

Chương V. YÊU CẦU VỀ KỸ THUẬT

Mục 1. Yêu cầu về kỹ thuật

1.1. Giới thiệu chung về dự toán mua sắm, gói thầu

a) Tên dự toán mua sắm: Mua sắm thay thế máy chủ RootCA và thiết bị HSM cho Hệ thống CA NHNN.

b) Mục tiêu: Thay thế, bổ sung thiết bị để bảo đảm hệ thống CA NHNN hoạt động liên tục, ổn định, an toàn.

c) Quy mô: Trang bị các thiết bị sau:

STT	Danh sách hạng mục mua sắm	Đơn vị tính	Số lượng
1	Máy chủ cho RootCA	Thiết bị	02
2	Thiết bị lưu khóa HSM cho RootCA	Thiết bị	02
3	Thiết bị lưu khóa HSM cho SubCA	Thiết bị	02
4	Thiết bị Backup HSM	Thiết bị	01

d) Hiện trạng hệ thống CA NHNN

Hệ thống CA NHNN là hệ thống có chức năng cung cấp dịch vụ chữ ký điện tử cho các hoạt động nghiệp vụ của NHNN: Giao dịch điện tử giữa các cá nhân, tổ chức thuộc NHNN; Giao dịch điện tử giữa NHNN và các tổ chức tín dụng, Kho bạc Nhà nước;... Hiện tại Hệ thống CA đã cung cấp trên 7000 chứng thư số cho các ứng dụng quan trọng của NHNN như Thanh toán điện tử liên ngân hàng (TTLNH), Báo cáo NHNN, Hệ thống Dịch vụ công trực tuyến (DVC), Hệ thống đấu thầu và nghiệp vụ Thị trường mở (OMO), Hệ thống hỗ trợ quản lý, giám sát và phòng ngừa rủi ro gian lận trong hoạt động thanh toán (SIMO), Hệ thống Phòng chống rửa tiền (PCRT).

Hệ thống CA NHNN hoạt động trên các máy chủ độc lập và máy chủ ảo hóa sử dụng hệ điều hành Red Hat Linux và hệ điều hành Microsoft Windows, phần mềm lõi Entrust Authority Security Manager phiên bản 10.2 của Hãng Entrust và kho dữ liệu người dùng LDAP sử dụng giải pháp AD LDS (Active Directory Lightweight Directory Services) của Microsoft. Phần mềm quản lý, kích hoạt chứng thư số cho người dùng cuối sử dụng Entrust Entelligence Security Provider Enterprise phiên bản 10.

Hệ thống CA NHNN bao gồm hệ thống vận hành chính thức tại Trung tâm dữ liệu chính (TTDL) đặt tại Cục Công nghệ thông tin (CNTT) và hệ thống dự phòng thảm họa đặt tại Trung tâm dữ liệu dự phòng (TTDLDP) hoạt động theo cơ chế Active – Standby.

Các thiết bị của Hệ thống CA NHNN cần thay thế như sau:

TT	Thiết bị	SL (chiếc)	Năm trang bị
1	Máy chủ cho RootCA tại Cục CNTT và TTDLDP (Cisco UCS C220 M4)	02	2018
2	Thiết bị lưu khóa HSM cho RootCA tại Cục CNTT và TTDLDP (Luna G5)	02	2018
3	Thiết bị lưu khóa HSM cho SubCA tại Cục CNTT (Luna SA 1700)	01	2016
4	Thiết bị lưu khóa HSM cho SubCA tại TTDLDP (Luna SA 1700)	01	2017

e) Thời gian thực hiện hợp đồng: 42 tháng (06 tháng thực hiện gói thầu và 36 tháng bảo hành) kể từ ngày hợp đồng có hiệu lực.

1.2. Yêu cầu về kỹ thuật

1.2.1. Yêu cầu về kỹ thuật chung

- Cam kết hàng hóa mới 100%, chưa qua sử dụng, không phải là sản phẩm đã trưng bày, qua thử nghiệm.
- Cam kết hàng hóa có xuất xứ rõ ràng, có Giấy chứng nhận xuất xứ (CO), Giấy chứng nhận chất lượng (CQ).
- Có catalogue, tài liệu kỹ thuật thiết bị (có bảng tham chiếu các thông số kỹ thuật chi tiết đến catalogue, tài liệu kỹ thuật của thiết bị)
- Cam kết hàng hóa cung cấp phù hợp với hiện trạng hệ thống CA NHNN.
- Cam kết sau khi lắp đặt cần kiểm tra Hệ thống CA NHNN đảm bảo hoạt động bình thường.

