
CÔNG TY CỔ PHẦN BẢO HIỂM NGÂN HÀNG NÔNG NGHIỆP (ABIC)**HỆ THỐNG QUẢN LÝ ĐỊNH DANH TẬP TRUNG
VÀ ĐĂNG NHẬP MỘT LẦN**

Xây dựng trên nền tảng Duende IdentityServer

YÊU CẦU KỸ THUẬT VÀ DANH MỤC TÍNH NĂNG

PHỤ LỤC 01: YÊU CẦU VỀ MÔ HÌNH HỆ THỐNG VÀ NỀN TẢNG CÔNG NGHỆ

1. Yêu cầu về mô hình kiến trúc tổng thể

Hệ thống phải được xây dựng theo kiến trúc phân tầng, tách bạch giữa máy chủ xác thực và hệ quản trị, triển khai dưới dạng các dịch vụ độc lập:

- Tầng xác thực (STS – Identity Provider): là điểm đăng nhập duy nhất của toàn bộ hệ sinh thái ứng dụng ABIC. Cung cấp giao diện đăng nhập, đăng ký, xác thực đa yếu tố, khóa truy cập passkey, màn hình đồng thuận cấp quyền, trang cá nhân người dùng và toàn bộ endpoint chuẩn OpenID Connect / OAuth 2.0 để các ứng dụng đầu nối.

- Tầng quản trị (Admin API và Admin UI): dịch vụ API quản trị được bảo vệ bằng OAuth 2.0, phục vụ ứng dụng quản trị một trang (SPA). Cho phép quản trị viên cấu hình ứng dụng client, tài nguyên, người dùng, vai trò, phân quyền, theo dõi nhật ký và kiểm tra cấu hình.

- Tầng tích hợp: gồm module đọc dữ liệu người dùng từ hệ thống Core của ABIC và module đồng bộ mật khẩu ra các dịch vụ thư mục bên ngoài. Hoạt động dưới dạng dịch vụ nền chạy theo chu kỳ, không phụ thuộc thao tác thủ công.

- Tầng dữ liệu: sáu nhóm cơ sở dữ liệu logic tách biệt theo chức năng; bắt buộc chạy được trên Oracle 19C, thông qua bộ migration riêng cho từng hệ quản trị.

2. Yêu cầu về nền tảng công nghệ

Các công nghệ và phiên bản nêu dưới đây là mức tối thiểu. Đơn vị thực hiện có thể đề xuất công nghệ tương đương hoặc mới hơn kèm thuyết minh, và phải được ABIC chấp thuận trước khi triển khai.

Hạng mục	Yêu cầu về công nghệ
Nền tảng ứng dụng	.NET 10 / ASP.NET Core 10.0 trở lên, ngôn ngữ C#
Máy chủ xác thực (IdP)	Duende IdentityServer phiên bản 7.x trở lên, tích hợp với ASP.NET Core Identity và Entity Framework Core
Quản lý người dùng	ASP.NET Core Identity trên Entity Framework Core

Hạng mục	Yêu cầu về công nghệ
Giao diện đăng nhập (STS)	ASP.NET Core MVC - Razor Views, TailwindCSS hoặc framework CSS tương đương
Giao diện quản trị (Admin UI)	Ứng dụng SPA: React 18 trở lên với TypeScript, công cụ đóng gói Vite; thư viện thành phần giao diện có khả năng truy cập (Radix UI / shaden-ui hoặc tương đương); quản lý truy vấn và bảng dữ liệu (TanStack Query, TanStack Table hoặc tương đương); kiểm tra hợp lệ biểu mẫu; biểu đồ thống kê; đa ngôn ngữ Việt/Anh
Truy cập dữ liệu	Entity Framework Core - mô hình Code-First, migration tách riêng theo từng hệ quản trị cơ sở dữ liệu
Hệ quản trị CSDL	Bắt buộc hỗ trợ Oracle; khuyến khích hỗ trợ đồng thời Microsoft SQL Server và PostgreSQL
Ánh xạ đối tượng	Thư viện ánh xạ sinh mã tại thời điểm biên dịch, hạn chế sử dụng reflection nhằm bảo đảm hiệu năng
API và tài liệu API	ASP.NET Core Web API; sinh đặc tả OpenAPI/Swagger và thư viện client TypeScript cho ứng dụng quản trị
Ghi log và kiểm toán	Ghi log tập trung có cấu trúc (Serilog hoặc tương đương) với nhiều đích ghi: tệp, cơ sở dữ liệu, hệ thống log tập trung; nhật ký kiểm toán riêng cho thao tác quản trị
Giám sát tình trạng	Health check cho máy chủ xác thực, cơ sở dữ liệu và các dịch vụ phụ thuộc, có giao diện theo dõi
Bảo mật tầng HTTP	Content Security Policy, HSTS, chống clickjacking, chống MIME sniffing thông qua middleware security headers
Bảo vệ khóa dữ liệu	ASP.NET Core Data Protection lưu trữ trên cơ sở dữ liệu; hỗ trợ tùy chọn bảo vệ khóa bằng kho khóa tập trung

