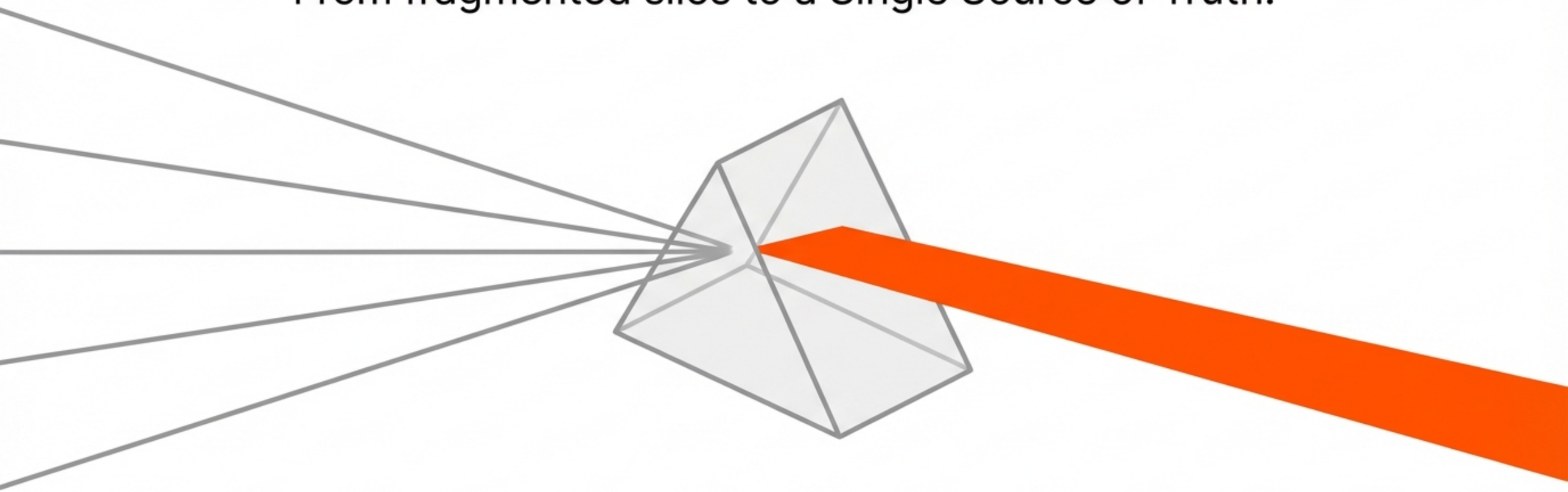
