PHẦN 2. YÊU CẦU VỀ KỸ THUẬT
CHƯƠNG V. YÊU CẦU VỀ KỸ THUẬT

I. Giới thiệu chung về dự án/dự toán mua sắm, gói thầu:

- Tên của Phương án mua sắm: Mua sắm giải pháp bảo vệ, chống dịch ngược mã nguồn ứng dụng mobile
- Tên gói thầu: Mua sắm giải pháp bảo vệ, chống dịch ngược mã nguồn ứng dụng mobile
- Nội dung công việc chính của gói thầu: Mua sắm giải pháp bảo vệ, chống dịch ngược mã nguồn ứng dụng mobile.
- Lĩnh vực LCNT: Mua sắm hàng hóa
- Thời gian thực hiện gói thầu: 25 tháng kể từ ngày hợp đồng có hiệu lực
- Tên Chủ đầu tư: Ngân hàng TMCP Đầu tư và Phát triển Việt Nam

II. Yêu cầu về kỹ thuật

1. Yêu cầu về nội dung, phạm vi mua sắm, thời gian của PAMS.

- Nội dung, phạm vi mua sắm:

Mua sắm bản quyền giải pháp bảo vệ, chống dịch ngược mã nguồn mobile trên nền tảng iOS và Android của từng ứng dụng như sau:

STT	Tên ứng dụng	Thời hạn bản quyền (tháng)	Số lượng	Đơn vị tính	Số lượt tải trên mỗi nền tảng (IOS / Android)
1	*BIDV iBank*	12	1	License	500.000
2	*B.One*	24	1	License	50.000
3	*Smart OTP*	36	1	License	500.000
4	*SmartSales*	36	1	License	50.000
5	*BIDV Home*	36	1	License	100.000
6	*VCash*	36	1	License	10.000

- Thời gian thực hiện hợp đồng: 37 tháng kể từ ngày hợp đồng có hiệu lực cụ thể như sau:

+ Thời gian bàn giao hàng hóa là 01 tháng

+ Thời gian sử dụng bản quyền phần mềm từ 12 đến 36 tháng (tùy yêu cầu của ứng dụng) kể từ ngày ký biên bản nghiệm thu hàng hóa.

- Địa điểm triển khai: Trung tâm Phát triển phần mềm.

2. Yêu cầu về tiêu chuẩn kỹ thuật chi tiết.

STT	YÊU CẦU KỸ THUẬT
I	**YÊU CẦU CHUNG**
1.1	Giải pháp có thể cài đặt triển khai trên các thiết bị hạ tầng của BIDV.
1.2	Giải pháp có Dashboard giám sát bảo vệ thiết bị, thống kê dữ liệu

1.3	Giải Giải pháp cung cấp bản cập nhật định kỳ hoặc khi có CVE (Common Vulnerabilities and Exposures - Lỗ hổng và Tiếp xúc Phổ biến) ảnh hưởng trực tiếp.
1.4	Giải pháp phải có khả năng bảo vệ ứng dụng Android được phát hành dưới dạng APK và AAB.
1.5	Giải pháp phải có khả năng bảo vệ ứng dụng iOS được phát hành dưới dạng IPA
1.6	Giải pháp phải hỗ trợ các ngôn ngữ Swift, Objective C, Java, Kotlin, Dart.
1.7	Giải pháp hỗ trợ phiên bản hệ điều hành với iOS từ 14,0, Android từ 6,0. Với ứng dụng viết bằng Flutter yêu cầu hỗ trợ Flutter từ phiên bản 3.7.3 trở lên.
1.8	Giải pháp không được lưu trữ thông tin của khách hàng sử dụng ứng dụng mobile app dưới bất kỳ hình thức nào
1.9	Nhà thầu cung cấp bản quyền chính hãng của giải pháp
1.10	Hỗ trợ BIDV gia hạn sử dụng hoặc dừng sử dụng mà không phát sinh lỗi từ ứng dụng và không cần cập nhật lại ứng dụng
II	**YÊU CẦU BẢO VỆ ỨNG DỤNG**
2.1	Giải pháp cung cấp khả năng phát hiện và ngăn chặn thiết bị root/jailbreak
2.2	Giải pháp có khả năng ngăn chặn Overlay
2.3	Giải pháp bảo vệ ứng dụng khi ứng dụng khác có quyền accessibility trên thiết bị.
2.4	Giải pháp có khả năng chống đóng gói lại ứng dụng
2.5	Giải pháp chống lại các công cụ gỡ lỗi (Debug), phát hiện debug mode
2.6	Giải pháp có khả năng chống lại môi trường giả lập (Emulator, Virtual Environment)
2.7	Giải pháp phát hiện được việc mở khóa bootloader
2.8	Giải pháp có khả năng bảo vệ ứng dụng trước các cuộc tấn công bằng kỹ thuật Hooking (Frida, Xposed, Magisk, Substrate …)
2.9	Giải pháp cần phát hiện và ngăn chặn Memory Injection hoặc Runtime Code Injection (ví dụ thông qua ptrace, mmap, hoặc các kỹ thuật tương tự)
2.10	Giải pháp cần có khả năng bảo vệ chống lại Dynamic Instrumentation (ví dụ Frida Gadget, Objection, LLDB attach …)