Hạng mục	Yêu cầu về công nghệ
Quản lý bí mật, chứng thư số	Hỗ trợ tệp PFX, kho chứng thư của máy chủ và kho khóa tập trung (Azure Key Vault hoặc tương đương)
Đăng nhập qua nhà cung cấp ngoài	Azure AD / Microsoft Entra ID, Google Workspace, LDAP; có khả năng mở rộng thêm nhà cung cấp OpenID Connect khác
Đồng bộ Directory	Google Admin SDK Directory API (Google Workspace), Microsoft Graph (Entra ID), System.DirectoryServices (Active Directory)
Xác thực không mật khẩu	Passkey / WebAuthn (FIDO2)
Gửi thư điện tử	SMTP hoặc dịch vụ gửi thư qua API
Định tuyến, cân bằng tải	Hoạt động được sau reverse proxy; hỗ trợ triển khai nhiều nút phía sau bộ cân bằng tải
Đóng gói và triển khai	Đóng gói bằng Docker, mỗi dịch vụ một container; kèm script hỗ trợ build, migration và triển khai
Tích hợp hệ thống Core ABIC	Đọc dữ liệu người dùng trực tiếp từ cơ sở dữ liệu Oracle của hệ thống Core theo hướng dẫn của ABIC

3. Danh mục thành phần phần mềm cần xây dựng

TT	Thành phần	Vai trò
1	Máy chủ xác thực tập trung (STS / Identity Provider)	Trang đăng nhập, đăng ký, xác thực đa yếu tố, passkey, đồng thuận cấp quyền, luồng thiết bị, quản lý phiên và hồ sơ người dùng; cung cấp toàn bộ endpoint OpenID Connect / OAuth 2.0
2	Dịch vụ API quản trị (Admin API)	Bộ API quản trị người dùng, vai trò, claim, ứng dụng client, tài nguyên API, phạm vi truy cập, tài nguyên định danh, nhà cung cấp định danh, khóa

TT	Thành phần	Vai trò
		ký, ủy quyền đã cấp, bảng điều khiển, nhật ký và kiểm tra cấu hình
3	Ứng dụng quản trị (Admin UI)	Ứng dụng một trang (SPA) cung cấp toàn bộ giao diện quản trị, đa ngôn ngữ Việt/Anh
4	Máy chủ phục vụ ứng dụng quản trị	Phục vụ ứng dụng quản trị, xác thực quản trị viên qua chính máy chủ xác thực tập trung
5	Tầng nghiệp vụ dùng chung	Service, DTO, kiểm tra hợp lệ và ánh xạ dữ liệu dùng chung cho các thành phần
6	Tầng truy cập dữ liệu	DbContext, repository, cấu hình mô hình dữ liệu và các tùy biến riêng cho Oracle
7	Bộ migration cơ sở dữ liệu	Migration tách riêng cho từng hệ quản trị cơ sở dữ liệu được hỗ trợ
8	Module tích hợp hệ thống Core ABIC	Đọc hồ sơ người dùng và trạng thái tài khoản từ hệ thống Core; đồng bộ mật khẩu về Core
9	Module đồng bộ dịch vụ thư mục	Đồng bộ mật khẩu sang Google Workspace, Microsoft Entra ID và Active Directory
10	Thư viện cấu hình và tiện ích dùng chung	Cấu hình tập trung, tiện ích dùng chung cho toàn bộ giải pháp
11	Bộ công cụ và tài liệu tích hợp cho ứng dụng client	Script phát hiện đăng xuất SSO, tài liệu hướng dẫn đầu nối và mẫu cấu hình cho các ứng dụng nội bộ