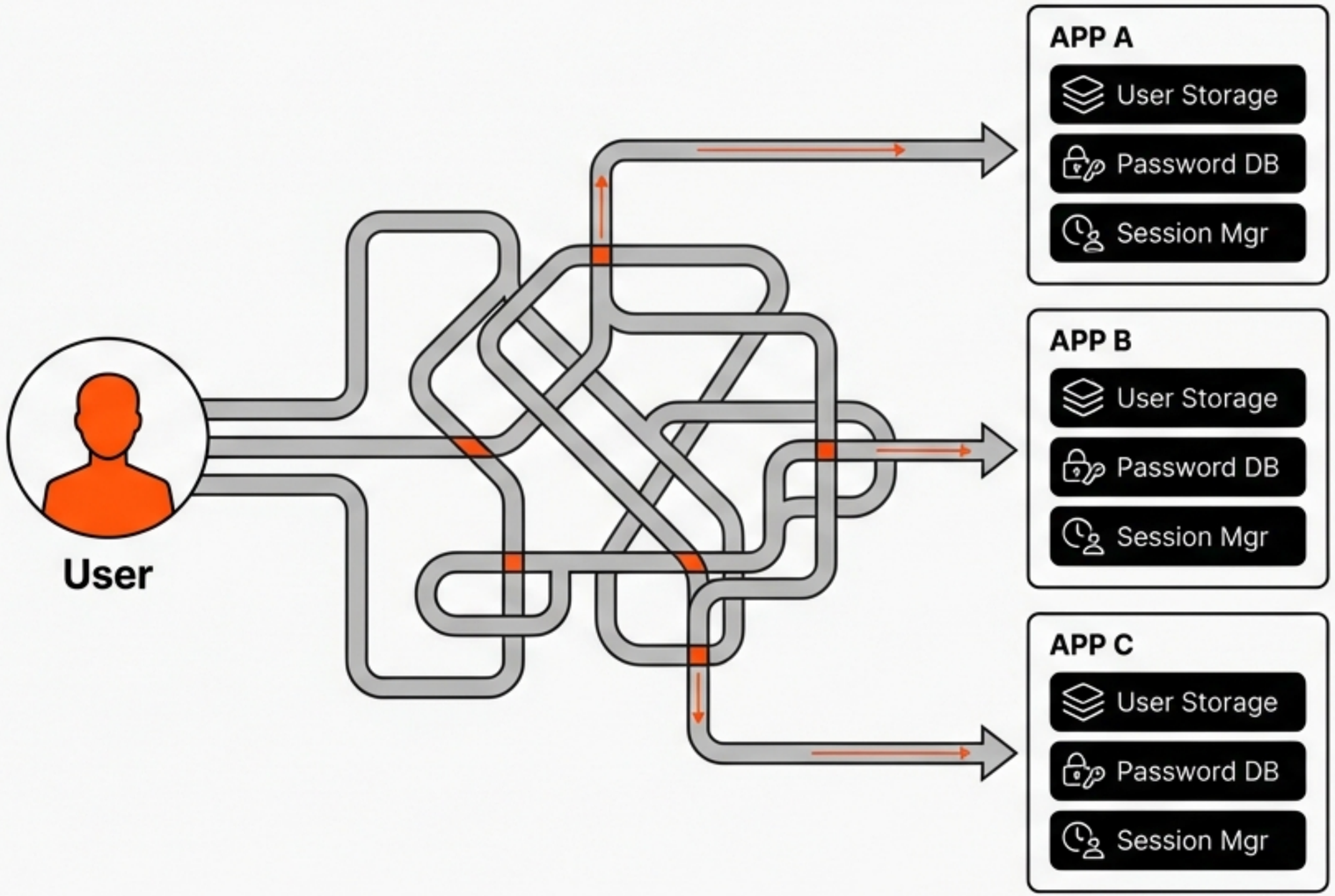
UNIFIED IDENTITY ACCESS

