an existing user with a password proceeds to credential validation; a user who exists but has no password is routed into first-time onboarding; and an unrecognized identifier is routed into sign-up. This routing is what makes a single entry point serve every category of user gracefully.

6. Onboarding Migrated Users without Friction

A particularly demanding scenario is migrated users — those brought over from a legacy system who may have signed in with a username rather than an email and who have no password in the new system. The solution detects a first-time sign-in of a migrated user and guides them through a controlled onboarding: capturing and verifying a new email address, setting a new password, and updating the account to the modern email-based sign-in. Handling this in the identity layer, rather than forcing a disruptive mass password reset, lets legacy users transition smoothly into the new platform on their first visit.

7. Unified Sign-Up With Domain-Specific Verification

Sign-up supports more than one path within a single, consistent experience. A standard email sign-up verifies the address by one-time passcode and captures a password; a second variant additionally captures a CIN / PPL ID, which is verified against a backend service before the account is created. Supporting distinct sign-up flows through the same policy framework — driven by parameters rather than separate, duplicated implementations — keeps the experience coherent while accommodating the business's need to tie certain accounts to a verified identifier.

8. Adaptive Throttling and Group-Based Authorization

Customer identity systems are exposed to the open internet and must defend against abuse — credential stuffing, automated sign-up fraud, and traffic spikes. The solution incorporates an authorization step that checks group membership and applies adaptive

throttling, governed by a configuration store holding throttling settings and overrides and enforced as a limit expressed in users per hour. Because the throttling configuration is data-driven and periodically refreshed rather than hard-coded, the protection can be tuned in response to conditions without redeploying the identity flows. This is the kind of control that keeps a high-volume customer identity system both available to legitimate users and resistant to abuse.

9. Step-Up MFA and Token Issuance

Multi-factor authentication is offered across channels — email one-time passcode, phone one-time passcode, and a phone call option — with users able to register and select the method that suits them. MFA is applied as a step-up in the journey, challenging the user at the appropriate point before access is granted. Once identity and any required factors are satisfied, the solution issues standard OAuth 2.0 / OpenID Connect tokens, granting the application the access and identity claims it needs. Standard token issuance is what lets the many client applications — web and mobile alike — integrate with the identity system through well-understood, interoperable protocols.

Workforce identity secures the people who build the platform; customer identity secures the people it serves. A complete strategy treats both as first-class.

10. Designing Both for Resilience

Because identity governs access to everything, its availability is critical on both sides. For workforce identity, this meant redundancy in the synchronization and authentication paths and avoiding architectures where a single component's failure could cascade into an organization-wide inability to log in. For customer identity, it meant building the B2C solution and its supporting APIs to remain available under the high and variable load of a million-user population. Resilient identity is a precondition for resilient operations: if people cannot authenticate, nothing else the platform does matters.

11. Consistency across the Whole Strategy

Although workforce and customer identity use different technologies and serve different populations, I held them to a consistent security philosophy: strong authentication as a baseline, least-privilege and context-aware access, protection of sensitive data appropriate to a HIPAA context, comprehensive monitoring and auditability, and resilience as a first-class requirement. That consistency is what makes the two halves feel like one strategy rather than two disconnected systems, and it ensures that the organization's overall identity posture is coherent no matter which population is being served.

12. Principles for a Complete Identity Strategy

The transferable principles are these: recognize that workforce and customer identity are distinct problems and use the right tool for each; give every user one identity within their domain; design entry points that resolve user state and route intelligently; handle hard cases like migrated users in the identity layer rather than through disruptive workarounds; defend high-volume customer identity with adaptive, data-driven throttling and authorization; apply MFA as a contextual step-up; issue standard tokens for interoperable integration; build both halves for resilience; and unify them under a single, consistent security philosophy. Identity done well is the connective tissue that lets an organization operate securely — for the people who build the platform and the far larger number of people who depend on it.

References

[1] Gratton, Lynda. *Redesigning work: How to transform your organization and make hybrid work for everyone*. MIT Press, 2022.
[2] Alkire, Linda, et al. "Transformative service research, service design, and social entrepreneurship: An interdisciplinary framework advancing wellbeing and social impact." *Journal of Service Management* 31.1 (2020): 24-50.
[3] Cornelissen, Joep P., et al. "Building character: The formation of a hybrid organizational identity in a social enterprise." *Journal of Management Studies* 58.5 (2021): 1294-1330.
[4] Kannothra, Chacko G., Stephan Manning, and Nardia Haigh. "How hybrids manage growth and social–business tensions in global supply chains: The case of impact sourcing." *Journal of Business Ethics* 148.2 (2018): 271-290.
[5] TOROSYAN, MARIANNA. "Redesigning Luxury Brand Organizations: Hybrid Jobs and Inclusivity." (2024).
[6] Hopkins, John, and Anne Bardoel. "The future is hybrid: how organisations are designing and supporting sustainable hybrid work models in post-pandemic Australia." *Sustainability* 15.4 (2023): 3086.
[7] Dowling, Bonnie, et al. "Hybrid work: Making it fit with your diversity, equity, and inclusion strategy." *The McKinsey Quarterly* 4 (2022): 1-9.

[8] He, Tong, et al. "Toward social enterprise sustainability: The role of digital hybridity." *Technological Forecasting and Social Change* 175 (2022): 121360.
[9] Oppong Peprah, Emmanuel. "Hybrid workplace: current status, positives, negatives, challenges, and team learning." *The Learning Organization* 31.1 (2024): 88-103.
[10] Battilana, Julie, and Silvia Dorado. "Building sustainable hybrid organizations: The case of commercial microfinance organizations." *Academy of management Journal* 53.6 (2010): 1419-1440.
[11] Manning, Stephan, Chacko G. Kannothra, and Nichole K. Wissman-Weber. "The strategic potential of community-based hybrid models: The case of global business services in Africa." *Global Strategy Journal* 7.1 (2017): 125-149.
[12] Borg, Cornelia, and Caoimhe O'Sullivan. "The corporate brand identity in a hybrid workplace model." (2021).
[13] Tahsiri, Mina. "Towards designing for the postdigital hybrid workplace: A systematic literature review." *Enquiry The ARCC Journal for Architectural Research* 20.1 (2023): 1-19.
[14] Pearce, Brandi, et al. "Cultivating place identity at work." *Organizational Dynamics* 52.3 (2023): 100997.
[15] Boyd, Brewster, et al. *Hybrid organizations: New business models for environmental leadership*. Routledge, 2017.