

PHẦN 2. YÊU CẦU VỀ KỸ THUẬT

CHƯƠNG V. YÊU CẦU VỀ KỸ THUẬT

1. Yêu cầu chung

- Địa điểm thực hiện: Tại các Trung tâm dữ liệu của BIDV tại Hà Nội (TTDL chính Duy Tân và TTDL Dự phòng IDC Viettel Hòa Lạc).
- Sản phẩm còn được hỗ trợ lâu dài và đảm bảo không bị ngừng hỗ trợ từ hãng (End of Support) trong suốt thời gian sử dụng của BIDV.
- Thời gian thực hiện hợp đồng: 43 tháng kể từ ngày hợp đồng có hiệu lực, trong đó:
 - Thời gian bàn giao, nghiệm thu hàng hóa và triển khai cài đặt là 06 tháng kể từ ngày hợp đồng có hiệu lực.
 - Bản quyền có thời hạn sử dụng 36 tháng kèm hỗ trợ kỹ thuật kể từ ngày nghiệm thu hoàn thành triển khai, kích hoạt bản quyền.
 - Thời gian nghiệm thu tổng thể và thanh lý hợp đồng là 01 tháng.
- Danh sách các hạng mục cần mua sắm:

STT	Hạng mục/cấu phần mua sắm	Số lượng	Đơn vị tính	Mô tả, Ghi chú
1	Bản quyền phần mềm hệ thống quản lý thông tin bí mật kèm hỗ trợ kỹ thuật trong 36 tháng	1	Gói	Bản quyền phần mềm hệ thống quản lý thông tin bí mật cho ứng dụng trong 36 tháng kèm dịch vụ hỗ trợ kỹ thuật, đáp ứng khả năng: - Cho phép triển khai mô hình HA kết hợp DR, đảm bảo tính sẵn sàng cao cho hệ thống. - Cho phép tối thiểu 50 đối tượng truy cập/tích hợp vào hệ thống, không phân biệt người dùng/ứng dụng/dịch vụ, trong đó mỗi ứng dụng/dịch vụ được tính là một đối tượng, không phụ thuộc vào số lượng container hoặc pod instance đang chạy.
2	Dịch vụ triển khai	1	Gói	Triển khai tích hợp ứng dụng của BIDV, đảm bảo tính sẵn sàng cho hệ thống.

2. Yêu cầu về tiêu chuẩn kỹ thuật chi tiết

Mua sắm triển khai hệ thống quản lý thông tin bí mật cho ứng dụng, đảm bảo các yêu cầu kỹ thuật sau:

2.1 Yêu cầu về triển khai cài đặt

- Giải pháp phải cho phép triển khai tại chỗ (On-premise).
- Giải pháp cho phép cài đặt trên các nền tảng sau: Openshift, Vmware Tanzu, K8S.
- Giải pháp cho phép triển khai Tính sẵn sàng cao (High Availability) trên môi trường production, hoạt động theo cơ chế Active – Active hoặc Active – Standby.
- Giải pháp phải cho phép mở rộng quy mô (scaling-up và scaling-out).
- Giải pháp phải cho phép triển khai cụm Khôi phục thảm họa (Disaster Recovery Cluster) sao chép cấu hình và dữ liệu của cụm Chính (Primary cluster) để duy trì tính liên tục.
- Giải pháp cho phép triển khai thêm cụm/region hoạt động song song nhằm tăng hiệu suất và giảm độ trễ. Cụm phụ (secondary/replica) phải có khả năng đồng bộ dữ liệu từ cụm

chính để bảo đảm ứng dụng tại các vùng khác nhau vẫn truy xuất được bí mật một cách nhanh chóng.

2.2 Yêu cầu về xác thực

- Giải pháp phải cho phép nhiều phương thức xác thực, bao gồm nhưng không giới hạn: Username và password, token, LDAP, JWT, Kubernetes auth method.
- Giải pháp phải có tính năng Xác thực đa yếu tố (Multi-Factor Authentication) trước khi cấp quyền truy cập.
- Client bắt buộc phải xác thực trước khi có thể truy cập bí mật, khóa mã hóa, chứng chỉ.