4. Yêu cầu về tổ chức cơ sở dữ liệu

Hệ thống phải tách thành sáu nhóm cơ sở dữ liệu logic dưới đây, có thể đặt trên cùng một hoặc nhiều máy chủ cơ sở dữ liệu tùy quy mô triển khai:

Nhóm cơ sở dữ liệu	Nội dung lưu trữ
Cấu hình IdentityServer	Ứng dụng client, tài nguyên API, phạm vi truy cập, tài nguyên định danh, nhà cung cấp định danh
Ủy quyền đã cấp	Ủy quyền đã lưu, mã ủy quyền, refresh token, khóa ký, phiên phía máy chủ
Định danh người dùng	Người dùng, vai trò, claim, đăng nhập ngoài, token, lịch sử hoạt động đăng nhập
Nhật ký hệ thống	Log vận hành của các dịch vụ
Nhật ký kiểm toán	Nhật ký thao tác quản trị
Khóa bảo vệ dữ liệu	Khóa mã hóa của ASP.NET Core Data Protection

5. Chuẩn và giao thức bắt buộc tuân thủ

Nhóm chuẩn	Nội dung
OpenID Connect 1.0	Authorization Code Flow kèm PKCE, Hybrid Flow, Discovery Document, UserInfo, JWKS
OAuth 2.0 / 2.1	Client Credentials, Refresh Token, Device Authorization Grant, Token Introspection, Token Revocation, DPoP
Đăng xuất	Front-channel logout, Back-channel logout, End Session Endpoint, kiểm tra trạng thái phiên
Định dạng token	JWT có chữ ký số, Reference Token; luân chuyển khóa ký tự động
Xác thực đa yếu tố	TOTP theo RFC 6238 (ứng dụng Authenticator), mã khôi phục
Xác thực không mật khẩu	WebAuthn / FIDO2 Passkey
Thư mục người dùng	LDAP v3, Microsoft Graph, Google Admin SDK Directory API

Nhóm chuẩn	Nội dung
Khác	SMTP, HTTPS/TLS, Content Security Policy, CORS, Forwarded Headers (reverse proxy)

6. Yêu cầu về mô hình triển khai

- Mỗi dịch vụ phải được đóng gói thành một container Docker độc lập, hoạt động được sau reverse proxy đảm nhiệm chấm dứt TLS và định tuyến theo tên miền; triển khai được trên máy chủ vật lý, máy ảo hoặc cụm Kubernetes.

- Máy chủ xác thực được công bố tại một tên miền duy nhất (<https://sso.abic.com.vn>); giao diện quản trị và API quản trị được công bố tại tên miền riêng, giới hạn truy cập theo dải mạng nội bộ.

- Chứng thư số ký token và các bí mật cấu hình phải được quản lý tập trung qua kho khóa hoặc kho chứng thư của máy chủ; khóa mã hóa dữ liệu lưu trên cơ sở dữ liệu và tự động luân chuyển.

- Quá trình di trú cơ sở dữ liệu và khởi tạo dữ liệu ban đầu phải thực hiện tự động khi khởi động dịch vụ, kèm bộ script hỗ trợ tạo và hoàn tác migration.

- Hệ thống phải vận hành được ở chế độ nhiều nút phía sau bộ cân bằng tải, phục vụ giai đoạn mở rộng.

