SHB
Solid partners, flexible solutions

NGÂN HÀNG TMCP SÀI GÒN - HÀ NỘI

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập – Tự do – Hạnh phúc

Hà Nội, ngày 18 tháng 11 năm 2020

THƯ MỜI

Kính gửi: **Quý Công ty**

Ngân hàng TMCP Sài Gòn - Hà Nội có nhu cầu nâng cấp hệ thống 3D Secure 2.0, vậy trân trọng kính mời Quý Công ty tham dự chào hàng gói dịch vụ nêu trên.

Quý Công ty có thể tìm hiểu thêm các thông tin cần thiết trong Hồ sơ yêu cầu chào hàng kèm theo.

Hồ sơ chào hàng phải được gửi tới địa chỉ: Trung tâm mua sắm, Ngân hàng TMCP Sài Gòn Hà Nội, tầng 3, Toà nhà 81 Trần Hưng Đạo, Hoàn Kiếm, Hà Nội trước 15h ngày 28 tháng 11 năm 2020.

Mọi chi tiết xin liên hệ:

Ngân hàng TMCP Sài Gòn - Hà Nội

Trung tâm mua sắm, Ngân hàng TMCP Sài Gòn Hà Nội, tầng 3, Toà nhà 81 Trần Hưng Đạo, Hoàn Kiếm, Hà Nội

Liên hệ: – Nguyễn Ngọc Cầu - Chuyên viên mua sắm cấp 1

- Điện thoại 0243.9423388 máy lẻ 2914.
- Điện thoại di động: 097.790.1188

Trân trọng./.

NGÂN HÀNG TMCP SÀI GÒN HÀ NỘI

M.S.D.N: 1800278630 - C.T.C.P - NGÂN HÀNG THƯƠNG MẠI CỔ PHẦN SÀI GÒN - HÀ NỘI - Q. HOÀN KIẾM - TP. HÀ NỘI

PHÓ TỔNG GIÁM ĐỐC

Ngô Thu Hà

4

NGÂN HÀNG TMCP SÀI GÒN – HÀ NỘI

SHB

Solid partners, flexible solutions

HỒ SƠ YÊU CẦU CHÀO HÀNG

NÂNG CẤP HỆ THỐNG 3D SECURE 2.0

2020

PHẦN I
CÁC YÊU CẦU VỀ HỒ SƠ CHÀO HÀNG

1. Yêu cầu về Hồ sơ chào hàng

- Hồ sơ chào hàng phải được lập thành 02 bản **(01 bản gốc + 01 bản sao)**, đóng trong phong bì có niêm phong và phải được gửi tới đúng địa điểm trước thời gian quy định trong hồ sơ yêu cầu chào hàng.
- Hồ sơ chào hàng được đóng trong phong bì riêng biệt. Bên ngoài phong bì ghi rõ: **Hồ sơ chào hàng: "Cung cấp dịch vụ hệ thống 3D Secure 2.0''**
- Hồ sơ chào hàng phải có đầy đủ các nội dung sau:
    - Đơn chào hàng: Phải có chữ ký của người đại diện theo pháp luật của công ty hoặc người được ủy quyền (Có giấy ủy quyền kèm theo);
    - Bảng chào giá chi tiết (phải chào đầy đủ số lượng, chủng loại, giá trước VAT, giá sau VAT…) theo như Phần II Mục 1 của hồ sơ yêu cầu;
    - Bản sao Giấy phép đăng ký kinh doanh (Có lĩnh vực kinh doanh liên quan đến hàng hóa cung cấp);
    - Hiệu lực của Hồ sơ chào hàng tối thiểu **30** ngày kể từ thời điểm 15h00' ngày ..28../..11./2020.
    - Ghi rõ tên nhãn hiệu, xuất xứ hàng hóa kèm theo;
    - Đơn giá được tính bằng tiền Việt Nam đồng;
    - Đơn giá chào trên cơ sở cung cấp dịch vụ nâng cấp, bảo hành, bảo trì và hỗ trợ kỹ thuật cho hệ thống 3D Secure tại địa điểm do SHB quy định trong Phần II;
    - Có vốn điều lệ tối thiểu 05 tỷ đồng;
    - Đơn vị phải có tối thiểu 03 năm kinh nghiệm trong lĩnh vực cung cấp dịch vụ bảo hành, bảo trì và hỗ trợ kỹ thuật cho các thiết bị bảo mật;
    - Đơn vị phải có tối thiểu 02 hợp đồng cung cấp hệ thống thẻ, 3D secure trong 05 năm gần nhất cho các tổ chức tín dụng, mỗi hợp đồng có giá trị không thấp hơn giá chào thầu;
    - Đơn vị phải cung cấp thư hỗ trợ của hãng để đảm bảo sản phẩm chào giá là hàng chính hãng và được sự hỗ trợ của hãng trong quá trình bảo hành;
    - Đơn vị cung cấp giấy tờ chứng minh mối quan hệ với hãng sản xuất;
    - Đơn vị phải nêu rõ phương pháp tổ chức hỗ trợ kỹ thuật trong hồ sơ chào hàng (bố trí nhân sự, phương pháp liên lạc, quy trình xử lý yêu cầu hỗ trợ kỹ thuật) khi có yêu cầu của Bên Mua;
    - Cam kết chấp nhận yêu cầu về kỹ thuật, chất lượng, theo yêu cầu tại Phần II của Hồ sơ yêu cầu chào hàng;
    - Cam kết chấp nhận yêu cầu về điều kiện tài chính thương mại theo yêu cầu tại Phần II của Hồ sơ yêu cầu chào hàng;
    - Cam kết bảo hành và hỗ trợ kỹ thuật khi hàng hóa có sự cố do lỗi của nhà sản xuất gây ra cho Bên Mua theo yêu cầu tại Phần II của Hồ sơ yêu cầu chào hàng;
    - Cam kết đảm bảo sản phẩm chào giá là sản phẩm nguyên bản của nhà sản xuất;
    - Cam kết trách nhiệm của đơn vị cung cấp về sản phẩm chào giá đối với các khiếu kiện của bên thứ ba.