2.3 Yêu cầu về bảo mật

- Nhà cung cấp giải pháp phải có tối thiểu một trong các chứng nhận/báo cáo kiểm toán về An toàn bảo mật sau: ISO/IEC 27001, SOC 2.
- Tất cả dữ liệu nhạy cảm được lưu trữ trên hệ thống phải được mã hóa theo tiêu chuẩn AES-256 hoặc tuân thủ theo khuyến nghị của tối thiểu một trong các bộ tiêu chuẩn quốc tế đã được công nhận: FIPS 140-2, NIST 800-57, OWASP, PCI-DSS, GDPR.
- Dữ liệu trong quá trình truyền tải (in transit) phải được mã hóa theo tiêu chuẩn TLS 1.2 trở lên.
- Giải pháp phải cho phép tích hợp với thiết bị bảo mật phần cứng (HSM) để bảo vệ khóa chủ của hệ thống.

2.4 Yêu cầu về quản lý thông tin bí mật

- Giải pháp phải hỗ trợ quản lý bí mật tập trung để giảm sự phân tán bí mật và bảo mật thông tin nhạy cảm. Nó sẽ quản lý và thực thi quyền truy cập vào các bí mật dựa trên các nguồn danh tính đáng tin cậy của client.
- Giải pháp phải có khả năng cung cấp các khả năng quản lý bí mật tĩnh (static secrets management) thông qua các tính năng như kho khóa-giá trị (Key - Value store).
- Giải pháp có thể quản lý đa dạng các loại bí mật (secret) gồm: thông tin xác thực, keys, token, certificates và không giới hạn số lượng bí mật được quản lý.
- Giải pháp phải hỗ trợ quy trình làm việc trong đó cho phép tạo yêu cầu phê duyệt đối với các thao tác truy cập hoặc sử dụng thông tin bí mật nhạy cảm.
- Giải pháp phải hỗ trợ quản lý tập trung và tự động xoay vòng (rotate) các loại thông tin bí mật sau: mật khẩu DB (PostgreSQL, MySQL, Oracle, MSSQL, MongoDB, Redis), LDAP, Linux OS, Cloud credential (AWS, Azure, Google). Việc xoay vòng được thực hiện trực tiếp thông qua engine tích hợp sẵn của hệ thống, theo cơ chế agentless.
- Giải pháp có khả năng phân quyền truy cập theo namespace (khả năng phân quyền riêng biệt theo phòng ban/nhóm người dùng, cho phép các nhóm tự quản lý các policies, secrets để phân quyền phù hợp theo mục đích sử dụng trong phạm vi của mình)

2.5 Khả năng truy vấn thông tin bí mật

- Giải pháp phải hỗ trợ tối thiểu 50 đối tượng truy cập/tích hợp vào hệ thống, không phân biệt tài khoản người dùng (human identity) và tài khoản dịch vụ/ứng dụng (machine/service identity), trong đó mỗi dịch vụ/ứng dụng được tính là một đối tượng, không phụ thuộc vào số lượng container hoặc pod instance đang chạy.
- Giải pháp hỗ trợ phương thức truy vấn/thu hồi/xoay vòng thông tin bí mật thông qua REST API.

- Giải pháp phải hỗ trợ cơ chế agent/sidecar để chèn bí mật vào ứng dụng dưới dạng file hoặc biến môi trường mà không cần thay đổi code ứng dụng.
- Giải pháp phải tích hợp với Kubernetes Secrets Store CSI Driver hoặc cơ chế tương tự, cho phép mount secret ra file trong volume để ứng dụng đọc.