PHỤ LỤC 02: MÔ TẢ CHI TIẾT HẠNG MỤC CÔNG VIỆC

TT	Danh mục công việc	Mô tả chi tiết công việc
1	Khảo sát, tư vấn, thiết kế kiến trúc hệ thống định danh tập trung (SSO/IdP) theo đặc thù ABIC	- Khảo sát hiện trạng các ứng dụng nội bộ của ABIC và cơ chế đăng nhập đang sử dụng. - Tư vấn mô hình xác thực tập trung theo chuẩn OpenID Connect / OAuth 2.0. - Thiết kế kiến trúc ba thành phần: máy chủ xác thực (STS), dịch vụ API quản trị và giao diện quản trị. - Chuẩn hóa dữ liệu người dùng, cơ cấu tổ chức, vai trò và claim dùng chung cho toàn bộ ứng dụng.
2	Xây dựng máy chủ xác thực tập trung (STS – Security Token Service)	- Đăng nhập, đăng xuất tập trung; đăng nhập một lần (SSO) và đăng xuất một lần (SLO). - Hỗ trợ đầy đủ các luồng cấp phát token: Authorization Code kèm PKCE, Client Credentials, Refresh Token, Device Flow. - Xác thực đa yếu tố (2FA/TOTP), mã khôi phục, khóa truy cập Passkey/WebAuthn. - Quản lý phiên phía máy chủ và thu hồi phiên từ xa.
3	Xây dựng phần mềm quản trị định danh (Admin UI và Admin API)	- Xây dựng giao diện quản trị dạng SPA và bộ API quản trị tương ứng. - Quản lý người dùng, vai trò, claim, ứng dụng client, tài nguyên API và tài nguyên định danh, phạm vi truy cập, khóa ký, phiên và ủy quyền đã cấp. - Bảng điều khiển thống kê, kiểm tra cấu hình và nhật ký kiểm toán. - Đa ngôn ngữ Việt/Anh, giao diện sáng/tối, nhận diện thương hiệu ABIC.

TT	Danh mục công việc	Mô tả chi tiết công việc
4	Tích hợp và đồng bộ dữ liệu người dùng với hệ thống Core của ABIC	- Xây dựng dịch vụ đồng bộ dữ liệu người dùng từ Core - Đồng bộ toàn bộ người dùng lần đầu và dịch vụ nền đồng bộ gia tăng theo chu kỳ. - Đồng bộ trạng thái khóa tài khoản; đồng bộ thông tin đơn vị, phòng ban, chức danh sang claim. - Lọc dữ liệu theo loại đối tượng người dùng và miền thư điện tử được phép.
5	Tích hợp nhà cung cấp định danh ngoài và đồng bộ mật khẩu Directory	- Tích hợp đăng nhập qua Azure AD / Microsoft Entra ID, Google Workspace, Facebook, GitHub và LDAP. - Đồng bộ mật khẩu sang Google Workspace, Entra ID, Active Directory và Core khi người dùng đổi hoặc đặt lại mật khẩu. - Cấu hình bật/tắt từng đích đồng bộ, thời gian chờ và cách hiển thị lỗi cho người dùng.
6	Xây dựng bộ API và cơ chế phát hiện đăng xuất cho ứng dụng client	- Cung cấp bộ API quản trị được bảo vệ bằng OAuth 2.0 kèm tài liệu Swagger. - Xây dựng endpoint kiểm tra trạng thái phiên và script nhúng để ứng dụng client tự động đăng xuất khi phiên SSO kết thúc hoặc bị thu hồi. - Hướng dẫn tích hợp cho từng ứng dụng: chỉ bổ sung một dòng script, không phải sửa cấu hình ứng dụng.
7	Thiết lập hệ thống ban đầu, di trú cơ sở dữ liệu cho mỗi đơn vị	- Tự động tạo và di trú cơ sở dữ liệu, khởi tạo dữ liệu ban đầu: vai trò, tài khoản quản trị, ứng dụng client và tài nguyên mặc định. - Hỗ trợ đa hệ quản trị cơ sở dữ liệu: Oracle, SQL Server, PostgreSQL. - Cấu hình chứng thư số ký token, bảo vệ khóa dữ liệu, chính sách CSP và reverse proxy.

TT	Danh mục công việc	Mô tả chi tiết công việc
8	Đào tạo vận hành, chuyển giao hệ thống	- Lớp đào tạo cán bộ quản trị hệ thống: vận hành giao diện quản trị, cấp phát ứng dụng client, phân quyền người dùng. - Lớp đào tạo cán bộ công nghệ thông tin tích hợp ứng dụng: đấu nối OIDC, đọc claim, xử lý đăng xuất SSO. - Bàn giao mã nguồn và tài liệu kỹ thuật.
9	Dịch vụ bảo trì, hỗ trợ kỹ thuật	- Bố trí nhân sự hỗ trợ xử lý sự cố sau khi hệ thống được đưa vào vận hành chính thức. - Cập nhật bản vá bảo mật và nâng cấp phiên bản nền tảng.