From fragmented silos to a Single Source of Truth.



ARCHITECTURE | PROTOCOLS | BENEFITS

The Fragmentation of Identity



Redundant Logic

Every application independently handles passwords, sessions, and storage.

Synchronization Lag

Data becomes isolated and constantly out of sync across systems.

Friction

Users face multiple logins and fatigue.

The Hidden Costs of Decentralization

Expanded Attack Surface

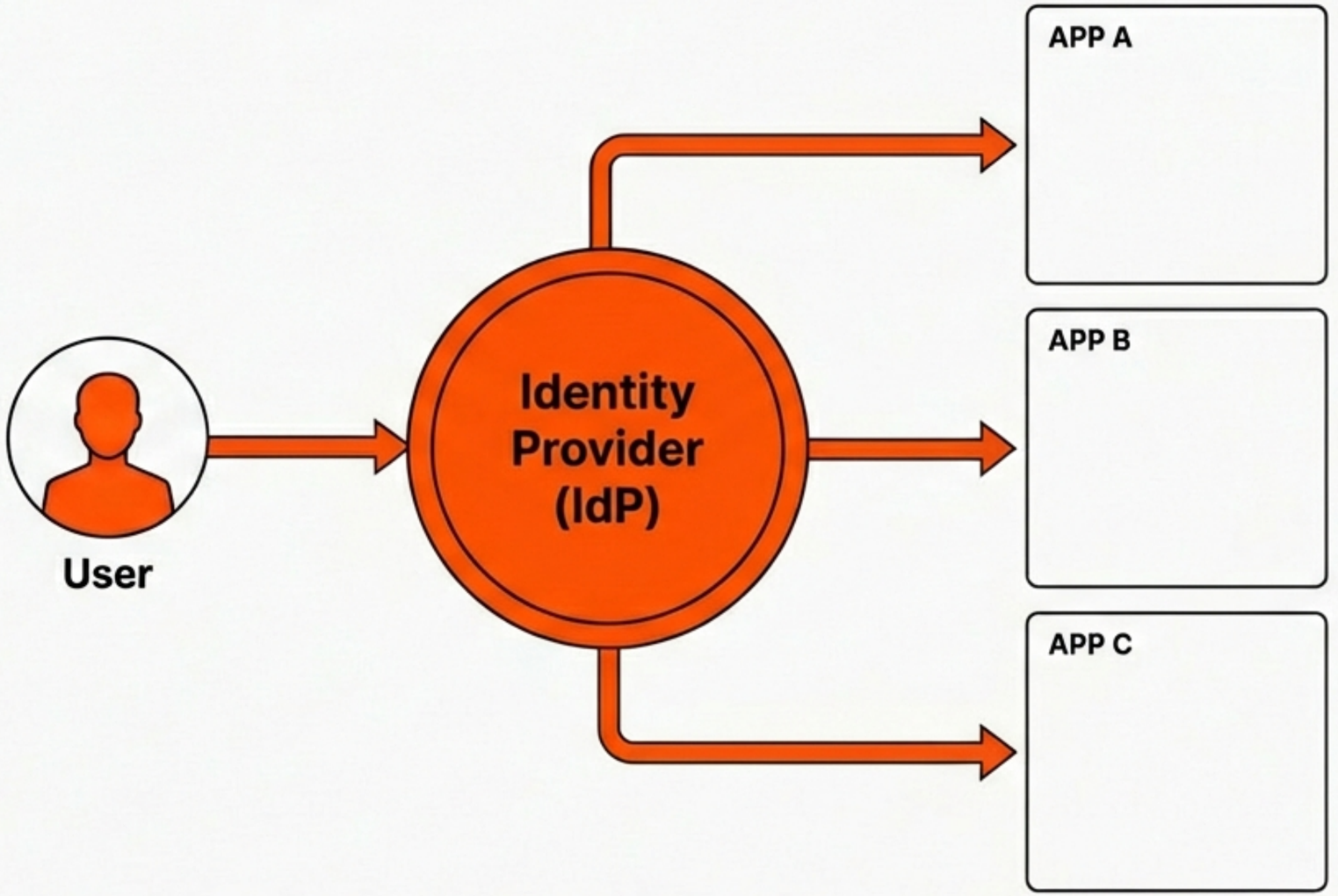
Management Overhead

Risk Multiplier: Storing credentials in multiple locations increases breach probability.

Scaling Friction: Security logic must be rebuilt for every new service.

Role Complexity: Permissions trapped in isolated databases are hard to manage.

The Single Sign-On (SSO) Standard



The Concept

Login once, access everything.

The Shift

Authentication responsibility is removed from apps and centralized in the IdP.

The Result

Apps stop acting as bouncers and start acting as gatekeepers verifying a pass.

Architectural Precision

The Architecture of Trust

THE USER: The entity seeking access (Human or Machine).

THE APP: The resource or service relying on the IdP (Service Provider).

THE IDP: The central authority (e.g., Azure Entra ID) that verifies identity.

THE TOKEN: The The digital proof issued by the IdP.

The Currency of Access: Tokens

ID TOKEN

Proves WHO you are.
Contains profile info.

