

Authorize services provide Identity and Access Management (IAM), which includes access control and secure, centralized mechanisms to manage identities, authentication, and authorization of users, services, and devices.

## Value

- **Enterprise-identity approach:** IAM provides capabilities for harmonizing multiple applications built on HSDP, enabling clients to use a single identity across multiple applications
- **Standard identity management workflows:** Standards-based identity, authentication, and authorization capabilities that eliminate redundant, error-prone, and often incomplete implementations of standard workflows
- **Cross-platform integration:** A centralized set of enterprise IAM mechanisms that enable identity integration across consumer or healthcare applications built on HSDP
- **Collaboration with third parties:** Support integration and collaboration with third-party applications and services through federation and single sign-on capabilities

**Authentication services** in IAM ensure that users and machines are who they claim to be before they are granted access to resources. These services support the following protocols to enable secure, scalable, and seamless authentication across applications and systems:

- OAuth 2.0
- SAML (Security Assertion Markup Language)
- OIDC (OpenID Connect)
- MFA (Multi-Factor Authentication)

**Authorization services** in IAM determine what actions a user or machine is allowed to perform after authentication. These services enforce access policies based on identity roles, attributes, and permissions while supporting key functionalities like token validation, introspection, and policy evaluation.

## Features

**Identity management services** are a core component of IAM, responsible for managing user identities, M2M identities, roles, and access privileges across an IAM account's organizational hierarchy. These services ensure that the right individuals have the appropriate access to resources while maintaining security, compliance, and operational efficiency.

Key functions of these services include organization management, user life cycle management, M2M life cycle management, fine-grained access control for user roles and group memberships, self-service and delegated administration, and audit and compliance management.

- **Identity Token Validation** – Verifies OAuth 2.0, JWT, or SAML tokens to confirm a user's or machine's identity before granting access.
- **Token Introspection** – Allows APIs or services to check the validity and metadata of an access token (e.g., active status, expiration, scopes).
- **Policy-Based Access Control (PBAC)** – Evaluates access requests based on predefined RBAC (Role-Based Access Control) or GBAC (Group-Based Access Control) policies.
- **Fine-Grained Authorization** – Supports context-aware access based on dynamic conditions like organization context, type of resource, subject context, and permission.
- **Delegated Authorization** – Implements standards like OAuth 2.0 Scopes and Consent Management for third-party access control.

For more information,  
please go to [hsdp.io](https://hsdp.io).