2. Thời gian và địa điểm nộp Hồ sơ chào hàng

- **Thời gian:** trước 15h00' ngày ..28../..11.../2020.
- **Địa điểm:** Trung tâm mua sắm, Ngân hàng TMCP Sài Gòn Hà Nội, tầng 3, Toà nhà 81 Trần Hưng Đạo, Hoàn Kiếm, Hà Nội (Liên hệ Mr. Cầu, Điện thoại 0243.9423388 máy lẻ 2914, DĐ: 097.790.1188). Mọi Hồ sơ chào hàng gửi tới sau thời điểm nêu trên đều không có giá trị.

PHẦN II

YÊU CẦU CỤ THỂ

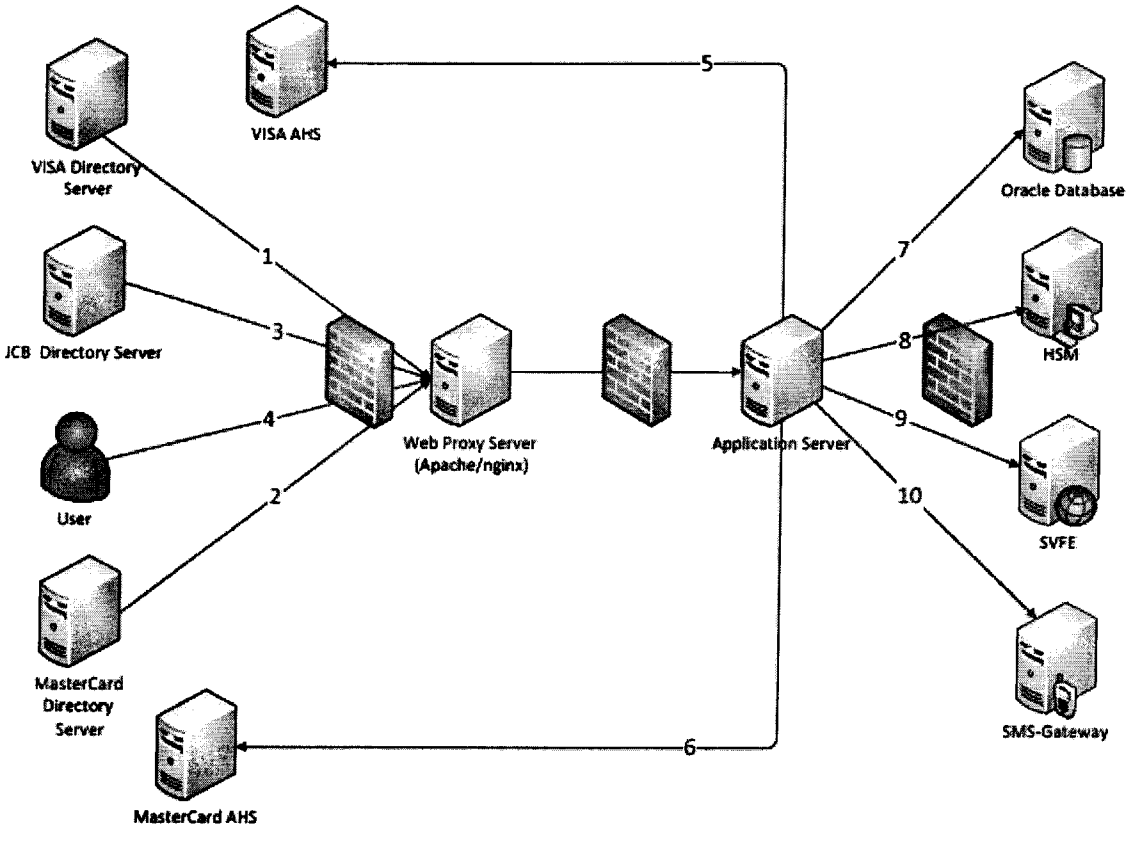
1. **Yêu cầu đối với hàng hóa:** Hàng hóa cung cấp phải đảm bảo các yêu cầu cụ thể như sau:

   Danh mục hàng hóa: **Dịch vụ hệ thống 3D Secure 2.0**

2. **Yêu cầu về kỹ thuật:** Nhà thầu phải cung cấp các giấy tờ, tài liệu chứng minh được khả năng đáp ứng các yêu cầu được nêu cụ thể dưới đây:

2.1. Kiến trúc hệ thống: Mô tả hiện trạng hệ thống 3D Secure của Ngân hàng SHB

Hệ thống 3D của ngân hàng SHB đang dung hệ thống 3D của đối tác BPC cung cấp với kiến trúc hệ thống như sau



(1) Kết nối giữa VISA Directory Server và ACS system.