1.2.2. Yêu cầu về kỹ thuật cụ thể

STT	Tên thiết bị/hàng hóa	Thông số kỹ thuật chi tiết	Đơn vị	Số lượng
1	Máy chủ cho RootCA		Chiếc	02
	Form Factor	Rackmount		

STT	Tên thiết bị/hàng hóa	Thông số kỹ thuật chi tiết	Đơn vị	Số lượng
	Processor	Intel Xeon Scalable Processor thế hệ thứ 5 Yêu cầu với Processor: - Tốc độ ≥ 2.4 GHz - Số core ≥ 12 - Số luồng (Thread) ≥ 24 Bộ nhớ đệm (Cache) ≥ 18 MB		
	Memory	Tối thiểu 16GB RDIMM, 3200MT/s		
	Storage Controller	Support RAID 0,1,5,6		
	Ổ cứng	2 ổ dung lượng 600 GB 10K RPM SAS 12Gbps 512n 2.5in Hỗ trợ Hot-plug		
	Ethernet Card	1 x Dual 1GbE;		
	Interfaces	+ 1 x VGA/Display Port; + 2 USB 2.0/3.0;		
	Quản trị	Có sẵn công cụ quản trị RJ45 cho phép quản lý máy chủ từ xa: Cập nhật firmware, driver, triển khai cài đặt hệ điều hành, giám sát tình trạng, virtual console		
	Nguồn (Power Supply)	Hot-Plug, Redundant		
	Quạt (Fan)	Hot-Plug, Redundant		
	Hỗ trợ hệ điều hành	Microsoft Windows Server Red Hat Enterprise Linux (RHEL)		
	Bảo hành	3 năm theo tiêu chuẩn của nhà sản xuất kể từ thời điểm nghiệm thu tổng thể.		
	Vị trí lắp đặt	- Trung tâm dữ liệu chính tại Số 64 Nguyễn Chí Thanh, Phường Láng Thành Phố Hà Nội. - Trung tâm dữ liệu dự phòng tại Phố Thanh Vy, phường Tùng Thiện,		

STT	Tên thiết bị/hàng hóa	Thông số kỹ thuật chi tiết	Đơn vị	Số lượng
		thành phố Hà Nội (DR).		
	Khác	Máy chủ mới phải có đầy đủ trang thiết bị, phụ kiện cần thiết để kết nối với hạ tầng công nghệ thông tin hiện có của NHNN		
2	Thiết bị lưu khóa HSM cho RootCA		Chiếc	02
	Các chức năng chính	- Lưu khóa trong phần cứng (keys in hardware) - Xác thực đa thành tố (Multi-factor Authentication) - Chống xâm nhập và phần cứng giả mạo (Intrusion-resistant, tamper-evident hardware) - Quản trị từ xa (remote management)		
	Hệ điều hành hỗ trợ	Windows, Linux		
	Hỗ trợ tích hợp qua các giao thức	PKCS#11, Microsoft CAPI and CNG, JCA/JCE, OpenSSL		
	Tốc độ ký	Tối thiểu 62 giao dịch/giây (tps) đối với khóa RSA-2048		
	Thuật toán hỗ trợ	- Mật mã phi đối xứng (Asymmetric): RSA, DSA, Diffie-Hellman, KCDSA, Elliptic Curve Cryptography (ECDSA, ECDH, ECIES) - Mật mã đối xứng (Symmetric): AES, RC4, RC5, CAST, DES, Triple DES, ARIA, SEED - Hàm băm (Hash/Message Digest/HMAC): SHA-2, SHA3,		
	Chứng nhận bảo mật	Tối thiểu đạt FIPS 140-3 mức 3 (Level 3)		
	Yêu cầu	Cho phép chuyển đổi dữ liệu và		

STT	Tên thiết bị/hàng hóa	Thông số kỹ thuật chi tiết	Đơn vị	Số lượng
	chuyển đổi khóa	cặp khóa bảo mật máy chủ RootCA của hệ thống CA NHNN hiện tại đang sử dụng sang thiết bị mới này.		
	Bảo hành	Bảo hành 03 năm theo tiêu chuẩn của nhà sản xuất kể từ thời điểm nghiệm thu tổng thể		
	Khác	Có đầy đủ trang thiết bị, phụ kiện cần thiết để kết nối với hạ tầng công nghệ thông tin hiện có của NHNN		
3	Thiết bị lưu khóa HSM cho SubCA		Chiếc	02
	Các chức năng chính	- Lưu khóa trong phần cứng (keys in hardware) - Xác thực đa thành tố (Multi-factor (PED) Authentication) - Chống xâm nhập và phần cứng giả mạo (Intrusion-resistant, tamper-evident hardware) - Quản trị từ xa (remote management)		
	Hỗ trợ các hệ điều hành	- Windows, Linux, AIX - Virtual: VMware, Hyper-V, Xen, KVM		
	Hỗ trợ tích hợp qua các giao thức	PKCS#11, Java (JCA/JCE), Microsoft CAPI and CNG, OpenSSL - REST API để quản trị - IPv4 và IPv6		
	Tốc độ	1000 giao dịch/ giây (tps) với RSA-2048		
	Số lượng Partition	05		
	Hỗ trợ thuật toán	- Mật mã phi đối xứng (Asymmetric): RSA, DSA, Diffie-		