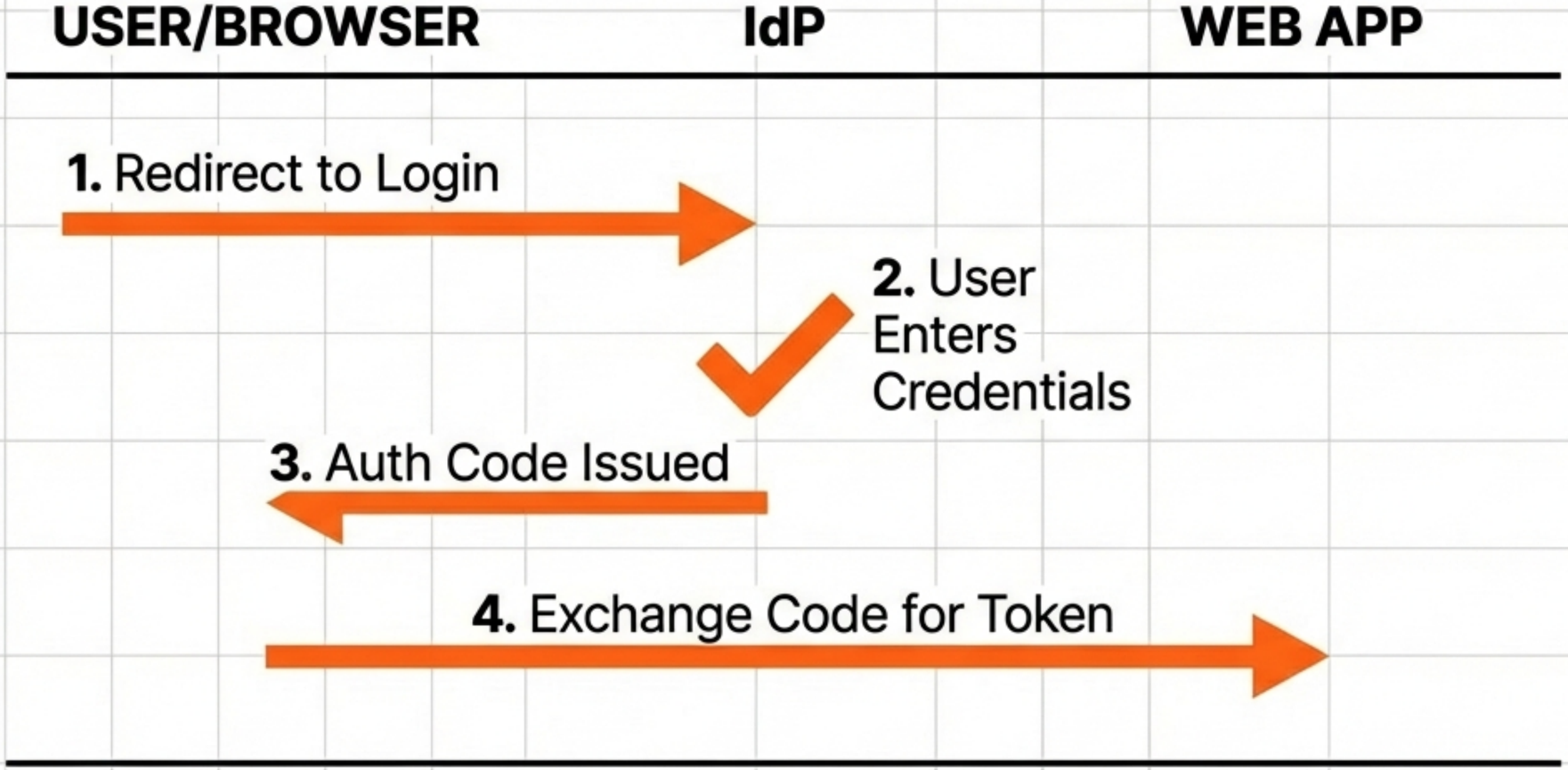
ACCESS TOKEN

Proves WHAT you can do.
Authorizes access to resources.