(2) Kết nối giữa Mastercard Directory Server và ACS system.

(3) Kết nối giữa JCB Directory Server và ACS system.

(4) Kết nối giữa khách hàng và ACS system.

(5) Kết nối giữa VISA AHS (Authentication History Server) và ACS system.

(6) Kết nối giữa Mastercard AHS (Authentication History Server) ACS system.

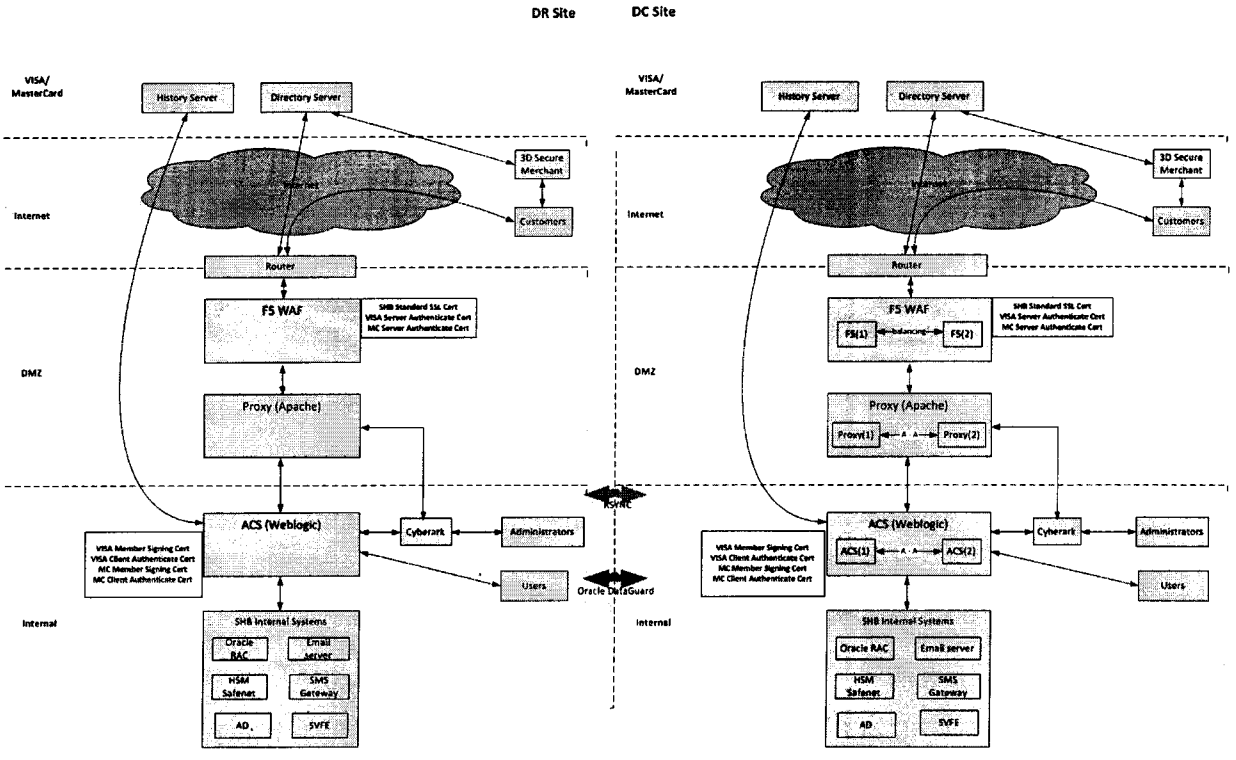
(7) Kết nối giữa ACS server và Oracle Database.

(8) Kết nối giữa ACS server và HSM(HSM Safenet)

(9) Kết nối giữa ACS server và SVFE.

(10) Kết nối giữa ACS server và SMS/ Email Gateway

2.2 Mô hình kết nối



(1) Proxies Server (gồm 2 máy chủ chạy cân bằng tải): Cài đặt Apache 2.2 đóng vai trò là Reverse Proxies.

(2) ACS Server (gồm 2 máy chủ chạy cân bằng tải): Cài đặt Weblogic12c và thành phần gồm có ACS xử lý giao dịch 3DSecure & ACS UI dành cho việc quản trị hệ thống

(3) Database Server: Oracle RAC - schema ACS.

(4) Cặp thiết bị F5 bảo vệ các ứng dụng trong vùng DMZ, tạo thêm một lớp bảo vệ, tập trung ngăn chặn các tấn công vào lớp ứng dụng.

(5) Cặp thiết bị F5 giúp phân tải các kết nối vào các Proxy server (load balancing).

(6) Proxies server giúp bảo vệ các máy chủ ứng dụng ACS trong vùng Internal, tạo thêm một lớp bảo vệ, ngăn chặn các tấn công (nếu có thể vượt qua được F5) vào ứng dụng, giúp cho hệ thống của SHB được bảo vệ toàn diện hơn.