STT	Tên thiết bị/hàng hóa	Thông số kỹ thuật chi tiết	Đơn vị	Số lượng
	và chuẩn mã hóa	Hellman, ECC (ECDSA, ECDH, Ed25519, ECIES) - Mật mã đối xứng (Symmetric): AES, AES-GCM, Triple DES, DES, ARIA, SEED, RC2, RC4, RC5, CAST - Hàm băm (Hash/Message Digest/HMAC): SHA-2, SHA-3, SM2, SM3, SM4.		
	Chứng nhận bảo mật	Tối thiểu đạt FIPS 140-3 mức 3 (Level 3)		
	Yêu cầu chuyển đổi khóa	Cho phép chuyển đổi dữ liệu và cặp khóa bảo mật của các máy chủ SubCA hệ thống CA NHNN hiện tại sang thiết bị mới này.		
	Bảo hành	Bảo hành 03 năm theo tiêu chuẩn của nhà sản xuất kể từ thời điểm nghiệm thu tổng thể		
	Khác	Có đầy đủ trang thiết bị, phụ kiện cần thiết để kết nối với hạ tầng công nghệ thông tin hiện có của NHNN		
4	Thiết bị Backup HSM		Chiếc	01
	Yêu cầu chung	Tương thích và cho phép chuyển đổi khóa bảo mật từ các thiết bị HSM nêu tại mục 2 và mục 3 Phụ lục này		
	Chức năng chính	Lưu trữ và phục hồi các khóa bảo mật từ các thiết bị HSM nêu tại mục 2 và mục 3 Phụ lục này		
	Chứng nhận bảo mật	Tối thiểu đạt FIPS 140-3 mức 3 (Level 3)		
	Cấu hình	128 MB storage, up to 100 Partitions		

1.3. Các yêu cầu khác

1.3.1. Yêu cầu về biện pháp tổ chức cung cấp, lắp đặt hàng hóa

Có biện pháp tổ chức cung cấp, lắp đặt hàng hóa hợp lý, bảo đảm hoạt động liên tục của Hệ thống CA NHNN, cụ thể như sau:

- Nhà thầu phải có kế hoạch triển khai theo các mốc thời gian cụ thể. Kế hoạch triển khai bao gồm đầy đủ thông tin về nhân lực thực hiện, thời gian, tiến độ hoàn thành và các công việc cần thiết để khởi tạo, kết nối, cấu hình, đưa thiết bị vào hoạt động;
- Cam kết có phương án triển khai, quy trình thực hiện, kịch bản chuyển đổi dữ liệu và cặp khóa bảo mật từ thiết bị cũ hiện có sang thiết bị mới trang bị tại gói thầu này bảo đảm không ảnh hưởng đến hoạt động của Hệ thống CA NHNN. Triển khai theo phương án, kế hoạch, kịch bản đã được các bên thống nhất, phê duyệt.
- Nhà thầu trình bày phương án, quy trình từng bước triển khai, lắp đặt thiết bị, chuyển đổi dữ liệu và cặp khóa bảo mật từ các thiết bị hiện tại sang thiết bị mới trang bị tại gói thầu này đảm bảo thiết bị mới tương thích với hệ thống CA NHNN và đảm bảo Hệ thống CA NHNN hoạt động liên tục, ổn định.

1.3.2. Yêu cầu về dịch vụ bảo hành

- Cam kết bảo hành tại địa điểm lắp đặt, sử dụng.
- Cam kết thời gian bảo hành 03 năm (1095 ngày) theo tiêu chuẩn của nhà sản xuất kể từ ngày nghiệm thu tổng thể.
- Có quy trình tiếp nhận, xử lý yêu cầu bảo hành từ Cục CNTT
- Nhà thầu phải có đầu mối tiếp nhận, xử lý thông báo yêu cầu bảo hành 24x7 từ Cục CNTT (email, điện thoại, văn bản,...).

1.3.3. Yêu cầu về tiến độ cung cấp hàng hóa

- Nhà thầu cung cấp hàng hóa trong vòng 04 tháng hoặc 120 ngày kể từ ngày hợp đồng có hiệu lực.

