PHILIPS

HealthSuite

digital platform

Authorize

Our secure identity and access management with a unified view into security policy, authorization, consent and data privacy.

Authorize services provide Identity and Access Management (IAM), the secure, centralized mechanisms to manage identities, authentication and authorization of users, services and devices and enable access control. It also includes Terms and Conditions Management to manage consent and ensure data security and privacy.

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 to eliminate redundant, error-prone, and often incomplete (re)-implementation of standard workflows
- **Cross-platform integration**: Centralized set of enterprise identity and access management mechanisms that enable identity integration across consumer or healthcare applications built on HSDP
- **Cross-infrastructure integration**: access across the HSDP cloud infrastructure with a single credential
- **Collaboration with third parties**: Support integration and collaboration with third-party applications and services through federation and single sign-on capabilities

Features

- **Identity Management** services enable the management and verification of identities across multiple applications built on the HSDP
  - Creation and management of identities for users, devices, applications, and services
  - Creation and management of groups, roles, permissions, and organizations to model the desired organizational structure and role-based access patterns
- **Authentication services** provide mechanisms for verifying identities and managing passwords and policies,
  - Verification of identities based on OAuth2 authorization grant types (code grants, authentication code grants, and client credentials), JSON Web Token (JWT) grant type, and client credentials
  - Two-factor authentication based on one-time password (OTP)
  - Identity federation with third-party identity systems through OpenID Connect and SAML2
  - Social sign-on support with Facebook and Google
- **Authorization** services enable flexible role-based authorization and access control
  - Authorization of identities based on group membership to ensure controlled access to data by identities with specific roles
  - Token management and policy management
  - Consumer self-registration with account management and password management, including standardized policies for expiration, history, and complexity
- **Terms and Conditions Management** service provides a mechanism to control and track user acceptance of terms and conditions documents. This service stores and manages URLs of application terms and conditions and enables a workflow to enforce acceptance of the latest versions

Consult hsdp.io for details