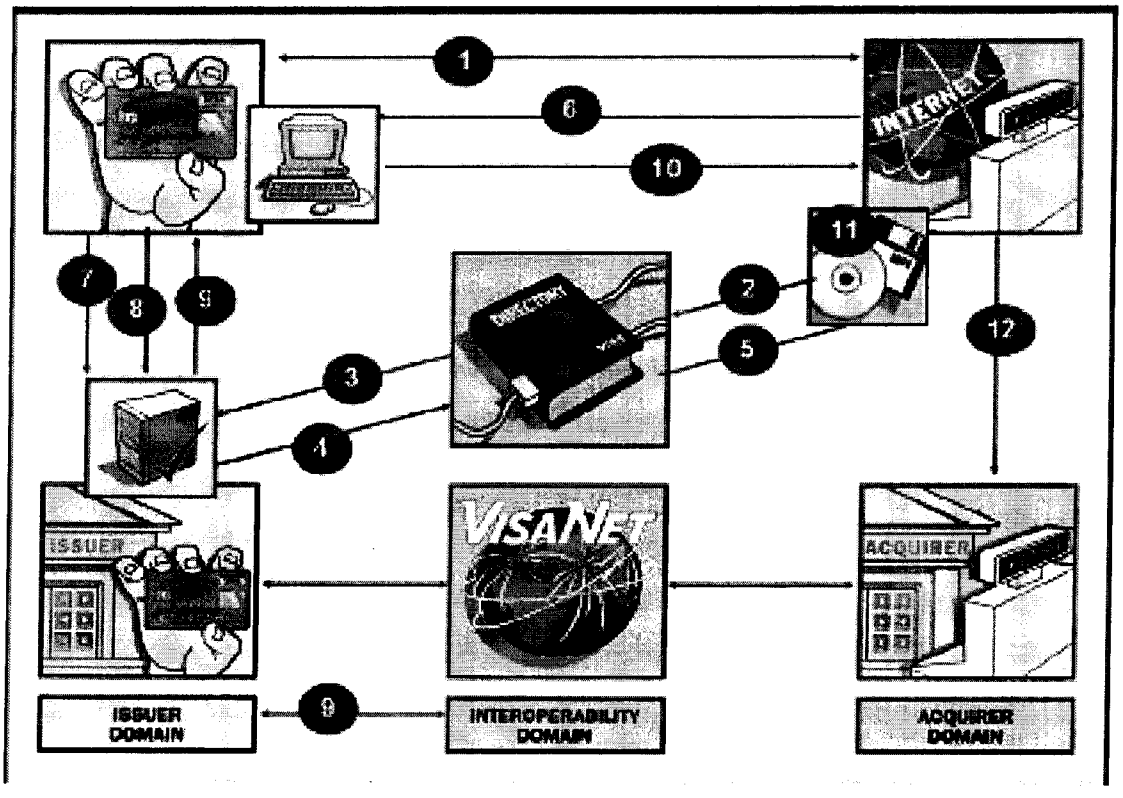
(7) Các SSL certificates được cài đặt trên F5 (các kết nối trao đổi giữa client và ACS được giải mã/ mã hóa trên F5 thay vì trên ACS), do đó giúp giảm tải cho máy chủ ứng dụng ACS.

(8) Hệ thống 3DSecure bên DR site bao gồm 01 Proxy server và 01 ACS server.

(9) Hệ thống DR được đồng bộ online từ DC bằng cơ chế RSYNC (application) và Dataguard (DB).

2.3 Luồng giao dịch

Figure 4–1: Sample Purchase Transaction



(1) Khách hàng thực hiện giao dịch trên website của merchant chấp nhận giao dịch 3DSecure.

(2) Merchant Server Plug-in (MPI) gửi VEReq (Verification Request) có chứa số thẻ (PAN) về Directory Server (VISA/ MasterCard).

(3) Directory Server kiểm tra số PAN thuộc member bank nào? member bank có đăng ký dịch vụ 3DSecure?

Directory Server gửi VEReq về ACS Server.

(4) ACS Server kiểm tra số PAN có đăng ký dịch vụ 3DSecure, gửi phản hồi VERes về Directory Server.

(5) Directory Server gửi VERes của ACS Server đến MPI.

(6) MPI gửi PAReq (Payer Authentication Request) qua thiết bị của người dùng đến ACS.

(7) ACS nhận PAReq.

(8) ACS xác thực khách hàng bằng OTP hoặc Static password.

(9) ACS gửi PARes có chứa CAVV (VISA Cardholder Authentication Verification Value)/ UCAF (MasterCard Universal Cardholder Authentication Field) cho MPI.

ACS gửi PATransReq cho Authentication History Server (AHS) và AHS gửi phản hồi PATransRes cho ACS.

(10) MPI nhận PARes từ ACS.

(11) MPI xác thực dữ liệu mã hóa được ký bởi ACS.

(12) Merchant gửi Authorisation message (có chứa CAVV/ UCAF nhận được từ ACS) qua về ngân hàng phát hành để chuẩn chi giao dịch.