PHỤ LỤC 03: DANH MỤC TÍNH NĂNG BẮT BUỘC ĐÁP ỨNG

Danh mục chức năng mà hệ thống quản lý định danh người dùng và đăng nhập một lần phải đáp ứng.

Chức năng	Nội dung
A. XÁC THỰC VÀ ĐĂNG NHẬP MỘT LẦN (SSO)	
Đăng nhập tập trung	Đăng nhập bằng tài khoản và mật khẩu; ghi nhớ đăng nhập; tự động khóa tài khoản khi sai mật khẩu nhiều lần; kiểm soát an toàn địa chỉ chuyển hướng sau đăng nhập
Đăng nhập một lần / Đăng xuất một lần	Một lần đăng nhập dùng chung cho mọi ứng dụng nội bộ; đăng xuất đồng loạt theo cơ chế front-channel và back-channel logout
Xác thực đa yếu tố (2FA)	Kích hoạt và hủy ứng dụng xác thực (TOTP, mã QR); đăng nhập bằng mã 2FA; sinh và sử dụng mã khôi phục; ghi nhớ hoặc quên thiết bị tin cậy
Khóa truy cập (Passkey / WebAuthn)	Đăng ký, đổi tên, cập nhật và xóa passkey; đăng nhập không cần mật khẩu
Đăng nhập qua nhà cung cấp ngoài	Azure AD / Microsoft Entra ID, Google Workspace (giới hạn theo tên miền), Facebook, GitHub, LDAP; liên kết và gỡ liên kết tài khoản ngoài
Đăng ký và xác minh tài khoản	Đăng ký có hoặc không có tên đăng nhập; gửi thư xác nhận; xác minh địa chỉ thư điện tử
Quên và đặt lại mật khẩu	Gửi liên kết đặt lại qua thư điện tử; đặt lại mật khẩu; đổi mật khẩu; thiết lập mật khẩu lần đầu cho tài khoản đăng nhập bằng nhà cung cấp ngoài
Đồng thuận cấp quyền (Consent)	Màn hình xin phép người dùng cấp quyền cho ứng dụng; ghi nhớ lựa chọn đã đồng thuận

Chức năng	Nội dung
Luồng thiết bị (Device Flow)	Xác thực cho thiết bị không có trình duyệt thông qua mã người dùng
Trang cá nhân người dùng	Xem và cập nhật hồ sơ; quản lý các tài khoản đăng nhập ngoài đã liên kết; tải xuống dữ liệu cá nhân; xóa dữ liệu cá nhân
Hoạt động đăng nhập	Nhật ký đăng nhập của chính người dùng gồm thời gian, địa chỉ IP, trình duyệt, ứng dụng, nhà cung cấp và kết quả thành công/thất bại; thu hồi phiên đang mở trên thiết bị khác
Giao diện đăng nhập	Đa ngôn ngữ Việt/Anh; tùy biến theo nhận diện thương hiệu ABIC (logo, favicon, tiêu đề, CSS chủ đề); áp dụng Content Security Policy
B. QUẢN TRỊ NGƯỜI DÙNG VÀ PHÂN QUYỀN	
Quản lý người dùng	Tìm kiếm, phân trang, xem chi tiết; thêm, sửa, xóa người dùng; đổi mật khẩu; khóa và mở khóa tài khoản
Quản lý vai trò	Thêm, sửa, xóa vai trò; xem danh sách người dùng theo vai trò; gán và gỡ vai trò cho người dùng
Quản lý claim	Quản lý claim của người dùng và claim của vai trò; tra cứu người dùng theo loại claim và giá trị claim
Quản lý đăng nhập ngoài của người dùng	Xem danh sách và gỡ liên kết tài khoản nhà cung cấp định danh ngoài
Phân quyền quản trị	Phân quyền theo vai trò quản trị; bảo vệ từng tuyến giao diện và từng endpoint API theo quyền
Cơ cấu tổ chức	Claim đơn vị, phòng ban, chức danh, tên hiển thị được đồng bộ tự động từ hệ thống Core
C. QUẢN TRỊ ỨNG DỤNG VÀ TÀI NGUYÊN OAUTH 2.0 / OIDC	