1.3.4. Yêu cầu thích ứng về mặt địa lý, môi trường

Thiết bị phải hoạt động ổn định trong môi trường Trung tâm dữ liệu: Nhiệt độ 20-25⁰C; độ ẩm tương đối 40-55%.

1.3.5. Yêu cầu về tác động với môi trường và biện pháp giải quyết

- Cam kết hàng hóa cung cấp không tác động nhiều đến môi trường và nếu có tác động phải đề xuất biện pháp giải quyết hợp lý.
- Cam kết thu hồi hàng hóa trong trường hợp hàng hóa không đảm bảo yêu cầu chất lượng mà không do lỗi của Chủ đầu tư.

1.3.6. Yêu cầu thân thiện với môi trường

- Cam kết hàng hóa cung cấp phải thân thiện với môi trường.

1.3.7. Yêu cầu về tài liệu

Nhà thầu phải cam kết chuyển giao các hồ sơ, tài liệu sau:

- Tài liệu khảo sát, đánh giá vị trí lắp đặt thiết bị;
- Bản vẽ mô tả vị trí lắp đặt, các kết nối sử dụng;
- Tài liệu hướng dẫn cài đặt, cấu hình, quản trị, vận hành máy chủ RootCA bằng tiếng Việt;
- Tài liệu hướng dẫn cài đặt, cấu hình, quản trị, vận hành thiết bị HSM bằng tiếng Việt;
- Tài liệu chuyển đổi dữ liệu và cặp khóa bảo mật máy chủ RootCA, SubCA của hệ thống CA NHNN hiện tại đang sử dụng sang thiết bị mới trang bị tại gói thầu này;
- Tài liệu đề xuất, khuyến nghị cách thức triển khai tại NHNN.

Mục 2. Bản vẽ: Không có

Mục 3. Kiểm tra và thử nghiệm

3.1. Kiểm tra sơ bộ hàng hóa

- Thời điểm thực hiện: Khi tiếp nhận hàng hóa.
- Địa điểm kiểm tra:
 - + Trung tâm dữ liệu: 64 Nguyễn Chí Thanh, Phường Láng, Thành phố Hà Nội;
 - + Trung tâm dữ liệu dự phòng: Phường Tùng Thiện, Thành phố Hà Nội.
- Nội dung: Kiểm tra theo danh mục những khối chính của hàng hóa bàn giao. Kiểm tra đối chiếu hàng hóa bàn giao với Chứng nhận xuất xứ (CO), Chứng nhận chất lượng (CQ) của hàng hóa.
- Biên bản yêu cầu: Biên bản kiểm tra sơ bộ hàng hóa và Biên bản bàn giao hàng hóa.

3.2. Kiểm tra kỹ thuật và chấp nhận hàng hóa

- Thời điểm thực hiện: Sau khi hoàn thành lắp đặt, khởi tạo hoạt động.
- Địa điểm:
 - + Trung tâm dữ liệu: 64 Nguyễn Chí Thanh, Phường Láng, Thành phố Hà Nội;
 - + Trung tâm dữ liệu dự phòng: Phường Tùng Thiện, Thành phố Hà Nội.

- Nội dung: Kiểm tra các thông số kỹ thuật, tình trạng hoạt động của thiết bị; Kiểm tra hoạt động của Hệ thống CA NHNN.
- Biên bản yêu cầu: Biên bản kiểm tra kỹ thuật và chấp nhận hàng hóa.

3.3. Nghiệm thu tổng thể

Được thực hiện sau khi kiểm tra sơ bộ hàng hóa, kiểm tra kỹ thuật và chấp nhận hàng hóa. Nhà thầu được xác nhận là hoàn thành nghĩa vụ triển khai nếu kết quả kiểm tra là đáp ứng yêu cầu kỹ thuật và nhà thầu bàn giao đầy đủ các tài liệu nêu tại mục 1.3.7.

Mục 4. Yêu cầu khác

Nhà thầu độc lập hoặc Thành viên liên danh chịu trách nhiệm cung cấp thiết bị HSM phải có giấy phép kinh doanh sản phẩm, dịch vụ mật mã dân sự còn hiệu lực tối thiểu 10 tháng kể từ ngày đăng thông báo mời thầu. Tại Giấy phép kinh doanh sản phẩm, dịch vụ mật mã dân sự, thiết bị HSM do nhà thầu chào thầu phải thuộc tên nhóm sản phẩm được phép kinh doanh trong phạm vi, lĩnh vực cung cấp: ngân hàng.

Trường hợp thiết bị chào thầu (HSM) được nhập khẩu, Nhà thầu cam kết đơn vị nhập khẩu phải có giấy phép nhập khẩu sản phẩm mật mã dân sự còn hiệu lực tại thời điểm nhập khẩu.