3. Yêu cầu về nghiệp vụ:

Nhà thầu phải cung cấp các giấy tờ, tài liệu chứng minh được khả năng đáp ứng các yêu cầu được nêu cụ thể dưới đây:

3.1.Đáp ứng các yêu cầu nghiệp vụ sau

- Có chức năng Risk-based Authentication (RBA) và hệ thống có khả năng học máy (ML) là một lợi thế.
- Có kinh nghiệm tích hợp với Hệ thống Quản lý Thẻ (CMS) SmartVista là một lợi thế
- Các phương thức xác thực: RBA, OTP, Biometric, Token và các PTXT mở rộng khác (OOB), Payment Authentication (PA), Non-Payment Authentication (NPA), Frictionless Authentication, Challenge Authentication, Browser-based channel, App-based channel
- Các luật tạo sẵn và khả năng chỉnh sửa luật đáp ứng yêu cầu của Bên Mua, cho phép người dùng chỉnh sửa hoặc tạo mới các luật.
- Hệ thống báo cáo tối thiểu bao gồm: báo cáo chi tiết giao dịch, báo cáo lịch sử đăng ký sử dụng dịch vụ, lịch sử xác thực.
- Các chức năng cơ bản khác, tối thiểu bao gồm: tra cứu giao dịch, báo cáo, Audit người dùng, xử lý khóa/mở khóa dịch vụ 3DS cho khách hàng…
- Thực hiện tinh chỉnh và cấu hình các tham số hệ thống để tối ưu năng lực xử lý của hệ thống theo yêu cầu của Bên Mua.
- Đáp ứng tiêu chuẩn PCI – DSS.
- Đáp ứng tiêu chuẩn của Tổ chức thẻ Visa và MasterCard về 3D Secure 2.0 đồng thời mở rộng kết nối tới các tổ chức thẻ khác như AMEX, JCB, CUP, Napas,.. trong trường hợp SHB là thành viên.
- Hệ thống phải linh hoạt để hỗ trợ tích hợp với hệ thống xác thực bên ngoài nguyên bản trong 3DS2 (không có OOB) sẽ được hỗ trợ.
- Hệ thống phải linh hoạt để hỗ trợ tích hợp với hệ thống xác thực bên ngoài thông qua xác thực OOB sẽ được hỗ trợ.
- Hỗ trợ quản lý phương pháp xác thực linh hoạt(primary and fallback methods, multi-step methods).
- Hỗ trợ cả hai phương thức 3DS 1.0 và 3DS 2.0 trong cùng 1 giải pháp.
- Hỗ trợ đăng ký thẻ theo lô và có API để tích hợp.
- Hệ thống tích hợp với AD or LDAP cho đăng nhập 1 lần.
- Hệ thống hỗ trợ đăng nhập single sign-on (SSO).
- Hệ thống sẽ có log ghi nhận quá trình xác thực giao dịch.

3.2 Đáp ứng yêu cầu về tiến độ

- Thời gian triển khai tối đa 04 tháng.

3.3 Dịch vụ bảo trì: Hàng năm.

3.4 Xử lý lỗi

- Bên Bán cam kết đáp ứng hỗ trợ kỹ thuật 8x5 NBD trong thời gian thực hiện dịch vụ. Chế độ hỗ trợ kỹ thuật 8x5 NBD bao gồm các yêu cầu cụ thể sau:
  - Thời gian hỗ trợ kỹ thuật: 08 giờ/ngày và 05 ngày/tuần;

- Thời gian đáp ứng: kỹ sư của Bên Bán có mặt tại địa điểm của Bên Mua trong vòng 01h (một giờ) sau khi nhận được thông báo và yêu cầu về việc khắc phục, xử lý sự cố. Trong vòng 04h (bốn giờ) từ thời điểm có mặt tại địa điểm của Bên Mua phải đề xuất được giải pháp khả thi để khắc phục sự cố và hoàn thành thực hiện theo giải pháp được sự đồng ý của Bên Mua;
- Các hoạt động hỗ trợ phải được ghi nhận nhật ký thực hiện.

- Đối với các lỗi xảy ra do phiên bản phần mềm đang vận hành, Bên Bán có trách nhiệm yêu cầu hãng tạo mới hoặc cung cấp các bản vá để xử lý các lỗi đã xảy ra của Bên Mua trong vòng 04 (bốn) giờ đảm bảo hệ thống hoạt động bình thường.

3.5 Dịch vụ hỗ trợ kỹ thuật

- Bên Bán cung cấp thông tin cán bộ đầu mối để Bên Mua liên lạc khi Bên Mua có yêu cầu tư vấn về hỗ trợ kỹ thuật. Khi có sự thay đổi về cán bộ đầu mối, Bên Bán có trách nhiệm thông báo bằng văn bản tới Bên Mua và cung cấp thông tin cán bộ thay thế;
- Có đội ngũ cán bộ hỗ trợ kỹ thuật người Việt làm việc tại Việt Nam là một lợi thế.
- Phải sử dụng các công cụ quản lý và theo dõi các yêu cầu hỗ trợ như JIRA hoặc tương đương.
- Bên Bán có trách nhiệm tư vấn và hỗ trợ cán bộ kỹ thuật của Bên Mua trong các công tác sau:
  - Quản trị, vận hành hệ thống;
  - Thay đổi/nâng cấp cấu hình phần cứng các thiết bị CNTT thuộc danh mục thiết bị chào giá.