Chức năng	Nội dung
Quản lý ứng dụng (Client)	Thêm, sửa, xóa, nhân bản ứng dụng; cấu hình grant type, địa chỉ chuyển hướng, CORS origin, thời hạn token, kiểu token, PKCE, DPoP, thuật toán ký; quản lý secret và thuộc tính mở rộng
Quản lý tài nguyên API	Thêm, sửa, xóa API Resource; quản lý secret và thuộc tính; gán phạm vi truy cập
Quản lý phạm vi API (API Scope)	Thêm, sửa, xóa scope; quản lý thuộc tính; kiểm tra trùng tên khi tạo mới
Quản lý tài nguyên định danh	Thêm, sửa, xóa Identity Resource; quản lý thuộc tính; cấu hình danh sách claim đi kèm
Quản lý nhà cung cấp định danh	Thêm, sửa, xóa Identity Provider động theo schema (kết nối OIDC bên ngoài)
Quản lý khóa ký (Keys)	Danh sách khóa ký được luân chuyển tự động; xem chi tiết; thu hồi khóa
Quản lý ủy quyền đã cấp	Danh sách chủ thể và ủy quyền đã lưu; xem chi tiết; thu hồi theo từng ủy quyền hoặc toàn bộ theo chủ thể
Quản lý phiên phía máy chủ	Danh sách phiên đang hoạt động; thu hồi phiên
D. GIÁM SÁT, NHẬT KÝ VÀ KIỂM TRA CẤU HÌNH	
Bảng điều khiển (Dashboard)	Thống kê tổng quan IdentityServer (ứng dụng, tài nguyên, phạm vi, ủy quyền) và thống kê Identity (người dùng, vai trò); biểu đồ hoạt động theo số ngày gần nhất
Nhật ký kiểm toán (Audit Log)	Ghi nhận mọi thao tác quản trị: ai thực hiện, thời điểm, nội dung thay đổi; lọc theo người dùng, loại sự kiện và khoảng thời gian

Chức năng	Nội dung
Nhật ký hệ thống	Ghi log tập trung xuống cơ sở dữ liệu và tệp; ghi nhận sự kiện của IdentityServer
Kiểm tra cấu hình (Configuration Issues)	Tự động rà soát và cảnh báo các cấu hình rủi ro; bảng tổng hợp theo mức độ nghiêm trọng
Bộ quy tắc kiểm tra (Configuration Rules)	Tự định nghĩa, bật/tắt quy tắc: grant type lỗi thời (Implicit, Password), thiếu PKCE, địa chỉ chuyển hướng không dùng HTTPS, ứng dụng không có phạm vi truy cập, thời hạn access/refresh token quá dài, quy ước đặt tên scope và API resource, Identity Resource bị tắt, scope không được sử dụng, secret sắp hết hạn
Kiểm tra tình trạng hệ thống	Health check cho IdentityServer, cơ sở dữ liệu và các dịch vụ phụ thuộc
E. ĐỒNG BỘ VÀ TÍCH HỢP HỆ THỐNG	
Đồng bộ người dùng từ Core ABIC	Đồng bộ toàn bộ người dùng lần đầu; dịch vụ nền đồng bộ gia tăng theo chu kỳ dựa trên mốc thời gian thay đổi; tạo mới và cập nhật người dùng; ánh xạ trạng thái khóa tài khoản; đồng bộ claim đơn vị, phòng ban, chức danh; lọc theo loại người dùng và miễn thư điện tử được phép
Đồng bộ mật khẩu ra Directory	Khi người dùng đổi hoặc đặt lại mật khẩu, hệ thống tự động đồng bộ sang Google Workspace, Microsoft Entra ID, Active Directory và Core; cấu hình bật/tắt từng đích, thời gian chờ và cách hiển thị lỗi
Phát hiện đăng xuất SSO cho ứng dụng client	Endpoint kiểm tra trạng thái phiên (không gia hạn cookie) kết hợp script nhúng; ứng dụng client tự chuyển về trang đăng xuất khi phiên SSO kết thúc hoặc bị thu hồi từ thiết bị khác; cấu hình danh sách origin tin cậy