Issued by the IdP, consumed by the App.
No passwords exchanged.

Protocol 01: Authorization Code Flow

Standard for Web Applications

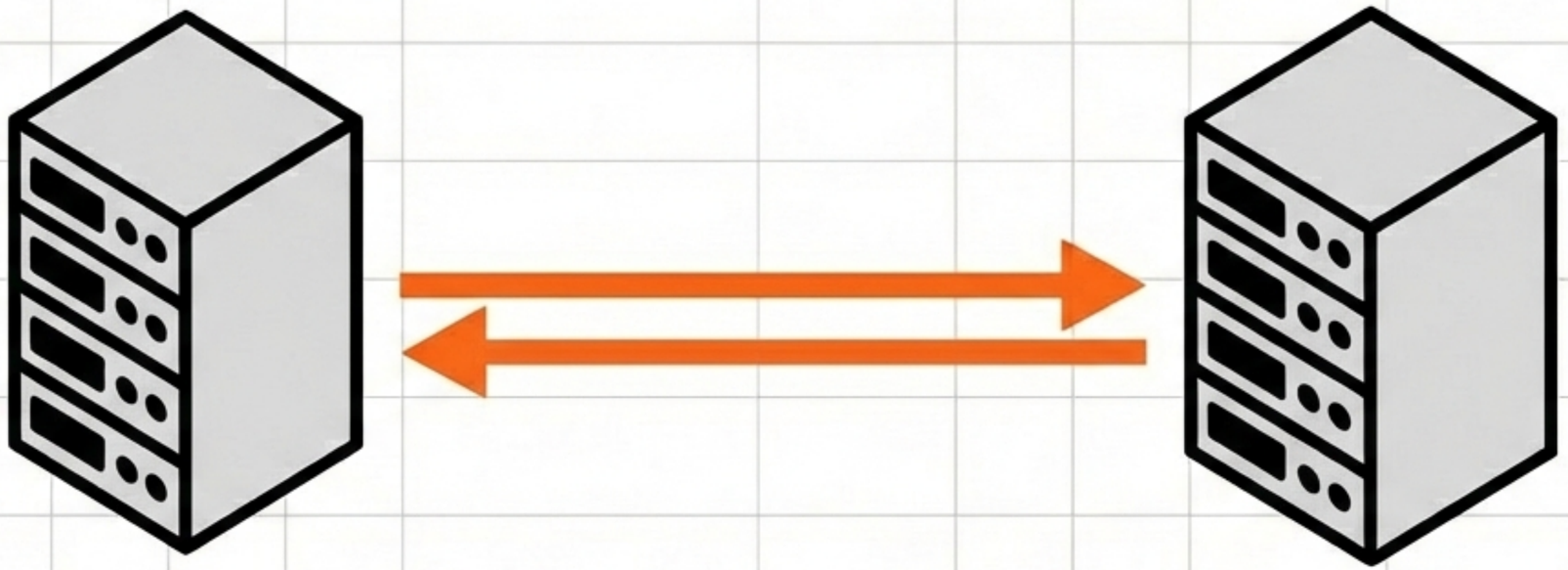


The “Handshake” ensures tokens are never exposed in the browser URL.

The app exchanges a one-time code plus a secret to get the final Access Token.