4. **Yêu cầu về An toàn bảo mật:** Nhà thầu phải cung cấp các giấy tờ, tài liệu chứng minh được khả năng đáp ứng các yêu cầu được nêu cụ thể dưới đây:

a) Quản trị và bảo mật hệ thống

STT	Yêu cầu của SHB (Nhà thầu phải thực hiện tối thiểu nhưng không giới hạn các hạng mục công việc sau, đảm bảo đạt được Mục tiêu nêu trên)	Mức độ đáp ứng	Bắt buộc / Tùy chọn	Mô tả đáp ứng chi tiết	Cấu phần tương ứng của giải pháp đề xuất
1	Giải pháp có chứng chỉ đáp ứng tiêu chuẩn bảo mật PA DSS		Bắt buộc		
2	Giải pháp có khả năng xác thực, ủy quyền và cấp quyền truy cập cho một tài khoản hoặc một nhóm tài khoản.		Bắt buộc		
3	Giải pháp có khả năng tích hợp với các hệ thống quản trị directory hiện tại của SHB như LDAP, MS Active Directory, Cyber Ask		Bắt buộc		
4	Giải pháp hỗ trợ kết nối đến các hệ thống Single Sign-On		Tùy chọn		
5	Mã hóa thông tin nhạy cảm như số thẻ tín dụng trong cơ sở dữ liệu theo quy định PCI-DSS		Bắt buộc		
6	Giải pháp phải cung cấp cơ chế logging và auditing. Mô tả chi tiết cách thức giải pháp thực hiện logging và auditing. Tối thiểu bao gồm các thông tin: Thời gian thực hiện, người thực hiện, các thao tác thực hiện, kết quả, IP máy thực hiện, …		Bắt buộc		
7	Quản lý mật khẩu người sử dụng - Mật khẩu của người sử dụng phải mã hóa trong dữ liệu lưu trữ. - Mật khẩu của người dùng phải được mã hóa khi		Bắt buộc		

STT	Yêu cầu của SHB (Nhà thầu phải thực hiện tối thiểu nhưng không giới hạn các hạng mục công việc sau, đảm bảo đạt được Mục tiêu nêu trên)	Mức độ đáp ứng	Bắt buộc / Tùy chọn	Mô tả đáp ứng chi tiết	Cấu phần tương ứng của giải pháp đề xuất
	truyền tải dữ liệu. - Mật khẩu phải được lưu trữ bằng cách sử dụng mã hóa một chiều (hash). - Các dữ liệu được kiểm tra tính toàn vẹn dữ liệu không được phép sửa đổi trái phép. - Mật khẩu hiển thị trên màn hình của người dùng phải được làm mờ, che giấu tránh bên thứ 3 phát hiện. - Chặn tính năng ghi nhớ mật khẩu hoặc tự điền mật khẩu người dùng. - Sử dụng lần cuối (thành công hoặc không thành công) của tài khoản người dùng phải được thông báo hoặc báo cáo tới người sử dụng tại lần đăng nhập thành công tiếp theo. - Hỗ trợ phương án xác thực người sử dụng như: Xác thực qua domain, qua chữ ký điện tử,... SHB có thể tuy biến lựa chọn phương án một cách linh hoạt.				
8	Kiểm soát truy cập - Phải có chức năng kiểm soát truy nhập, chỉ có các người dùng đầu cuối đã được cấp phép được phép mới được truy nhập hệ thống. - Hệ thống phải hỗ trợ cơ chế thông báo, cảnh báo và ngăn chặn việc cố tình sử dụng mã truy cập của người khác để truy cập hệ thống. - Chức năng kiểm soát truy nhập phải xác nhận việc kết nối của các thiết bị đầu cuối cũng như chấp thuận cho các thiết bị đầu cuối được thực hiện giao dịch. - Cho phép cấu hình đình chỉ tạm thời việc truy nhập hệ thống nếu người sử dụng thực hiện tối đa ba lần truy nhập không hợp lệ vào hệ thống. Tất cả lần truy cập không thành công phải được ghi lại và có báo cáo để theo dõi. - Cho phép tham số hóa số lần tối đa truy cập không hợp lệ vào hệ thống. Tất cả lần truy cập không thành công phải được ghi lại và có báo cáo để theo dõi		Bắt buộc		
9	Quản lý phiên làm việc: - Cơ chế đăng xuất luôn có sẵn cho tất cả người sử dụng trên mọi màn hình, khi được thực thi phải lập tức chấm dứt phiên hoặc kết nối. - Thời gian chờ (timeouts) cho phiên làm việc phải được cấu hình. - Phiên làm việc hoặc cookies có thời gian tồn tại phải được cấu hình. - Mỗi một định danh phiên (SessionID) và cookies phải được khởi tạo khi người dùng đăng nhập - Tại một thời điểm hệ thống chỉ được phép duy trì 1		Bắt buộc		