2.11	Giải pháp phải có cơ chế Runtime Self-Defense (RASP): tự động chặn và dừng hoạt động ứng dụng khi phát hiện hành vi tiêm mã, hooking hoặc debug bất thường
2.12	Giải pháp phải phát hiện, cảnh báo và ngăn chặn hành vi chụp màn hình (screenshot) và ghi hình (record) màn hình ứng dụng.
2.13	Giải pháp phải có khả năng phát hiện và ngăn chặn Remote Access Tools (RAT) nhằm truy cập, điều khiển ứng dụng từ xa trái phép
2.14	Giải pháp cần hoạt động ngay cả khi thiết bị ở chế độ Offline.
2.15	Giải pháp phải bảo vệ tính toàn vẹn của ứng dụng.
2.16	Giải pháp có khả năng mã hoá và lưu trữ bảo mật thông tin nhạy cảm
2.17	Giải pháp có khả năng làm rối, mã hóa mã nguồn
2.18	Giải pháp có khả năng chống phân tích code tĩnh bằng các giải pháp như JADX, Hopper, IDA
2.19	Giải pháp có khả năng làm nhiễu luồng xử lý (control flow obfuscation)
2.20	Giải pháp có khả năng mã hóa tài nguyên của ứng dụng
2.21	Giải pháp có khả năng mã hóa chuỗi trong mã nguồn
2.22	Giải pháp cần xác minh và bảo vệ chữ ký để ngăn chặn việc giả mạo ứng dụng và ký lại
2.23	Giải pháp phải có khả năng phát hiện và ngăn chặn kỹ thuật DYLD Injection (trên iOS) và các hình thức tương tự nhằm tiêm thư viện động vào ứng dụng để can thiệp trái phép
2.24	Giải pháp phải có khả năng phát hiện và ngăn chặn kỹ thuật LD_PRELOAD Injection (trên Android) và các hình thức tương tự nhằm chèn thư viện động hoặc ghi đè hàm của hệ thống để can thiệp trái phép vào ứng dụng
2.25	Giải pháp phải đảm bảo và giám sát cơ chế SSL/TLS Pinning, đồng thời phát hiện và ngăn chặn các hành vi bypass
2.26	Giải pháp cho phép cấu hình cách thức ứng xử khi phát hiện hành vi tấn công, bao gồm nhưng không giới hạn: cảnh báo người dùng, tự động thoát ứng dụng, điều hướng sang trang web thông báo
2.27	Giải pháp có khả năng phát hiện và ngăn chặn Malware.
2.28	Giải pháp phải phát hiện và ngăn chặn Camera Injection / Spy Camera.
2.29	Giải pháp phát hiện được ứng dụng tải từ các cửa hàng ứng dụng bên thứ ba không chính thức

2.30	Giải pháp có khả năng phát hiện ứng dụng được cài đặt từ TrollStore (trên iOS)
2.31	Chặn các cuộc tấn công xen giữa (MITM)
III	**YÊU CẦU VỀ BÁO CÁO, QUẢN TRỊ**
3.1	Giải pháp hỗ trợ dashboard trên nền tảng On Cloud hoặc On Premise
3.2	Dashboard hiển thị tổng quan về các mối đe dọa ở các cấp độ khác nhau
3.3	Dashboard hiển thị theo thời gian thực chi tiết các mối đe dọa kèm thông tin thiết bị, phiên bản ứng dụng
3.4	Giải pháp phải xuất được dữ liệu (ví dụ: danh sách thiết bị, nhật ký mối đe dọa) sang tệp CSV, xlxs ...
IV	**YÊU CẦU VỀ TÍCH HỢP VÀ TRIỂN KHAI**
4.1	Giải pháp đảm bảo mức suy giảm hiệu suất của ứng dụng không đáng kể, dưới 5% so với trường hợp chưa triển khai giải pháp bảo vệ
4.2	Giải pháp đảm bảo trải nghiệm người dùng không bị ảnh hưởng bao gồm nhưng không giới hạn việc không gây crash và không làm tăng thời gian tải tài nguyên ứng dụng một cách bất thường
4.3	Giải pháp có thể hỗ trợ triển khai trên các môi trường (DEV/SIT/UAT/PILOT/PROD)
4.4	Giải pháp bảo vệ ứng dụng liên tục trong khi ứng dụng đang chạy mà không chỉ dựa vào việc kiểm tra ban đầu khi khởi động ứng dụng
4.5	Các SDK, tool phục vụ cho việc triển khai giải pháp phải có khả năng cài đặt và chạy trên IDE và các thiết bị nội bộ của BIDV
4.6	Nhà thầu phải thực hiện hỗ trợ BIDV tích hợp giải pháp miễn phí. Trong trường hợp giải pháp có các phiên bản nâng cấp, nhà thầu thông báo và phải thực hiện việc nâng cấp miễn phí trong suốt thời gian BIDV sử dụng giải pháp của Nhà thầu
4.7	Giải pháp chịu được tải cao, phục vụ lên đến 20.000 người dùng đồng thời và có khả năng mở rộng theo lượng người dùng thực tế
4.8	Giải pháp tuân thủ các chính sách của Apple và Google liên quan đến việc phát hành ứng dụng lên Store
V	**YÊU CẦU VỀ TUÂN THỦ**
5.1	Giải pháp đáp ứng các yêu cầu về tuân thủ về bảo mật ứng dụng mobile banking theo quy định của BIDV và pháp luật Việt Nam, bao gồm nhưng không giới hạn các nghị định, thông tư sau: - Nghị định 13/2023/NĐ-CP Bảo Vệ Dữ Liệu Cá Nhân