Protocol 02: Client Credentials Flow

Standard for Service-to-Service Communication



1. Identity: The Service holds its own **Client ID & Secret**.

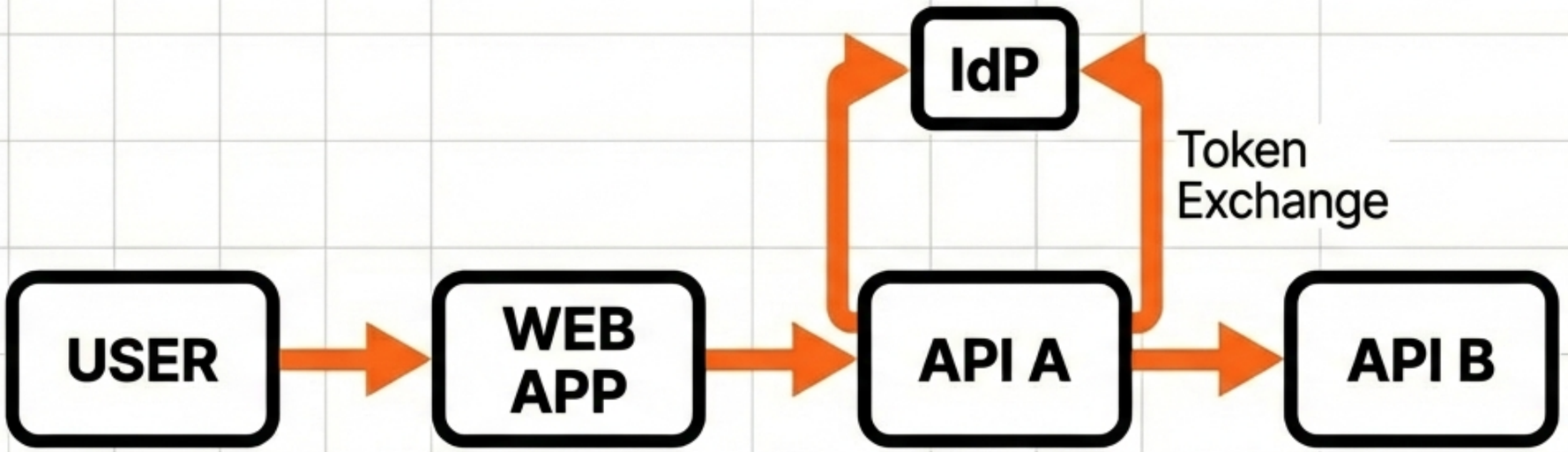
2. Request: Service authenticates directly with IdP.

3. Access: IdP issues Token for machine access.

Best for background processes and daemons. No human interaction required.

Protocol 03: On-Behalf-Of (OBO) Flow

Chaining Identity across APIs



The Context: User calls API A.

The Problem: API A needs to call API B *as the user**, not as itself.

The Solution: API A sends the user's token to the IdP to get a *new* token specifically for API B.

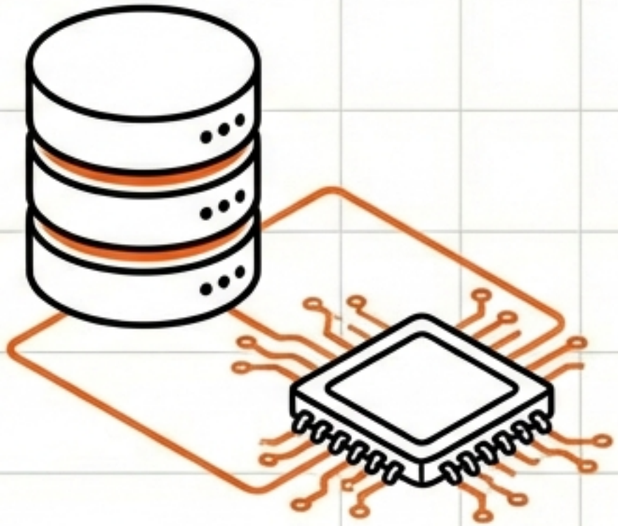
Result: Identity context is preserved down the chain.

Applied Architecture: Real-World Use Cases

THE WORKFORCE

Employees accessing HR portals. Uses **Authorization Code Flow** for secure, interactive login via Azure Entra ID.