STT	Yêu cầu của SHB (Nhà thầu phải thực hiện tối thiểu nhưng không giới hạn các hạng mục công việc sau, đảm bảo đạt được Mục tiêu nêu trên)	Mức độ đáp ứng	Bắt buộc / Tùy chọn	Mô tả đáp ứng chi tiết	Cấu phần tương ứng của giải pháp đề xuất
	phiên làm việc của người dùng.				
10	Xác nhận đầu vào, đầu ra - Tất cả dữ liệu từ phía người dùng (bao gồm các chuỗi truy vấn, cookies, nội dung tiêu đề HTTP, SOAP và các yêu cầu dịch vụ Web khác, nội dung tự động post-back và nội dung chuyển hướng) đều phải được kiểm duyệt trước khi được xử lý. - Tất cả dữ liệu được mã hóa với một bảng mã ký tự chung (UTF-8 hoặc Unicode) trước khi kiểm duyệt. - Tất cả các dữ liệu đầu vào đều phải được xác nhận về phạm vi dự kiến (range), độ dài (length), định dạng (format) và kiểu dữ liệu (datatype). - Tất cả dữ liệu đầu vào được xác nhận loại trừ khỏi một danh sách các ký tự được cho phép (white list). Trong trường hợp bộ lọc "white list" không được sử dụng, tất cả dữ liệu đầu vào được xác nhận loại trừ theo một bộ lọc "black-list" để chặn bất kỳ một ký tự nào có khả năng nguy hiểm. Ví dụ về các ký tự có khả năng gây nguy hiểm: + <> " ' ( ) & + \ \' \" + Null bytes (%00) + Ký tự new line (%0d, %0a, \r, \n) + Ký tự đường dẫn (../ or ..\) - Tất cả dữ liệu được xác nhận đảm bảo không thể giả mạo Cross-site scripting (XSS) - Tất cả dữ liệu được xác nhận đảm bảo không thể giả mạo SQL Injection. - Xác nhận ứng dụng không bị LDAP Injection hoặc có các kiểm soát an ninh ngăn chặn LDAP Injection. - Xác nhận ứng dụng không bị OS Command Injection hoặc có các kiểm soát an ninh ngăn chặn OS Command Injection. - Xác nhận ứng dụng không bị lỗi tràn bộ đệm hoặc có các kiểm soát an ninh ngăn chặn tràn bộ đệm. - Xác nhận đầu vào là file upload không bị tấn công Shell Injection		Bắt buộc		
11	Quản lý về file - Tất cả các mật khẩu được cài đặt (hard-coded) trong mã nguồn (source code) đều phải được gỡ bỏ. - Bộ nhớ (Cached) và những bản sao lưu tạm (temporary) của những thông tin nhạy cảm được lưu trữ trên máy chủ phải được bảo vệ khỏi các truy cập trái phép. Các dữ liệu này phải được hủy bỏ ngay sau		Bắt buộc		

STT	Yêu cầu của SHB (Nhà thầu phải thực hiện tối thiểu nhưng không giới hạn các hạng mục công việc sau, đảm bảo đạt được Mục tiêu nêu trên)	Mức độ đáp ứng	Bắt buộc / Tùy chọn	Mô tả đáp ứng chi tiết	Cấu phần tương ứng của giải pháp đề xuất
	khi không còn nhu cầu sử dụng. - Tất cả các thông tin nhạy cảm được mã hóa khi lưu trữ. - Mã hóa các dữ liệu cấu hình nhạy cảm (ví dụ như mật khẩu, chuỗi kết nối - connection string) được lưu trữ trên máy chủ. - Những trang chứa thông tin nhạy cảm thì phải vô hiệu hóa tính năng lưu vào bộ nhớ tạm (caching) ở phía trình duyệt của người dùng.				

b) Giám sát, kiểm tra, truy vết

STT	Yêu cầu của SHB (Nhà thầu phải thực hiện tối thiểu nhưng không giới hạn các hạng mục công việc sau, đảm bảo đạt được Mục tiêu nêu trên)	Mức độ đáp ứng	Bắt buộc / Tùy chọn	Mô tả đáp ứng chi tiết	Cấu phần tương ứng của giải pháp đề xuất
1	Tất cả các sự kiện sau được ghi (log) lại: - Các chức năng trên tài khoản/bản ghi người dùng. - Lỗi xác nhận đầu vào. - Cố gắng xác thực nhiều lần - Lỗi kiểm soát truy cập. - Các sự kiện giả mạo. - Cố gắng kết nối tới những phiên làm việc không hợp lệ/hết hạn. - Các thay đổi do người dùng tạo ra trong qua trình tương tác với hệ thống. - Các ngoại lệ về hệ thống và truyền dữ liệu. - Thông tin được lưu trữ trong log theo một định dạng thuận tiện cho việc truy xuất. - Các truy xuất vào log được giới hạn theo thẩm quyền người sử dụng. - Các thông tin nhậy cảm không được lưu trữ trong log. - Tối thiểu các sự kiện log audit cần được ghi lại: + Thời gian của sự kiện. + Tiêu đề định danh (như định danh người dùng, IP) + Định danh loại sự kiện và mô tả sự kiện. - Hệ thống phải hỗ trợ người quản trị theo dõi các hành động của người sử dụng trên hệ thống một cách trực quan, đầy đủ thông tin, có thể truy xuất		Bắt buộc		