2.6 Khả năng tích hợp

- Cho phép tích hợp các công cụ trong luồng CI/CD, bao gồm và không hạn chế: Github Actions, Azure DevOps, Jenkins thông qua các Plugin/Connector hoặc cơ chế sẵn có của giải pháp.
- Giải pháp phải cho phép đẩy log audit về các phần mềm SIEM (Security Information and Event Management) bên ngoài như Qradar, Splunk, ElasticSearch để theo dõi các sự bất thường và phân tích sự kiện bảo mật.
- Giải pháp có khả năng tích hợp với các nền tảng Cloud bên ngoài sau: AWS, Azure, GCP để hỗ trợ quản lý và truy xuất thông tin bí mật, phục vụ mô hình hybrid cloud của BIDV.

2.7 Yêu cầu về quản trị

- Giải pháp phải cung cấp giao diện quản trị tập trung (Web UI, CLI, API) để cấu hình, giám sát, và vận hành.
- Giải pháp phải hỗ trợ phân quyền chi tiết đến từng nhóm, ứng dụng chỉ được truy cập các thông tin bí mật cho phép.
- Giải pháp phải ghi log đầy đủ (ai, lúc nào, secret nào, hành động gì).
- Chính sách truy cập secret phải quản lý, triển khai được dưới dạng code (YAML/HCL/DSL).
- Giải pháp phải cho phép sao lưu (backup) toàn bộ dữ liệu định kỳ và cho phép khôi phục (restore) bản sao lưu lên cụm mới độc lập.

3. Yêu cầu hỗ trợ kỹ thuật

- Thời gian thực hiện: 36 tháng kể từ ngày nghiệm thu hoàn thành triển khai.
- Tiêu chuẩn hỗ trợ kỹ thuật: theo tiêu chuẩn của chính hãng cung cấp sản phẩm.
- Cung cấp miễn phí các bản nâng cấp phần mềm, cài đặt bản vá, các tài liệu có liên quan.
- Hướng dẫn, hỗ trợ khắc phục sự cố qua điện thoại 24x7x365, Fax hoặc email từ nhà cung cấp tại Việt Nam.
- Rà soát, đưa ra khuyến nghị, hỗ trợ cài đặt miễn phí các bản nâng cấp phần mềm, các tính năng cải tiến, bản vá (patches), các bản sửa lỗi và thiết lập chính sách trên hệ thống theo yêu cầu của BIDV.
- Cung cấp tài khoản truy cập vào hệ thống hỗ trợ kỹ thuật trên Web 24x7 của hãng.
- Kiểm tra, phân tích đánh giá các vấn đề kỹ thuật (dựa trên nhật ký hệ thống) khi xảy ra sự cố.
- Hình thức hỗ trợ: On-site và Off-site, phụ thuộc vào tính cấp thiết và khả năng của sự hỗ trợ cần thiết. Trong trường hợp có sự cố nghiêm trọng theo yêu cầu của BIDV, chuyên gia kỹ thuật của nhà thầu phải có mặt tại địa điểm triển khai trong suốt thời gian triển khai để phối hợp với các bên cung cấp khác liên quan (nếu có) để kiểm tra khắc phục sự cố.
- Khi kết thúc hợp đồng, nhà thầu phải hỗ trợ kỹ thuật để BIDV có thể xuất các thông tin bí mật đang lưu trữ trên hệ thống dưới dạng có thể sử dụng lại, đồng thời đề xuất phương án đảm bảo hoạt động cho các ứng dụng của BIDV đã tích hợp.

- Thời gian tiếp nhận yêu cầu bảo trì hỗ trợ 24/7 kể cả ngày lễ, ngày tết. Nhà thầu phải cung cấp danh sách nhân sự hỗ trợ đảm bảo giữ liên lạc 24/7.
- Thời gian tối đa cho các yêu cầu hỗ trợ kể từ khi BIDV gửi yêu cầu:

Cấp độ nghiêm trọng	Mô tả	Thời gian phản hồi tối đa (kể từ thời điểm BIDV thông báo tới nhà thầu)	Phương thức hỗ trợ
1	Lỗi gây cho sản phẩm không hoạt động, hoặc gây ảnh hưởng nghiêm trọng như ảnh hưởng toàn hệ thống, hoặc hệ thống bị dừng	01 giờ	Tại chỗ 24x7
2	Lỗi làm giảm hiệu năng của sản phẩm, hoặc hạn chế các dịch vụ kinh doanh như ảnh hưởng nhẹ đến hệ thống, làm treo hệ thống	04 giờ	Tại chỗ 24x7
3	Lỗi gây ra ảnh hưởng nhỏ đến việc sử dụng sản phẩm, các ảnh hưởng nhẹ đến hệ thống, các ảnh hưởng đến hiệu năng và chức năng	08 giờ	Từ xa 8x5
4	Lỗi liên quan đến license mà không ảnh hưởng nhiều đến việc sử dụng chức năng sản phẩm để thực hiện hoạt động kinh doanh	24 giờ	Từ xa 8x5

4. Yêu cầu về dịch vụ triển khai

➤ Yêu cầu về thời gian triển khai

- Bàn giao, nghiệm thu hàng hóa và triển khai cài đặt: Trong vòng 06 tháng kể từ ngày hợp đồng có hiệu lực.

➤ Yêu cầu về cài đặt triển khai

- Nhà thầu chịu trách nhiệm triển khai cài đặt phần mềm do nhà thầu chào thầu theo đúng yêu cầu tính năng kỹ thuật của sản phẩm.
- Đề xuất, cài đặt, cập nhật các phiên bản phần mềm phù hợp của sản phẩm, còn hiệu lực hỗ trợ từ nhà sản xuất.
- Nhà thầu đề xuất mô hình triển khai phù hợp với hạ tầng của BIDV, cụ thể:
 - o Thiết kế phương án sao lưu và khôi phục.
 - o Thiết kế phương án tích hợp với các hệ thống khác.
 - o Thiết kế đảm bảo HA và DR.
 - o Thực hiện kiểm thử fail-over, fail-back cho DR.
 - o Đảm bảo sizing hệ thống đáp ứng yêu cầu về hiệu năng, tăng trưởng trong suốt thời gian sử dụng của BIDV.
- Triển khai hệ thống theo mô hình đã đề xuất, nội dung cụ thể:
 - o Chuyển đổi dữ liệu từ hệ thống quản lý thông tin bí mật đang dùng sang hệ thống quản lý thông tin bí mật mới, đảm bảo hoạt động ổn định cho các ứng dụng liên quan.
 - o Tích hợp quản lý secret thêm cho 5 ứng dụng của BIDV chạy trên nền tảng

container.

- Triển khai tính năng tự động xoay vòng mật khẩu cơ sở dữ liệu phù hợp hiện trạng của BIDV.
- Tích hợp quản lý secret cho luồng CI/CD đang sử dụng tại BIDV.
- Cập nhật quy trình DevSecOps hiện có của BIDV nếu cần thiết để đảm bảo phù hợp với hệ thống quản lý thông tin bí mật được triển khai.
- Xây dựng policy quản trị tập trung, phân quyền truy cập hệ thống cho ứng dụng, cho người dùng trong các phòng ban phù hợp với chức năng nhiệm vụ.
- Tích hợp với hệ thống log tập trung của BIDV.
- Tích hợp với hệ thống xác thực tập trung của BIDV.

➤ **Yêu cầu về quy trình triển khai**

Nhà thầu phải đề xuất kế hoạch triển khai chi tiết, bao gồm nhưng không giới hạn các bước sau đây:

- Khảo sát hiện trạng hệ thống hiện tại.
- Đề xuất mô hình triển khai.
- Lập kế hoạch triển khai.
- Bàn giao/nghiệm thu hàng hóa.
- Triển khai cài đặt, tích hợp.
- Nghiệm thu hoàn thành triển khai.

➤ **Yêu cầu về đào tạo, hướng dẫn sử dụng**

- Đào tạo về quản trị vận hành và tích hợp hệ thống.
- Nhà thầu phải cung cấp các tài liệu bao gồm:
 - Tài liệu khảo sát, thiết kế và triển khai hệ thống.
 - Tài liệu hướng dẫn quản trị, tích hợp hệ thống.