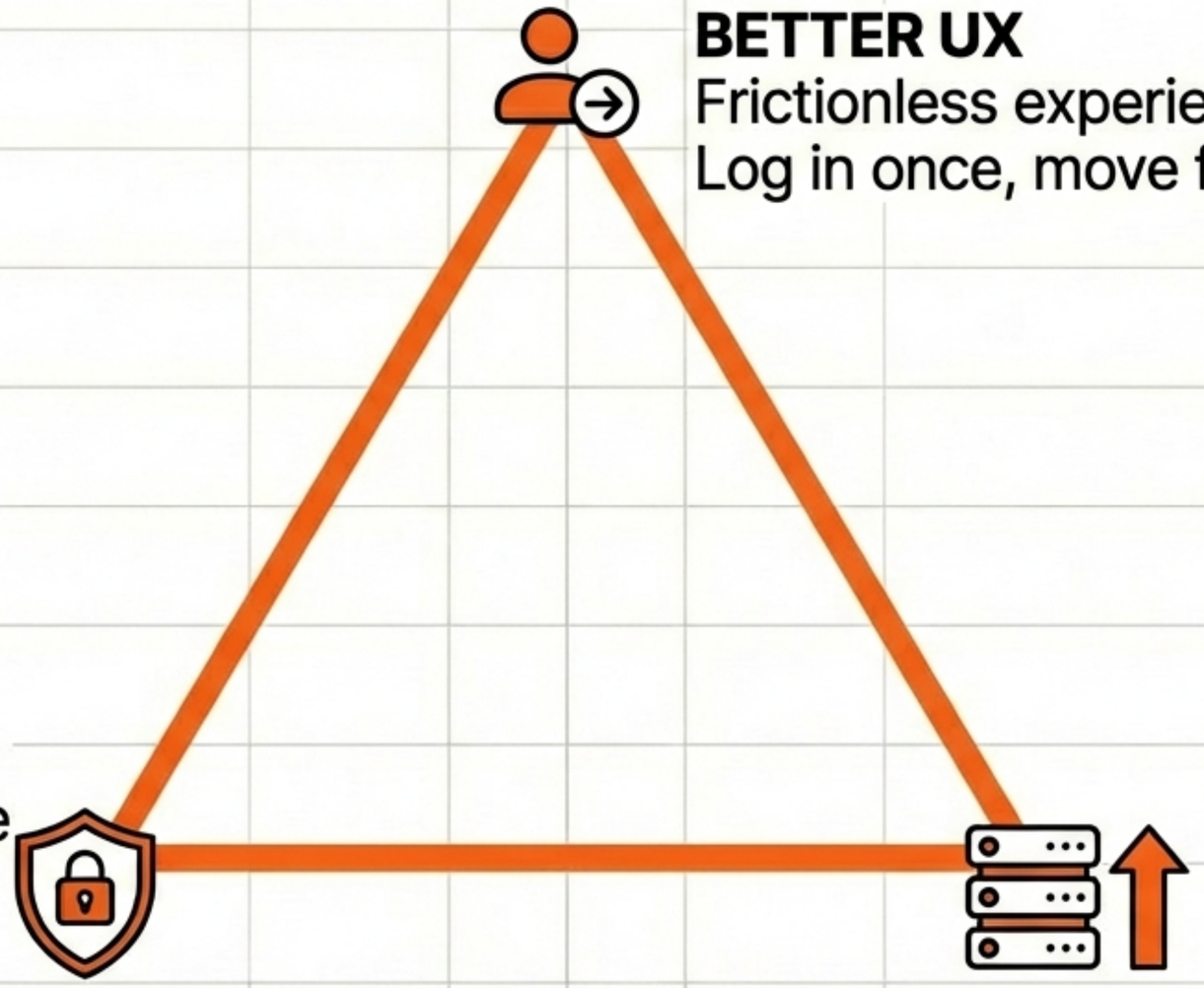
THE ENGINE ROOM



Order processing service talking to inventory DB. Uses **Client Credentials Flow** for high-speed machine-to-machine communication.