	- Thông tư số 50/2024/TT-NHNN quy định về an toàn, bảo mật cho việc cung cấp dịch vụ trực tuyến trong ngành Ngân hàng. Trong trường hợp có quy định, nghị định, thông tư mới, hoặc các quy định, nghị định, thông tư cũ có sửa đổi, bổ sung, nhà thầu có trách nhiệm hỗ trợ BIDV cập nhật miễn phí (nếu phát sinh thay đổi đối với giải pháp) nhằm đáp ứng tuân thủ đầy đủ yêu cầu và thời hạn các yêu cầu về bảo mật theo quy định.

3. Yêu cầu về bản quyền

Cung cấp bản quyền sử dụng giải pháp bảo vệ, chống dịch ngược mã nguồn 6 ứng dụng mobile BIDV iBank, BIDV Smart OTP, BIDV SmartSales, B.One, BIDV Home và Vcash đáp ứng tối thiểu các yêu cầu sau:

- Thời gian sử dụng bản quyền: (i) của ứng dụng B.One là 24 tháng kể từ tháng 10/2026; (ii) của ứng dụng BIDV iBank là 12 tháng và 4 ứng dụng còn lại (BIDV Smart OTP, BIDV SmartSales, BIDV Home và Vcash) là 36 tháng kể từ ngày ký biên bản nghiệm thu hàng hóa.
- Được nâng cấp lên các phiên bản cao hơn/cập nhật bản vá của giải pháp miễn phí

4. Trách nhiệm của nhà thầu

- Nhà thầu chịu trách nhiệm liên hệ với Hãng trong trường hợp BIDV không liên hệ được với hãng.
- Nhà thầu chịu trách nhiệm làm việc với hãng để cung cấp danh sách và bộ cài đặt sản phẩm thuộc danh mục sản phẩm của hợp đồng, với phiên bản là phiên bản còn hỗ trợ của hãng và do BIDV có nhu cầu và có yêu cầu sử dụng.

5. Yêu cầu về hỗ trợ kỹ thuật

- Ngay sau khi BIDV phát hiện sự cố thông báo cho bên nhà thầu về các lỗi phát sinh, lỗi hệ thống theo hình thức điện thoại, email.Nhà thầu có trách nhiệm cung cấp cho BIDV tối thiểu hai (02) số điện thoại liên lạc khẩn cấp. Các số điện thoại này phải đảm bảo luôn hoạt động và có người trực 24/7 (24 giờ mỗi ngày, 7 ngày mỗi tuần) để tiếp nhận và xử lý sự cố
- Căn cứ vào tính chất và mức độ nghiêm trong của sự số, nhà thầu thự hiện hỗ trợ tại chỗ (tại địa điểm gặp lỗi) hoặc hỗ trợ từ xa.. Toàn bộ chi phí liên quan đến việc khắc phục các lỗi do nhà thầu chịu trách nghiệm.
- Thời gian phản hồi và giải quyết sự cố: Trong suốt thời gian bảo hành, bên nhà thầu phải thực hiện kịp thời các công việc cần thiết để khắc phục nhược điểm hoặc lỗi chương trình. Thời gian cụ thể như sau:

Cấp độ nghiêm trọng	**Mô tả**	**Thời gian tiếp nhận**	**Thời gian phản hồi** (Tính từ thời điểm nhà thầu nhận được thông báo của BIDV)	**Thời gian hoàn thành** (Tính từ thời điểm nhà thầu nhận được thông báo của BIDV)

1	Sự cố ảnh hưởng đến lượng lớn tổng thiết bị (>30%) không thể sử dụng dịch vụ, chưa có phương án xử lý cụ thể.	24/7	02 giờ	Trong vòng 02 ngày
2	Sự cố ảnh hưởng đến lượng trung bình thiết bị (10%-30%) hoặc chỉ sử dụng được một phần dịch vụ.	8/5	06 giờ	Hoàn thành xử lý trong vòng 05 ngày
3	Sự cố ảnh hưởng đến lượng ít thiết bị (<10%) hoặc đã có phương án xử lý cụ thể.	8/5	03 ngày	Hoàn thành xử lý trong vòng 10 ngày