Chức năng	Nội dung
Tích hợp ứng dụng nội bộ	Đầu nối theo chuẩn OIDC/OAuth 2.0; cung cấp bộ claim đã chuẩn hóa để ứng dụng đọc trực tiếp (tài khoản, tên hiển thị, đơn vị, phòng ban, chức danh, thư điện tử)
Thông báo qua thư điện tử	Gửi thư qua SMTP hoặc SendGrid: xác nhận tài khoản, đặt lại mật khẩu, cảnh báo bảo mật
F. QUẢN TRỊ HỆ THỐNG VÀ HẠ TẦNG	
Hỗ trợ đa hệ quản trị cơ sở dữ liệu	Oracle (bắt buộc), Microsoft SQL Server, PostgreSQL
Di trú và khởi tạo dữ liệu	Tự động áp dụng migration khi khởi động; khởi tạo vai trò, tài khoản quản trị, ứng dụng client và tài nguyên mặc định
Quản lý chứng thư số ký token	Sử dụng tệp PFX, chứng thư trong kho của máy chủ, Azure Key Vault hoặc khóa tạm cho môi trường phát triển; tự động luân chuyển khóa ký
Bảo vệ khóa dữ liệu	Data Protection lưu trên cơ sở dữ liệu; tùy chọn bảo vệ bằng Azure Key Vault
Cấu hình từ Key Vault	Đọc cấu hình nhảy cảm trực tiếp từ Azure Key Vault thay vì lưu trong tệp cấu hình
Bảo mật hạ tầng	Chính sách Content Security Policy với danh sách tên miền tin cậy; xử lý Forwarded Headers cho reverse proxy; cấu hình CORS; chống tấn công CSRF
Chính sách mật khẩu và tài khoản	Cấu hình độ dài và độ phức tạp mật khẩu, khóa tạm thời, yêu cầu tài khoản và thư điện tử duy nhất, yêu cầu xác minh thư điện tử trước khi đăng nhập
Đa ngôn ngữ và giao diện	Tiếng Việt và tiếng Anh cho cả trang đăng nhập và trang quản trị; chế độ sáng/tối; tùy biến logo, favicon, tiêu đề và CSS thương hiệu

Chức năng	Nội dung
G. BỘ API VÀ TÀI LIỆU KỸ THUẬT	
Các endpoint chuẩn OIDC/OAuth 2.0	Discovery, Authorize, Token, UserInfo, Introspection, Revocation, End Session, JWKS, Device Authorization
Bộ API quản trị (Admin API)	API người dùng, vai trò và claim; API ứng dụng client và secret; API tài nguyên API, phạm vi API và tài nguyên định danh; API nhà cung cấp định danh; API khóa ký; API ủy quyền đã cấp; API bảng điều khiển; API nhật ký kiểm toán; API kiểm tra cấu hình và bộ quy tắc; API thông tin ứng dụng
API phiên đăng nhập	API kiểm tra trạng thái phiên dành cho ứng dụng client; API thu hồi phiên
Bảo mật API	Xác thực bằng OAuth 2.0 Bearer token, phân quyền theo phạm vi truy cập và vai trò quản trị; tài liệu Swagger/OpenAPI có tích hợp đăng nhập OIDC
Tài liệu triển khai	Hướng dẫn triển khai SSO; hướng dẫn tích hợp phát hiện đăng xuất SSO cho ứng dụng client; hướng dẫn đồng bộ mật khẩu Google Workspace và Microsoft Entra ID
Thời hạn hỗ trợ kỹ thuật	Theo thỏa thuận hợp đồng

Ghi chú:

- Toàn bộ chức năng nêu tại Phụ lục 02 là yêu cầu bắt buộc. Đơn vị thực hiện phải đáp ứng đầy đủ và nghiệm thu theo từng nhóm chức năng.
- Bản quyền nền tảng Duende IdentityServer do ABIC trực tiếp trang bị và đứng tên sở hữu khi hệ thống chuyển sang vận hành chính thức, không thuộc phạm vi chào giá. Hạ tầng ảo hoá do ABIC cung cấp.
- ABIC cung cấp thông tin kết nối hệ thống Core, khóa dịch vụ Google Workspace và Microsoft Entra ID, danh sách tên miền tin cậy của các ứng dụng client để đơn vị thực hiện tích hợp.

- Đơn vị thực hiện bàn giao đầy đủ mã nguồn, tài liệu thiết kế và tài liệu vận hành; ABIC sở hữu toàn bộ sản phẩm bàn giao.
- Thời hạn bảo hành, phạm vi bảo trì và mức độ đáp ứng sự cố thực hiện theo thỏa thuận tại hợp đồng.