The Dividends of Unified Access

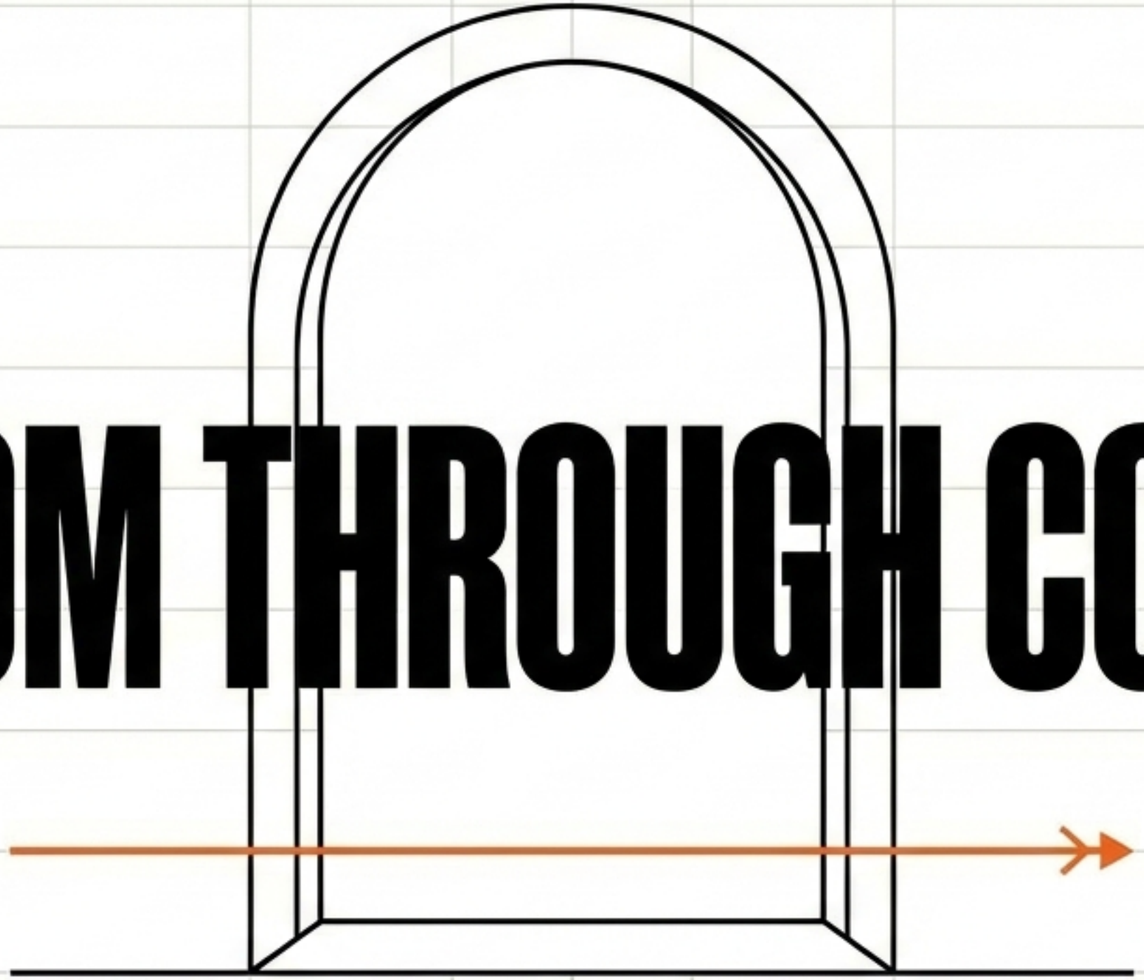
BETTER UX
Frictionless experience.
Log in once, move freely.



CENTRALIZED SECURITY
Policy enforced in one place. Ecosystem-wide protection.

EASIER SCALING
Add apps without rebuilding logic.
Zero sync lag.

FREEDOM THROUGH CONTROL



By **centralizing the entrance**, we open the ecosystem. Unified Identity Access transforms security from a roadblock into an enabler of scale.