STT	Yêu cầu của SHB (Nhà thầu phải thực hiện tối thiểu nhưng không giới hạn các hạng mục công việc sau, đảm bảo đạt được Mục tiêu nêu trên)	Mức độ đáp ứng	Bắt buộc / Tùy chọn	Mô tả đáp ứng chi tiết	Cấu phần tương ứng của giải pháp đề xuất
	lại được các hành động của người sử dụng đã thực hiện theo thời gian - Hệ thống không ghi lại dữ liệu nhạy cảm như: mật khẩu hoặc mã băm mật khẩu của người dùng, sốt hẻ tín dụng ...				

c) Quản lý cấu hình, phiên bản

STT	Yêu cầu của SHB (Nhà thầu phải thực hiện tối thiểu nhưng không giới hạn các hạng mục công việc sau, đảm bảo đạt được Mục tiêu nêu trên)	Mức độ đáp ứng	Bắt buộc / Tùy chọn	Mô tả đáp ứng chi tiết	Cấu phần tương ứng của giải pháp đề xuất
1	- Trong quá trình triển khai tại Ngân hàng, Nhà thầu phải xây dựng cơ chế quản lý cấu hình, phiên bản phù hợp, đầy đủ, chi tiết đảm bảo quản lý được các yêu cầu phát sinh như các thay đổi trong quy trình nghiệp vụ, thay đổi trong chức năng của hệ thống, thay đổi về mặt dữ liệu. Các phiên bản này phải đảm bảo có thể khôi phục lại được trong trường hợp Ngân hàng có yêu cầu; - Nhà thầu phải xây dựng cơ chế kiểm soát đầy đủ tất cả các thay đổi ảnh hưởng đến việc phát triển một sản phẩm. Mọi sự thay đổi đều phải được thông báo tới các thành viên liên quan; - Cơ chế quản lý cấu hình/phiên bản phải đảm bảo khả năng đồng bộ giữa các phiên bản với nhau; - Nhà thầu phải đề xuất giải pháp quản lý cấu hình/phiên bản và kế hoạch triển khai các công cụ, môi trường và cơ sở hạ tầng cần thiết;		Bắt buộc		

d) Sao lưu, phục hồi dữ liệu

STT	Yêu cầu của SHB (Nhà thầu phải thực hiện tối thiểu nhưng không giới hạn các hạng mục công việc sau, đảm bảo đạt được Mục tiêu nêu trên)	Mức độ đáp ứng	Bắt buộc / Tùy chọn	Mô tả đáp ứng chi tiết	Cấu phần tương ứng của giải pháp đề xuất
1	Cung cấp giải pháp sao lưu và phục hồi cho các cấu phần của hệ thống, bao gồm: - Dữ liệu chứa trong Cơ sở dữ liệu; - Dữ liệu dạng file; - Phần mềm hệ thống, phần mềm ứng dụng,..; - Cấu hình hệ thống và các loại dữ liệu liên quan khác.		Tùy chọn		

5. Yêu cầu về thương mại

5.1. ***Đồng tiền chào giá:*** Việt Nam đồng.

5.2. ***Đồng tiền thanh toán:*** Việt Nam đồng.

5.3. ***Phương thức thanh toán:*** Chuyển khoản vào tài khoản quy định trong Hợp đồng của Bên Bán.

5.4. ***Điều kiện thanh toán***

- Đợt 1: Tạm ứng 30% trong vòng 07 (bảy) ngày kể từ ngày Bên Bán bàn giao cho Bên Mua các giấy tờ, tài liệu sau:
  - Thư bảo lãnh thực hiện Hợp đồng có giá trị bằng 10% tổng giá trị Hợp đồng và có hiệu lực kể từ ngày phát hành đến hết ngày bảo hành, bảo trì.
- Đợt 2: Bên Mua thanh toán cho Bên Bán 70% tổng giá trị hợp đồng trong vòng 07 (bảy) kể từ ngày Bên Bán bàn giao cho bên mua các giấy tờ, tài liệu sau:
  - Giấy chứng nhận dịch vụ bảo hành chính hãng (bản gốc) cho Dịch vụ hệ thống 3D Secure 2.0 của Bên Mua theo danh mục được mô tả trong Mục 1 – Phần II của Hồ sơ Yêu cầu chào hàng này;
  - Giấy đề nghị thanh toán;
  - Hóa đơn tài chính hợp lệ;
  - Biên bản nghiệm thu kỹ thuật.

6. Bảng chào giá chi tiết

Nhà thầu trình bày Bảng chào giá chi tiết như sau: (Giá cung cấp được tính bằng đồng tiền quy định tại Phần II, Mục 2).

STT	Hạng mục	Số lượng	Đơn giá	Thành tiền chưa VAT	Thuế VAT (%)	Thành tiền đã có VAT
1	2	3	4	5=3*4	6=5*%VAT	7=5+6
TỔNG SỐ						

NGÂN HÀNG TMCP SÀI GÒN – HÀ NỘI

M.S.D.N: 1800278630 - C.T.C.P
NGÂN HÀNG THƯƠNG MẠI CỔ PHẦN SÀI GÒN - HÀ NỘI
Q. HOÀN KIẾM - TP. HÀ NỘI

PHÓ TỔNG GIÁM ĐỐC

Ngô Thu Hà